Kotarak

10.10.10.55

Network Setup

- Connected to HTB OpenVPN Server via OVPN file

Found Vulnerabilities

- A possible SSRF (Server-Side Request Forgery)

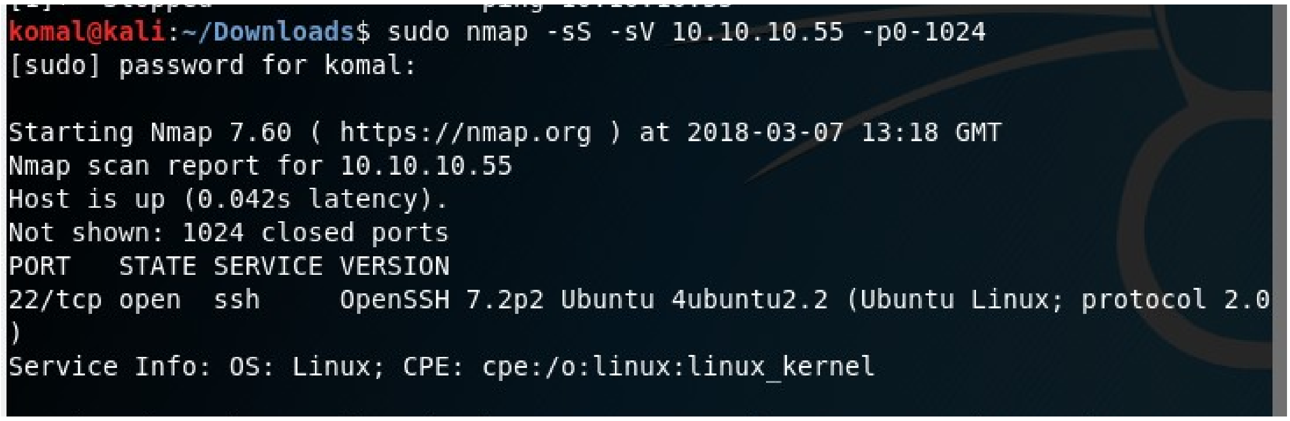
Exploits/Payloads Used

- scanner/http/tomcat_mgr_login
-

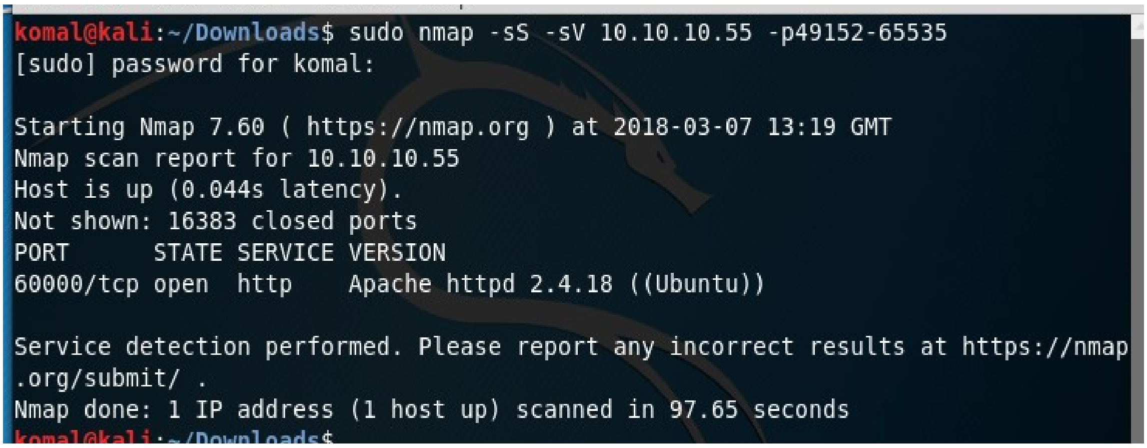
Key Findings

- **Open Ports:** 22, 60000(HTTP), 8009, 8080
  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
  Apache httpd 2.4.18 ((Ubuntu))
  Apache Tomcat/8.5.5
  Apache Jserv (Protocol v1.3)
- **System:** Linux kotarak-dmz 4.4.0-83-generic #106-Ubuntu SMP Mon Jun 26 17:54:43 UTC 2017 x86_64
- **Webserver:**
- **OS:** Ubunutu
- **Credentials:**
- **Extensions:** jsp, php, html,
- **Database:** mysqlnd 5.0.11-dev - 20120503 - $Id: 76b08b24596e12d4553bd41fc93cccd5bac2fe7a $
- **Server-side Language:** PHP 5.6.31-1~ubuntu16.04.1+deb.sury.org+1
- **To find login credentials of Tomcat Manager Application on** http://10.10.10.55:8080/manager/html
- **Use PUT Method in ajp13 port 8009 to exploit the vulnerability**

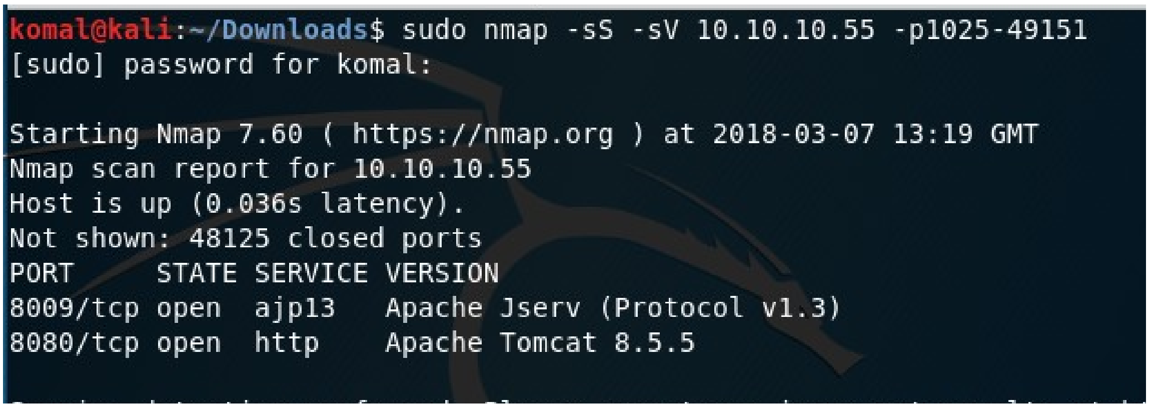
Write-Ups & Screenshots



```
komal@kali:~/Downloads$ sudo nmap -sS -sV 10.10.10.55 -p0-1024
[sudo] password for komal:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 13:18 GMT
Nmap scan report for 10.10.10.55
Host is up (0.042s latency).
Not shown: 1024 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0
)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

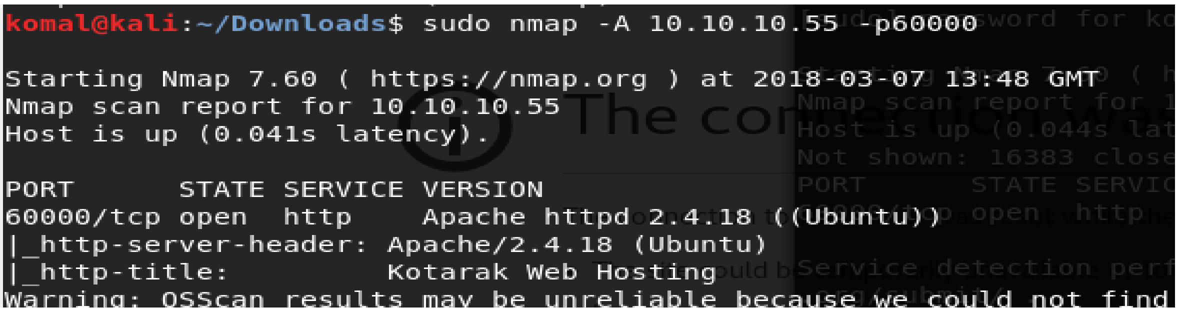


```
komal@kali:~/Downloads$ sudo nmap -sS -sV 10.10.10.55 -p49152-65535
[sudo] password for komal:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 13:19 GMT
Nmap scan report for 10.10.10.55
Host is up (0.044s latency).
Not shown: 16383 closed ports
PORT      STATE SERVICE VERSION
60000/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.65 seconds
komal@kali:~/Downloads$
```

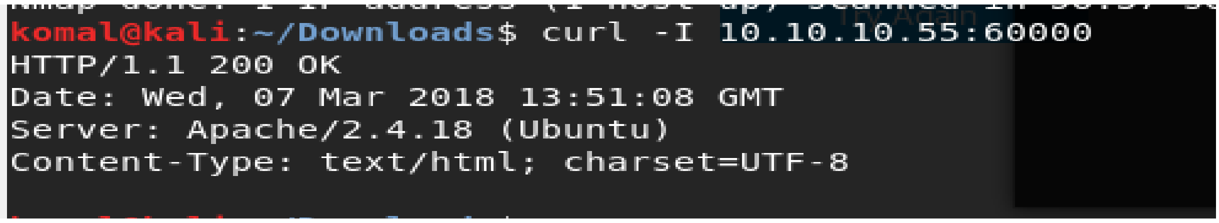


```
komal@kali:~/Downloads$ sudo nmap -sS -sV 10.10.10.55 -p1025-49151
[sudo] password for komal:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 13:19 GMT
Nmap scan report for 10.10.10.55
Host is up (0.036s latency).
Not shown: 48125 closed ports
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp open  http    Apache Tomcat 8.5.5
```

---------------------------------- PORT 60000 ENUM ---------------------------------------

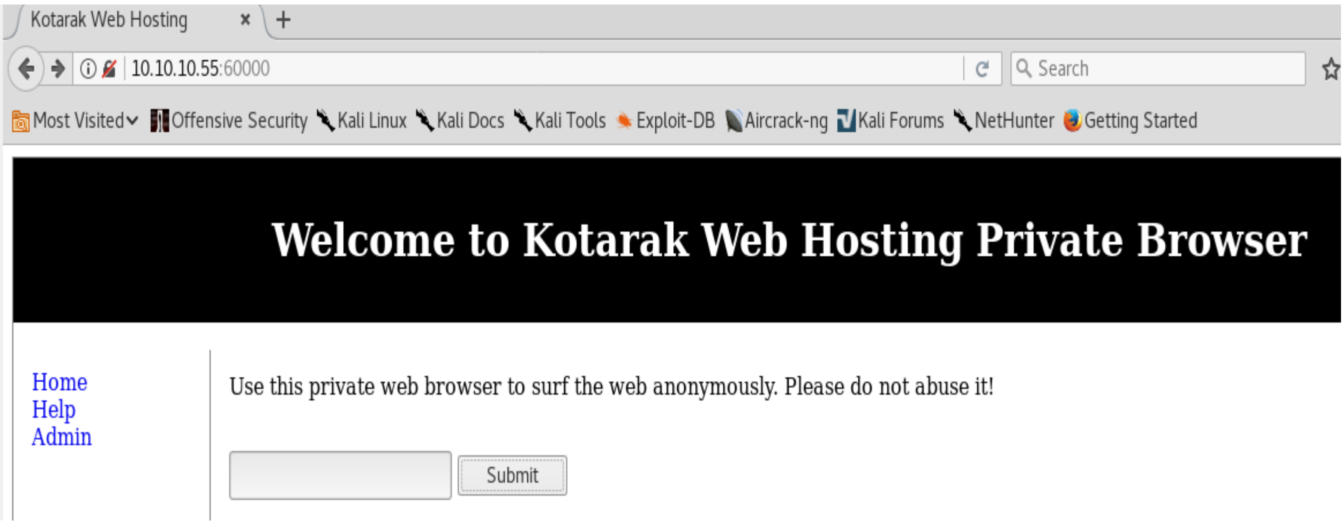


```
komal@kali:~/Downloads$ sudo nmap -A 10.10.10.55 -p60000

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 13:48 GMT
Nmap scan report for 10.10.10.55
Host is up (0.041s latency).

PORT      STATE SERVICE VERSION
60000/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title:         Kotarak Web Hosting
Warning: OSScan results may be unreliable because we could not find
```



```
komal@kali:~/Downloads$ curl -I 10.10.10.55:60000
HTTP/1.1 200 OK
Date: Wed, 07 Mar 2018 13:51:08 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Type: text/html; charset=UTF-8
```

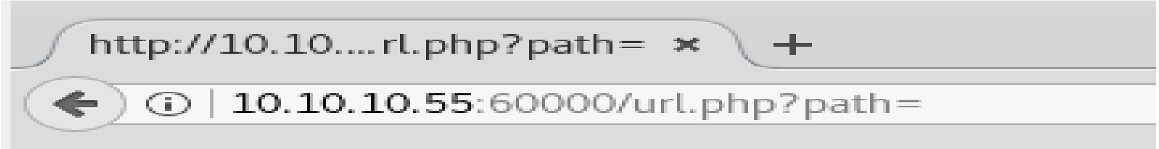
>> Clicking on the ‘submit’ button redirects to a GET parameter as shown below



Welcome to Kotarak Web Hosting Private Browser

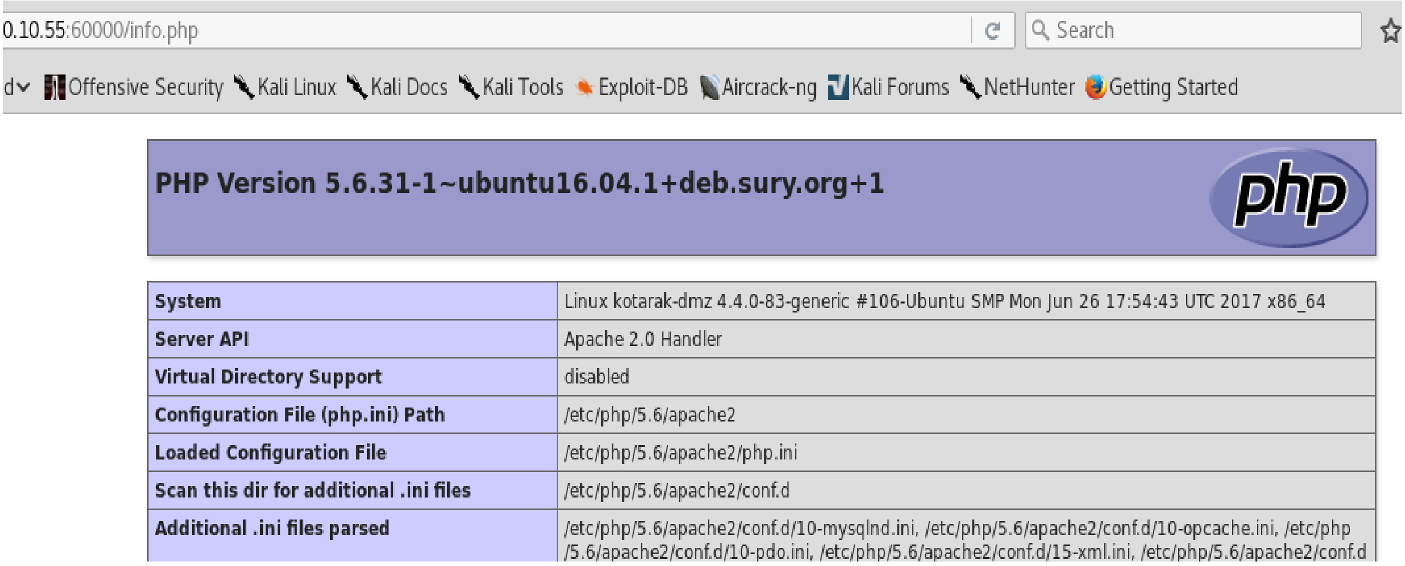
Home
Help
Admin

Use this private web browser to surf the web anonymously. Please do not abuse it!



http://10.10....rl.php?path=

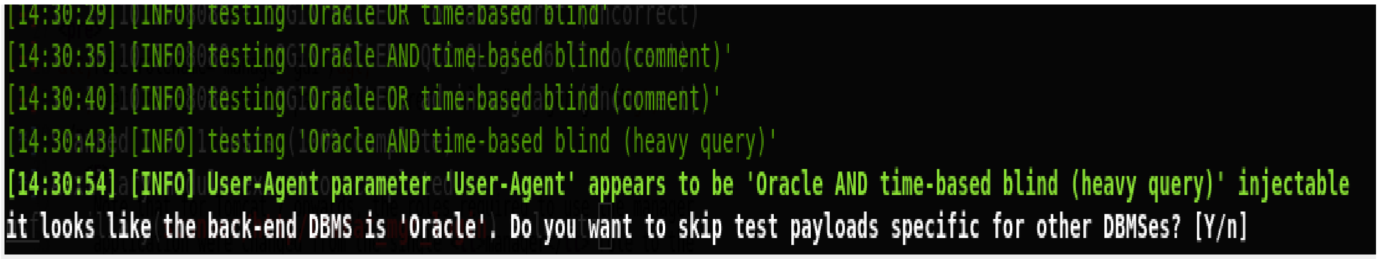
10.10.10.55:60000/url.php?path=



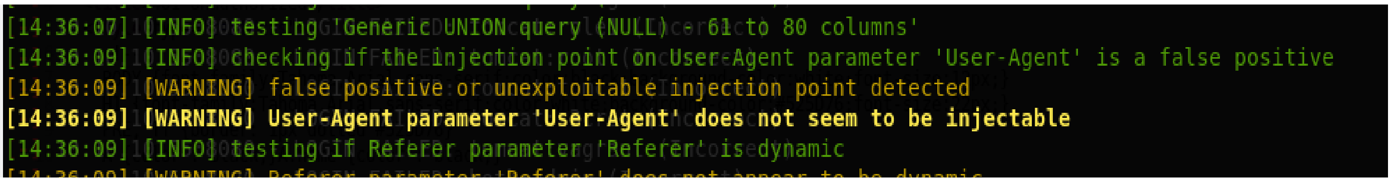
PHP Version 5.6.31-1~ubuntu16.04.1+deb.sury.org+1

System	Linux kotarak-dmz 4.4.0-83-generic #106-Ubuntu SMP Mon Jun 26 17:54:43 UTC 2017 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/apache2
Loaded Configuration File	/etc/php/5.6/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/apache2/conf.d
Additional .ini files parsed	/etc/php/5.6/apache2/conf.d/10-mysqlnd.ini, /etc/php/5.6/apache2/conf.d/10-opcache.ini, /etc/php/5.6/apache2/conf.d/10-pdo.ini, /etc/php/5.6/apache2/conf.d/15-xml.ini, /etc/php/5.6/apache2/conf.d

>> Using sqlmap, I found ‘User-Agent’ to be injectable and therefore possibly exploitable. However, when tests for ‘false positive’ was carried out it was found that the ‘User-Agent’ was false positive and therefore not injectable.

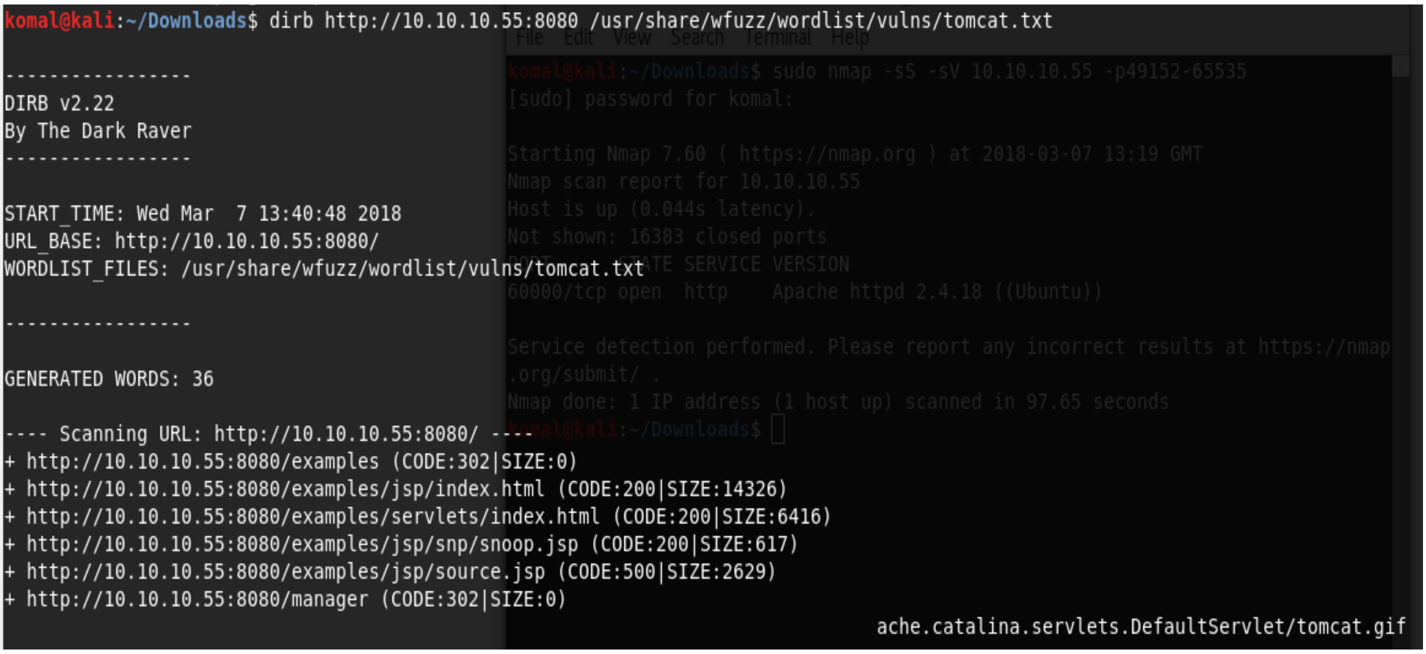


```
[14:30:29] [INFO] testing 'Oracle OR time-based blind'
[14:30:35] [INFO] testing 'Oracle AND time-based blind (comment)'
[14:30:40] [INFO] testing 'Oracle OR time-based blind (comment)'
[14:30:43] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[14:30:54] [INFO] User-Agent parameter 'User-Agent' appears to be 'Oracle AND time-based blind (heavy query)' injectable
it looks like the back-end DBMS is 'Oracle'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
```



```
[14:36:07] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[14:36:09] [INFO] checking if the injection point on User-Agent parameter 'User-Agent' is a false positive
[14:36:09] [WARNING] false positive or unexploitable injection point detected
[14:36:09] [WARNING] User-Agent parameter 'User-Agent' does not seem to be injectable
[14:36:09] [INFO] testing if Referer parameter 'Referer' is dynamic
[14:36:09] [WARNING] Referer parameter 'Referer' does not appear to be dynamic
```

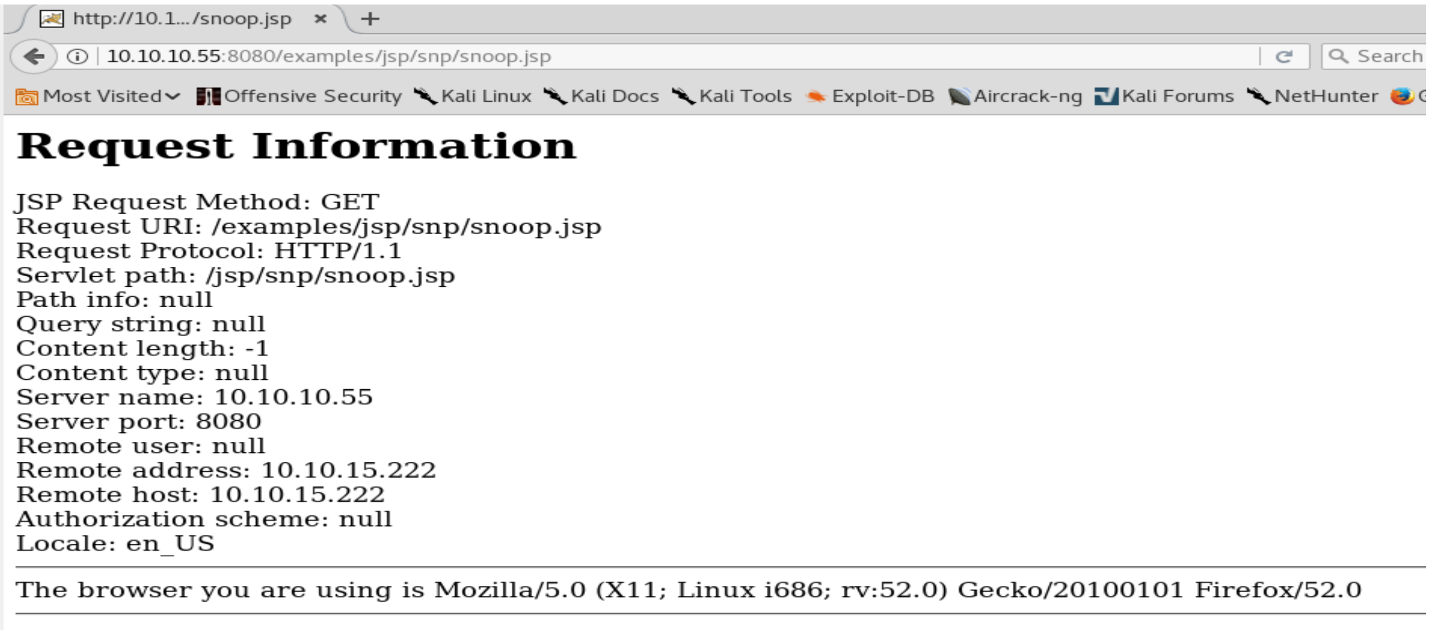
---------------------------------- PORT 8080 ENUM ---------------------------------------



```
komal@kali:~/Downloads$ dirb http://10.10.10.55:8080 /usr/share/wfuzz/wordlist/vulns/tomcat.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar  7 13:40:48 2018
URL_BASE: http://10.10.10.55:8080/
WORDLIST_FILES: /usr/share/wfuzz/wordlist/vulns/tomcat.txt

-----------------

GENERATED WORDS: 36

---- Scanning URL: http://10.10.10.55:8080/ ----
+ http://10.10.10.55:8080/examples (CODE:302|SIZE:0)
+ http://10.10.10.55:8080/examples/jsp/index.html (CODE:200|SIZE:14326)
+ http://10.10.10.55:8080/examples/servlets/index.html (CODE:200|SIZE:6416)
+ http://10.10.10.55:8080/examples/jsp/snp/snoop.jsp (CODE:200|SIZE:617)
+ http://10.10.10.55:8080/examples/jsp/source.jsp (CODE:500|SIZE:2629)
+ http://10.10.10.55:8080/manager (CODE:302|SIZE:0)
```

```
komal@kali:~/Downloads$ sudo nmap -sS -sV 10.10.10.55 -p49152-65535
[sudo] password for komal:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 13:19 GMT
Nmap scan report for 10.10.10.55
Host is up (0.044s latency).
Not shown: 16383 closed ports
PORT      STATE SERVICE VERSION
60000/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.65 seconds
komal@kali:~/Downloads$
```

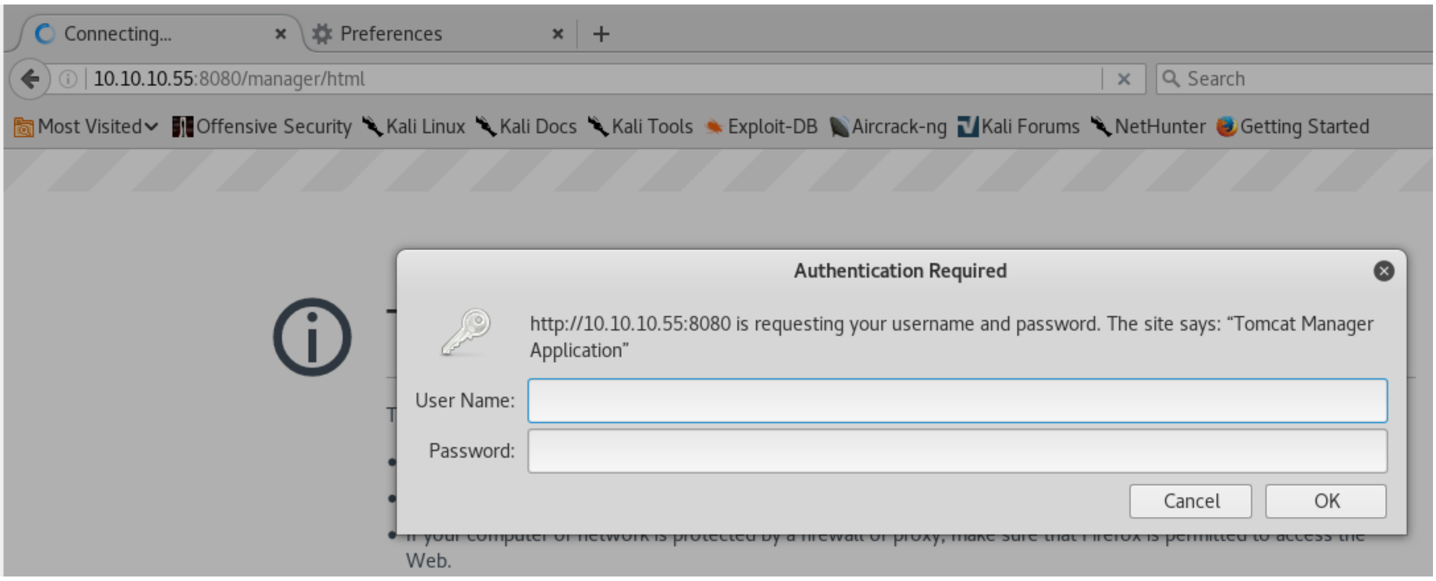
```
ache.catalina.servlets.DefaultServlet/tomcat.gif
```



Request Information

JSP Request Method: GET
Request URI: /examples/jsp/snp/snoop.jsp
Request Protocol: HTTP/1.1
Servlet path: /jsp/snp/snoop.jsp
Path info: null
Query string: null
Content length: -1
Content type: null
Server name: 10.10.10.55
Server port: 8080
Remote user: null
Remote address: 10.10.15.222
Remote host: 10.10.15.222
Authorization scheme: null
Locale: en_US

The browser you are using is Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0



Authentication Required

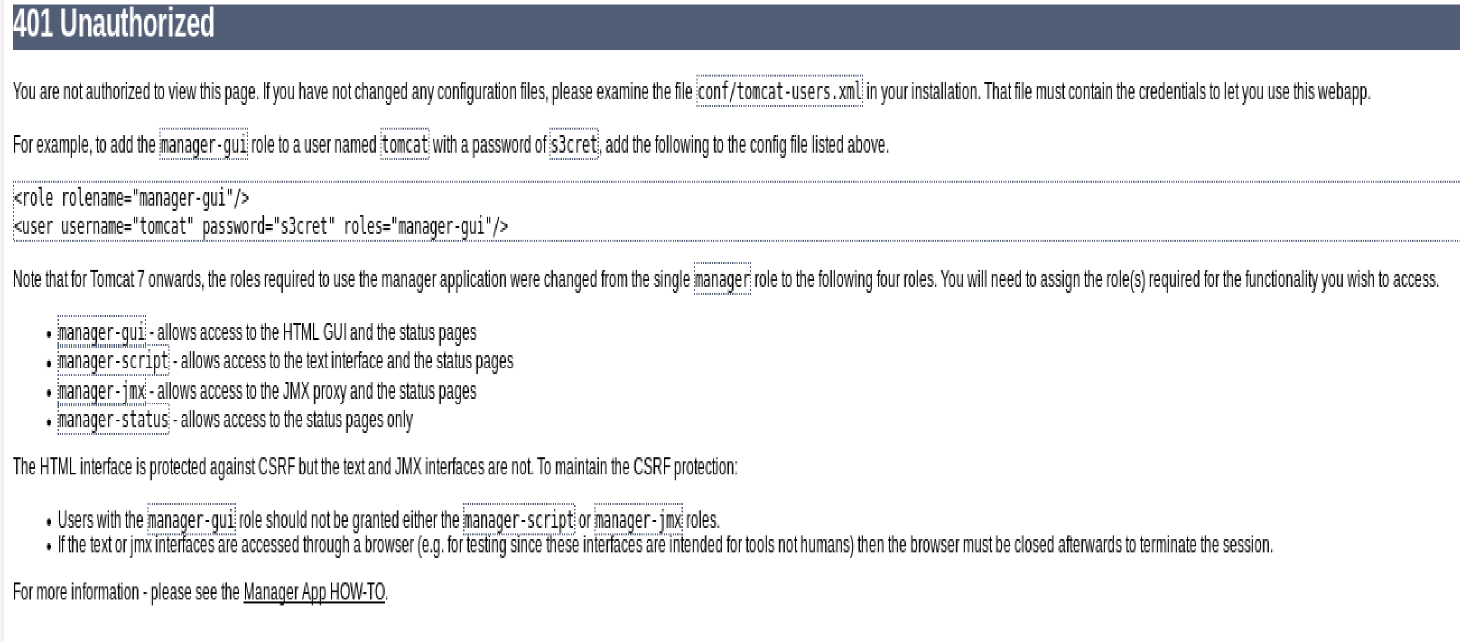
http://10.10.10.55:8080 is requesting your username and password. The site says: “Tomcat Manager Application”

User Name:

Password:

If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

>> Upon hitting the cancel button, I am redirected to an error page revealing a path directory and some other information.



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

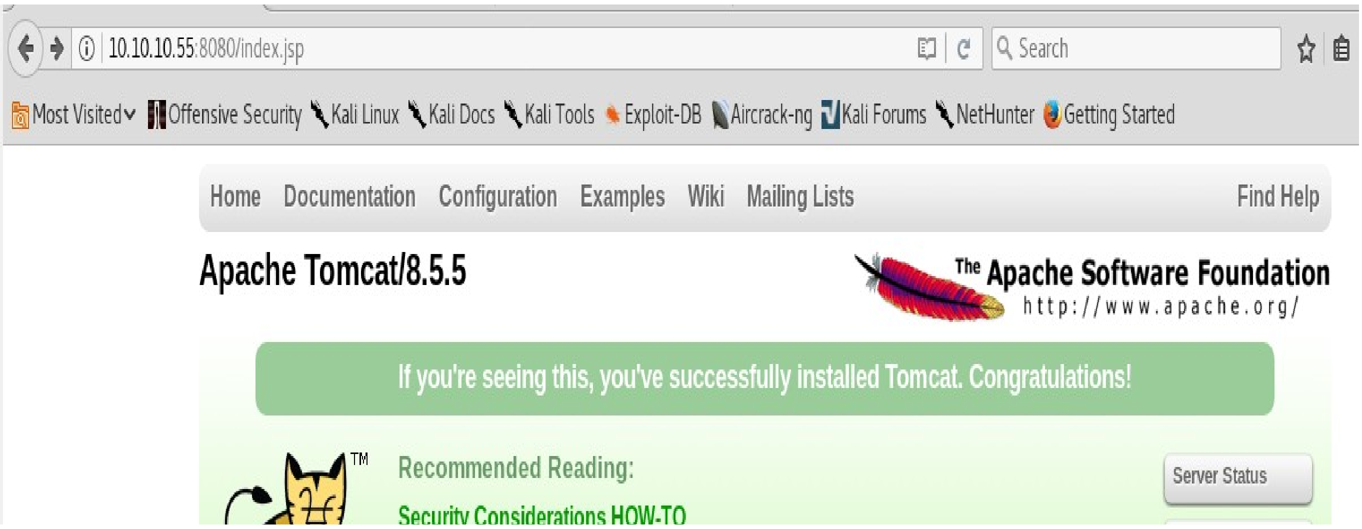
The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App HOW-TO.

>> Have used the metasploit module ‘scanner/http/tomcat_mgr_login’ to attempt bruteforce login at:

/manager/status
/manager/text
/manager/html
/host-manager/html



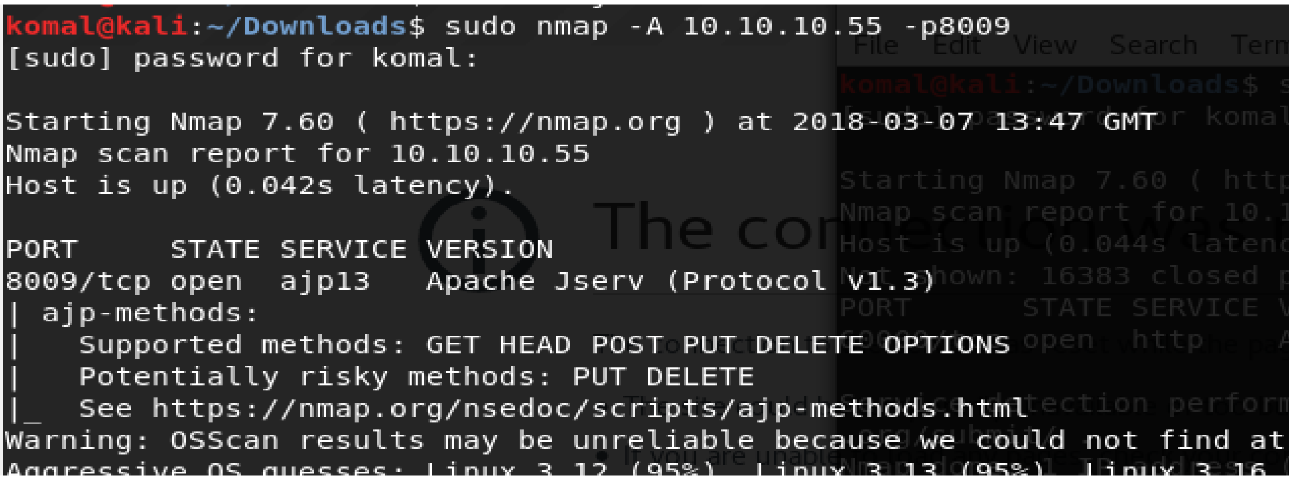
Apache Tomcat/8.5.5

If you're seeing this, you've successfully installed Tomcat. Congratulations!

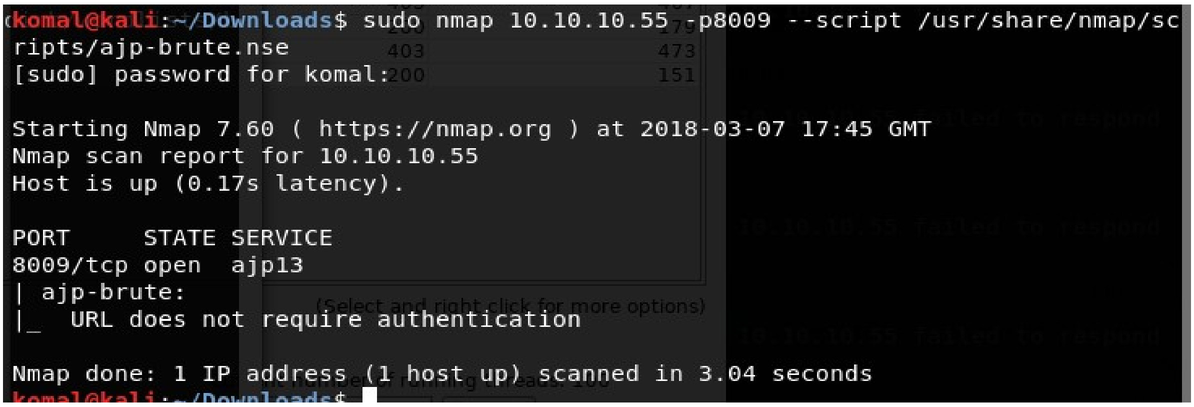
Recommended Reading:

Security Considerations HOW-TO

---------------------------------- PORT 8009 ENUM --

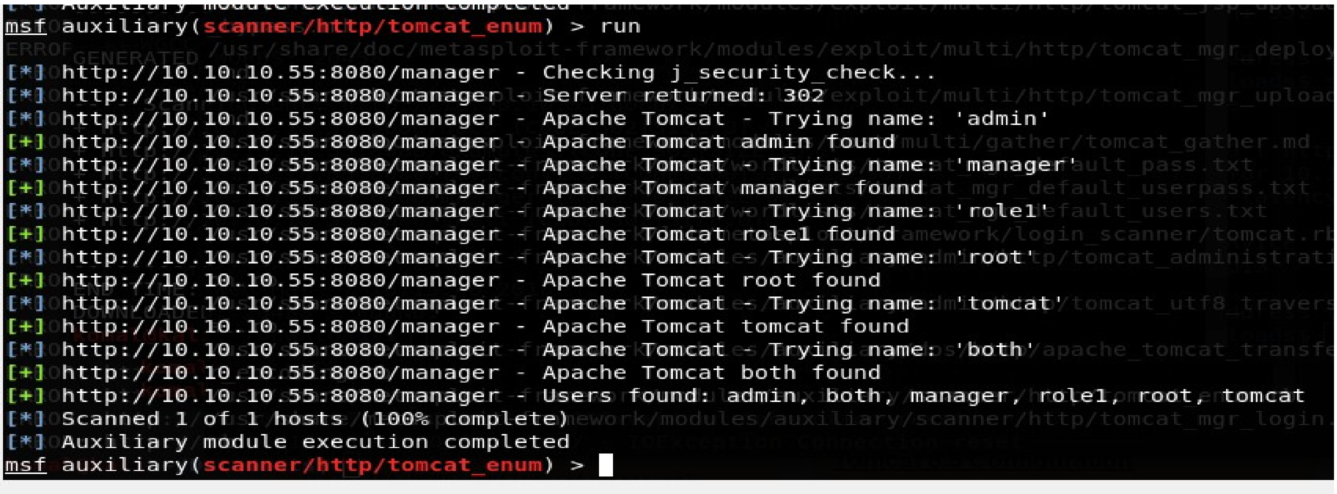


```
komal@kali:~/Downloads$ sudo nmap -A 10.10.10.55 -p8009
[sudo] password for komal:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 13:47 GMT
Nmap scan report for 10.10.10.55
Host is up (0.042s latency).

PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
| ajp-methods:
|   Supported methods: GET HEAD POST PUT DELETE OPTIONS
|   Potentially risky methods: PUT DELETE
|_  See https://nmap.org/nsedoc/scripts/ajp-methods.html
Warning: OSScan results may be unreliable because we could not find at
Aggressive OS guesses: Linux 3.12 (95%), Linux 3.13 (95%), Linux 3.16 (
```



```
komal@kali:~/Downloads$ sudo nmap 10.10.10.55 -p8009 --script /usr/share/nmap/sc
ripts/ajp-brute.nse
[sudo] password for komal:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 17:45 GMT
Nmap scan report for 10.10.10.55
Host is up (0.17s latency).

PORT     STATE SERVICE
8009/tcp open  ajp13
| ajp-brute:
|_  URL does not require authentication

Nmap done: 1 IP address (1 host up) scanned in 3.04 seconds
komal@kali:~/Downloads$
```

>> For User enumeration at http://10.10.10.55:8080/manager, The following valid userames were found.



```
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_enum) > run

[*] http://10.10.10.55:8080/manager - Checking j_security_check...
[*] http://10.10.10.55:8080/manager - Server returned: 302
[*] http://10.10.10.55:8080/manager - Apache Tomcat - Trying name: 'admin'
[+] http://10.10.10.55:8080/manager - Apache Tomcat admin found
[*] http://10.10.10.55:8080/manager - Apache Tomcat - Trying name: 'manager'
[+] http://10.10.10.55:8080/manager - Apache Tomcat manager found
[*] http://10.10.10.55:8080/manager - Apache Tomcat - Trying name: 'role1'
[+] http://10.10.10.55:8080/manager - Apache Tomcat role1 found
[*] http://10.10.10.55:8080/manager - Apache Tomcat - Trying name: 'root'
[+] http://10.10.10.55:8080/manager - Apache Tomcat root found
[*] http://10.10.10.55:8080/manager - Apache Tomcat - Trying name: 'tomcat'
[+] http://10.10.10.55:8080/manager - Apache Tomcat tomcat found
[*] http://10.10.10.55:8080/manager - Apache Tomcat - Trying name: 'both'
[+] http://10.10.10.55:8080/manager - Apache Tomcat both found
[+] http://10.10.10.55:8080/manager - Users found: admin, both, manager, role1, root, tomcat
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_enum) >
```