

攻防世界WEB进阶之PHP2

原创

[harry_c](#) 于 2019-07-31 14:06:26 发布 4848 收藏 6

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#) [web进阶](#) [PHP2](#) [安全](#)

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/harry_c/article/details/97913194

版权



[攻防世界](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

攻防世界WEB进阶之PHP2

第一步: 分析

第二步: 实操

第三步: 答案

难度系数: 1星

题目来源: 暂无

题目描述: 暂无

第一步: 分析

根据题目, 没有给出任何信息, 直接是一个场景, 点击打开场景页面我们发现是一串文字: Can you authenticate to this website?

第二步: 实操

首先想到尝试index.php, 未果。再尝试index.phps, 成功发现了代码泄露。

```
<?php if("admin"===$_GET[id]) { echo("
not allowed!

"); exit(); } $_GET[id] = urldecode($_GET[id]); if($_GET[id] == "admin") { echo "
Access granted!

"; echo "
Key: xxxxxxx

"; } ?>
```

通过代码分析我们应该很清晰的知道需要使得"admin"===

$ET[id]$ 不成立, 并且 $GET[id] == "admin"$ 成立, 通过语句

$ET[id] = urldecode(GET[id]);$ 我们知道代码经过了url编码转换, 所以这里应该是突破口

第三步: 答案

Access granted!

Key: cyberpeace{565b59ecd7b747cc76d72562c9c353a4}

Can you authenticate to this website?

https://blog.csdn.net/harry_c

至此flag为: cyberpeace{565b59ecd7b747cc76d72562c9c353a4}