

# 云演CTF: 008.后台管理系统

转载

wangguixiu



于 2021-06-10 08:49:16 发布



301



收藏

原文链接: <https://www.wangguixiu.top/%E4%BA%91%E6%BC%94/%E4%BA%91%E6%BC%94CTF-008-%E5%90%8E%E5%8F%B0%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9F.html>

版权

## 云演CTF: 008.后台管理系统

- 作者: [admin](#)
- 时间: 2021-05-31
- 分类: [云演CTF](#)

右下角点击注册了个test用户，提示管理员才能拿到flag，

再注册admin用户，返回用户已存在，

尝试注册"admin"，注册成功拿到flag，

想想不应该这么简单，百度"基于约束的sql注入"，

sql中字段有固定的长度，超出的部分就丢弃了，所有以"admin"加上大量空格加'1'做为用户名，超出长度的'1'被舍弃，空格忽略，成功绕过

标签: [ctf](#), [sql注入](#)