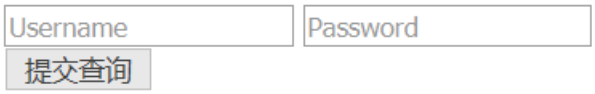
ACTF新生赛 SQL注入

原创

penson by 小乌 于 2020-03-17 17:46:13 发布 74 收藏

分类专栏： 笔记

本文链接：https://blog.csdn.net/SopRomeo/article/details/104926542



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