

# 00截断文件上传CTF例题详解

原创

無名之连 于 2020-07-06 22:02:56 发布 497 收藏 1

分类专栏: [CTF](#) 文章标签: [CTF](#)

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/107168709>

版权



[CTF 专栏收录该内容](#)

37 篇文章 0 订阅

订阅专栏

## 00截断文件上传CTF例题详解

题目

解法

### 题目

CTFHub 文件上传 - 00截断

challenge-733eec8f9e1ef0df.sandbox.ctfhub.com:10080

INT SQL XSS Encryption Encoding Other

Load URL Split URL Execute

Enable Post data Enable Referrer

Filename: 浏览... 未选择文件.

Submit

```

6 <title>CTFHub 文件上传 - 00截断</title>
7 </head>
8
9 <body>
10 <h1>CTFHub 文件上传 - 00截断</h1>
11 <form action=?road=/var/www/html/upload/ method="post" enctype="multipart/form-data">
12 <label for="file">Filename:</label>
13 <input type="file" name="file" id="file" />
14 <br />
15 <input type="submit" name="submit" value="Submit" />
16 </form>
17 <!--
18 if (!empty($_POST['submit'])) {
19     $name = basename($_FILES['file']['name']);
20     $info = pathinfo($name);
21     $ext = $info['extension'];
22     $whitelist = array("jpg", "png", "gif");
23     if (in_array($ext, $whitelist)) {
24         $des = $_GET['road'] . "/" . rand(10, 99) . date("YmdHis") . "." . $ext;
25         if (move_uploaded_file($_FILES['file']['tmp_name'], $des)) {
26             echo "<script>alert('上传成功')</script>";
27         } else {
28             echo "<script>alert('上传失败')</script>";
29         }
30     } else {
31         echo "文件类型不匹配";
32     }
33 }
34 -->
35 </body>
36
37 </html>

```

## 解法

抓包进行尝试php文件果然不行

**Request**

```

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=-----1682087205669
Content-Length: 321
Referer:
http://challenge-733eec8f9e1ef0df.sandbox.ctfhub.com:10080/
Connection: close
Upgrade-Insecure-Requests: 1
-----1682087205669
Content-Disposition: form-data; name="file"; filename="2.php"
Content-Type: image/jpeg

```

**Response**

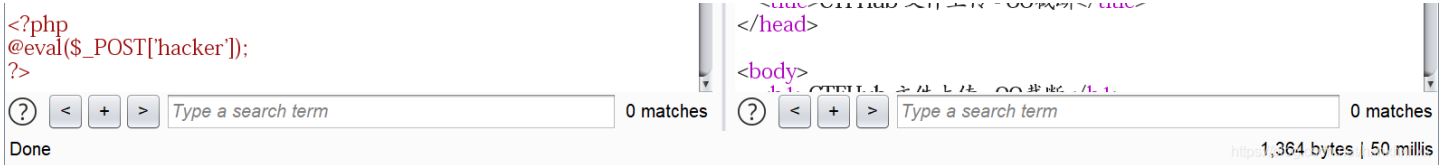
```

HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Mon, 06 Jul 2020 13:46:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1064
Connection: close
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

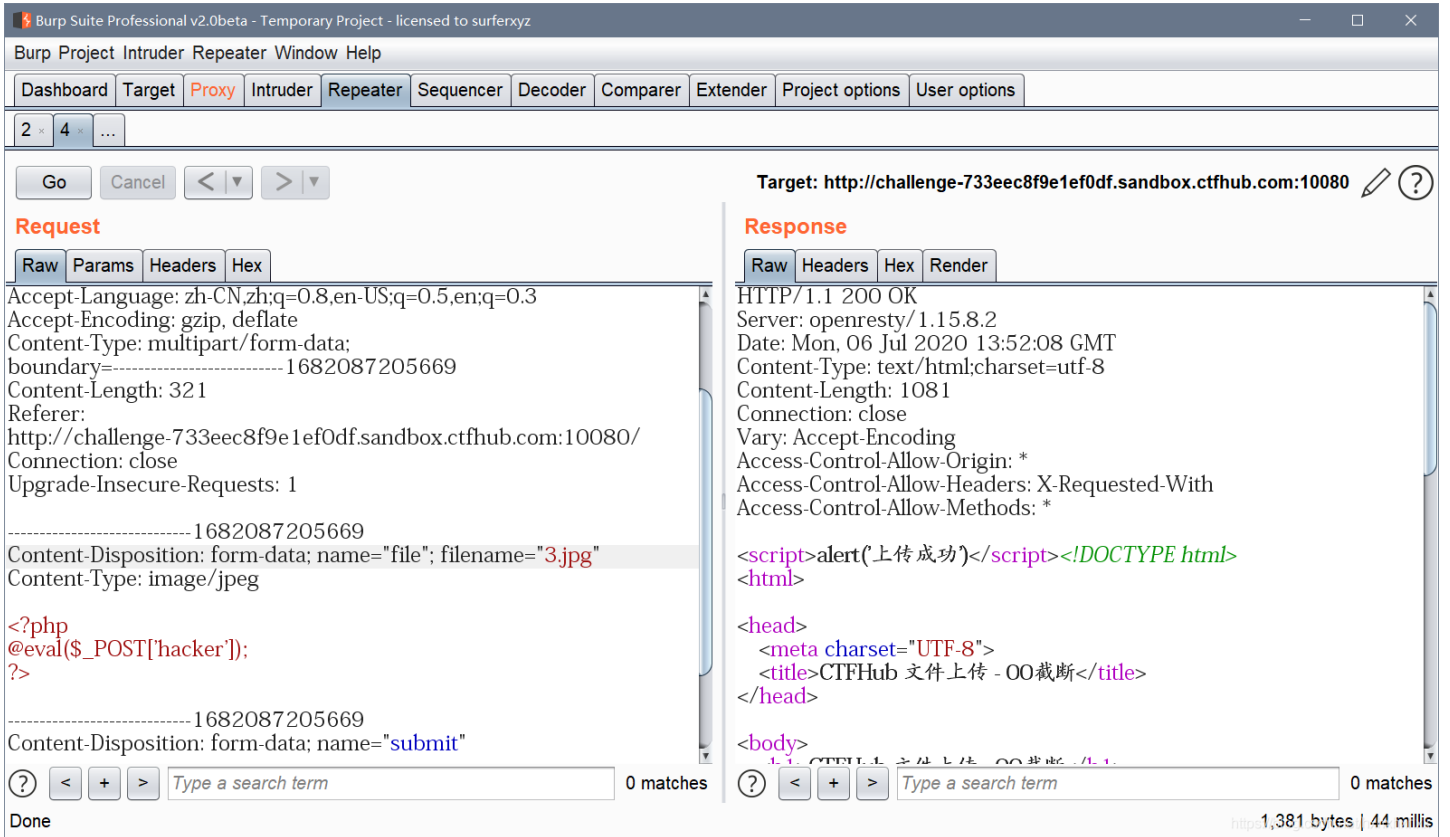
文件类型不匹配<!DOCTYPE html>
<html>

<head>
<meta charset="UTF-8">
<title>CTFHub 文件上传 - 00截断</title>

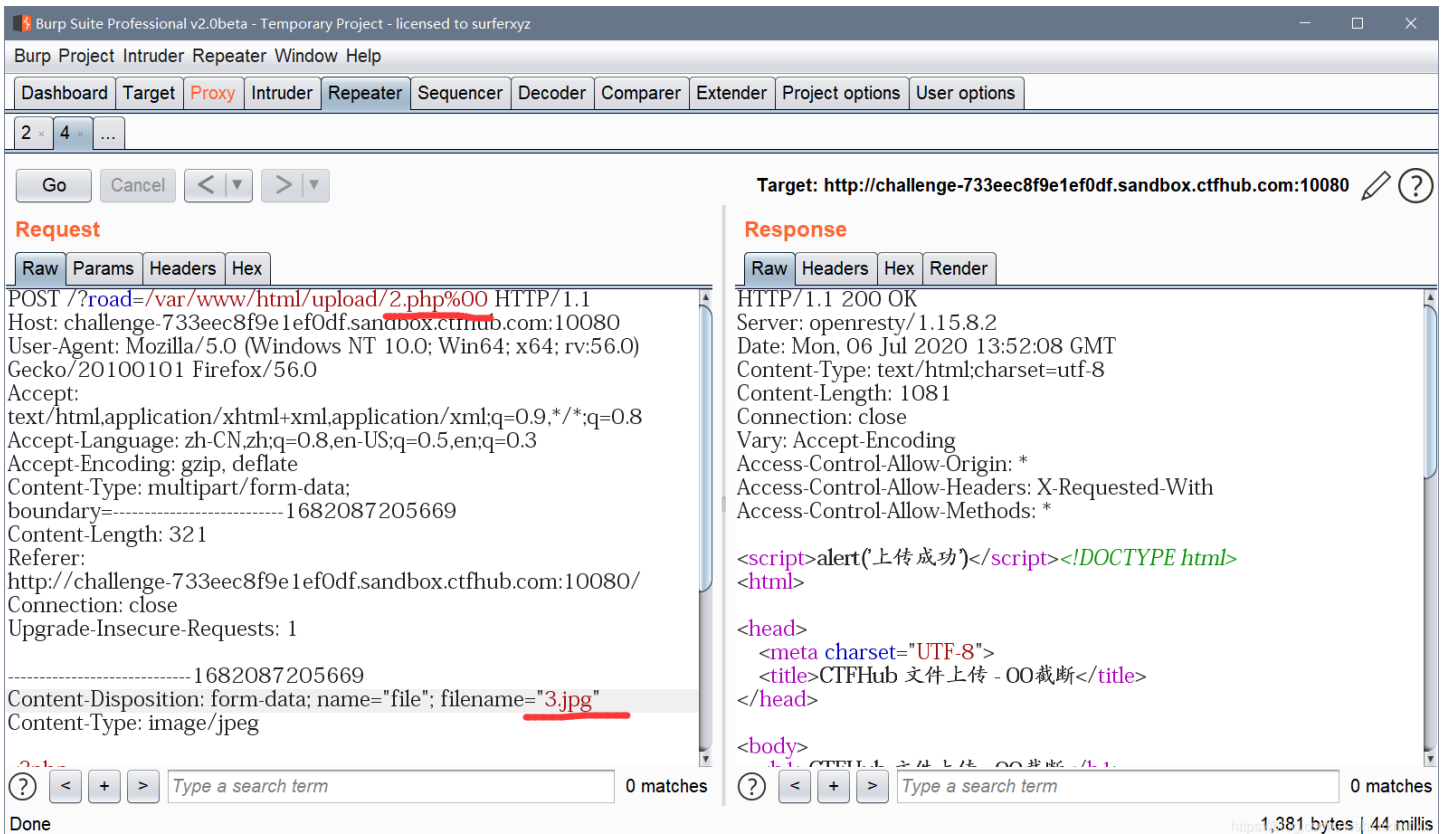
```



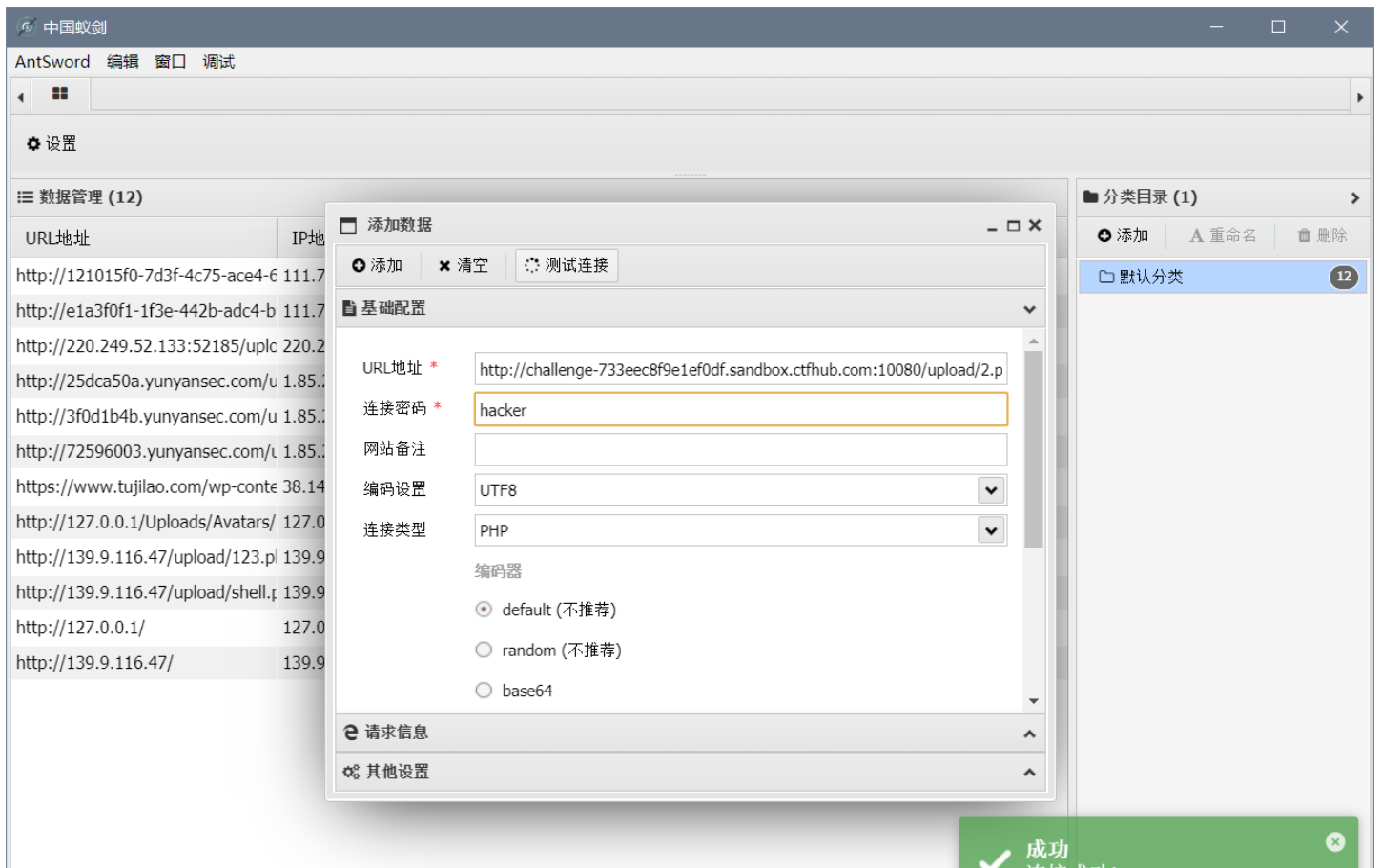
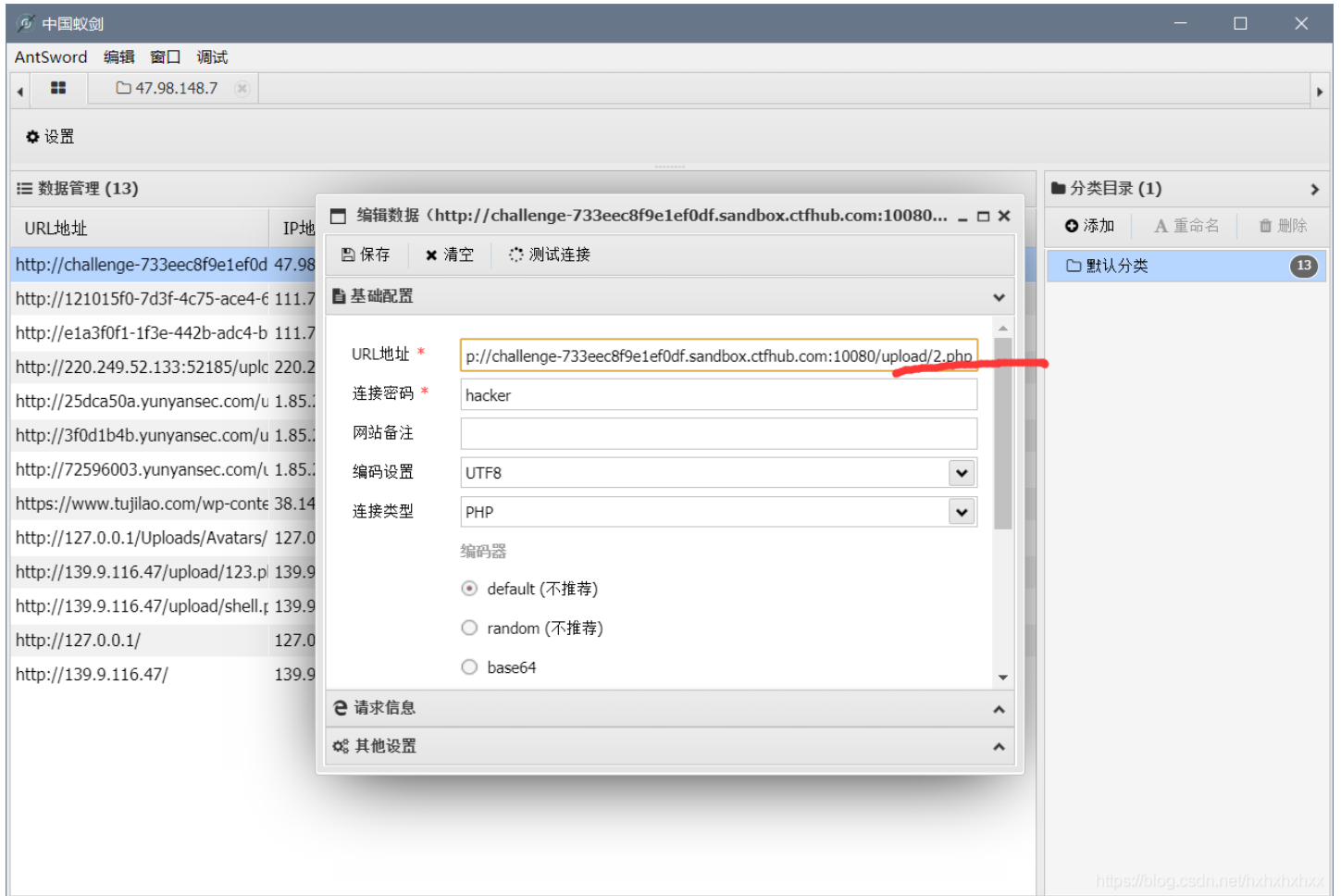
jpg文件可以上传成功



这里因为有文件路径，那么使用%00截断的时候，让他生成了一个2.php的文件，然后将3.jpg的内容写了进去

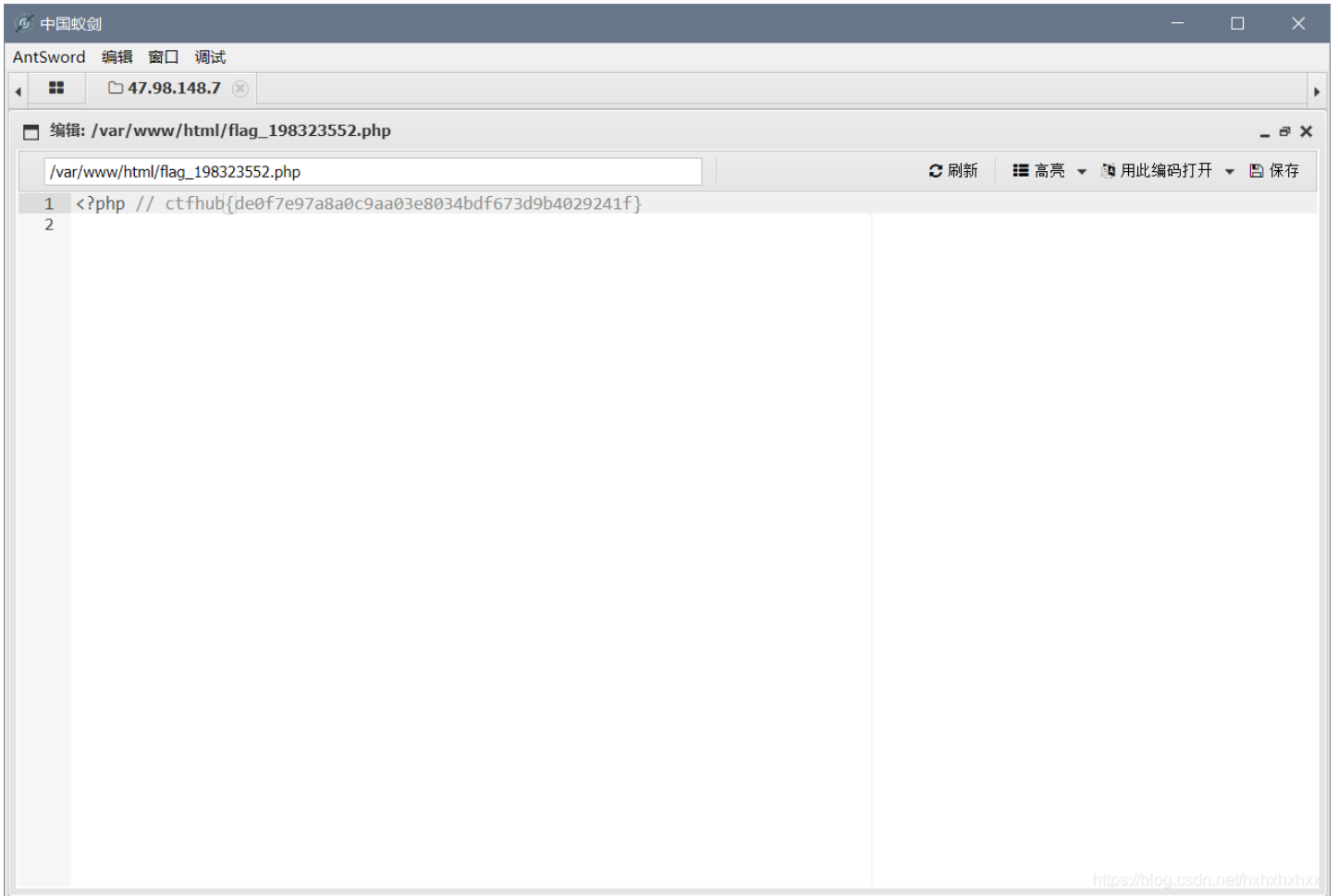


这里链接的也是2.php



连接成功!

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



16进制的0x00截断见

16进制CTF题目解答