

XSS vulnerability on Apache Tomcat server

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-08/0024.html>

From: Erwin van der Zwan (erwin.zwan-van-der@siemens.nl)

Date: 08/13/02

Date: 13 Aug 2002 06:59:40 -0000

From: Erwin van der Zwan <erwin.zwan-van-der@siemens.nl>

To: pen-test@securityfocus.com

('binary' encoding is not supported, stored as-is)

I am currently pen-testing an Apache Tomcat v4.0.3 web server running on a Windows 2000 box. The server just provides access to an LDAP database through a search query. The box is connected directly to the Internet and seems to be protected by McAfee/PGP personal firewall/IDS which blocks the IP address for 30 minutes or so. TCP ports 21, 80, 389, 1002 and 1720 seems to be open, the rest is filtered/blocked. The server is running tomcat_server/servlet/JNDISearch Java LDAP search code.

It seems to be vulnerable for XSS and path disclosure vulnerabilities. I got the path (D:\Tomcat\webapps) but any ideas on how to exploit the XSS vulnerability or advance with the test?

Ideas?

EvdZ

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** [Ali Saifullah Khan: "Re: Re: Buffer Overflow Help"](#)
- **Next in thread:** [Anthony LaMantia: "Re: XSS vulnerability on Apache Tomcat server"](#)
- **Reply:** [Anthony LaMantia: "Re: XSS vulnerability on Apache Tomcat server"](#)
- **Reply:** [Muhammad Faisal Rauf Danka: "Re: XSS vulnerability on Apache Tomcat server"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)