

# XCTF攻防世界 Web高手进阶区 PHP2 writeup

原创

[Senimo\\_](#)



于 2020-03-30 14:51:51 发布



358



收藏

分类专栏: [各CTF平台 Writeup](#) 文章标签: [php web](#) [XCTF攻防世界 writeup](#) [Web高手进阶区](#)

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/weixin\\_44037296/article/details/105198912](https://blog.csdn.net/weixin_44037296/article/details/105198912)

版权



[各CTF平台 Writeup](#) 专栏收录该内容

16 篇文章 6 订阅

订阅专栏

## XCTF攻防世界 Web高手进阶区 PHP2 writeup

### PHP2

难度系数: 2.0

题目来源: 暂无

题目描述: 暂无

启动靶机, 打开环境:

Can you authenticate to this website?

你能浏览这个网站嘛?

首先访问 `index.php`，可以正常访问，尝试查看 `index.php` 文件（`.php` 文件就是 `php` 的源代码文件，通常用于提供给访问者查看 `php` 代码）：

```
<?php
if("admin"===$_GET[id]) {
    echo("<p>not allowed!</p>");
    exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
    echo "<p>Access granted!</p>";
    echo "<p>Key: xxxxxxxx </p>";
}
?>
```

Can you authenticate to this website?

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

得到网页的源代码，分析代码：

需要传入变量 `id` 的值，不能等于 `admin`，经过 `URL` 解码后等于 `admin` 将输出 `key`，因为服务器会进行一次 `URL` 解码，所以我们将 `admin` 进行二次编码：

URI(URL)文本:  选择字符集: utf8编码 (unicode编码) 复杂程度: 复杂类型(所有字符都编码)

↑ 将你电脑文件直接拖入试试^-^

转换结果:

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

Elements Console Sources Network Performance Memory Application Security Audits EditThisCookie HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING

URL

http://111.198.29.45:56064/index.php?id=%2561%2564%256d%2569%256e

Enable POST

ADD HEADER

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

得到最后的传输值为：

```
?id=%2561%2564%256d%2569%256e
```

传输数据得到 flag :

Access granted!

Key: cyberpeace{c8db69a5623be8553b95da3f45a6db2a}

Can you authenticate to this website?