<vulnerabilities>
<host host-name="was-demo.trendmicro.com">
<vulnerability vuln-type="weak-password" id="2" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="direct-access-to-resources-circumventing-authentication" id="1" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="privilege-escalation" id="2" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>

<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="integer-overflows" id="3" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sensitive-form-data-transmitted-without-ssl" id="4" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="insecure-transition-from-https-to-http-in-form-post" id="5" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>

<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="site-uses-https-but-has-references-to-http-resources" id="6" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="asp-net-view-state-mac-not-enabled" id="236" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name/>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>

</vulnerability>
<vulnerability vuln-type="weak-ssl-cipher-support" id="7" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="older-version-of-ssl-supported" id="8" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="invalid-tlsssl-certificate" id="9" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>

GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="untrusted-tlsssl-certificate" id="10" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="tlsssl-certificate-expired" id="11" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="tlsssl-certificate-expires-soon" id="12" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234

</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="exposure-to-beast-attack" id="13" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="remote-file-inclusion" id="14" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="format-string" id="15" severity="high">

<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="buffer-overflow" id="16" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-scripting" id="17" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET

CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-scripting" id="18" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-scripting" id="19" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-scripting" id="20" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>

</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-scripting" id="21" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-scripting" id="22" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-scripting" id="23" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>

<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cross-site-request-forgery" id="24" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="denial-of-service" id="25" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close

</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="lack-of-account-lockout" id="26" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="password-guessinguser-name-enumeration-attacks" id="27" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="content-spoofing" id="28" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>

<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="open-cross-domain-policy-for-flash" id="29" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sensitive-information-in-code-comments" id="30" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sensitive-error-messages-leakage" id="31" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>

<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="possible-access-to-backup-files" id="32" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="include-file-source-code-disclosure" id="33" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>

</vulnerability>
<vulnerability vuln-type="embedded-email-address-discovered" id="34" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="internal-ip-address-leaked" id="35" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="iis-webdav-propfind-method-leaks-internal-ip-address" id="36" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>

GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="local-path-disclosure" id="37" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sensitive-information-stored-in-browser-cache" id="38" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sensitive-data-exposed-via-browser-history" id="39" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234

</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sensitive-data-stored-in-aspnet-view-state" id="40" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="login-failure-messages-elevates-brute-force-attack-risks" id="41" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="unencrypted-view-state-in-aspnet-could-leak-sensitive-information" id="42"

severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="autocomplete-enabled-for-sensitive-form-fields" id="43" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="public-access-to-web-servers-htaccess-file" id="44" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0

(compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="http-put-method-enabled" id="45" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="http-delete-method-enabled" id="46" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="unauthorized-http-method-track" id="47" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>

<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="unauthorized-http-method-trace" id="48" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="unauthorized-http-method-webdav" id="49" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="aspnet-debug-feature-enabled" id="50" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-

reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="http-basic-authentication-enabled" id="51" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="password-field-submitted-using-http-get-method" id="52" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-

demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="ssl-cookie-missing-secure-attribute" id="53" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="cookie-missing-httponly-attribute" id="54" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="directory-browsing" id="55" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>

<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="improper-filesystem-permissions" id="56" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sequential-session-token" id="57" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="non-random-session-token" id="58" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>

<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sql-injection" id="59" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sql-injection" id="60" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>

</info>
</vulnerability>
<vulnerability vuln-type="sql-injection" id="61" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="improper-input-handling" id="62" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="input-validation-missing-on-server-side" id="63" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>

<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="malicious-file-upload-risk-to-server" id="64" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="insufficient-anti-automation" id="65" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="improper-output-handling" id="66" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>

http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="xml-injection" id="67" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="http-request-splitting" id="68" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>

<vulnerability vuln-type="http-response-splitting" id="69" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="http-request-smuggling" id="70" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="http-response-smuggling" id="71" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0

(compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="null-byte-injection" id="72" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="ldap-injection" id="73" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="mail-command-injection" id="74" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>

<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="os-commanding" id="75" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="routing-detour" id="76" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="path-traversal" id="77" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-

reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="predictable-resource-location" id="78" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="soap-array-abuse" id="79" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-

demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="ssi-injection" id="80" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="session-fixation" id="81" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="url-redirector-abuse" id="82" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>

<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="sql-injection" id="83" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="insufficient-process-validation" id="84" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="xml-attribute-blowup" id="85" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>

<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="abuse-of-functionality" id="86" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="xml-external-entities" id="87" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>

</info>
</vulnerability>
<vulnerability vuln-type="xml-entity-expansion" id="88" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="website-programming-language-nameversion-disclosure" id="89" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="server-nameversion-disclosure" id="90" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>

<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="xquery-injection" id="91" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="session-unchanged-on-logout" id="92" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="session-token-embedded-outside-of-cookie" id="93" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>

http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="session-not-terminated-when-browser-window-closed-without-logout" id="94" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="attacker-can-steal-session-token-from-history" id="95" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>

</vulnerability>
<vulnerability vuln-type="insecure-indexing" id="96" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
<vulnerability vuln-type="insufficient-password-recovery" id="97" severity="high">
<source src-type="Trend Micro Web Application Security" scan-id="12354" scan-date="2013-01-07 15:37:00" src-reference=""/>
<parameters>
<http-method>GET</http-method>
<url>
http://was-demo.trendmicro.com/vulnerabilities.php?id=234
</url>
<param-name>id</param-name>
</parameters>
<info>
<attack-vector>/var/boo"'`205.cnf</attack-vector>
<raw-request>
GET /vulnerabilities.php?id=234 HTTP/1.1 Referer: http://was-demo.trendmicro.com User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; MDDS; InfoPath.2; .NET4.0C; .NET4.0E; Tablet PC 2.0) Host: was-demo.trendmicro.com Connection: Close
</raw-request>
</info>
</vulnerability>
</host>
</vulnerabilities>