<!-- FILE: Id -->
<!-- LAST CHECKIN: $Author$ -->
<!-- $Date$ -->
<!--
-->
<!--
Copyright 2011 Citrix Systems, Inc. All rights reserved.
-->
<SignaturesFile version="1" schema_version="2">
<Signatures>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="803" source="Snort" sourceid="803" type="" version="16">
<LogString>
WEB-CGI HyperSeek hsx.cgi directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/hsx.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../../</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%00</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2314</Reference>
<Reference>cve,2001-0253</Reference>
<Reference>nessus,10602</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1607" source="Snort" sourceid="1607" type="" version="10">
<LogString>WEB-CGI HyperSeek hsx.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/hsx.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2314</Reference>
<Reference>cve,2001-0253</Reference>
<Reference>nessus,10602</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="809" source="Snort" sourceid="809" type="" version="14">
<LogString>
WEB-CGI whois_raw.cgi arbitrary command execution attempt
</LogString>
<PatternList>

<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/whois_raw.cgi?</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">|0A|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,466</Reference>
<Reference>bugtraq,304</Reference>
<Reference>cve,1999-1063</Reference>
<Reference>nessus,10306</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="810" source="Snort" sourceid="810" type="" version="14">
<LogString>WEB-CGI whois_raw.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/whois_raw.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,466</Reference>
<Reference>bugtraq,304</Reference>
<Reference>cve,1999-1063</Reference>
<Reference>nessus,10306</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="811" source="Snort" sourceid="811" type="" version="13">
<LogString>WEB-CGI websitepro path access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Match type="LITERAL"> /HTTP/1.</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,468</Reference>
<Reference>bugtraq,932</Reference>
<Reference>cve,2000-0066</Reference>
<Reference>nessus,10303</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1571" source="Snort" sourceid="1571" type="" version="12">
<LogString>WEB-CGI dcforum.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dcforum.cgi</Match>

</Pattern>
<Pattern>
<Match type="LITERAL">forum=../..</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2611</Reference>
<Reference>cve,2001-0436</Reference>
<Reference>cve,2001-0437</Reference>
<Reference>nessus,10583</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="818" source="Snort" sourceid="818" type="" version="13">
<LogString>WEB-CGI dcforum.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dcforum.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2728</Reference>
<Reference>cve,2001-0527</Reference>
<Reference>nessus,10583</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="817" source="Snort" sourceid="817" type="" version="15">
<LogString>WEB-CGI dcboard.cgi invalid user addition attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dcboard.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">command=register</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%7cadmin</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2728</Reference>
<Reference>cve,2001-0527</Reference>
<Reference>nessus,10583</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1410" source="Snort" sourceid="1410" type="" version="12">
<LogString>WEB-CGI dcboard.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>

<Match type="LITERAL">/dcboard.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2728</Reference>
<Reference>cve,2001-0527</Reference>
<Reference>nessus,10583</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="820" source="Snort" sourceid="820" type="" version="14">
<LogString>WEB-CGI anaconda directory transversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/apexec.pl</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">template=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2338</Reference>
<Reference>bugtraq,2388</Reference>
<Reference>cve,2000-0975</Reference>
<Reference>cve,2001-0308</Reference>
<Reference>nessus,10536</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="853" source="Snort" sourceid="853" type="" version="12">
<LogString>WEB-CGI wrap access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wrap</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,234</Reference>
<Reference>bugtraq,373</Reference>
<Reference>cve,1999-0149</Reference>
<Reference>nessus,10317</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1536" source="Snort" sourceid="1536" type="" version="13">
<LogString>
WEB-CGI calendar_admin.pl arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/calendar_admin.pl?config=|7C|</Match>

</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1215</Reference>
<Reference>cve,2000-0432</Reference>
<Reference>nessus,10506</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1537" source="Snort" sourceid="1537" type="" version="11">
<LogString>WEB-CGI calendar_admin.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/calendar_admin.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1215</Reference>
<Reference>cve,2000-0432</Reference>
<Reference>nessus,10506</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1397" source="Snort" sourceid="1397" type="" version="11">
<LogString>WEB-CGI wayboard attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/way-board/way-board.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">db=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../..</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2370</Reference>
<Reference>cve,2001-0214</Reference>
<Reference>nessus,10610</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1572" source="Snort" sourceid="1572" type="" version="10">
<LogString>WEB-CGI commerce.cgi arbitrary file access attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/commerce.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">page=</Match>

</Pattern>
<Pattern>
<Match type="LITERAL">/../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2361</Reference>
<Reference>cve,2001-0210</Reference>
<Reference>nessus,10612</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1395" source="Snort" sourceid="1395" type="" version="12">
<LogString>WEB-CGI zml.cgi attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/zml.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">file=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3759</Reference>
<Reference>cve,2001-1209</Reference>
<Reference>nessus,10830</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1396" source="Snort" sourceid="1396" type="" version="12">
<LogString>WEB-CGI zml.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/zml.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3759</Reference>
<Reference>cve,2001-1209</Reference>
<Reference>nessus,10830</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1574" source="Snort" sourceid="1574" type="" version="11">
<LogString>WEB-CGI directorypro.cgi attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/directorypro.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">show=</Match>

</Pattern>
<Pattern>
<Match type="LITERAL">../..</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2793</Reference>
<Reference>cve,2001-0780</Reference>
<Reference>nessus,10679</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1704" source="Snort" sourceid="1704" type="" version="11">
<LogString>WEB-CGI cal_make.pl directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cal_make.pl</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">p0=../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2663</Reference>
<Reference>cve,2001-0463</Reference>
<Reference>nessus,10664</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1479" source="Snort" sourceid="1479" type="" version="12">
<LogString>WEB-CGI ttawebtop.cgi arbitrary file attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">/ttawebtop.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">pg=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2890</Reference>
<Reference>cve,2001-0805</Reference>
<Reference>nessus,10696</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1730" source="Snort" sourceid="1730" type="" version="12">
<LogString>
WEB-CGI ustorekeeper.pl directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>

<Match type="LITERAL">/ustorekeeper.pl</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">file=../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2536</Reference>
<Reference>cve,2001-0466</Reference>
<Reference>nessus,10645</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1606" source="Snort" sourceid="1606" type="" version="9">
<LogString>WEB-CGI icat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/icat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1069</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1617" source="Snort" sourceid="1617" type="" version="11">
<LogString>WEB-CGI Bugzilla doeditvotes.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/doeditvotes.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3800</Reference>
<Reference>cve,2002-0011</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1501" source="Snort" sourceid="1501" type="" version="11">
<LogString>
WEB-CGI a1stats a1disp3.cgi directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/a1disp3.cgi?/../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2705</Reference>
<Reference>cve,2001-0561</Reference>
<Reference>nessus,10669</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1502" source="Snort" sourceid="1502" type="" version="11">
<LogString>WEB-CGI a1stats a1disp3.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/a1disp3.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2705</Reference>
<Reference>cve,2001-0561</Reference>
<Reference>nessus,10669</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1731" source="Snort" sourceid="1731" type="" version="10">
<LogString>WEB-CGI a1stats access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/a1stats/</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2705</Reference>
<Reference>cve,2001-0561</Reference>
<Reference>nessus,10669</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1503" source="Snort" sourceid="1503" type="" version="11">
<LogString>WEB-CGI admentor admin.asp access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admentor/admin/admin.asp</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4152</Reference>
<Reference>cve,2002-0308</Reference>
<Reference>nessus,10880</Reference>
<Reference>
url,www.securiteam.com/windowsntfocus/5DP0N1F6AW.html
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1505" source="Snort" sourceid="1505" type="" version="11">
<LogString>
WEB-CGI alchemy http server PRN arbitrary command execution attempt
</LogString>

<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/PRN/../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3599</Reference>
<Reference>cve,2001-0871</Reference>
<Reference>nessus,10818</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1506" source="Snort" sourceid="1506" type="" version="11">
<LogString>
WEB-CGI alchemy http server NUL arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/NUL/../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3599</Reference>
<Reference>cve,2001-0871</Reference>
<Reference>nessus,10818</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1507" source="Snort" sourceid="1507" type="" version="13">
<LogString>
WEB-CGI alibaba.pl arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/alibaba.pl|7C|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,770</Reference>
<Reference>cve,1999-0885</Reference>
<Reference>nessus,10013</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1508" source="Snort" sourceid="1508" type="" version="12">
<LogString>WEB-CGI alibaba.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/alibaba.pl</Match>

</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,770</Reference>
<Reference>cve,1999-0885</Reference>
<Reference>nessus,10013</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1509" source="Snort" sourceid="1509" type="" version="12">
<LogString>
WEB-CGI AltaVista Intranet Search directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/query?mss=..</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,896</Reference>
<Reference>cve,2000-0039</Reference>
<Reference>nessus,10015</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1510" source="Snort" sourceid="1510" type="" version="12">
<LogString>
WEB-CGI test.bat arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/test.bat|7C|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>
<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1511" source="Snort" sourceid="1511" type="" version="12">
<LogString>WEB-CGI test.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/test.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>

<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1512" source="Snort" sourceid="1512" type="" version="12">
<LogString>
WEB-CGI input.bat arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/input.bat|7C|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>
<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1513" source="Snort" sourceid="1513" type="" version="12">
<LogString>WEB-CGI input.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/input.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>
<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1514" source="Snort" sourceid="1514" type="" version="12">
<LogString>
WEB-CGI input2.bat arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/input2.bat|7C|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>
<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1515" source="Snort" sourceid="1515" type="" version="12">
<LogString>WEB-CGI input2.bat access</LogString>

<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/input2.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>
<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1516" source="Snort" sourceid="1516" type="" version="13">
<LogString>
WEB-CGI envout.bat arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/envout.bat|7C|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>
<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1517" source="Snort" sourceid="1517" type="" version="12">
<LogString>WEB-CGI envout.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/envout.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,762</Reference>
<Reference>cve,1999-0947</Reference>
<Reference>nessus,10016</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1705" source="Snort" sourceid="1705" type="" version="10">
<LogString>
WEB-CGI echo.bat arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/echo.bat</Match>

```
</Pattern>
<Pattern>
<Match type="LITERAL">&</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1002</Reference>
<Reference>cve,2000-0213</Reference>
<Reference>nessus,10246</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1706" source="Snort" sourceid="1706"
type="" version="10">
<LogString>WEB-CGI echo.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/echo.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1002</Reference>
<Reference>cve,2000-0213</Reference>
<Reference>nessus,10246</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1707" source="Snort" sourceid="1707"
type="" version="10">
<LogString>
WEB-CGI hello.bat arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/hello.bat</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">&</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1002</Reference>
<Reference>cve,2000-0213</Reference>
<Reference>nessus,10246</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1708" source="Snort" sourceid="1708"
type="" version="10">
<LogString>WEB-CGI hello.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/hello.bat</Match>
</Pattern>
```

</RequestPatterns>
</PatternList>
<Reference>bugtraq,1002</Reference>
<Reference>cve,2000-0213</Reference>
<Reference>nessus,10246</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1650" source="Snort" sourceid="1650" type="" version="10">
<LogString>WEB-CGI tst.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/tst.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,770</Reference>
<Reference>cve,1999-0885</Reference>
<Reference>nessus,10014</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1547" source="Snort" sourceid="1547" type="" version="14">
<LogString>
WEB-CGI csSearch.cgi arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/csSearch.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">setup=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">`</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">`</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4368</Reference>
<Reference>cve,2002-0495</Reference>
<Reference>nessus,10924</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1548" source="Snort" sourceid="1548" type="" version="12">
<LogString>WEB-CGI csSearch.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>

<Match type="LITERAL">/csSearch.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4368</Reference>
<Reference>cve,2002-0495</Reference>
<Reference>nessus,10924</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1554" source="Snort" sourceid="1554" type="" version="12">
<LogString>WEB-CGI dbman db.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dbman/db.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1178</Reference>
<Reference>cve,2000-0381</Reference>
<Reference>nessus,10403</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1569" source="Snort" sourceid="1569" type="" version="13">
<LogString>WEB-CGI loadpage.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/loadpage.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">file=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2109</Reference>
<Reference>cve,2000-1092</Reference>
<Reference>nessus,10065</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1590" source="Snort" sourceid="1590" type="" version="10">
<LogString>
WEB-CGI faqmanager.cgi arbitrary file access attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/faqmanager.cgi?toc=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>

<Match type="LITERAL">|00|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3810</Reference>
<Reference>nessus,10837</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1628" source="Snort" sourceid="1628" type="" version="14">
<LogString>
WEB-CGI FormHandler.cgi directory traversal attempt attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/FormHandler.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">reply_message_attach=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">/../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,798</Reference>
<Reference>bugtraq,799</Reference>
<Reference>cve,1999-1050</Reference>
<Reference>nessus,10075</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1598" source="Snort" sourceid="1598" type="" version="12">
<LogString>
WEB-CGI Home Free search.cgi directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/search.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">letter=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,921</Reference>
<Reference>cve,2000-0054</Reference>
<Reference>nessus,10101</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1657" source="Snort" sourceid="1657" type="" version="10">
<LogString>WEB-CGI pagelog.cgi directory traversal attempt</LogString>

<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pagelog.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">name=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1864</Reference>
<Reference>cve,2000-0940</Reference>
<Reference>nessus,10591</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1719" source="Snort" sourceid="1719" type="" version="10">
<LogString>WEB-CGI talkback.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/talkbalk.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">article=../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2547</Reference>
<Reference>cve,2001-0420</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1723" source="Snort" sourceid="1723" type="" version="10">
<LogString>WEB-CGI emumail.cgi NULL attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/emumail.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">type=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%00</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,5824</Reference>
<Reference>cve,2002-1526</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1642" source="Snort" sourceid="1642" type="" version="10">

<LogString>WEB-CGI document.d2w access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/document.d2w</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2017</Reference>
<Reference>cve,2000-1110</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1643" source="Snort" sourceid="1643" type="" version="9">
<LogString>WEB-CGI db2www access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/db2www</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2000-0677</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1668" source="Snort" sourceid="1668" type="" version="10">
<LogString>WEB-CGI /cgi-bin/ access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgi-bin/</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">/cgi-bin/ HTTP</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1669" source="Snort" sourceid="1669" type="" version="9">
<LogString>WEB-CGI /cgi-dos/ access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgi-dos/</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">/cgi-dos/ HTTP</Match>
</Pattern>
</RequestPatterns>
</PatternList>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1088" source="Snort" sourceid="1088" type="" version="14">
<LogString>WEB-CGI eXtropia webstore directory traversal</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/web_store.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">page=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1774</Reference>
<Reference>cve,2000-1005</Reference>
<Reference>nessus,10532</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1611" source="Snort" sourceid="1611" type="" version="10">
<LogString>WEB-CGI eXtropia webstore access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/web_store.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1774</Reference>
<Reference>cve,2000-1005</Reference>
<Reference>nessus,10532</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1089" source="Snort" sourceid="1089" type="" version="12">
<LogString>WEB-CGI shopping cart directory traversal</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/shop.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">page=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1777</Reference>
<Reference>cve,2000-0921</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1092" source="Snort" sourceid="1092" type="" version="15">
<LogString>

WEB-CGI Armada Style Master Index directory traversal
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/search.cgi?keys</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">catigory=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1772</Reference>
<Reference>cve,2000-0924</Reference>
<Reference>nessus,10562</Reference>
<Reference>
url,www.synnergy.net/downloads/advisories/SLA-2000-16.masterindex.txt
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1093" source="Snort" sourceid="1093" type="" version="13">
<LogString>
WEB-CGI cached_feed.cgi moreover shopping cart directory traversal
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cached_feed.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1762</Reference>
<Reference>cve,2000-0906</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2051" source="Snort" sourceid="2051" type="" version="6">
<LogString>
WEB-CGI cached_feed.cgi moreover shopping cart access
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cached_feed.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1762</Reference>
<Reference>cve,2000-0906</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1865" source="Snort" sourceid="1865" type="" version="8">
<LogString>WEB-CGI webdist.cgi arbitrary command attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/webdist.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">distloc=|3B|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,374</Reference>
<Reference>cve,1999-0039</Reference>
<Reference>nessus,10299</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1163" source="Snort" sourceid="1163" type="" version="14">
<LogString>WEB-CGI webdist.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/webdist.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,374</Reference>
<Reference>cve,1999-0039</Reference>
<Reference>nessus,10299</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1172" source="Snort" sourceid="1172" type="" version="13">
<LogString>WEB-CGI bigconf.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bigconf.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,778</Reference>
<Reference>cve,1999-1550</Reference>
<Reference>nessus,10027</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1174" source="Snort" sourceid="1174" type="" version="13">
<LogString>WEB-CGI /cgi-bin/jj access</LogString>
<PatternList>
<RequestPatterns>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgi-bin/jj</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2002</Reference>
<Reference>cve,1999-0260</Reference>
<Reference>nessus,10131</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1204" source="Snort" sourceid="1204" type="" version="9">
<LogString>WEB-CGI ax-admin.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ax-admin.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1205" source="Snort" sourceid="1205" type="" version="9">
<LogString>WEB-CGI axs.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/axs.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1206" source="Snort" sourceid="1206" type="" version="13">
<LogString>WEB-CGI cachemgr.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cachemgr.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2059</Reference>
<Reference>cve,1999-0710</Reference>
<Reference>nessus,10034</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1208" source="Snort" sourceid="1208" type="" version="11">
<LogString>WEB-CGI responder.cgi access</LogString>
<PatternList>
<RequestPatterns>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/responder.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3155</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1211" source="Snort" sourceid="1211" type="" version="9">
<LogString>WEB-CGI web-map.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/web-map.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1305" source="Snort" sourceid="1305" type="" version="10">
<LogString>WEB-CGI txt2html.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/txt2html.cgi</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">/../../../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1306" source="Snort" sourceid="1306" type="" version="12">
<LogString>
WEB-CGI store.cgi product directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/store.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">product=</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">../..</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,2385</Reference>
<Reference>cve,2001-0305</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1494" source="Snort" sourceid="1494" type="" version="11">
<LogString>WEB-CGI SIX webboard generate.cgi attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/generate.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">content=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3175</Reference>
<Reference>cve,2001-1115</Reference>
<Reference>nessus,10725</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1495" source="Snort" sourceid="1495" type="" version="10">
<LogString>WEB-CGI SIX webboard generate.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/generate.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3175</Reference>
<Reference>cve,2001-1115</Reference>
<Reference>nessus,10725</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1496" source="Snort" sourceid="1496" type="" version="10">
<LogString>WEB-CGI spin_client.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/spin_client.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10393</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1787" source="Snort" sourceid="1787" type="" version="10">
<LogString>WEB-CGI csPassword.cgi access</LogString>
<PatternList>
<RequestPatterns>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/csPassword.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4885</Reference>
<Reference>bugtraq,4886</Reference>
<Reference>bugtraq,4887</Reference>
<Reference>bugtraq,4889</Reference>
<Reference>cve,2002-0917</Reference>
<Reference>cve,2002-0918</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1788" source="Snort" sourceid="1788" type="" version="6">
<LogString>WEB-CGI csPassword password.cgi.tmp access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/password.cgi.tmp</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4889</Reference>
<Reference>cve,2002-0920</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1763" source="Snort" sourceid="1763" type="" version="11">
<LogString>WEB-CGI Nortel Contivity cgiproc DOS attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgiproc?Nocfile=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,938</Reference>
<Reference>cve,2000-0063</Reference>
<Reference>cve,2000-0064</Reference>
<Reference>nessus,10160</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1764" source="Snort" sourceid="1764" type="" version="11">
<LogString>WEB-CGI Nortel Contivity cgiproc DOS attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgiproc?|24|</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,938</Reference>
<Reference>cve,2000-0063</Reference>
<Reference>cve,2000-0064</Reference>
<Reference>nessus,10160</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1765" source="Snort" sourceid="1765" type="" version="11">
<LogString>WEB-CGI Nortel Contivity cgiproc access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgiproc</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,938</Reference>
<Reference>cve,2000-0063</Reference>
<Reference>cve,2000-0064</Reference>
<Reference>nessus,10160</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1805" source="Snort" sourceid="1805" type="" version="7">
<LogString>WEB-CGI Oracle reports CGI access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/rwcgi60</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">setauth=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4848</Reference>
<Reference>cve,2002-0947</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1822" source="Snort" sourceid="1822" type="" version="10">
<LogString>WEB-CGI alienform.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/alienform.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">.|7C|./.|7C|.</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4983</Reference>
<Reference>cve,2002-0934</Reference>

<Reference>nessus,11027</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1823" source="Snort" sourceid="1823" type="" version="10">
<LogString>
WEB-CGI AlienForm af.cgi directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/af.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">.|7C|./.|7C|.</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4983</Reference>
<Reference>cve,2002-0934</Reference>
<Reference>nessus,11027</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1824" source="Snort" sourceid="1824" type="" version="9">
<LogString>WEB-CGI alienform.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/alienform.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4983</Reference>
<Reference>cve,2002-0934</Reference>
<Reference>nessus,11027</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1825" source="Snort" sourceid="1825" type="" version="9">
<LogString>WEB-CGI AlienForm af.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/af.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4983</Reference>
<Reference>cve,2002-0934</Reference>
<Reference>nessus,11027</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1868" source="Snort" sourceid="1868" type="" version="8">

<LogString>WEB-CGI story.pl arbitrary file read attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/story.pl</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">next=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3028</Reference>
<Reference>cve,2001-0804</Reference>
<Reference>nessus,10817</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1869" source="Snort" sourceid="1869" type="" version="8">
<LogString>WEB-CGI story.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/story.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3028</Reference>
<Reference>cve,2001-0804</Reference>
<Reference>nessus,10817</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1870" source="Snort" sourceid="1870" type="" version="8">
<LogString>WEB-CGI siteUserMod.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/.cobalt/siteUserMod/siteUserMod.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,951</Reference>
<Reference>cve,2000-0117</Reference>
<Reference>nessus,10253</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1875" source="Snort" sourceid="1875" type="" version="8">
<LogString>WEB-CGI cgicso access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgicso</Match>

</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6141</Reference>
<Reference>cve,2002-1652</Reference>
<Reference>nessus,10779</Reference>
<Reference>nessus,10780</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1876" source="Snort" sourceid="1876" type="" version="7">
<LogString>WEB-CGI nph-publish.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/nph-publish.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1177</Reference>
<Reference>nessus,10164</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1877" source="Snort" sourceid="1877" type="" version="10">
<LogString>WEB-CGI printenv access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/printenv</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1658</Reference>
<Reference>cve,2000-0868</Reference>
<Reference>nessus,10188</Reference>
<Reference>nessus,10503</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1878" source="Snort" sourceid="1878" type="" version="8">
<LogString>WEB-CGI sdbsearch.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/sdbsearch.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1658</Reference>
<Reference>cve,2000-0868</Reference>
<Reference>nessus,10503</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1931" source="Snort" sourceid="1931"

type="" version="7">
<LogString>WEB-CGI rpc-nlog.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/rpc-nlog.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1278</Reference>
<Reference>
url,marc.theaimsgroup.com/?l=bugtraq&m=91470326629357&w=2
</Reference>
<Reference>
url,marc.theaimsgroup.com/?l=bugtraq&m=91471400632145&w=2
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1932" source="Snort" sourceid="1932"
type="" version="6">
<LogString>WEB-CGI rpc-smb.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/rpc-smb.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1278</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1933" source="Snort" sourceid="1933"
type="" version="8">
<LogString>WEB-CGI cart.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cart.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1115</Reference>
<Reference>cve,2000-0252</Reference>
<Reference>nessus,10368</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1994" source="Snort" sourceid="1994"
type="" version="6">
<LogString>WEB-CGI vpasswd.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/vpasswd.cgi</Match>

</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6038</Reference>
<Reference>nessus,11165</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1995" source="Snort" sourceid="1995" type="" version="5">
<LogString>WEB-CGI alya.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/alya.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11118</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1996" source="Snort" sourceid="1996" type="" version="8">
<LogString>WEB-CGI viralator.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/viralator.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3495</Reference>
<Reference>cve,2001-0849</Reference>
<Reference>nessus,11107</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2001" source="Snort" sourceid="2001" type="" version="6">
<LogString>WEB-CGI smartsearch.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/smartsearch.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7133</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1862" source="Snort" sourceid="1862" type="" version="10">
<LogString>WEB-CGI mrtg.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>

<Match type="LITERAL">/mrtg.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">cfg=/../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4017</Reference>
<Reference>cve,2002-0232</Reference>
<Reference>nessus,11001</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2052" source="Snort" sourceid="2052" type="" version="8">
<LogString>WEB-CGI overflow.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/overflow.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6326</Reference>
<Reference>cve,2002-1361</Reference>
<Reference>nessus,11190</Reference>
<Reference>url,www.cert.org/advisories/CA-2002-35.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2086" source="Snort" sourceid="2086" type="" version="8">
<LogString>WEB-CGI streaming server parse_xml.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Match type="LITERAL">/parse_xml.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6960</Reference>
<Reference>cve,2003-0054</Reference>
<Reference>nessus,11278</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2115" source="Snort" sourceid="2115" type="" version="7">
<LogString>WEB-CGI album.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Match type="LITERAL">/album.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7444</Reference>
<Reference>nessus,11581</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2433" source="Snort" sourceid="2433" type="" version="7">
<LogString>WEB-CGI MDaemon form2raw.cgi overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Match type="LITERAL">/form2raw.cgi</Match>
</Pattern>
<Pattern>
<Match type="PCRE">\Wfrom=[^\x3b&\n]{100}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9317</Reference>
<Reference>cve,2003-1200</Reference>
<Reference>url,secunia.com/advisories/10512/</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2434" source="Snort" sourceid="2434" type="" version="7">
<LogString>WEB-CGI MDaemon form2raw.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Match type="LITERAL">/form2raw.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9317</Reference>
<Reference>cve,2003-1200</Reference>
<Reference>url,secunia.com/advisories/10512/</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2670" source="Snort" sourceid="2670" type="" version="5">
<LogString>WEB-CGI pgpmail.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pgpmail.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3605</Reference>
<Reference>cve,2001-0937</Reference>
<Reference>nessus,11070</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3062" source="Snort" sourceid="3062" type="" version="5">
<LogString>WEB-CGI NetScreen SA 5000 delhomepage.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/delhomepage.cgi</Match>

</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9791</Reference>
<Reference>cve,2004-0347</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3131" source="Snort" sourceid="3131" type="" version="5">
<LogString>WEB-CGI mailman directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/mailman/</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">.../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2005-0202</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3468" source="Snort" sourceid="3468" type="" version="4">
<LogString>WEB-CGI math_sum.mscgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/math_sum.mscgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10831</Reference>
<Reference>nessus,14182</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2203" source="Snort" sourceid="2203" type="" version="12">
<LogString>WEB-CGI everythingform.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/everythingform.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2101</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2001-0023</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2116" source="Snort" sourceid="2116"

type="" version="11">
<LogString>WEB-CGI chipcfg.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/chipcfg.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2767</Reference>
<Reference>cve,2001-1341</Reference>
<Reference>
url,archives.neohapsis.com/archives/bugtraq/2001-05/0233.html
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="872" source="Snort" sourceid="872"
type="" version="14">
<LogString>WEB-CGI tcsh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/tcsh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1454" source="Snort" sourceid="1454"
type="" version="12">
<LogString>WEB-CGI wwwwais access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wwwwais</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2001-0223</Reference>
<Reference>nessus,10597</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1570" source="Snort" sourceid="1570"
type="" version="14">
<LogString>WEB-CGI loadpage.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/loadpage.cgi</Match>
</Pattern>
</RequestPatterns>

</PatternList>
<Reference>bugtraq,2109</Reference>
<Reference>cve,2000-1092</Reference>
<Reference>nessus,10065</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1644" source="Snort" sourceid="1644" type="" version="14">
<LogString>WEB-CGI test-cgi attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/test-cgi/*?*</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,218</Reference>
<Reference>bugtraq,2003</Reference>
<Reference>cve,1999-0070</Reference>
<Reference>nessus,10282</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1655" source="Snort" sourceid="1655" type="" version="12">
<LogString>
WEB-CGI pfdispaly.cgi arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pfdispaly.cgi?'</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0270</Reference>
<Reference>nessus,10174</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1535" source="Snort" sourceid="1535" type="" version="15">
<LogString>WEB-CGI bizdbsearch access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bizdb1-search.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1104</Reference>
<Reference>cve,2000-0287</Reference>
<Reference>nessus,10383</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1710" source="Snort" sourceid="1710" type="" version="12">

<LogString>WEB-CGI bbs_forum.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bbs_forum.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2177</Reference>
<Reference>cve,2001-0123</Reference>
<Reference>url,www.cgisecurity.com/advisory/3.1.txt</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="883" source="Snort" sourceid="883" type="" version="11">
<LogString>WEB-CGI flexform access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/flexform</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>url,www.wiretrip.net/rfp/p/doc.asp/i2/d6.htm</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2212" source="Snort" sourceid="2212" type="" version="12">
<LogString>WEB-CGI imageFolio.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/imageFolio.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,6265</Reference>
<Reference>cve,2002-1334</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="901" source="Snort" sourceid="901" type="" version="16">
<LogString>WEB-CGI webspirs.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/webspirs.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2362</Reference>

<Reference>cve,2001-0211</Reference>
<Reference>nessus,10616</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1473" source="Snort" sourceid="1473" type="" version="14">
<LogString>WEB-CGI newsdesk.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/newsdesk.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2172</Reference>
<Reference>cve,2001-0232</Reference>
<Reference>nessus,10586</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="881" source="Snort" sourceid="881" type="" version="11">
<LogString>WEB-CGI archie access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/archie</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="813" source="Snort" sourceid="813" type="" version="16">
<LogString>WEB-CGI webplus directory traversal</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/webplus?script</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,471</Reference>
<Reference>bugtraq,1102</Reference>
<Reference>cve,2000-0282</Reference>
<Reference>nessus,10367</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3464" source="Snort" sourceid="3464" type="" version="8">
<LogString>WEB-CGI awstats.pl command execution attempt</LogString>
<PatternList>
<RequestPatterns>

<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/awstats.pl?</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">update=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">update=[^\r\n\x26]+</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">logfile=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">awstats.pl\?[^\r\n]*logfile=\x7C</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12572</Reference>
<Reference>nessus,16456</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="10999" source="Snort" sourceid="10999" type="" version="8">
<LogString>WEB-CGI chetcpasswd access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">chetcpasswd.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,21102</Reference>
<Reference>bugtraq,6472</Reference>
<Reference>cve,2002-2220</Reference>
<Reference>cve,2006-6679</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2055" source="Snort" sourceid="2055" type="" version="9">
<LogString>WEB-CGI enter_bug.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/enter_bug.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3272</Reference>
<Reference>cve,2002-0008</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1716" source="Snort" sourceid="1716" type="" version="12">
<LogString>WEB-CGI gbook.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/gbook.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1940</Reference>
<Reference>cve,2000-1131</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1600" source="Snort" sourceid="1600" type="" version="13">
<LogString>
WEB-CGI htsearch arbitrary configuration file attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/htsearch?-c</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3410</Reference>
<Reference>cve,2001-0834</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="850" source="Snort" sourceid="850" type="" version="11">
<LogString>WEB-CGI wais.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wais.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1565" source="Snort" sourceid="1565" type="" version="15">
<LogString>
WEB-CGI eshop.pl arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/eshop.pl?seite=|3B|</Match>
</Pattern>

</RequestPatterns>
</PatternList>
<Reference>bugtraq,3340</Reference>
<Reference>cve,2001-1014</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1194" source="Snort" sourceid="1194" type="" version="16">
<LogString>WEB-CGI sojourn.cgi File attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/sojourn.cgi?cat=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%00</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1052</Reference>
<Reference>cve,2000-0180</Reference>
<Reference>nessus,10349</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2223" source="Snort" sourceid="2223" type="" version="11">
<LogString>WEB-CGI csNews.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/csNews.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4994</Reference>
<Reference>cve,2002-0923</Reference>
<Reference>nessus,11726</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1097" source="Snort" sourceid="1097" type="" version="12">
<LogString>WEB-CGI Talentsoft Web+ exploit attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/webplus.cgi?Script=/webplus/webping/webping.wml</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1725</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="838" source="Snort" sourceid="838" type="" version="15">
<LogString>WEB-CGI webgais access</LogString>

<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/webgais</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,472</Reference>
<Reference>bugtraq,2058</Reference>
<Reference>cve,1999-0176</Reference>
<Reference>nessus,10300</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="896" source="Snort" sourceid="896" type="" version="17">
<LogString>WEB-CGI way-board access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/way-board</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2370</Reference>
<Reference>cve,2001-0214</Reference>
<Reference>nessus,10610</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1478" source="Snort" sourceid="1478" type="" version="11">
<LogString>WEB-CGI swc access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/swc</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10493</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="898" source="Snort" sourceid="898" type="" version="15">
<LogString>WEB-CGI commerce.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/commerce.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2361</Reference>
<Reference>cve,2001-0210</Reference>

<Reference>nessus,10612</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2205" source="Snort" sourceid="2205" type="" version="12">
<LogString>WEB-CGI ezboard.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ezboard.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4068</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2002-0263</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2220" source="Snort" sourceid="2220" type="" version="12">
<LogString>WEB-CGI simplestmail.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/simplestmail.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2106</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2001-0022</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1591" source="Snort" sourceid="1591" type="" version="12">
<LogString>WEB-CGI faqmanager.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/faqmanager.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3810</Reference>
<Reference>nessus,10837</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1469" source="Snort" sourceid="1469" type="" version="11">
<LogString>WEB-CGI Web Shopper shopper.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/shopper.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1776</Reference>
<Reference>cve,2000-0922</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2210" source="Snort" sourceid="2210" type="" version="11">
<LogString>WEB-CGI global.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/global.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2000-0952</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="806" source="Snort" sourceid="806" type="" version="18">
<LogString>WEB-CGI yabb directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/YaBB</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,462</Reference>
<Reference>bugtraq,1668</Reference>
<Reference>cve,2000-0853</Reference>
<Reference>nessus,10512</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1106" source="Snort" sourceid="1106" type="" version="17">
<LogString>WEB-CGI Poll-it access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pollit/Poll_It_SSI_v2.0.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1431</Reference>

<Reference>cve,2000-0590</Reference>
<Reference>nessus,10459</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1531" source="Snort" sourceid="1531" type="" version="12">
<LogString>WEB-CGI bb-hist.sh attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-hist.sh?HISTFILE=../..</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,142</Reference>
<Reference>cve,1999-1462</Reference>
<Reference>nessus,10025</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="886" source="Snort" sourceid="886" type="" version="17">
<LogString>WEB-CGI phf access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/phf</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,128</Reference>
<Reference>bugtraq,629</Reference>
<Reference>cve,1999-0067</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="819" source="Snort" sourceid="819" type="" version="16">
<LogString>WEB-CGI mmstdod.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/mmstdod.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2063</Reference>
<Reference>cve,2001-0021</Reference>
<Reference>nessus,10566</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1456" source="Snort" sourceid="1456" type="" version="11">
<LogString>WEB-CGI calender_admin.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/calender_admin.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2000-0432</Reference>
<Reference>nessus,10506</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2195" source="Snort" sourceid="2195" type="" version="12">
<LogString>WEB-CGI alert.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/alert.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4211</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2002-0346</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1651" source="Snort" sourceid="1651" type="" version="11">
<LogString>WEB-CGI environ.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/environ.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="864" source="Snort" sourceid="864" type="" version="13">
<LogString>WEB-CGI day5datanotifier.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/day5datanotifier.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1232</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1722" source="Snort" sourceid="1722" type="" version="12">
<LogString>WEB-CGI MachineInfo access</LogString>
<PatternList>
<RequestPatterns>

<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/MachineInfo</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1067</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1466" source="Snort" sourceid="1466" type="" version="14">
<LogString>WEB-CGI cgiforum.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgiforum.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1963</Reference>
<Reference>cve,2000-1171</Reference>
<Reference>nessus,10552</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1533" source="Snort" sourceid="1533" type="" version="13">
<LogString>WEB-CGI bb-hostscv.sh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-hostsvc.sh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1455</Reference>
<Reference>cve,2000-0638</Reference>
<Reference>nessus,10460</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2197" source="Snort" sourceid="2197" type="" version="13">
<LogString>WEB-CGI cvsview2.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cvsview2.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,5517</Reference>
<Reference>cve,2003-0153</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="826" source="Snort" sourceid="826" type="" version="15">
<LogString>WEB-CGI htmlscript access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/htmlscript</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2001</Reference>
<Reference>cve,1999-0264</Reference>
<Reference>nessus,10106</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1392" source="Snort" sourceid="1392" type="" version="16">
<LogString>WEB-CGI lastlines.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/lastlines.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3754</Reference>
<Reference>bugtraq,3755</Reference>
<Reference>cve,2001-1205</Reference>
<Reference>cve,2001-1206</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1602" source="Snort" sourceid="1602" type="" version="15">
<LogString>WEB-CGI htsearch access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/htsearch</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1026</Reference>
<Reference>cve,2000-0208</Reference>
<Reference>nessus,10105</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1219" source="Snort" sourceid="1219" type="" version="17">
<LogString>WEB-CGI dfire.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dfire.cgi</Match>

</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,564</Reference>
<Reference>cve,1999-0913</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2128" source="Snort" sourceid="2128" type="" version="12">
<LogString>WEB-CGI swsrv.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/swsrv.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7510</Reference>
<Reference>cve,2003-0217</Reference>
<Reference>nessus,11608</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="804" source="Snort" sourceid="804" type="" version="15">
<LogString>WEB-CGI SWSoft ASPSeek Overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/s.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">tmpl=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2492</Reference>
<Reference>cve,2001-0476</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2323" source="Snort" sourceid="2323" type="" version="8">
<LogString>WEB-CGI quickstore.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/quickstore.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9282</Reference>
<Reference>nessus,11975</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1542" source="Snort" sourceid="1542" type="" version="14">

<LogString>WEB-CGI cgimail access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgimail</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1623</Reference>
<Reference>cve,2000-0726</Reference>
<Reference>nessus,11721</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="836" source="Snort" sourceid="836" type="" version="16">
<LogString>WEB-CGI textcounter.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/textcounter.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2265</Reference>
<Reference>cve,1999-1479</Reference>
<Reference>nessus,11451</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="857" source="Snort" sourceid="857" type="" version="16">
<LogString>WEB-CGI faxsurvey access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/faxsurvey</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2056</Reference>
<Reference>cve,1999-0262</Reference>
<Reference>nessus,10067</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="852" source="Snort" sourceid="852" type="" version="16">
<LogString>WEB-CGI wguest.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wguest.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,2024</Reference>
<Reference>cve,1999-0287</Reference>
<Reference>cve,1999-0467</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1475" source="Snort" sourceid="1475" type="" version="12">
<LogString>WEB-CGI mailit.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/mailit.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10417</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2225" source="Snort" sourceid="2225" type="" version="9">
<LogString>WEB-CGI gozila.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/gozila.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6086</Reference>
<Reference>cve,2002-1236</Reference>
<Reference>nessus,11773</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="848" source="Snort" sourceid="848" type="" version="15">
<LogString>WEB-CGI view-source directory traversal</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/view-source</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2251</Reference>
<Reference>bugtraq,8883</Reference>
<Reference>cve,1999-0174</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1481" source="Snort" sourceid="1481" type="" version="10">
<LogString>WEB-CGI upload.cgi access</LogString>
<PatternList>

<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/upload.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10290</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1703" source="Snort" sourceid="1703" type="" version="13">
<LogString>WEB-CGI auktion.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/auktion.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">menue=../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2367</Reference>
<Reference>cve,2001-0212</Reference>
<Reference>nessus,10638</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2194" source="Snort" sourceid="2194" type="" version="12">
<LogString>WEB-CGI CSMailto.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/CSMailto.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,6265</Reference>
<Reference>cve,2002-0749</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1458" source="Snort" sourceid="1458" type="" version="12">
<LogString>WEB-CGI user_update_passwd.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/user_update_passwd.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,1486</Reference>
<Reference>cve,2000-0627</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="875" source="Snort" sourceid="875" type="" version="15">
<LogString>WEB-CGI win-c-sample.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/win-c-sample.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,231</Reference>
<Reference>bugtraq,2078</Reference>
<Reference>cve,1999-0178</Reference>
<Reference>nessus,10008</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1539" source="Snort" sourceid="1539" type="" version="13">
<LogString>WEB-CGI /cgi-bin/ls access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgi-bin/ls</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,936</Reference>
<Reference>cve,2000-0079</Reference>
<Reference>nessus,10037</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2218" source="Snort" sourceid="2218" type="" version="12">
<LogString>WEB-CGI service.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/service.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4211</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2002-0346</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1601" source="Snort" sourceid="1601" type="" version="15">
<LogString>WEB-CGI htsearch arbitrary file read attempt</LogString>
<PatternList>

<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/htsearch?exclude=`</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1026</Reference>
<Reference>cve,2000-0208</Reference>
<Reference>nessus,10105</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2200" source="Snort" sourceid="2200" type="" version="12">
<LogString>WEB-CGI dnewsweb.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dnewsweb.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1172</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2000-0423</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="892" source="Snort" sourceid="892" type="" version="16">
<LogString>WEB-CGI AnyForm2 access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/AnyForm2</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,719</Reference>
<Reference>cve,1999-0066</Reference>
<Reference>nessus,10277</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1052" source="Snort" sourceid="1052" type="" version="16">
<LogString>
WEB-CGI technote print.cgi directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/technote/print.cgi</Match>
</Pattern>
<Pattern>

<Match type="LITERAL">board=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../../</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%00</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2156</Reference>
<Reference>cve,2001-0075</Reference>
<Reference>nessus,10584</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2207" source="Snort" sourceid="2207" type="" version="12">
<LogString>WEB-CGI fileseek.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/fileseek.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,6784</Reference>
<Reference>cve,2002-0611</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="846" source="Snort" sourceid="846" type="" version="14">
<LogString>WEB-CGI bnbform.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bnbform.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2147</Reference>
<Reference>cve,1999-0937</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="859" source="Snort" sourceid="859" type="" version="15">
<LogString>WEB-CGI man.sh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/man.sh</Match>
</Pattern>
</RequestPatterns>

</PatternList>
<Reference>bugtraq,2276</Reference>
<Reference>cve,1999-1179</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="862" source="Snort" sourceid="862" type="" version="14">
<LogString>WEB-CGI csh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/csh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="824" source="Snort" sourceid="824" type="" version="20">
<LogString>WEB-CGI php.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/php.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,232</Reference>
<Reference>bugtraq,2250</Reference>
<Reference>bugtraq,712</Reference>
<Reference>cve,1999-0058</Reference>
<Reference>cve,1999-0238</Reference>
<Reference>nessus,10178</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="851" source="Snort" sourceid="851" type="" version="13">
<LogString>WEB-CGI files.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/files.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1081</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2668" source="Snort" sourceid="2668" type="" version="8">
<LogString>WEB-CGI processit access</LogString>
<PatternList>
<RequestPatterns>

<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/processit.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10649</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1556" source="Snort" sourceid="1556" type="" version="13">
<LogString>WEB-CGI DCShop orders.txt access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/orders/orders.txt</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2889</Reference>
<Reference>cve,2001-0821</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1470" source="Snort" sourceid="1470" type="" version="14">
<LogString>WEB-CGI listrec.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/listrec.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3328</Reference>
<Reference>cve,2001-0997</Reference>
<Reference>nessus,10769</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="869" source="Snort" sourceid="869" type="" version="14">
<LogString>WEB-CGI dumpenv.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dumpenv.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1178</Reference>
<Reference>nessus,10060</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1850" source="Snort" sourceid="1850" type="" version="9">
<LogString>WEB-CGI way-board.cgi access</LogString>

<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/way-board.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10610</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1222" source="Snort" sourceid="1222" type="" version="15">
<LogString>WEB-CGI pals-cgi arbitrary file access attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pals-cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">documentName=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2372</Reference>
<Reference>cve,2001-0217</Reference>
<Reference>nessus,10611</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1468" source="Snort" sourceid="1468" type="" version="14">
<LogString>WEB-CGI Web Shopper shopper.cgi attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/shopper.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">newpage=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1776</Reference>
<Reference>cve,2000-0922</Reference>
<Reference>nessus,10533</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1593" source="Snort" sourceid="1593" type="" version="16">
<LogString>
WEB-CGI FormHandler.cgi external site redirection attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/FormHandler.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">redirect=http</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,798</Reference>
<Reference>bugtraq,799</Reference>
<Reference>cve,1999-1050</Reference>
<Reference>nessus,10075</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1720" source="Snort" sourceid="1720" type="" version="12">
<LogString>WEB-CGI talkback.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/talkbalk.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2547</Reference>
<Reference>cve,2001-0420</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1482" source="Snort" sourceid="1482" type="" version="13">
<LogString>WEB-CGI view_source access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/view_source</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2251</Reference>
<Reference>cve,1999-0174</Reference>
<Reference>nessus,10294</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="885" source="Snort" sourceid="885" type="" version="14">
<LogString>WEB-CGI bash access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bash</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>

<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="829" source="Snort" sourceid="829" type="" version="17">
<LogString>WEB-CGI nph-test-cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/nph-test-cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,224</Reference>
<Reference>bugtraq,686</Reference>
<Reference>cve,1999-0045</Reference>
<Reference>nessus,10165</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1532" source="Snort" sourceid="1532" type="" version="13">
<LogString>WEB-CGI bb-hostscv.sh attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-hostsvc.sh?HOSTSVC?../..</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1455</Reference>
<Reference>cve,2000-0638</Reference>
<Reference>nessus,10460</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1405" source="Snort" sourceid="1405" type="" version="11">
<LogString>WEB-CGI AHG search.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/publisher/search.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">template=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3985</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2396" source="Snort" sourceid="2396" type="" version="10">
<LogString>
WEB-CGI CCBill whereami.cgi arbitrary command execution attempt
</LogString>

<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/whereami.cgi?g=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8095</Reference>
<Reference>url,secunia.com/advisories/9191/</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="807" source="Snort" sourceid="807" type="" version="17">
<LogString>WEB-CGI /wwwboard/passwd.txt access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wwwboard/passwd.txt</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,463</Reference>
<Reference>bugtraq,649</Reference>
<Reference>cve,1999-0953</Reference>
<Reference>cve,1999-0954</Reference>
<Reference>nessus,10321</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2216" source="Snort" sourceid="2216" type="" version="12">
<LogString>WEB-CGI readmail.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/readmail.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3427</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2001-1283</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2567" source="Snort" sourceid="2567" type="" version="9">
<LogString>WEB-CGI Emumail init.emu access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/init.emu</Match>
</Pattern>
</RequestPatterns>

</PatternList>
<Reference>bugtraq,9861</Reference>
<Reference>nessus,12095</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1185" source="Snort" sourceid="1185" type="" version="18">
<LogString>WEB-CGI bizdbsearch attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bizdb1-search.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">mail</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1104</Reference>
<Reference>cve,2000-0287</Reference>
<Reference>nessus,10383</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2199" source="Snort" sourceid="2199" type="" version="12">
<LogString>WEB-CGI multidiff.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/multidiff.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,5517</Reference>
<Reference>cve,2003-0153</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1646" source="Snort" sourceid="1646" type="" version="11">
<LogString>WEB-CGI test.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/test.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1701" source="Snort" sourceid="1701" type="" version="12">
<LogString>WEB-CGI calendar-admin.pl access</LogString>
<PatternList>

<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/calendar-admin.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1215</Reference>
<Reference>cve,2000-0432</Reference>
<Reference>nessus,10506</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="815" source="Snort" sourceid="815" type="" version="15">
<LogString>WEB-CGI websendmail access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/websendmail</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,469</Reference>
<Reference>bugtraq,2077</Reference>
<Reference>cve,1999-0196</Reference>
<Reference>nessus,10301</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="877" source="Snort" sourceid="877" type="" version="13">
<LogString>WEB-CGI rksh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/rksh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1724" source="Snort" sourceid="1724" type="" version="12">
<LogString>WEB-CGI emumail.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/emumail.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,5824</Reference>
<Reference>cve,2002-1526</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="894" source="Snort" sourceid="894" type="" version="14">
<LogString>WEB-CGI bb-hist.sh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-hist.sh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,142</Reference>
<Reference>cve,1999-1462</Reference>
<Reference>nessus,10025</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2209" source="Snort" sourceid="2209" type="" version="13">
<LogString>WEB-CGI getdoc.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/getdoc.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2000-0288</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1196" source="Snort" sourceid="1196" type="" version="17">
<LogString>WEB-CGI SGI InfoSearch fname attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/infosrch.cgi?</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">fname=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,290</Reference>
<Reference>bugtraq,1031</Reference>
<Reference>cve,2000-0207</Reference>
<Reference>nessus,10128</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2214" source="Snort" sourceid="2214" type="" version="12">
<LogString>WEB-CGI mailview.cgi access</LogString>
<PatternList>

<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/mailview.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1335</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2000-0526</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="16079" source="Snort" sourceid="16079" type="" version="5">
<LogString>WEB-CGI uselang code injection</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wiki</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">?uselang=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
\x2fwiki[^\n]*\x3fuselang=[^\n\x26\x3f]*[a-zA-Z\x2d]
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,15703</Reference>
<Reference>cve,2005-4031</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1472" source="Snort" sourceid="1472" type="" version="15">
<LogString>WEB-CGI book.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/book.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3178</Reference>
<Reference>cve,2001-1114</Reference>
<Reference>nessus,10721</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1090" source="Snort" sourceid="1090" type="" version="13">
<LogString>WEB-CGI Allaire Pro Web Shell attempt</LogString>

<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/authenticate.cgi?PASSWORD</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">config.ini</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1308" source="Snort" sourceid="1308" type="" version="14">
<LogString>WEB-CGI sendmessage.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/sendmessage.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3673</Reference>
<Reference>cve,2001-1100</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1215" source="Snort" sourceid="1215" type="" version="12">
<LogString>WEB-CGI ministats admin access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ministats/admin.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="868" source="Snort" sourceid="868" type="" version="14">
<LogString>WEB-CGI rsh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/rsh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2388" source="Snort" sourceid="2388" type="" version="10">

<LogString>WEB-CGI streaming server view_broadcast.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/view_broadcast.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8257</Reference>
<Reference>cve,2003-0422</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="887" source="Snort" sourceid="887"
type="" version="12">
<LogString>WEB-CGI www-sql access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/www-sql</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>
url,marc.theaimsgroup.com/?l=bugtraq&m=88704258804054&w=2
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="849" source="Snort" sourceid="849"
type="" version="14">
<LogString>WEB-CGI view-source access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/view-source</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2251</Reference>
<Reference>bugtraq,8883</Reference>
<Reference>cve,1999-0174</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="880" source="Snort" sourceid="880"
type="" version="14">
<LogString>WEB-CGI LWGate access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/LWGate</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>

url,www.netspace.org/~dwb/lwgate/lwgate-history.html
</Reference>
<Reference>url,www.wiretrip.net/rfp/p/doc.asp/i2/d6.htm</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="902" source="Snort" sourceid="902" type="" version="15">
<LogString>WEB-CGI tstisapi.dll access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">tstisapi.dll</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2381</Reference>
<Reference>cve,2001-0302</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="827" source="Snort" sourceid="827" type="" version="15">
<LogString>WEB-CGI info2www access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/info2www</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1995</Reference>
<Reference>cve,1999-0266</Reference>
<Reference>nessus,10127</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3463" source="Snort" sourceid="3463" type="" version="8">
<LogString>WEB-CGI awstats access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/awstats.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12572</Reference>
<Reference>nessus,16456</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1714" source="Snort" sourceid="1714" type="" version="10">
<LogString>WEB-CGI newdesk access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>

<Match type="LITERAL">/newdesk</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2053" source="Snort" sourceid="2053" type="" version="10">
<LogString>WEB-CGI process_bug.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/process_bug.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3272</Reference>
<Reference>cve,2002-0008</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="839" source="Snort" sourceid="839" type="" version="13">
<LogString>WEB-CGI finger access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/finger</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,221</Reference>
<Reference>cve,1999-0612</Reference>
<Reference>nessus,10071</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1461" source="Snort" sourceid="1461" type="" version="11">
<LogString>WEB-CGI bb-rep.sh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-rep.sh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,142</Reference>
<Reference>cve,1999-1462</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="825" source="Snort" sourceid="825" type="" version="15">
<LogString>WEB-CGI glimpse access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/glimpse</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2026</Reference>
<Reference>cve,1999-0147</Reference>
<Reference>nessus,10095</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="844" source="Snort" sourceid="844" type="" version="15">
<LogString>WEB-CGI args.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/args.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1180</Reference>
<Reference>nessus,11465</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3638" source="Snort" sourceid="3638" type="" version="13">
<LogString>WEB-CGI SoftCart.exe CGI buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/SoftCart.exe</Match>
</Pattern>
<Pattern>
<Match type="PCRE">\/SoftCart.exe\?[^\s]{100}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10926</Reference>
<Reference>cve,2004-2221</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1656" source="Snort" sourceid="1656" type="" version="13">
<LogString>WEB-CGI pfdispaly.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pfdispaly.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,64</Reference>
<Reference>cve,1999-0270</Reference>
<Reference>nessus,10174</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="856" source="Snort" sourceid="856" type="" version="11">
<LogString>WEB-CGI environ.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/environ.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1557" source="Snort" sourceid="1557" type="" version="13">
<LogString>WEB-CGI DCShop auth_user_file.txt access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/auth_data/auth_user_file.txt</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2889</Reference>
<Reference>cve,2001-0821</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1718" source="Snort" sourceid="1718" type="" version="13">
<LogString>WEB-CGI statsconfig.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/statsconfig.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2211</Reference>
<Reference>cve,2001-0113</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2224" source="Snort" sourceid="2224" type="" version="7">
<LogString>WEB-CGI psunami.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/psunami.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6607</Reference>
<Reference>nessus,11750</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="837" source="Snort" sourceid="837" type="" version="16">
<LogString>WEB-CGI uploader.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/uploader.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1611</Reference>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wguest.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2024</Reference>
<Reference>cve,1999-0287</Reference>
<Reference>cve,1999-0467</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1475" source="Snort" sourceid="1475" type="" version="12">
<LogString>WEB-CGI mailit.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/mailit.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10417</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2225" source="Snort" sourceid="2225" type="" version="9">
<LogString>WEB-CGI gozila.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/gozila.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6086</Reference>
<Reference>cve,2002-1236</Reference>
<Reference>nessus,11773</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="848" source="Snort" sourceid="848"

type="" version="15">
<LogString>WEB-CGI view-source directory traversal</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/view-source</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2251</Reference>
<Reference>bugtraq,8883</Reference>
<Reference>cve,1999-0174</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1481" source="Snort" sourceid="1481"
type="" version="10">
<LogString>WEB-CGI upload.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/upload.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10290</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1703" source="Snort" sourceid="1703"
type="" version="13">
<LogString>WEB-CGI auktion.cgi directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/auktion.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">menue=../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2367</Reference>
<Reference>cve,2001-0212</Reference>
<Reference>nessus,10638</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2194" source="Snort" sourceid="2194"
type="" version="12">
<LogString>WEB-CGI CSMailto.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/CSMailto.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,6265</Reference>
<Reference>cve,2002-0749</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1458" source="Snort" sourceid="1458" type="" version="12">
<LogString>WEB-CGI user_update_passwd.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/user_update_passwd.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1486</Reference>
<Reference>cve,2000-0627</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="875" source="Snort" sourceid="875" type="" version="15">
<LogString>WEB-CGI win-c-sample.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/win-c-sample.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,231</Reference>
<Reference>bugtraq,2078</Reference>
<Reference>cve,1999-0178</Reference>
<Reference>nessus,10008</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1539" source="Snort" sourceid="1539" type="" version="13">
<LogString>WEB-CGI /cgi-bin/ls access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cgi-bin/ls</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,936</Reference>
<Reference>cve,2000-0079</Reference>
<Reference>nessus,10037</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2218" source="Snort" sourceid="2218" type="" version="12">
<LogString>WEB-CGI service.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/service.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4211</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2002-0346</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1601" source="Snort" sourceid="1601" type="" version="15">
<LogString>WEB-CGI htsearch arbitrary file read attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/htsearch?exclude=`</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1026</Reference>
<Reference>cve,2000-0208</Reference>
<Reference>nessus,10105</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2200" source="Snort" sourceid="2200" type="" version="12">
<LogString>WEB-CGI dnewsweb.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dnewsweb.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1172</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2000-0423</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="892" source="Snort" sourceid="892" type="" version="16">
<LogString>WEB-CGI AnyForm2 access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/AnyForm2</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,719</Reference>
<Reference>cve,1999-0066</Reference>
<Reference>nessus,10277</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1052" source="Snort" sourceid="1052" type="" version="16">
<LogString>
WEB-CGI technote print.cgi directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/technote/print.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">board=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../../</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%00</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2156</Reference>
<Reference>cve,2001-0075</Reference>
<Reference>nessus,10584</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2207" source="Snort" sourceid="2207" type="" version="12">
<LogString>WEB-CGI fileseek.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/fileseek.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,6784</Reference>
<Reference>cve,2002-0611</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="846" source="Snort" sourceid="846" type="" version="14">
<LogString>WEB-CGI bnbform.cgi access</LogString>

<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bnbform.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2147</Reference>
<Reference>cve,1999-0937</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="859" source="Snort" sourceid="859" type="" version="15">
<LogString>WEB-CGI man.sh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/man.sh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2276</Reference>
<Reference>cve,1999-1179</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="862" source="Snort" sourceid="862" type="" version="14">
<LogString>WEB-CGI csh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/csh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="824" source="Snort" sourceid="824" type="" version="20">
<LogString>WEB-CGI php.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/php.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,232</Reference>
<Reference>bugtraq,2250</Reference>
<Reference>bugtraq,712</Reference>
<Reference>cve,1999-0058</Reference>

<Reference>cve,1999-0238</Reference>
<Reference>nessus,10178</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="851" source="Snort" sourceid="851" type="" version="13">
<LogString>WEB-CGI files.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/files.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1081</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2668" source="Snort" sourceid="2668" type="" version="8">
<LogString>WEB-CGI processit access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/processit.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10649</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1556" source="Snort" sourceid="1556" type="" version="13">
<LogString>WEB-CGI DCShop orders.txt access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/orders/orders.txt</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2889</Reference>
<Reference>cve,2001-0821</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1470" source="Snort" sourceid="1470" type="" version="14">
<LogString>WEB-CGI listrec.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/listrec.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,3328</Reference>
<Reference>cve,2001-0997</Reference>
<Reference>nessus,10769</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="869" source="Snort" sourceid="869" type="" version="14">
<LogString>WEB-CGI dumpenv.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dumpenv.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1178</Reference>
<Reference>nessus,10060</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1850" source="Snort" sourceid="1850" type="" version="9">
<LogString>WEB-CGI way-board.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/way-board.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,10610</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1222" source="Snort" sourceid="1222" type="" version="15">
<LogString>WEB-CGI pals-cgi arbitrary file access attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pals-cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">documentName=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2372</Reference>
<Reference>cve,2001-0217</Reference>
<Reference>nessus,10611</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1468" source="Snort" sourceid="1468" type="" version="14">
<LogString>WEB-CGI Web Shopper shopper.cgi attempt</LogString>
<PatternList>
<RequestPatterns>

<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/shopper.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">newpage=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1776</Reference>
<Reference>cve,2000-0922</Reference>
<Reference>nessus,10533</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1593" source="Snort" sourceid="1593" type="" version="16">
<LogString>
WEB-CGI FormHandler.cgi external site redirection attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/FormHandler.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">redirect=http</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,798</Reference>
<Reference>bugtraq,799</Reference>
<Reference>cve,1999-1050</Reference>
<Reference>nessus,10075</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1720" source="Snort" sourceid="1720" type="" version="12">
<LogString>WEB-CGI talkback.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/talkbalk.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2547</Reference>
<Reference>cve,2001-0420</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1482" source="Snort" sourceid="1482" type="" version="13">
<LogString>WEB-CGI view_source access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/view_source</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2251</Reference>
<Reference>cve,1999-0174</Reference>
<Reference>nessus,10294</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="885" source="Snort" sourceid="885" type="" version="14">
<LogString>WEB-CGI bash access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bash</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="829" source="Snort" sourceid="829" type="" version="17">
<LogString>WEB-CGI nph-test-cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/nph-test-cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,224</Reference>
<Reference>bugtraq,686</Reference>
<Reference>cve,1999-0045</Reference>
<Reference>nessus,10165</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1532" source="Snort" sourceid="1532" type="" version="13">
<LogString>WEB-CGI bb-hostscv.sh attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-hostsvc.sh?HOSTSVC?../..</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1455</Reference>
<Reference>cve,2000-0638</Reference>
<Reference>nessus,10460</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1405" source="Snort" sourceid="1405" type="" version="11">
<LogString>WEB-CGI AHG search.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/publisher/search.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">template=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3985</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2396" source="Snort" sourceid="2396" type="" version="10">
<LogString>
WEB-CGI CCBill whereami.cgi arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/whereami.cgi?g=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8095</Reference>
<Reference>url,secunia.com/advisories/9191/</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="807" source="Snort" sourceid="807" type="" version="17">
<LogString>WEB-CGI /wwwboard/passwd.txt access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wwwboard/passwd.txt</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,463</Reference>
<Reference>bugtraq,649</Reference>
<Reference>cve,1999-0953</Reference>
<Reference>cve,1999-0954</Reference>
<Reference>nessus,10321</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2216" source="Snort" sourceid="2216" type="" version="12">
<LogString>WEB-CGI readmail.cgi access</LogString>
<PatternList>
<RequestPatterns>

<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/readmail.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3427</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2001-1283</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2567" source="Snort" sourceid="2567" type="" version="9">
<LogString>WEB-CGI Emumail init.emu access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/init.emu</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9861</Reference>
<Reference>nessus,12095</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1185" source="Snort" sourceid="1185" type="" version="18">
<LogString>WEB-CGI bizdbsearch attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bizdb1-search.cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">mail</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1104</Reference>
<Reference>cve,2000-0287</Reference>
<Reference>nessus,10383</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2199" source="Snort" sourceid="2199" type="" version="12">
<LogString>WEB-CGI multidiff.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/multidiff.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,4579</Reference>
<Reference>bugtraq,5517</Reference>
<Reference>cve,2003-0153</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1646" source="Snort" sourceid="1646" type="" version="11">
<LogString>WEB-CGI test.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/test.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1701" source="Snort" sourceid="1701" type="" version="12">
<LogString>WEB-CGI calendar-admin.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/calendar-admin.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1215</Reference>
<Reference>cve,2000-0432</Reference>
<Reference>nessus,10506</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="815" source="Snort" sourceid="815" type="" version="15">
<LogString>WEB-CGI websendmail access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/websendmail</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,469</Reference>
<Reference>bugtraq,2077</Reference>
<Reference>cve,1999-0196</Reference>
<Reference>nessus,10301</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="877" source="Snort" sourceid="877" type="" version="13">
<LogString>WEB-CGI rksh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/rksh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1724" source="Snort" sourceid="1724" type="" version="12">
<LogString>WEB-CGI emumail.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/emumail.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,5824</Reference>
<Reference>cve,2002-1526</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="894" source="Snort" sourceid="894" type="" version="14">
<LogString>WEB-CGI bb-hist.sh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-hist.sh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,142</Reference>
<Reference>cve,1999-1462</Reference>
<Reference>nessus,10025</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2209" source="Snort" sourceid="2209" type="" version="13">
<LogString>WEB-CGI getdoc.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/getdoc.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2000-0288</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1196" source="Snort" sourceid="1196" type="" version="17">

<LogString>WEB-CGI SGI InfoSearch fname attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/infosrch.cgi?</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">fname=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,290</Reference>
<Reference>bugtraq,1031</Reference>
<Reference>cve,2000-0207</Reference>
<Reference>nessus,10128</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2214" source="Snort" sourceid="2214" type="" version="12">
<LogString>WEB-CGI mailview.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/mailview.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1335</Reference>
<Reference>bugtraq,4579</Reference>
<Reference>cve,2000-0526</Reference>
<Reference>nessus,11748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="16079" source="Snort" sourceid="16079" type="" version="5">
<LogString>WEB-CGI uselang code injection</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wiki</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">?uselang=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
\x2fwiki[^\n]*\x3fuselang=[^\n\x26\x3f]*[a-zA-Z\x2d]
</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,15703</Reference>
<Reference>cve,2005-4031</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1472" source="Snort" sourceid="1472" type="" version="15">
<LogString>WEB-CGI book.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/book.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3178</Reference>
<Reference>cve,2001-1114</Reference>
<Reference>nessus,10721</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1090" source="Snort" sourceid="1090" type="" version="13">
<LogString>WEB-CGI Allaire Pro Web Shell attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/authenticate.cgi?PASSWORD</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">config.ini</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1308" source="Snort" sourceid="1308" type="" version="14">
<LogString>WEB-CGI sendmessage.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/sendmessage.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3673</Reference>
<Reference>cve,2001-1100</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1215" source="Snort" sourceid="1215" type="" version="12">
<LogString>WEB-CGI ministats admin access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>

<Match type="LITERAL">/ministats/admin.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="868" source="Snort" sourceid="868"
type="" version="14">
<LogString>WEB-CGI rsh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/rsh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-0509</Reference>
<Reference>url,www.cert.org/advisories/CA-1996-11.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2388" source="Snort" sourceid="2388"
type="" version="10">
<LogString>WEB-CGI streaming server view_broadcast.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/view_broadcast.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8257</Reference>
<Reference>cve,2003-0422</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="887" source="Snort" sourceid="887"
type="" version="12">
<LogString>WEB-CGI www-sql access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/www-sql</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>
url,marc.theaimsgroup.com/?l=bugtraq&m=88704258804054&w=2
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="849" source="Snort" sourceid="849"
type="" version="14">
<LogString>WEB-CGI view-source access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/view-source</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2251</Reference>
<Reference>bugtraq,8883</Reference>
<Reference>cve,1999-0174</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="880" source="Snort" sourceid="880" type="" version="14">
<LogString>WEB-CGI LWGate access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/LWGate</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>
url,www.netspace.org/~dwb/lwgate/lwgate-history.html
</Reference>
<Reference>url,www.wiretrip.net/rfp/p/doc.asp/i2/d6.htm</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="902" source="Snort" sourceid="902" type="" version="15">
<LogString>WEB-CGI tstisapi.dll access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">tstisapi.dll</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2381</Reference>
<Reference>cve,2001-0302</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="827" source="Snort" sourceid="827" type="" version="15">
<LogString>WEB-CGI info2www access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/info2www</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1995</Reference>
<Reference>cve,1999-0266</Reference>
<Reference>nessus,10127</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3463" source="Snort" sourceid="3463" type="" version="8">
<LogString>WEB-CGI awstats access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/awstats.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12572</Reference>
<Reference>nessus,16456</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1714" source="Snort" sourceid="1714" type="" version="10">
<LogString>WEB-CGI newdesk access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/newdesk</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2053" source="Snort" sourceid="2053" type="" version="10">
<LogString>WEB-CGI process_bug.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/process_bug.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3272</Reference>
<Reference>cve,2002-0008</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="839" source="Snort" sourceid="839" type="" version="13">
<LogString>WEB-CGI finger access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/finger</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,221</Reference>
<Reference>cve,1999-0612</Reference>
<Reference>nessus,10071</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1461" source="Snort" sourceid="1461" type="" version="11">
<LogString>WEB-CGI bb-rep.sh access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb-rep.sh</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,142</Reference>
<Reference>cve,1999-1462</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="825" source="Snort" sourceid="825" type="" version="15">
<LogString>WEB-CGI glimpse access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/glimpse</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2026</Reference>
<Reference>cve,1999-0147</Reference>
<Reference>nessus,10095</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="844" source="Snort" sourceid="844" type="" version="15">
<LogString>WEB-CGI args.bat access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/args.bat</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,1999-1180</Reference>
<Reference>nessus,11465</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="3638" source="Snort" sourceid="3638" type="" version="13">
<LogString>WEB-CGI SoftCart.exe CGI buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/SoftCart.exe</Match>
</Pattern>
<Pattern>

<Match type="PCRE">\/SoftCart.exe\?[^\s]{100}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10926</Reference>
<Reference>cve,2004-2221</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1656" source="Snort" sourceid="1656" type="" version="13">
<LogString>WEB-CGI pfdispaly.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pfdispaly.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,64</Reference>
<Reference>cve,1999-0270</Reference>
<Reference>nessus,10174</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="856" source="Snort" sourceid="856" type="" version="11">
<LogString>WEB-CGI environ.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/environ.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1557" source="Snort" sourceid="1557" type="" version="13">
<LogString>WEB-CGI DCShop auth_user_file.txt access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/auth_data/auth_user_file.txt</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2889</Reference>
<Reference>cve,2001-0821</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="1718" source="Snort" sourceid="1718" type="" version="13">
<LogString>WEB-CGI statsconfig.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">

<Location area="HTTP_URL"/>
<Match type="LITERAL">/statsconfig.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,2211</Reference>
<Reference>cve,2001-0113</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="2224" source="Snort" sourceid="2224" type="" version="7">
<LogString>WEB-CGI psunami.cgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/psunami.cgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6607</Reference>
<Reference>nessus,11750</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="OFF" id="837" source="Snort" sourceid="837" type="" version="16">
<LogString>WEB-CGI uploader.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/uploader.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1611</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2239" source="Snort" sourceid="2239" type="" version="7">
<LogString>WEB-MISC redirect.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/redirect.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1256</Reference>
<Reference>cve,2000-0401</Reference>
<Reference>nessus,11723</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2240" source="Snort" sourceid="2240" type="" version="7">
<LogString>WEB-MISC changepw.exe access</LogString>
<PatternList>

<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/changepw.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1256</Reference>
<Reference>cve,2000-0401</Reference>
<Reference>nessus,11723</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2241" source="Snort" sourceid="2241" type="" version="8">
<LogString>WEB-MISC cwmail.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cwmail.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4093</Reference>
<Reference>cve,2002-0273</Reference>
<Reference>nessus,11727</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2242" source="Snort" sourceid="2242" type="" version="7">
<LogString>WEB-MISC ddicgi.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ddicgi.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1657</Reference>
<Reference>cve,2000-0826</Reference>
<Reference>nessus,11728</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2243" source="Snort" sourceid="2243" type="" version="8">
<LogString>WEB-MISC ndcgi.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ndcgi.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3583</Reference>
<Reference>cve,2001-0922</Reference>

<Reference>nessus,11730</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2244" source="Snort" sourceid="2244" type="" version="7">
<LogString>WEB-MISC VsSetCookie.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/VsSetCookie.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3784</Reference>
<Reference>cve,2002-0236</Reference>
<Reference>nessus,11731</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2245" source="Snort" sourceid="2245" type="" version="8">
<LogString>WEB-MISC Webnews.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/Webnews.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4124</Reference>
<Reference>cve,2002-0290</Reference>
<Reference>nessus,11732</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2246" source="Snort" sourceid="2246" type="" version="9">
<LogString>WEB-MISC webadmin.dll access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/webadmin.dll</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7438</Reference>
<Reference>bugtraq,7439</Reference>
<Reference>bugtraq,8024</Reference>
<Reference>cve,2003-0471</Reference>
<Reference>nessus,11771</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2276" source="Snort" sourceid="2276" type="" version="4">
<LogString>WEB-MISC oracle portal demo access</LogString>
<PatternList>
<RequestPatterns>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/pls/portal/PORTAL_DEMO</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11918</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2277" source="Snort" sourceid="2277" type="" version="7">
<LogString>WEB-MISC PeopleSoft PeopleBooks psdoccgi access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/psdoccgi</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9037</Reference>
<Reference>bugtraq,9038</Reference>
<Reference>cve,2003-0626</Reference>
<Reference>cve,2003-0627</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2580" source="Snort" sourceid="2580" type="" version="7">
<LogString>WEB-MISC server negative Content-Length attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">Content-Length</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^Content-Length\s*\x3a\s*-\d+</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10508</Reference>
<Reference>cve,2004-0492</Reference>
<Reference>url,www.guninski.com/modproxy1.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2327" source="Snort" sourceid="2327" type="" version="5">
<LogString>WEB-MISC bsml.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bsml.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9311</Reference>
<Reference>nessus,11973</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2369" source="Snort" sourceid="2369" type="" version="4">
<LogString>WEB-MISC ISAPISkeleton.dll access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ISAPISkeleton.dll</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9516</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2370" source="Snort" sourceid="2370" type="" version="5">
<LogString>WEB-MISC BugPort config.conf file access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/config.conf</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9542</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2371" source="Snort" sourceid="2371" type="" version="5">
<LogString>WEB-MISC Sample_showcode.html access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/Sample_showcode.html</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">fname</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9555</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2381" source="Snort" sourceid="2381" type="" version="14">
<LogString>
WEB-MISC Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">|3A|/</Match>
</Pattern>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">^[^\x3a\x3f]{11,}\x3a\x2f</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9581</Reference>
<Reference>cve,2004-0039</Reference>
<Reference>nessus,12084</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2394" source="Snort" sourceid="2394" type="" version="6">
<LogString>
WEB-MISC Compaq web-based management agent denial of service attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL"><!</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">></Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8014</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2395" source="Snort" sourceid="2395" type="" version="6">
<LogString>WEB-MISC InteractiveQuery.jsp access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/InteractiveQuery.jsp</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8938</Reference>
<Reference>cve,2003-0624</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2400" source="Snort" sourceid="2400" type="" version="4">
<LogString>WEB-MISC edittag.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/edittag.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6675</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2407" source="Snort" sourceid="2407" type="" version="4">
<LogString>WEB-MISC util.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/util.pl</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9748</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2408" source="Snort" sourceid="2408" type="" version="4">
<LogString>WEB-MISC Invision Power Board search.pl access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/search.pl</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">st=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9766</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2411" source="Snort" sourceid="2411" type="" version="10">
<LogString>
WEB-MISC Real Server DESCRIBE buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">DESCRIBE</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^DESCRIBE\s[^\n]{300}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8476</Reference>
<Reference>cve,2003-0725</Reference>
<Reference>nessus,11642</Reference>
<Reference>
url,www.service.real.com/help/faq/security/rootexploit091103.html
</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2441" source="Snort" sourceid="2441" type="" version="7">
<LogString>WEB-MISC NetObserve authentication bypass attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">login=0</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Cookie|3A|</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="PCRE">^Cookie\x3a(\s*|\s*\r?\n\s+)[^\n]*?login=0</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9319</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2442" source="Snort" sourceid="2442" type="" version="10">
<LogString>
WEB-MISC Quicktime User-Agent buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">User-Agent|3A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^User-Agent\x3a[^\n]{244,255}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9735</Reference>
<Reference>cve,2004-0169</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2484" source="Snort" sourceid="2484" type="" version="4">
<LogString>WEB-MISC source.jsp access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/source.jsp</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,12119</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2447" source="Snort" sourceid="2447" type="" version="7">
<LogString>WEB-MISC ServletManager access</LogString>

<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/servlet/ServletManager</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3697</Reference>
<Reference>cve,2001-1195</Reference>
<Reference>nessus,12122</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2448" source="Snort" sourceid="2448" type="" version="6">
<LogString>WEB-MISC setinfo.hts access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/setinfo.hts</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9973</Reference>
<Reference>cve,2004-1857</Reference>
<Reference>nessus,12120</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2562" source="Snort" sourceid="2562" type="" version="5">
<LogString>WEB-MISC McAfee ePO file upload attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">/spipe/repl_file</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">Command=BEGIN</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10200</Reference>
<Reference>cve,2004-0038</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2569" source="Snort" sourceid="2569" type="" version="5">
<LogString>WEB-MISC cPanel resetpass access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/resetpass</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,9848</Reference>
<Reference>cve,2004-1769</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2570" source="Snort" sourceid="2570" type="" version="11">
<LogString>WEB-MISC Invalid HTTP Version String</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">HTTP/</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^\w+\s+[^\x0D\x0A\s]+\s+HTTP\x2F[^\x0A]{5}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9809</Reference>
<Reference>nessus,11593</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2581" source="Snort" sourceid="2581" type="" version="5">
<LogString>
WEB-MISC Crystal Reports crystalimagehandler.aspx access
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/crystalimagehandler.aspx</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2004-0204</Reference>
<Reference>
url,www.microsoft.com/security/bulletins/200406_crystal.mspx
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2582" source="Snort" sourceid="2582" type="" version="9">
<LogString>
WEB-MISC Crystal Reports crystalImageHandler.aspx directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/crystalimagehandler.aspx</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">dynamicimage=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10260</Reference>

<Reference>cve,2004-0204</Reference>
<Reference>nessus,12271</Reference>
<Reference>
url,www.microsoft.com/technet/security/bulletin/ms04-017.mspx
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2597" source="Snort" sourceid="2597" type="" version="10">
<LogString>WEB-MISC Samba SWAT Authorization overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Authorization|3A| Basic</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="PCRE">^Authorization\x3a(\s*|\s*\r?\n\s+)Basic\s+=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10780</Reference>
<Reference>cve,2004-0600</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2598" source="Snort" sourceid="2598" type="" version="8">
<LogString>
WEB-MISC Samba SWAT Authorization port 901 overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">Authorization|3A| Basic</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^Authorization\x3a(\s*|\s*\r?\n\s+)Basic\s+=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10780</Reference>
<Reference>cve,2004-0600</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2672" source="Snort" sourceid="2672" type="" version="4">
<LogString>WEB-MISC sresult.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/sresult.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10837</Reference>

<Reference>nessus,14186</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2701" source="Snort" sourceid="2701" type="" version="6">
<LogString>WEB-MISC Oracle iSQLPlus sid overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/isqlplus</Match>
</Pattern>
<Pattern>
<Match type="PCRE">sid=[^&\x3b\r\n]{255}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10871</Reference>
<Reference>url,www.nextgenss.com/advisories/ora-isqlplus.txt</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2702" source="Snort" sourceid="2702" type="" version="6">
<LogString>WEB-MISC Oracle iSQLPlus username overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/isqlplus</Match>
</Pattern>
<Pattern>
<Match type="PCRE">username=[^&\x3b\r\n]{255}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10871</Reference>
<Reference>url,www.nextgenss.com/advisories/ora-isqlplus.txt</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2703" source="Snort" sourceid="2703" type="" version="6">
<LogString>
WEB-MISC Oracle iSQLPlus login.uix username overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/login.uix</Match>
</Pattern>
<Pattern>
<Match type="PCRE">username=[^&\x3b\r\n]{250}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10871</Reference>
<Reference>url,www.nextgenss.com/advisories/ora-isqlplus.txt</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="2704" source="Snort" sourceid="2704" type="" version="7">
<LogString>
WEB-MISC Oracle 10g iSQLPlus login.unix connectID overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/login.uix</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">connectID=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">connectID=[^&\x3b\r\n]{255}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10871</Reference>
<Reference>url,www.nextgenss.com/advisories/ora-isqlplus.txt</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3086" source="Snort" sourceid="3086" type="" version="4">
<LogString>
WEB-MISC 3Com 3CRADSL72 ADSL 11g Wireless Router app_sta.stm access attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/app_sta.stm</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,11408</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3467" source="Snort" sourceid="3467" type="" version="4">
<LogString>WEB-MISC CISCO VoIP Portinformation access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/PortInformation</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4798</Reference>
<Reference>cve,2002-0882</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3466" source="Snort" sourceid="3466" type="" version="11">

<LogString>WEB-MISC Authorization Basic overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Authorization|3A|</Match>
</Pattern>
<Pattern>
<Location area="HTTP_HEADER"/>
<Match type="LITERAL">Basic</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="PCRE">
^Authorization\x3a(\s*|\s*\r?\n\s+)Basic\s[^\n]{250}
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8375</Reference>
<Reference>cve,2003-0727</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3518" source="Snort" sourceid="3518" type="" version="5">
<LogString>
WEB-MISC MySQL MaxDB WebSQL wppassword buffer overflow
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">websql?logon</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">wqPassword=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">wqPassword=[^\r\n\x26]{294}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12265</Reference>
<Reference>cve,2005-0111</Reference>
<Reference>url,www.osvdb.org/displayvuln.php?osvdb_id=12919</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3546" source="Snort" sourceid="3546" type="" version="4">
<LogString>
WEB-MISC TrackerCam User-Agent buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">User-Agent|3A|</Match>
</Pattern>

<Pattern>
<Match type="PCRE">^User-Agent\x3a[^\n]{216}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12592</Reference>
<Reference>cve,2005-0481</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3544" source="Snort" sourceid="3544" type="" version="6">
<LogString>
WEB-MISC TrackerCam ComGetLogFile.php3 directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">/ComGetLogFile.php3</Match>
</Pattern>
<Pattern>
<Match type="PCRE">fn=\x2e\x2e(\x2f|\x5c)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12592</Reference>
<Reference>cve,2005-0481</Reference>
<Reference>nessus,17160</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3547" source="Snort" sourceid="3547" type="" version="4">
<LogString>
WEB-MISC TrackerCam overly long php parameter overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">php.*\x3f[^\n]{256}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12592</Reference>
<Reference>cve,2005-0481</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3545" source="Snort" sourceid="3545" type="" version="6">
<LogString>
WEB-MISC TrackerCam ComGetLogFile.php3 log information disclosure
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">/ComGetLogFile.php3</Match>

</Pattern>
<Pattern>
<Match type="PCRE">fn=Eye\d{4}_\d{2}.log</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12592</Reference>
<Reference>cve,2005-0481</Reference>
<Reference>nessus,17160</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3548" source="Snort" sourceid="3548" type="" version="5">
<LogString>
WEB-MISC TrackerCam negative Content-Length attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">Content-Length|3A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^Content-Length\x3a(\s*|\s*\r?\n\s+)-\d+</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12592</Reference>
<Reference>cve,2005-0481</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3629" source="Snort" sourceid="3629" type="" version="5">
<LogString>WEB-MISC sambar /search/results.stm access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">POST</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">/search/results.stm</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7975</Reference>
<Reference>bugtraq,9607</Reference>
<Reference>cve,2004-2086</Reference>
<Reference>nessus,18650</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3676" source="Snort" sourceid="3676" type="" version="6">
<LogString>WEB-MISC newsscript.pl admin attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/newsscript.pl</Match>

</Pattern>
<Pattern>
<Match type="LITERAL">mode=admin</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12761</Reference>
<Reference>cve,2005-0735</Reference>
<Reference>nessus,17309</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3694" source="Snort" sourceid="3694" type="" version="5">
<LogString>
WEB-MISC Squid content length cache poisoning attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Content-Length|3A|</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Content-Length|3A|</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="PCRE">
Content-Length\x3a(?!\x0d\x0a\x0d\x0a).*?Content-Length\x3a
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12412</Reference>
<Reference>cve,2005-0174</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3693" source="Snort" sourceid="3693" type="" version="4">
<LogString>
WEB-MISC IBM WebSphere j_security_check overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">POST</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">/admin/j_security_check</Match>
</Pattern>
<Pattern>
<Match type="PCRE">j_(username|password)=[^\n|^&]{256,}</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,13853</Reference>
<Reference>cve,2005-1872</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="3816" source="Snort" sourceid="3816" type="" version="9">
<LogString>WEB-MISC BadBlue ext.dll buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">ext.dll</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">mfcisapicommand=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">mfcisapicommand=[^&\r\n\x3b]{250}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,12673</Reference>
<Reference>cve,2005-0595</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="4650" source="Snort" sourceid="4650" type="" version="4">
<LogString>WEB-MISC cacti graph_image.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cacti/graph_image.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14042</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="4681" source="Snort" sourceid="4681" type="" version="4">
<LogString>
WEB-MISC Symantec admin interface client negative Content-Length attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">Content-Length|3A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
^Content-Length\x3a(\s*|\s*\r?\n\s+)(-1|4294967295)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,15001</Reference>

<Reference>cve,2005-2758</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="4987" source="Snort" sourceid="4987" type="" version="3">
<LogString>
WEB-MISC Twiki viewfile rev command injection attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/viewfile/</Match>
</Pattern>
<Pattern>
<Match type="PCRE">viewfile/[^\n]*rev[1|2]*=[^d\x20]+</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14834</Reference>
<Reference>cve,2005-2877</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="4988" source="Snort" sourceid="4988" type="" version="3">
<LogString>
WEB-MISC Barracuda IMG.PL directory traversal attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/img.pl</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">img.pl\x3f[^\r\n]*f=[^\x26\r\n\x2e]*\x2e\x2e</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14712</Reference>
<Reference>cve,2005-2847</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="4985" source="Snort" sourceid="4985" type="" version="3">
<LogString>WEB-MISC Twiki rdiff rev command injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/rdiff/</Match>
</Pattern>
<Pattern>
<Match type="PCRE">rdiff[^\n]*rev[1|2]*=[^d\x20]+</Match>
</Pattern>
</RequestPatterns>

</PatternList>
<Reference>bugtraq,14834</Reference>
<Reference>cve,2005-2877</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="4986" source="Snort" sourceid="4986" type="" version="3">
<LogString>WEB-MISC Twiki view rev command injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/view/</Match>
</Pattern>
<Pattern>
<Match type="PCRE">view/[^\n]*rev[1|2]*=[^d\x20]+</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14834</Reference>
<Reference>cve,2005-2877</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="5715" source="Snort" sourceid="5715" type="" version="4">
<LogString>WEB-MISC malformed ipv6 uri overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">|3A|/[</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
\x3a\x2f\x5b\s*([\x2F\x3F\x23]*)|([\x2F\x3F\x23]+.+)|(\x3a[^\x3a^\x5d]*)$
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,11187</Reference>
<Reference>cve,2004-0786</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="5997" source="Snort" sourceid="5997" type="" version="4">
<LogString>
WEB-MISC WinProxy overly long host header buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Host|3A|</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>

<Match type="PCRE">^Host\x3A\s+[A-Z\d\x5F\x2E\x2E]*\x3A[^\r\n]{100,}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,16147</Reference>
<Reference>cve,2005-4085</Reference>
<Reference>
url,www.bluecoat.com/support/knowledge/advisory_host_header_stack_overflow.html
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="6414" source="Snort" sourceid="6414" type="" version="4">
<LogString>
WEB-MISC Novell GroupWise Messenger Accept-Language header buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">Accept-Language</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^Accept-Language\x3A[^\r\n]{17}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,17503</Reference>
<Reference>cve,2006-0992</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="6507" source="Snort" sourceid="6507" type="" version="4">
<LogString>
WEB-MISC novell edirectory imonitor overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/nds</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">\x2fnds[^\r\n]{1000}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,18026</Reference>
<Reference>cve,2006-2496</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="6511" source="Snort" sourceid="6511" type="" version="3">
<LogString>
WEB-MISC ALT-N WebAdmin user param overflow attempt
</LogString>
<PatternList>

<RequestPatterns>
<Pattern>
<Match type="LITERAL">POST</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">/WebAdmin.dll?</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">View=Logon</Match>
</Pattern>
<Pattern>
<Location area="HTTP_POST_BODY"/>
<Match type="PCRE">[^\r\n\x26]*User=[^\r\n\x26]{100}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8024</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="7071" source="Snort" sourceid="7071" type="" version="4">
<LogString>
WEB-MISC encoded cross site scripting HTML Image tag set to javascript attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">img src=javascript</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4858</Reference>
<Reference>cve,2002-0902</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="7070" source="Snort" sourceid="7070" type="" version="7">
<LogString>WEB-MISC encoded cross site scripting attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL"><SCRIPT</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2009-1140</Reference>
<Reference>
url,www.microsoft.com/technet/security/bulletin/MS09-019.mspx
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8087" source="Snort" sourceid="8087" type="" version="7">
<LogString>
WEB-MISC HP Openview NNM freeIPaddrs.ovpl port 3443 Unix command execution attempt

</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/freeIPaddrs.ovpl</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">netid=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
freeIPaddrs.ovpl[^\r\n]*netid=[^\r\n]*%(\x2c|\x24|\x7c|\x3b|\x22|\x26|\x3c|\x3f)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14662</Reference>
<Reference>cve,2005-2773</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8089" source="Snort" sourceid="8089"
type="" version="7">
<LogString>
WEB-MISC HP Openview NNM cdpView.ovpl Unix command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cdpView.ovpl</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">cdpnode=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
cdpView.ovpl[^\r\n]*cdpnode=[^\r\n]*(\x2c|\x24|\x7c|\x3b|\x22|\x26|\x3c|\x3f)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14662</Reference>
<Reference>cve,2005-2773</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8085" source="Snort" sourceid="8085"
type="" version="6">
<LogString>
WEB-MISC HP Openview NNM connectedNodes.ovpl port 3443 Unix command execution attempt
</LogString>
<PatternList>

<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/connectedNodes.ovpl</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">node=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
connectedNodes.ovpl[^\r\n]*node=[^\r\n]*(\x2c|\x24|\x7c|\x3b|\x22|\x26|\x3c|\x3f)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14662</Reference>
<Reference>cve,2005-2773</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8086" source="Snort" sourceid="8086"
type="" version="7">
<LogString>
WEB-MISC HP Openview NNM cdpView.ovpl port 3443 Unix command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/cdpView.ovpl</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">cdpnode=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
cdpView.ovpl[^\r\n]*cdpnode=[^\r\n]*%(\x2c|\x24|\x7c|\x3b|\x22|\x26|\x3c|\x3f)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14662</Reference>
<Reference>cve,2005-2773</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8441" source="Snort" sourceid="8441"
type="" version="6">
<LogString>WEB-MISC McAfee header buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">AgentGuid=</Match>
</Pattern>

<Pattern>
<Match type="PCRE">^[^\x3e\x3f\x26]{63}</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">Source=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^[^\x3e\x3f\x26]{50}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,20288</Reference>
<Reference>cve,2006-5156</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8444" source="Snort" sourceid="8444" type="" version="2">
<LogString>
WEB-MISC Trend Micro atxconsole format string server response attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">-99 Cannot+find+</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,20284</Reference>
<Reference>cve,2006-5157</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8711" source="Snort" sourceid="8711" type="" version="5">
<LogString>
WEB-MISC Novell eDirectory HTTP redirection buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">Host|3A|</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">!"|0A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
^(GET|POST)\s+[^\s]*(\x2fnds|\x2fdhost)[^\n]*\nHost\x3a\s*[^\n]{63}
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,20655</Reference>
<Reference>cve,2006-5478</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="8701" source="Snort" sourceid="8701" type="" version="2">
<LogString>WEB-MISC IceCast header buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">HTTP/1.</Match>
</Pattern>
<Pattern>
<Match type="PCRE">HTTP\/1\.[01].*?\n([^\r\n]+?\r?\n){32}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,11271</Reference>
<Reference>cve,2004-1561</Reference>
<Reference>
url,archives.neohapsis.com/archives/bugtraq/2004-09/0366.html
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="9620" source="Snort" sourceid="9620" type="" version="4">
<LogString>WEB-MISC pajax call_dispatcher remote exec attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">pajax_call_dispatcher.php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
\x22method\x22\s*\x3a\s*\x22[^\x22]*\x3b\s*system\s*\x28
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,17519</Reference>
<Reference>cve,2006-1551</Reference>
<Reference>
url,www.redteam-pentesting.de/advisories/rt-sa-2006-001.php
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="9791" source="Snort" sourceid="9791" type="" version="3">
<LogString>WEB-MISC .cmd? access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">.cmd?</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4335</Reference>

<Reference>cve,2002-0061</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="10172" source="Snort"
sourceid="10172" type="" version="4">
<LogString>WEB-MISC uTorrent announce buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">d8|3A|announce</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^(\d{5,}|390[1-9]|39[1-9][0-9]|[4-9][0-9]{3})\x3A</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,22530</Reference>
<Reference>cve,2007-0927</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="10195" source="Snort"
sourceid="10195" type="" version="8">
<LogString>WEB-MISC Content-Length buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Content-Length|3A|</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="PCRE">^Content-Length\x3A\s*[^\r\n]{100}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2007-1260</Reference>
<Reference>url,djeyl.net/w.php</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="10990" source="Snort"
sourceid="10990" type="" version="3">
<LogString>
WEB-MISC encoded cross site scripting HTML Image tag attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">ONERROR=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,5847</Reference>
<Reference>cve,2002-0840</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11223" source="Snort"
sourceid="11223" type="" version="6">

<LogString>
WEB-MISC google proxystylesheet arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">proxystylesheet</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/search</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">proxystylesheet=[-a-z0-9_\.]*[^-a-z0-9_\.&\s]</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,15509</Reference>
<Reference>cve,2005-3757</Reference>
<Reference>
url,metasploit.com/research/vulns/google_proxystylesheet/
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11193" source="Snort"
sourceid="11193" type="" version="5">
<LogString>
WEB-MISC Oracle iSQL Plus cross site scripting attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/isqlplus</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">action=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">action(=|\x3f)[^(\n|&)]*\x3c[^(\n|&)]+\x3e</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9484</Reference>
<Reference>cve,2004-2115</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11194" source="Snort"
sourceid="11194" type="" version="5">
<LogString>
WEB-MISC Oracle iSQL Plus cross site scripting attempt
</LogString>

<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/isqlplus</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">username=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">username(=|\x3f)[^(\n|&)]*\x3c[^(\n|&)]+\x3e</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9484</Reference>
<Reference>cve,2004-2115</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11272" source="Snort"
sourceid="11272" type="" version="2">
<LogString>WEB-MISC Apache newline exploit attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">|0D 0A 0D 0A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">(\x0d\x0a){100}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7254</Reference>
<Reference>cve,2003-0132</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11273" source="Snort"
sourceid="11273" type="" version="4">
<LogString>
WEB-MISC Apache header parsing space saturation denial of service attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">HTTP/1.</Match>
</Pattern>
<Pattern>
<Match type="PCRE">HTTP\/1.[01]\n.*[\x20\t]{200}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2004-0942</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11616" source="Snort"
sourceid="11616" type="" version="8">

<LogString>
WEB-MISC Symantec Sygate Policy Manager SQL injection
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/servlet/Sygate.Servlet.login</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
[^\x26\x20\x0a]*insert[^\x26\x20\x0a]*Login[^\x26\x20\x0a]*Admin
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,16452</Reference>
<Reference>cve,2006-0522</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11685" source="Snort"
sourceid="11685" type="" version="4">
<LogString>
WEB-MISC Oracle iSQL Plus cross site scripting attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/isqlplus</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">password=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">password(=|\x3f)[^(\n|&)]*\x3c[^(\n|&)]+\x3e</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9484</Reference>
<Reference>cve,2004-2115</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11687" source="Snort"
sourceid="11687" type="" version="10">
<LogString>
WEB-MISC Apache SSI error page cross-site scripting
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">host|3A|</Match>
</Pattern>

<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="PCRE">
^Host\x3a[a-z0-9\x20\-\.\x3A\t]*[^a-z0-9\x20\-\.\x3A\t\r\n]
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,32476</Reference>
<Reference>bugtraq,5847</Reference>
<Reference>cve,2002-0840</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11679" source="Snort"
sourceid="11679" type="" version="4">
<LogString>
WEB-MISC Apache mod_rewrite buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">GET</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">ldap|3A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
ldap\x3A\x2F\x2F[^\x0A]*(%3f|\x3F)[^\x0A]*(%3f|\x3F)[^\x0A]*(%3f|\x3F)[^\x0A]*(%3f|\x3F)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2006-3747</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11834" source="Snort"
sourceid="11834" type="" version="8">
<LogString>
WEB-MISC Internet Explorer navcancl.htm url spoofing attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">ieframe.dll/navcancl.htm|23|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,22966</Reference>
<Reference>cve,2007-1499</Reference>
<Reference>
url,www.microsoft.com/technet/security/bulletin/MS07-033.mspx
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="11838" source="Snort"
sourceid="11838" type="" version="4">

<LogString>WEB-MISC Win32 API res buffer overflow attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">res|3A|//</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
\x2Edll[\x2F\x5C][^\x3E\x00\s\x2F\x5C]*[\x2F\x5C](\x23|%23)(\d{6}|[7-9]\d{4}|6[6-9]\d{3}|65[6-9]\d{2}|655[4-
9]\d|6553[6-9])
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2007-2219</Reference>
<Reference>
url,www.microsoft.com/technet/security/bulletin/MS07-035.mspx
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="12014" source="Snort"
sourceid="12014" type="" version="5">
<LogString>
WEB-MISC Internet Explorer navcancl.htm url spoofing attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">about|3A|cancel|23|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,22966</Reference>
<Reference>cve,2007-1499</Reference>
<Reference>
url,www.microsoft.com/technet/security/bulletin/MS07-033.mspx
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="12629" source="Snort"
sourceid="12629" type="" version="4">
<LogString>WEB-MISC sharepoint cross site scripting attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/sharepoint/</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">sharepoint[^\n]*\x22\s*\x29\s*\x3b</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,23832</Reference>
<Reference>cve,2007-2581</Reference>

<Reference>
url,www.microsoft.com/technet/security/bulletin/ms07-059.mspx
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="12711" source="Snort"
sourceid="12711" type="" version="3">
<LogString>
WEB-MISC Apache Tomcat WebDAV system tag remote file disclosure attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL"><!ENTITY RemoteX SYSTEM</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,26070</Reference>
<Reference>cve,2007-5461</Reference>
<Reference>url,issues.apache.org/jira/browse/GERONIMO-3549</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="13819" source="Snort"
sourceid="13819" type="" version="4">
<LogString>
WEB-MISC IBM Lotus Domino Web Server Accept-Language header buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">Accept-Language|3A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^Accept-Language\x3A[^\n]{100}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,29310</Reference>
<Reference>cve,2008-2240</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="14771" source="Snort"
sourceid="14771" type="" version="2">
<LogString>
WEB-MISC BEA WebLogic Apache Oracle connector Transfer-Encoding buffer overflow
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">POST</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">Transfer-Encoding|3A|</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^Transfer-Encoding\x3A\s*[^\r\n]{256}</Match>
</Pattern>

</RequestPatterns>
</PatternList>
<Reference>cve,2008-4008</Reference>
<Reference>
url,support.bea.com/application_content/product_portlets/securityadvisories/2806.html
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="15897" source="Snort"
sourceid="15897" type="" version="2">
<LogString>
WEB-MISC SSLv1 Client_Hello Challenge Length overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">|01 00 01|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,11015</Reference>
<Reference>cve,2004-0826</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="15908" source="Snort"
sourceid="15908" type="" version="2">
<LogString>
WEB-MISC Trend Micro OfficeScan multiple CGI modules HTTP form processing buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_METHOD"/>
<Match type="LITERAL">POST</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/officescan/cgi/cgi</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">multipart/form-data</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">|0A|--</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">!"|0A|--</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2008-3862</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="15990" source="Snort"
sourceid="15990" type="" version="2">
<LogString>
WEB-MISC Macromedia JRun 4.x server file disclosure attempt

</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">.jsp</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">^[^\x3b]*\x3b.*\x2ejsp</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,11245</Reference>
<Reference>cve,2004-0928</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="15978" source="Snort"
sourceid="15978" type="" version="2">
<LogString>
WEB-MISC Macromedia JRun 4 mod_jrun buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">.jsp</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">HOST</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^HOST\s*\x3a\s*[^\x0a]{1000}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,11245</Reference>
<Reference>cve,2004-0646</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="15980" source="Snort"
sourceid="15980" type="" version="3">
<LogString>
WEB-MISC Apache mod_ssl hook functions format string attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">https</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
^[a-z]+\s+https\x3a\x2f\x2f[^\x2f\x3a\x25\s]*\x25[sn]
</Match>
</Pattern>

</RequestPatterns>
</PatternList>
<Reference>bugtraq,10736</Reference>
<Reference>cve,2004-0700</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="15982" source="Snort"
sourceid="15982" type="" version="2">
<LogString>
WEB-MISC Ipswitch WhatsUp Gold DOS Device HTTP request denial of service attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">prn</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
^(GET|POST)\s+[^\x0a]*?\x2fprn\x2e(htm|html|asp|cgi)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,11110</Reference>
<Reference>cve,2004-0799</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="16194" source="Snort"
sourceid="16194" type="" version="1">
<LogString>
WEB-MISC Novell eDirectory HTTP request content-length heap buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">POST /SOAP</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^Content-Length\s*\x3A\s*[1-9][0-9]{8}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2008-4478</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="16195" source="Snort"
sourceid="16195" type="" version="2">
<LogString>
WEB-MISC Novell eDirectory HTTP request content-length heap buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">POST /SOAP</Match>
</Pattern>
<Pattern>

<Match type="PCRE">^Content-Length\s*\x3A\s*</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">-</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2008-4478</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="16283" source="Snort" sourceid="16283" type="" version="1">
<LogString>
WEB-MISC Borland StarTeam Multicast Service buffer overflow attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">GET AAAAAAAAAAAAAAAAAAAA</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,28602</Reference>
<Reference>cve,2008-0311</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-misc" enabled="OFF" id="16611" source="Snort" sourceid="16611" type="" version="1">
<LogString>
WEB-MISC Apache 413 error HTTP request method cross-site scripting attack
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL"><PROCHECKUP></Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,26663</Reference>
<Reference>cve,2007-6203</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1423" source="Snort" sourceid="1423" type="" version="20">
<LogString>WEB-PHP content-disposition memchr overflow</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Content-Disposition|3A|</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">name=|22 CC CC CC CC CC|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4183</Reference>

<Reference>cve,2002-0081</Reference>
<Reference>nessus,10867</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1425" source="Snort" sourceid="1425" type="" version="18">
<LogString>WEB-PHP content-disposition file upload attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Content-Disposition|3A|</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">form-data|3B|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4183</Reference>
<Reference>cve,2002-0081</Reference>
<Reference>nessus,10867</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1737" source="Snort" sourceid="1737" type="" version="10">
<LogString>
WEB-PHP squirrel mail theme arbitrary command attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/left_main.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">cmdd=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4385</Reference>
<Reference>cve,2002-0516</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1739" source="Snort" sourceid="1739" type="" version="10">
<LogString>
WEB-PHP DNSTools administrator authentication bypass attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dnstools.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">user_logged_in=true</Match>
</Pattern>

<Pattern type="fastmatch">
<Match type="LITERAL">user_dnstools_administrator=true</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4617</Reference>
<Reference>cve,2002-0613</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1815" source="Snort" sourceid="1815" type="" version="8">
<LogString>WEB-PHP directory.php arbitrary command attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/directory.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">dir=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">|3B|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4278</Reference>
<Reference>cve,2002-0434</Reference>
<Reference>nessus,11017</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1816" source="Snort" sourceid="1816" type="" version="6">
<LogString>WEB-PHP directory.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/directory.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4278</Reference>
<Reference>cve,2002-0434</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1968" source="Snort" sourceid="1968" type="" version="4">
<LogString>WEB-PHP phpbb quick-reply.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/quick-reply.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>bugtraq,6173</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1997" source="Snort" sourceid="1997" type="" version="7">
<LogString>WEB-PHP read_body.php access attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/read_body.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6302</Reference>
<Reference>cve,2002-1341</Reference>
<Reference>nessus,11415</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1998" source="Snort" sourceid="1998" type="" version="7">
<LogString>WEB-PHP calendar.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/calendar.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,5820</Reference>
<Reference>bugtraq,9353</Reference>
<Reference>nessus,11179</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1999" source="Snort" sourceid="1999" type="" version="7">
<LogString>WEB-PHP edit_image.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/edit_image.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3288</Reference>
<Reference>cve,2001-1020</Reference>
<Reference>nessus,11104</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2000" source="Snort" sourceid="2000" type="" version="6">
<LogString>WEB-PHP readmsg.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>

<Match type="LITERAL">/readmsg.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2001-1408</Reference>
<Reference>nessus,11073</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2002" source="Snort" sourceid="2002" type="" version="11">
<LogString>WEB-PHP remote include path</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">path=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">path=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1161" source="Snort" sourceid="1161" type="" version="12">
<LogString>WEB-PHP piranha passwd.php3 access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/passwd.php3</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,272</Reference>
<Reference>bugtraq,1149</Reference>
<Reference>cve,2000-0322</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1407" source="Snort" sourceid="1407" type="" version="11">
<LogString>WEB-PHP smssend.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/smssend.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3982</Reference>
<Reference>cve,2002-0220</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1490" source="Snort" sourceid="1490" type="" version="11">
<LogString>WEB-PHP Phorum /support/common.php attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/support/common.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">ForumLang=../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1997</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1491" source="Snort" sourceid="1491" type="" version="12">
<LogString>WEB-PHP Phorum /support/common.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/support/common.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,1997</Reference>
<Reference>bugtraq,9361</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1137" source="Snort" sourceid="1137" type="" version="12">
<LogString>WEB-PHP Phorum authentication access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Match type="LITERAL">PHP_AUTH_USER=boogieman</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,206</Reference>
<Reference>bugtraq,2274</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1085" source="Snort" sourceid="1085" type="" version="10">
<LogString>WEB-PHP strings overflow</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">|BA|I|FE FF FF F7 D2 B9 BF FF FF FF F7 D1|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,431</Reference>

<Reference>bugtraq,802</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1254" source="Snort" sourceid="1254" type="" version="12">
<LogString>WEB-PHP PHPLIB remote command attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Match type="LITERAL">_PHPLIB[libdir]</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3079</Reference>
<Reference>cve,2001-1370</Reference>
<Reference>nessus,14910</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1255" source="Snort" sourceid="1255" type="" version="11">
<LogString>WEB-PHP PHPLIB remote command attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/db_mysql.inc</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3079</Reference>
<Reference>cve,2001-1370</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2074" source="Snort" sourceid="2074" type="" version="6">
<LogString>
WEB-PHP Mambo uploadimage.php upload php file attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/uploadimage.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">userfile_name=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6572</Reference>
<Reference>cve,2003-1204</Reference>
<Reference>nessus,16315</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2075" source="Snort" sourceid="2075"

type="" version="6">
<LogString>WEB-PHP Mambo upload.php upload php file attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/upload.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">userfile_name=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6572</Reference>
<Reference>cve,2003-1204</Reference>
<Reference>nessus,16315</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2076" source="Snort" sourceid="2076"
type="" version="6">
<LogString>WEB-PHP Mambo uploadimage.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/uploadimage.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6572</Reference>
<Reference>cve,2003-1204</Reference>
<Reference>nessus,16315</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2077" source="Snort" sourceid="2077"
type="" version="6">
<LogString>WEB-PHP Mambo upload.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/upload.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6572</Reference>
<Reference>cve,2003-1204</Reference>
<Reference>nessus,16315</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2078" source="Snort" sourceid="2078"
type="" version="5">
<LogString>WEB-PHP phpBB privmsg.php access</LogString>
<PatternList>

<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/privmsg.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6634</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2140" source="Snort" sourceid="2140" type="" version="4">
<LogString>WEB-PHP p-news.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/p-news.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11669</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2141" source="Snort" sourceid="2141" type="" version="4">
<LogString>WEB-PHP shoutbox.php directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/shoutbox.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">conf=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11668</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2145" source="Snort" sourceid="2145" type="" version="7">
<LogString>
WEB-PHP TextPortal admin.php default password admin attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">op=admin_enter</Match>

```
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">password=admin</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7673</Reference>
<Reference>nessus,11660</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2146" source="Snort" sourceid="2146"
type="" version="7">
<LogString>
WEB-PHP TextPortal admin.php default password 12345 attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">op=admin_enter</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">password=12345</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7673</Reference>
<Reference>nessus,11660</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2147" source="Snort" sourceid="2147"
type="" version="11">
<LogString>
WEB-PHP BLNews objects.inc.php4 remote file include attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/objects.inc.php4</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">Server[path]=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">Server\x5bpath\x5d=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7677</Reference>
<Reference>cve,2003-0394</Reference>
<Reference>nessus,11647</Reference>
</SignatureRule>
```

<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2148" source="Snort" sourceid="2148" type="" version="7">
<LogString>WEB-PHP BLNews objects.inc.php4 access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/objects.inc.php4</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7677</Reference>
<Reference>cve,2003-0394</Reference>
<Reference>nessus,11647</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2151" source="Snort" sourceid="2151" type="" version="7">
<LogString>WEB-PHP ttCMS header.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin/templates/header.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7542</Reference>
<Reference>bugtraq,7543</Reference>
<Reference>bugtraq,7625</Reference>
<Reference>nessus,11636</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2154" source="Snort" sourceid="2154" type="" version="4">
<LogString>WEB-PHP autohtml.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/autohtml.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11630</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2155" source="Snort" sourceid="2155" type="" version="9">
<LogString>WEB-PHP ttforum remote file include attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">forum/index.php</Match>
</Pattern>
<Pattern>

<Match type="LITERAL">template=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">template=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7542</Reference>
<Reference>bugtraq,7543</Reference>
<Reference>nessus,11615</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2227" source="Snort" sourceid="2227" type="" version="5">
<LogString>WEB-PHP forum_details.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">forum_details.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7933</Reference>
<Reference>nessus,11760</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2306" source="Snort" sourceid="2306" type="" version="9">
<LogString>WEB-PHP gallery remote file include attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/setup/</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">GALLERY_BASEDIR=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">GALLERY_BASEDIR=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8814</Reference>
<Reference>nessus,11876</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2307" source="Snort" sourceid="2307" type="" version="11">
<LogString>
WEB-PHP PayPal Storefront remote file include attempt
</LogString>
<PatternList>
<RequestPatterns>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">do=ext</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">page=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">page=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8791</Reference>
<Reference>nessus,11873</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2353" source="Snort" sourceid="2353" type="" version="7">
<LogString>WEB-PHP IdeaBox cord.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/index.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">ideaDir=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">cord.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7488</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2354" source="Snort" sourceid="2354" type="" version="7">
<LogString>WEB-PHP IdeaBox notification.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/index.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">gorumDir=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">notification.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7488</Reference>

```
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2356" source="Snort" sourceid="2356"
type="" version="7">
<LogString>WEB-PHP WebChat db_mysql.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/defines.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">WEBCHATPATH=</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">db_mysql.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7000</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2357" source="Snort" sourceid="2357"
type="" version="7">
<LogString>WEB-PHP WebChat english.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/defines.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">WEBCHATPATH=</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">english.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7000</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2359" source="Snort" sourceid="2359"
type="" version="7">
<LogString>WEB-PHP Invision Board ipchat.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ipchat.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">root_path=</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">conf_global.php</Match>
</Pattern>
```

</RequestPatterns>
</PatternList>
<Reference>bugtraq,6976</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2360" source="Snort" sourceid="2360" type="" version="7">
<LogString>WEB-PHP myphpPagetool pt_config.inc file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/doc/admin</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">ptinclude=</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">pt_config.inc</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6744</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2366" source="Snort" sourceid="2366" type="" version="8">
<LogString>
WEB-PHP PhpGedView PGV authentication_index.php base directory manipulation attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/authentication_index.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">PGV_BASE_DIRECTORY</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9368</Reference>
<Reference>cve,2004-0030</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2367" source="Snort" sourceid="2367" type="" version="8">
<LogString>
WEB-PHP PhpGedView PGV functions.php base directory manipulation attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/functions.php</Match>
</Pattern>
<Pattern type="fastmatch">

<Match type="LITERAL">PGV_BASE_DIRECTORY</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9368</Reference>
<Reference>cve,2004-0030</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2368" source="Snort" sourceid="2368" type="" version="8">
<LogString>
WEB-PHP PhpGedView PGV config_gedcom.php base directory manipulation attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/config_gedcom.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">PGV_BASE_DIRECTORY</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9368</Reference>
<Reference>cve,2004-0030</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2926" source="Snort" sourceid="2926" type="" version="5">
<LogString>WEB-PHP PhpGedView PGV base directory manipulation</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">_conf.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">PGV_BASE_DIRECTORY</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9368</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2398" source="Snort" sourceid="2398" type="" version="5">
<LogString>
WEB-PHP WAnewsletter newsletter.php file include attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">newsletter.php</Match>
</Pattern>
<Pattern type="fastmatch">

<Match type="LITERAL">waroot</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">start.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6965</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2566" source="Snort" sourceid="2566" type="" version="8">
<LogString>WEB-PHP PHPBB viewforum.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/viewforum.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">topic_id=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9865</Reference>
<Reference>bugtraq,9866</Reference>
<Reference>nessus,12093</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2575" source="Snort" sourceid="2575" type="" version="6">
<LogString>
WEB-PHP Opt-X header.php remote file include attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/header.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">systempath=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">systempath=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9732</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2588" source="Snort" sourceid="2588" type="" version="6">
<LogString>WEB-PHP TUTOS path disclosure attempt</LogString>
<PatternList>
<RequestPatterns>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/note_overview.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">id=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,10129</Reference>
<Reference>url,www.securiteam.com/unixfocus/5FP0J15CKE.html</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2654" source="Snort" sourceid="2654" type="" version="6">
<LogString>
WEB-PHP PHPNuke Forum viewtopic SQL insertion attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/modules.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">name=Forums</Match>
</Pattern>
<Pattern type="fastmatch">
<Match type="LITERAL">file=viewtopic</Match>
</Pattern>
<Pattern>
<Match type="PCRE">forum=.*'</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7193</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="8708" source="Snort" sourceid="8708" type="" version="3">
<LogString>
WEB-PHP Wordpress cache_lastpostdate code injection attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">wp_filter</Match>
</Pattern>
<Pattern>
<Match type="PCRE">cache_lastpostdate\[[^\]]+\]=[^\x00\x3B\x3D]{30}</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14533</Reference>
<Reference>cve,2005-2612</Reference>
</SignatureRule>

<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="8713" source="Snort" sourceid="8713" type="" version="4">
<LogString>WEB-PHP cacti graph_image SQL injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">graph_image.php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">rra_id=(?!(\d+|all|)([\x26\s]|$))</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14128</Reference>
<Reference>bugtraq,14129</Reference>
<Reference>cve,2005-2148</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="8716" source="Snort" sourceid="8716" type="" version="4">
<LogString>WEB-PHP cacti graph_image SQL injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">graph.php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">local_graph_id=(?!(\d+|)([\x26\s]|$))</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14128</Reference>
<Reference>bugtraq,14129</Reference>
<Reference>cve,2005-2148</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="8712" source="Snort" sourceid="8712" type="" version="4">
<LogString>
WEB-PHP cacti graph_image arbitrary command execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">graph_image.php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">graph_(start|end|height|width)=(?!(\d+|)[\x26\s])</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14042</Reference>
<Reference>bugtraq,14129</Reference>

<Reference>cve,2005-1524</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="8715" source="Snort" sourceid="8715" type="" version="4">
<LogString>WEB-PHP cacti graph_image SQL injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">graph.php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">rra_id=(?!(\d+|all|)([\x26\s]|$))</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14128</Reference>
<Reference>bugtraq,14129</Reference>
<Reference>cve,2005-2148</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="8714" source="Snort" sourceid="8714" type="" version="4">
<LogString>WEB-PHP cacti graph_image SQL injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">graph_image.php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">local_graph_id=(?!(\d+|)([\x26\s]|$))</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14128</Reference>
<Reference>bugtraq,14129</Reference>
<Reference>cve,2005-2148</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="8734" source="Snort" sourceid="8734" type="" version="3">
<LogString>WEB-PHP Pajax arbitrary command execution attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">method</Match>
</Pattern>
<Pattern>
<Match type="PCRE">\x22method\x22\s*\x3a\s*\x22[A-Z]\w*[^\x22]</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,17519</Reference>
<Reference>cve,2006-1551</Reference>
<Reference>cve,2006-1789</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1967" source="Snort" sourceid="1967" type="" version="5">
<LogString>
WEB-PHP phpbb quick-reply.php arbitrary command attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/quick-reply.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">phpbb_root_path=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6173</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="11668" source="Snort" sourceid="11668" type="" version="4">
<LogString>WEB-PHP vbulletin php code injection</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">misc.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">template\s*=\s*\x7b\x24</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2005-0511</Reference>
<Reference>
url,marc.info/?l=bugtraq&m=110910899415763&w=2
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="12221" source="Snort" sourceid="12221" type="" version="4">
<LogString>
WEB-PHP file upload GLOBAL variable overwrite attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Content-Type|3A| multipart/form-data</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">name=</Match>
</Pattern>
<Pattern>

<Match type="LITERAL">GLOBALS</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,15250</Reference>
<Reference>cve,2005-3390</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="12360" source="Snort"
sourceid="12360" type="" version="4">
<LogString>WEB-PHP PHP function CRLF injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">|0A|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,5681</Reference>
<Reference>cve,2002-1783</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="12610" source="Snort"
sourceid="12610" type="" version="4">
<LogString>
WEB-PHP phpBB viewtopic double URL encoding attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">viewtopic.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">highlight=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">%25</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2004-1315</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2302" source="Snort" sourceid="2302"
type="" version="10">
<LogString>WEB-PHP Advanced Poll poll_ssi.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>

<Match type="LITERAL">/poll_ssi.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2150" source="Snort" sourceid="2150" type="" version="14">
<LogString>
WEB-PHP ttCMS header.php remote file include attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin/templates/header.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">admin_root=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">admin_root=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7542</Reference>
<Reference>bugtraq,7543</Reference>
<Reference>bugtraq,7625</Reference>
<Reference>nessus,11636</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1179" source="Snort" sourceid="1179" type="" version="13">
<LogString>WEB-PHP Phorum violation access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/violation.php3</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,209</Reference>
<Reference>bugtraq,2272</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1301" source="Snort" sourceid="1301" type="" version="17">
<LogString>WEB-PHP admin.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin.php</Match>
</Pattern>

</RequestPatterns>
</PatternList>
<Reference>bugtraq,3361</Reference>
<Reference>bugtraq,7532</Reference>
<Reference>bugtraq,9270</Reference>
<Reference>cve,2001-1032</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2289" source="Snort" sourceid="2289" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_embed.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_embed.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="11666" source="Snort" sourceid="11666" type="" version="7">
<LogString>WEB-PHP sphpblog upload_img_cgi access attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">sphpblog</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">upload_img_cgi.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14667</Reference>
<Reference>cve,2005-2733</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2331" source="Snort" sourceid="2331" type="" version="11">
<LogString>WEB-PHP MatrikzGB privilege escalation attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">new_rights=admin</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8430</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2393" source="Snort" sourceid="2393" type="" version="7">

<LogString>WEB-PHP /_admin access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/_admin/</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9537</Reference>
<Reference>nessus,12032</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1740" source="Snort" sourceid="1740" type="" version="11">
<LogString>WEB-PHP DNSTools authentication bypass attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dnstools.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">user_logged_in=true</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4617</Reference>
<Reference>cve,2002-0613</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2280" source="Snort" sourceid="2280" type="" version="8">
<LogString>WEB-PHP Title.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/Title.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9057</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2292" source="Snort" sourceid="2292" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_logout.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_logout.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>

<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2290" source="Snort" sourceid="2290" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_help.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_help.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2328" source="Snort" sourceid="2328" type="" version="9">
<LogString>WEB-PHP authentication_index.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/authentication_index.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>cve,2004-0032</Reference>
<Reference>nessus,11982</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2304" source="Snort" sourceid="2304" type="" version="8">
<LogString>WEB-PHP files.inc.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/files.inc.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8910</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2341" source="Snort" sourceid="2341" type="" version="9">
<LogString>
WEB-PHP DCP-Portal remote file include editor script attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/library/editor/editor.php</Match>
</Pattern>

<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">root=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6525</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="3827" source="Snort" sourceid="3827" type="" version="7">
<LogString>WEB-PHP xmlrpc.php post attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/xmlrpc.php</Match>
</Pattern>
<Pattern>
<Match type="PCRE">^POST(\s|$)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14088</Reference>
<Reference>cve,2005-1921</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="15432" source="Snort" sourceid="15432" type="" version="5">
<LogString>
WEB-PHP wordpress cat parameter arbitrary file execution attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/wordpress/</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">cat=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../</Match>
</Pattern>
<Pattern>
<Match type="PCRE">
\x2Fwordpress\x2F\x3F[^\r\n]*cat\s*=\s*[^\r\n\x26]*\x2F\x2E\x2E
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,28845</Reference>
<Reference>cve,2008-4769</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2346" source="Snort" sourceid="2346" type="" version="8">

<LogString>WEB-PHP myPHPNuke chatheader.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/chatheader.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6544</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2361" source="Snort" sourceid="2361" type="" version="9">
<LogString>WEB-PHP news.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/news.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">template=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6674</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1399" source="Snort" sourceid="1399" type="" version="18">
<LogString>WEB-PHP PHP-Nuke remote file include attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/index.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">file=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">file=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3889</Reference>
<Reference>cve,2002-0206</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2399" source="Snort" sourceid="2399" type="" version="7">
<LogString>WEB-PHP WAnewsletter db_type.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>

<Match type="LITERAL">/sql/db_type.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6964</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2285" source="Snort" sourceid="2285" type="" version="8">
<LogString>WEB-PHP rolis guestbook access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/insert.inc.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9057</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1743" source="Snort" sourceid="1743" type="" version="11">
<LogString>WEB-PHP Blahz-DNS dostuff.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dostuff.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4618</Reference>
<Reference>cve,2002-0599</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2287" source="Snort" sourceid="2287" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_comment.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_comment.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2296" source="Snort" sourceid="2296" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_stats.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>

<Match type="LITERAL">/admin_stats.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2363" source="Snort" sourceid="2363" type="" version="8">
<LogString>WEB-PHP Cyboards default_header.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/default_header.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6597</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2345" source="Snort" sourceid="2345" type="" version="10">
<LogString>WEB-PHP PhpGedView search.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/search.php</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">action=soundex</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">firstname=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9369</Reference>
<Reference>cve,2004-0032</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1741" source="Snort" sourceid="1741" type="" version="11">
<LogString>WEB-PHP DNSTools access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dnstools.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4617</Reference>

<Reference>cve,2002-0613</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2283" source="Snort" sourceid="2283" type="" version="8">
<LogString>WEB-PHP DatabaseFunctions.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/DatabaseFunctions.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9057</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="11665" source="Snort" sourceid="11665" type="" version="7">
<LogString>WEB-PHP sphpblog install03_cgi access attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">sphpblog</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">install03_cgi.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14667</Reference>
<Reference>cve,2005-2733</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1736" source="Snort" sourceid="1736" type="" version="12">
<LogString>
WEB-PHP squirrel mail spell-check arbitrary command attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/squirrelspell/modules/check_me.mod.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">SQSPELL_APP[</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3952</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2300" source="Snort" sourceid="2300" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_tpl_new.php access</LogString>

<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_tpl_new.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2228" source="Snort" sourceid="2228" type="" version="10">
<LogString>
WEB-PHP phpMyAdmin db_details_importdocsql.php access
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">db_details_importdocsql.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7962</Reference>
<Reference>bugtraq,7965</Reference>
<Reference>nessus,11761</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="15424" source="Snort" sourceid="15424" type="" version="5">
<LogString>WEB-PHP phpBB mod shoutbox sql injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">shoutbox_view.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">mode=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">id=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
shoutbox_view.php\x3F[^\r\n]*mode\s*=\s*(delete|edit)[^\r\n]*id\s*=\s*[^\r\n\x26]*[^\d]+
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,32123</Reference>

<Reference>cve,2008-6301</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2365" source="Snort" sourceid="2365" type="" version="8">
<LogString>WEB-PHP newsPHP Language file include attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/nphpd.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">LangFile</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8488</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2143" source="Snort" sourceid="2143" type="" version="10">
<LogString>
WEB-PHP b2 cafelog gm-2-b2.php remote file include attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/gm-2-b2.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">b2inc=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">b2inc=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11667</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2294" source="Snort" sourceid="2294" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_preview.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_preview.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1178" source="Snort" sourceid="1178"

type="" version="12">
<LogString>WEB-PHP Phorum read access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/read.php3</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,208</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="11667" source="Snort"
sourceid="11667" type="" version="7">
<LogString>WEB-PHP sphpblog arbitrary file delete attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">sphpblog</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">comment_delete_cgi.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">comment=[^\x26\s]*[\x2f\x5c]</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14667</Reference>
<Reference>cve,2005-2733</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2281" source="Snort" sourceid="2281"
type="" version="8">
<LogString>WEB-PHP Setup.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/Setup.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9057</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2295" source="Snort" sourceid="2295"
type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_settings.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>

<Match type="LITERAL">/admin_settings.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2279" source="Snort" sourceid="2279" type="" version="8">
<LogString>WEB-PHP UpdateClasses.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/UpdateClasses.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9057</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1773" source="Snort" sourceid="1773" type="" version="9">
<LogString>WEB-PHP php.exe access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/php.exe</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>
url,www.securitytracker.com/alerts/2002/Jan/1003104.html
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2303" source="Snort" sourceid="2303" type="" version="11">
<LogString>WEB-PHP Advanced Poll popup.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/popup.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">include_path=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="5709" source="Snort" sourceid="5709"

type="" version="7">
<LogString>WEB-PHP file upload directory traversal</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Match type="LITERAL">POST</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">upload.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="PCRE">^Content-Type\x3A\s+multipart\/form-data</Match>
</Pattern>
<Pattern>
<Location area="HTTP_RAW_HEADER"/>
<Match type="LITERAL">Content-Disposition|3A|</Match>
</Pattern>
<Pattern>
<Location area="HTTP_HEADER"/>
<Match type="PCRE">filename=\S*\x2e\x2e\x2f</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">|0A|</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>url,bugs.php.net/bug.php?id=28456</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2293" source="Snort" sourceid="2293"
type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_password.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_password.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2288" source="Snort" sourceid="2288"
type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_edit.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_edit.php</Match>
</Pattern>
</RequestPatterns>

</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2410" source="Snort" sourceid="2410" type="" version="8">
<LogString>
WEB-PHP IGeneric Free Shopping Cart page.php access
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/page.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9773</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2347" source="Snort" sourceid="2347" type="" version="8">
<LogString>WEB-PHP myPHPNuke partner.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/partner.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6544</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1300" source="Snort" sourceid="1300" type="" version="13">
<LogString>WEB-PHP admin.php file upload attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">file_name=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,3361</Reference>
<Reference>cve,2001-1032</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2149" source="Snort" sourceid="2149" type="" version="7">
<LogString>WEB-PHP Turba status.php access</LogString>
<PatternList>
<RequestPatterns>

<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/turba/status.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11646</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1774" source="Snort" sourceid="1774" type="" version="9">
<LogString>WEB-PHP bb_smilies.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/bb_smilies.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>
url,www.securiteam.com/securitynews/Serious_security_hole_in_PHP-Nuke__bb_smilies_.html
</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2226" source="Snort" sourceid="2226" type="" version="14">
<LogString>WEB-PHP pmachine remote file include attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">lib.inc.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">pm_path=</Match>
</Pattern>
<Pattern>
<Match type="PCRE">pm_path=(https?|ftps?|php)</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7919</Reference>
<Reference>nessus,11739</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2152" source="Snort" sourceid="2152" type="" version="7">
<LogString>WEB-PHP test.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/test.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>

<Reference>nessus,11617</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2405" source="Snort" sourceid="2405" type="" version="7">
<LogString>WEB-PHP phptest.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/phptest.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9737</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2291" source="Snort" sourceid="2291" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_license.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_license.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2305" source="Snort" sourceid="2305" type="" version="8">
<LogString>WEB-PHP chatbox.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/chatbox.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8930</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2298" source="Snort" sourceid="2298" type="" version="10">
<LogString>WEB-PHP Advanced Poll admin_templates.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_templates.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>

<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2286" source="Snort" sourceid="2286" type="" version="8">
<LogString>WEB-PHP friends.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/friends.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9088</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1745" source="Snort" sourceid="1745" type="" version="9">
<LogString>WEB-PHP Messagerie supp_membre.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/supp_membre.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4635</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2372" source="Snort" sourceid="2372" type="" version="8">
<LogString>WEB-PHP Photopost PHP Pro showphoto.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/showphoto.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9557</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1134" source="Snort" sourceid="1134" type="" version="13">
<LogString>WEB-PHP Phorum admin access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin.php3</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,205</Reference>
<Reference>bugtraq,2271</Reference>

</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1197" source="Snort" sourceid="1197" type="" version="12">
<LogString>WEB-PHP Phorum code access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/code.php3</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,207</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2565" source="Snort" sourceid="2565" type="" version="7">
<LogString>WEB-PHP modules.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/modules.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9879</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2362" source="Snort" sourceid="2362" type="" version="8">
<LogString>WEB-PHP YaBB SE packages.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/packages.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">packer.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6663</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1834" source="Snort" sourceid="1834" type="" version="11">
<LogString>WEB-PHP PHP-Wiki cross site scripting attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">/modules.php?</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>

<Match type="LITERAL">name=Wiki</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL"><script</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,5254</Reference>
<Reference>cve,2002-1070</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2142" source="Snort" sourceid="2142" type="" version="8">
<LogString>WEB-PHP shoutbox.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/shoutbox.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">conf=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11668</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2299" source="Snort" sourceid="2299" type="" version="10">
<LogString>
WEB-PHP Advanced Poll admin_tpl_misc_new.php access
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_tpl_misc_new.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2284" source="Snort" sourceid="2284" type="" version="9">
<LogString>
WEB-PHP rolis guestbook remote file include attempt
</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/insert.inc.php</Match>

</Pattern>
<Pattern>
<Match type="LITERAL">path=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9057</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2153" source="Snort" sourceid="2153" type="" version="7">
<LogString>WEB-PHP autohtml.php directory traversal attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/autohtml.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">name=</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">../../</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>nessus,11630</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2355" source="Snort" sourceid="2355" type="" version="9">
<LogString>WEB-PHP Invision Board emailer.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/ad_member.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">emailer.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7204</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2144" source="Snort" sourceid="2144" type="" version="7">
<LogString>WEB-PHP b2 cafelog gm-2-b2.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/gm-2-b2.php</Match>
</Pattern>
</RequestPatterns>

</PatternList>
<Reference>nessus,11667</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="15425" source="Snort" sourceid="15425" type="" version="5">
<LogString>WEB-PHP phpBB mod tag board sql injection attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">tag_board.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">action=delete</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">id=</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="PCRE">
tag_board.php\x3F[^\r\n]*action=delete[^\r\n]*id=[^\r\n\x26]*(select|insert|delete)
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,32701</Reference>
<Reference>cve,2008-6314</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2229" source="Snort" sourceid="2229" type="" version="11">
<LogString>WEB-PHP viewtopic.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/viewtopic.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">days=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,7979</Reference>
<Reference>cve,2003-0486</Reference>
<Reference>nessus,11767</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2342" source="Snort" sourceid="2342" type="" version="9">
<LogString>
WEB-PHP DCP-Portal remote file include lib script attempt

</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/library/lib.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">root=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6525</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="11664" source="Snort"
sourceid="11664" type="" version="7">
<LogString>WEB-PHP sphpblog password.txt access attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">sphpblog</Match>
</Pattern>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">password.txt</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,14667</Reference>
<Reference>cve,2005-2733</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1086" source="Snort" sourceid="1086"
type="" version="18">
<LogString>WEB-PHP strings overflow</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">?STRENGUR</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>arachnids,430</Reference>
<Reference>bugtraq,1786</Reference>
<Reference>cve,2000-0967</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2297" source="Snort" sourceid="2297"
type="" version="10">
<LogString>
WEB-PHP Advanced Poll admin_templates_misc.php access
</LogString>
<PatternList>

<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/admin_templates_misc.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2364" source="Snort" sourceid="2364" type="" version="8">
<LogString>WEB-PHP Cyboards options_form.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/options_form.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6597</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2358" source="Snort" sourceid="2358" type="" version="9">
<LogString>WEB-PHP Typo3 translations.php file include</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/translations.php</Match>
</Pattern>
<Pattern>
<Match type="LITERAL">ONLY=</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,6984</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2282" source="Snort" sourceid="2282" type="" version="8">
<LogString>WEB-PHP GlobalFunctions.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/GlobalFunctions.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,9057</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="1742" source="Snort" sourceid="1742" type="" version="11">

<LogString>WEB-PHP Blahz-DNS dostuff.php modify user attempt</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/dostuff.php?action=modify_user</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,4618</Reference>
<Reference>cve,2002-0599</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-php" enabled="OFF" id="2301" source="Snort" sourceid="2301" type="" version="10">
<LogString>WEB-PHP Advanced Poll booth.php access</LogString>
<PatternList>
<RequestPatterns>
<Pattern type="fastmatch">
<Location area="HTTP_URL"/>
<Match type="LITERAL">/booth.php</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<Reference>bugtraq,8890</Reference>
<Reference>nessus,11487</Reference>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="ON" id="3100000" version="1">
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">cgi-bin</Match>
</Pattern>
<Pattern>
<Location area="HTTP_FORM_FIELD">
<URL type="Literal">simple.cgi</URL>
<FieldName type="Literal">text_area</FieldName>
</Location>
<Match maxLength="512" type="Expression">
TEXT.XPATH_JSON(xp%/glossary/title%).CONTAINS("example glossary")
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<LogString>JSON XML Path Language Test</LogString>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="ON" id="3100001" version="1">
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">post_json.php</Match>
</Pattern>
<Pattern>

```
<Location area="HTTP_ANY"/>
<Match maxLength="512" type="Expression">
TEXT.XPATH_JSON(xp%/glossary/title%).CONTAINS("example glossary")
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<LogString>JSON XML Path Language Test</LogString>
</SignatureRule>
<SignatureRule actions="block,log" category="web-cgi" enabled="ON" id="3100002" version="1">
<PatternList>
<RequestPatterns>
<Pattern>
<Location area="HTTP_URL"/>
<Match type="LITERAL">login_post.php</Match>
</Pattern>
<Pattern>
<Location area="HTTP_ANY"/>
<Match maxLength="512" type="Expression">
TEXT.XPATH_JSON(xp%/web-app/servlet/Val/init-
param/dataStoreDriver%).EQ("com.microsoft.jdbc.sqlserver.SQLServerDriver")
</Match>
</Pattern>
</RequestPatterns>
</PatternList>
<LogString>JSON XML Path Language Test</LogString>
</SignatureRule>
</Signatures>
<Patterns>
 <!-- SQL injection parameters -->
 <!--
SQL delimiter is to be specified as an attribute of injection node
-->
<injection delimiter="not_alphanum" type="SQL">
 <!-- SQL keywords -->
<keyword type="LITERAL">select</keyword>
<keyword type="LITERAL">insert</keyword>
<keyword type="LITERAL">delete</keyword>
<keyword type="LITERAL">update</keyword>
<keyword type="LITERAL">drop</keyword>
<keyword type="LITERAL">create</keyword>
<keyword type="LITERAL">alter</keyword>
<keyword type="LITERAL">grant</keyword>
<keyword type="LITERAL">revoke</keyword>
<keyword type="LITERAL">commit</keyword>
<keyword type="LITERAL">rollback</keyword>
<keyword type="LITERAL">shutdown</keyword>
<keyword type="LITERAL">union</keyword>
<keyword type="LITERAL">intersect</keyword>
<keyword type="LITERAL">minus</keyword>
<keyword type="LITERAL">case</keyword>
<keyword type="LITERAL">decode</keyword>
<keyword type="LITERAL">where</keyword>
<keyword type="LITERAL">group</keyword>
```

<keyword type="LITERAL">begin</keyword>
<keyword type="LITERAL">join</keyword>
<keyword type="LITERAL">exists</keyword>
<keyword type="LITERAL">distinct</keyword>
<keyword type="LITERAL">add</keyword>
<keyword type="LITERAL">modify</keyword>
<keyword type="LITERAL">constraint</keyword>
<keyword type="LITERAL">null</keyword>
<keyword type="LITERAL">like</keyword>
<keyword type="LITERAL">exec</keyword>
<keyword type="LITERAL">execute</keyword>
<keyword type="LITERAL">char</keyword>
<keyword type="LITERAL">or</keyword>
<keyword type="LITERAL">and</keyword>
<keyword type="LITERAL">sp_sdidebug</keyword>
<keyword type="LITERAL">xp_availablemedia</keyword>
<keyword type="LITERAL">xp_cmdshell</keyword>
<keyword type="LITERAL">xp_deletemail</keyword>
<keyword type="LITERAL">xp_dirtree</keyword>
<keyword type="LITERAL">xp_dropwebtask</keyword>
<keyword type="LITERAL">xp_dsninfo</keyword>
<keyword type="LITERAL">xp_enumdsn</keyword>
<keyword type="LITERAL">xp_enumerrorlogs</keyword>
<keyword type="LITERAL">xp_enumgroups</keyword>
<keyword type="LITERAL">xp_enumqueuedtasks</keyword>
<keyword type="LITERAL">xp_eventlog</keyword>
<keyword type="LITERAL">xp_findnextmsg</keyword>
<keyword type="LITERAL">xp_fixeddrives</keyword>
<keyword type="LITERAL">xp_getfiledetails</keyword>
<keyword type="LITERAL">xp_getnetname</keyword>
<keyword type="LITERAL">xp_grantlogin</keyword>
<keyword type="LITERAL">xp_logevent</keyword>
<keyword type="LITERAL">xp_loginconfig</keyword>
<keyword type="LITERAL">xp_logininfo</keyword>
<keyword type="LITERAL">xp_makewebtask</keyword>
<keyword type="LITERAL">xp_msver</keyword>
<keyword type="LITERAL">xp_regread</keyword>
<keyword type="LITERAL">xp_perfend</keyword>
<keyword type="LITERAL">xp_perfmonitor</keyword>
<keyword type="LITERAL">xp_perfsample</keyword>
<keyword type="LITERAL">xp_perfstart</keyword>
<keyword type="LITERAL">xp_readerrorlog</keyword>
<keyword type="LITERAL">xp_readmail</keyword>
<keyword type="LITERAL">xp_revokelogin</keyword>
<keyword type="LITERAL">xp_runwebtask</keyword>
<keyword type="LITERAL">xp_schedulersignal</keyword>
<keyword type="LITERAL">xp_sendmail</keyword>
<keyword type="LITERAL">xp_servicecontrol</keyword>
<keyword type="LITERAL">xp_snmp_getstate</keyword>
<keyword type="LITERAL">xp_snmp_raisetrap</keyword>
<keyword type="LITERAL">xp_sprintf</keyword>
<keyword type="LITERAL">xp_sqlinventory</keyword>
<keyword type="LITERAL">xp_sqlregister</keyword>
<keyword type="LITERAL">xp_sqltrace</keyword>

<keyword type="LITERAL">xp_sscanf</keyword>
<keyword type="LITERAL">xp_startmail</keyword>
<keyword type="LITERAL">xp_stopmail</keyword>
<keyword type="LITERAL">xp_subdirs</keyword>
<keyword type="LITERAL">xp_unc_to_drive</keyword>
<keyword type="LITERAL">sysobjects</keyword>
<keyword type="LITERAL">syscolumns</keyword>
<keyword type="LITERAL">MSysACEs</keyword>
<keyword type="LITERAL">MSysObjects</keyword>
<keyword type="LITERAL">MSysQueries</keyword>
<keyword type="LITERAL">MSysRelationships</keyword>
<keyword type="LITERAL">SYS.USER_OBJECTS</keyword>
<keyword type="LITERAL">SYS.TAB</keyword>
<keyword type="LITERAL">SYS.USER_TABLES</keyword>
<keyword type="LITERAL">SYS.USER_VIEWS</keyword>
<keyword type="LITERAL">SYS.ALL_TABLES</keyword>
<keyword type="LITERAL">SYS.USER_TAB_COLUMNS</keyword>
<keyword type="LITERAL">SYS.USER_CONSTRAINTS</keyword>
<keyword type="LITERAL">SYS.USER_TRIGGERS</keyword>
<keyword type="LITERAL">SYS.USER_CATALOG</keyword>
<keyword type="LITERAL">SYS.ALL_CATALOG</keyword>
<keyword type="LITERAL">SYS.ALL_CONSTRAINTS</keyword>
<keyword type="LITERAL">SYS.ALL_OBJECTS</keyword>
<keyword type="LITERAL">SYS.ALL_TAB_COLUMNS</keyword>
<keyword type="LITERAL">SYS.ALL_TAB_PRIVS</keyword>
<keyword type="LITERAL">SYS.ALL_TRIGGERS</keyword>
<keyword type="LITERAL">SYS.ALL_USERS</keyword>
<keyword type="LITERAL">SYS.ALL_VIEWS</keyword>
<keyword type="LITERAL">SYS.USER_ROLE_PRIVS</keyword>
<keyword type="LITERAL">SYS.USER_SYS_PRIVS</keyword>
<keyword type="LITERAL">SYS.USER_TAB_PRIVS</keyword>
<!-- SQL special strings -->
<specialstring type="LITERAL">'</specialstring>
<specialstring type="LITERAL">\</specialstring>
<specialstring type="LITERAL">;</specialstring>
<transformrules>
<!-- SQL transform patterns -->
<!--
Note:
1)This is an ordered match of 'from' patterns
2)Empty tags can be specified to omit matched pattern
-->
<transform>
<from>"</from>
<to>"</to>
</transform>
<transform>
<from>'</from>
<to>"</to>
</transform>
<transform>
<from>\\</from>
<to>\\</to>
</transform>

<transform>
<from>\</from>
<to>\\</to>
</transform>
<transform>
<from>;</from>
<to/>
</transform>
</transformrules>
</injection>
<!-- XSS parameters -->
<xss>
<allowed>
<!-- XSS allowed tags -->
<tag>a</tag>
<tag>address</tag>
<tag>b</tag>
<tag>basefont</tag>
<tag>bgsound</tag>
<tag>big</tag>
<tag>blockquote</tag>
<tag>bq</tag>
<tag>br</tag>
<tag>caption</tag>
<tag>center</tag>
<tag>cite</tag>
<tag>dd</tag>
<tag>del</tag>
<tag>dfn</tag>
<tag>div</tag>
<tag>dl</tag>
<tag>dt</tag>
<tag>em</tag>
<tag>font</tag>
<tag>h1</tag>
<tag>h2</tag>
<tag>h3</tag>
<tag>h4</tag>
<tag>h5</tag>
<tag>h6</tag>
<tag>hr</tag>
<tag>i</tag>
<tag>img</tag>
<tag>kbd</tag>
<tag>li</tag>
<tag>map</tag>
<tag>marquee</tag>
<tag>ol</tag>
<tag>p</tag>
<tag>small</tag>
<tag>strike</tag>
<tag>strong</tag>
<tag>sub</tag>
<tag>sup</tag>

<tag>table</tag>
<tag>td</tag>
<tag>th</tag>
<tag>tr</tag>
<tag>tt</tag>
<tag>u</tag>
<tag>ul</tag>
<!-- XSS allowed attributes -->
<attribute>abbr</attribute>
<attribute>accesskey</attribute>
<attribute>align</attribute>
<attribute>alt</attribute>
<attribute>axis</attribute>
<attribute>bgcolor</attribute>
<attribute>border</attribute>
<attribute>cellpadding</attribute>
<attribute>cellspacing</attribute>
<attribute>char</attribute>
<attribute>charoff</attribute>
<attribute>charset</attribute>
<attribute>cite</attribute>
<attribute>class</attribute>
<attribute>clear</attribute>
<attribute>color</attribute>
<attribute>colspan</attribute>
<attribute>compact</attribute>
<attribute>coords</attribute>
<attribute>dir</attribute>
<attribute>face</attribute>
<attribute>headers</attribute>
<attribute>height</attribute>
<attribute>href</attribute>
<attribute>hreflang</attribute>
<attribute>hspace</attribute>
<attribute>id</attribute>
<attribute>ismap</attribute>
<attribute>lang</attribute>
<attribute>longdesc</attribute>
<attribute>name</attribute>
<attribute>noshade</attribute>
<attribute>nowrap</attribute>
<attribute>rel</attribute>
<attribute>rev</attribute>
<attribute>rowspan</attribute>
<attribute>rules</attribute>
<attribute>scope</attribute>
<attribute>shape</attribute>
<attribute>size</attribute>
<attribute>src</attribute>
<attribute>start</attribute>
<attribute>summary</attribute>
<attribute>tabindex</attribute>
<attribute>target</attribute>
<attribute>title</attribute>

<attribute>type</attribute>
<attribute>usemap</attribute>
<attribute>valign</attribute>
<attribute>value</attribute>
<attribute>vspace</attribute>
<attribute>width</attribute>
</allowed>
<!-- XSS denied patterns -->
<denied>
<!-- HTML 4.0 -->
<pattern>\bonblur\b</pattern>
<pattern>\bonchange\b</pattern>
<pattern>\bonclick\b</pattern>
<pattern>\bondblclick\b</pattern>
<pattern>\bonfocus\b</pattern>
<pattern>\bonkeydown\b</pattern>
<pattern>\bonkeypress\b</pattern>
<pattern>\bonkeyup\b</pattern>
<pattern>\bonload\b</pattern>
<pattern>\bonmousedown\b</pattern>
<pattern>\bonmousemove\b</pattern>
<pattern>\bonmouseout\b</pattern>
<pattern>\bonmouseover\b</pattern>
<pattern>\bonmouseup\b</pattern>
<pattern>\bonreset\b</pattern>
<pattern>\bonselect\b</pattern>
<pattern>\bonsubmit\b</pattern>
<pattern>\bonunload\b</pattern>
<pattern>\bjavascript:</pattern>
<pattern>&\{.+};</pattern>
<!-- HTML 5.0 -->
<pattern>\bonabort\b</pattern>
<pattern>\bonafterprint\b</pattern>
<pattern>\bonbeforeprint\b</pattern>
<pattern>\bonbeforeunload\b</pattern>
<pattern>\boncanplay\b</pattern>
<pattern>\boncanplaythrough\b</pattern>
<pattern>\boncontextmenu\b</pattern>
<pattern>\bondrag\b</pattern>
<pattern>\bondragend\b</pattern>
<pattern>\bondragenter\b</pattern>
<pattern>\bondragleave\b</pattern>
<pattern>\bondragover\b</pattern>
<pattern>\bondragstart\b</pattern>
<pattern>\bondrop\b</pattern>
<pattern>\bondurationchange\b</pattern>
<pattern>\bonemptied\b</pattern>
<pattern>\bonended\b</pattern>
<pattern>\bonerror\b</pattern>
<pattern>\bonformchange\b</pattern>
<pattern>\bonforminput\b</pattern>
<pattern>\bonhashchange\b</pattern>
<pattern>\boninput\b</pattern>
<pattern>\boninvalid\b</pattern>

<pattern>\bonloadeddata\b</pattern>
<pattern>\bonloadedmetadata\b</pattern>
<pattern>\bonloadstart\b</pattern>
<pattern>\bonmessage\b</pattern>
<pattern>\bonmousewheel\b</pattern>
<pattern>\bonoffline\b</pattern>
<pattern>\bononline\b</pattern>
<pattern>\bonpagehide\b</pattern>
<pattern>\bonpageshow\b</pattern>
<pattern>\bonpause\b</pattern>
<pattern>\bonplay\b</pattern>
<pattern>\bonplaying\b</pattern>
<pattern>\bonpopstate\b</pattern>
<pattern>\bonprogress\b</pattern>
<pattern>\bonratechange\b</pattern>
<pattern>\bonreadystatechange\b</pattern>
<pattern>\bonredo\b</pattern>
<pattern>\bonresize\b</pattern>
<pattern>\bonscroll\b</pattern>
<pattern>\bonseeked\b</pattern>
<pattern>\bonseeking\b</pattern>
<pattern>\bonshow\b</pattern>
<pattern>\bonstalled\b</pattern>
<pattern>\bonstorage\b</pattern>
<pattern>\bonsuspend\b</pattern>
<pattern>\bontimeupdate\b</pattern>
<pattern>\bonundo\b</pattern>
<pattern>\bonvolumechange\b</pattern>
<pattern>\bonwaiting\b</pattern>
</denied>
</xss>
</Patterns>
</SignaturesFile>