R7-1锐捷-SmartWeb管理系统-InformationLeakage

漏洞描述：

锐捷网络股份有限公司无线smartweb管理系统存在逻辑缺陷漏洞，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：

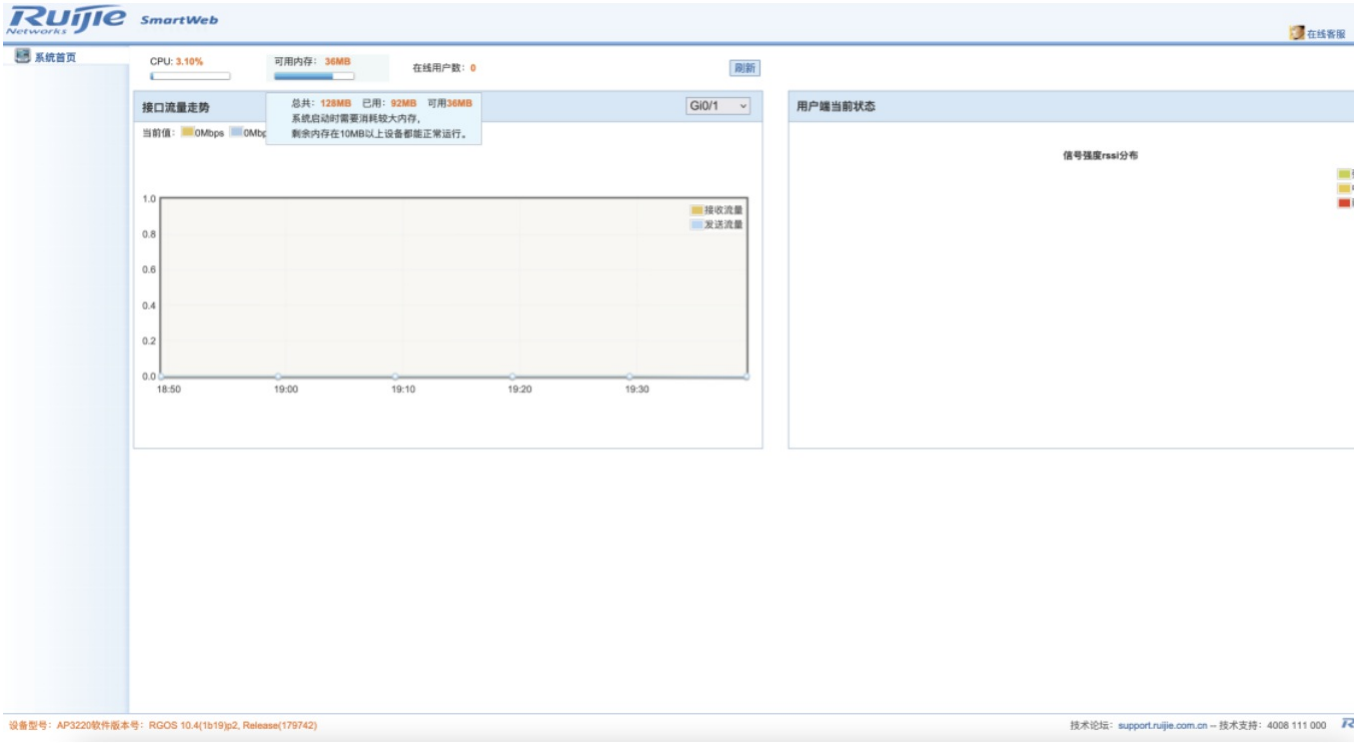
网络测绘：

Hunter 语法：

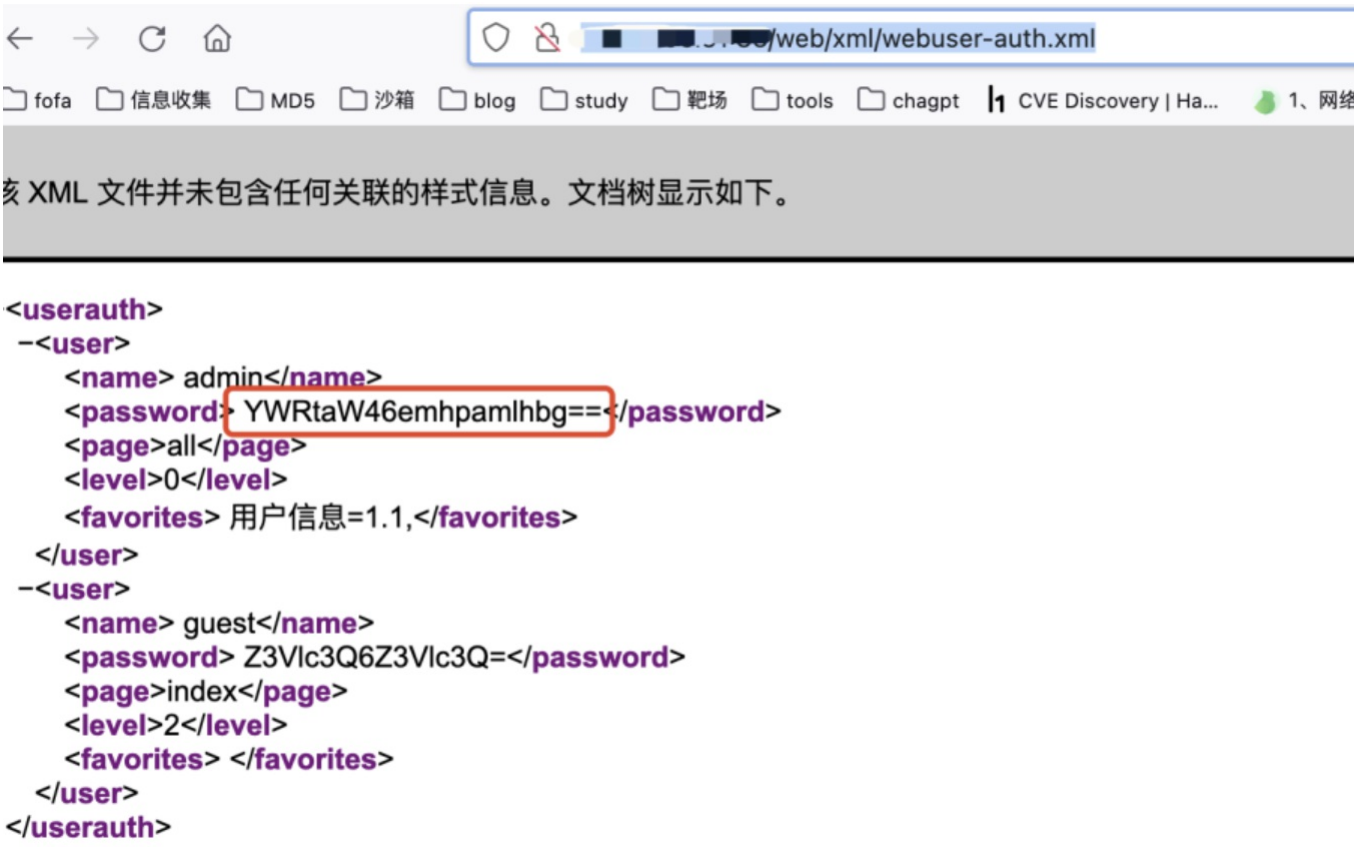
- hunterapp.name="Ruijie 锐捷 Smartweb"

漏洞复现：

1. 使用默认口令guest/guest登录系统

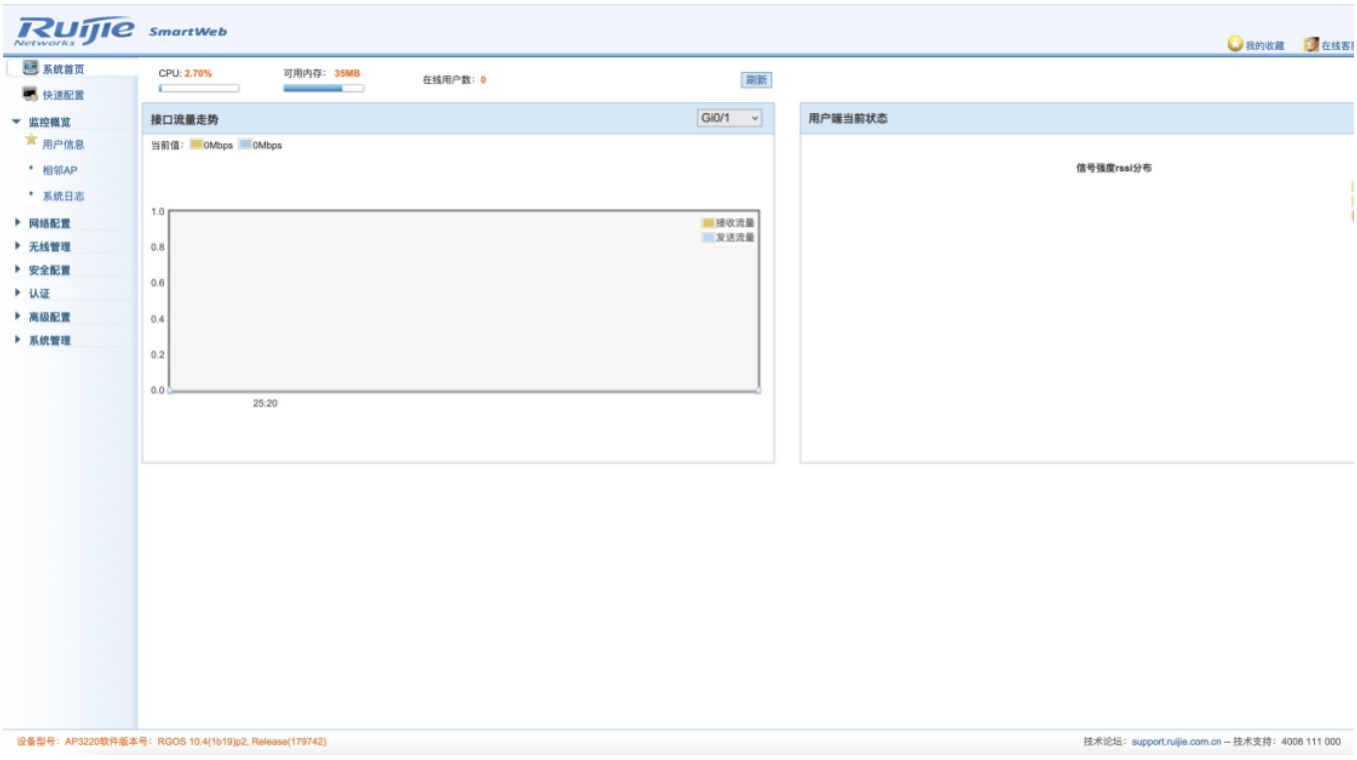


1. 使用poc获取管理员admin账号密码



base64解码后获取账号密码

使用获取的管理账号admin登录系统


Ruijie Networks
SmartWeb
我的收藏
在线客
系统首页
快速配置
监控概览
用户信息
相邻AP
系统日志
网络配置
无线管理
安全配置
认证
高级配置
系统管理
CPU: 2.70%
可用内存: 35MB
在线用户数: 0
刷新
接口流量走势
Gi0/1
当前值: 0Mbps 0Mbps
1.0
0.8
0.6
0.4
0.2
0.0
25:20
接收流量
发送流量
用户端当前状态
信号强度rssi分布
设备型号：AP3220软件版本号：RGOS 10.4(1b19)p2, Release(179742)
技术论坛：support.ruijie.com.cn -- 技术支持：4008 111 000