## TOTOLINK路由器N200RE存在命令执行漏洞

## 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

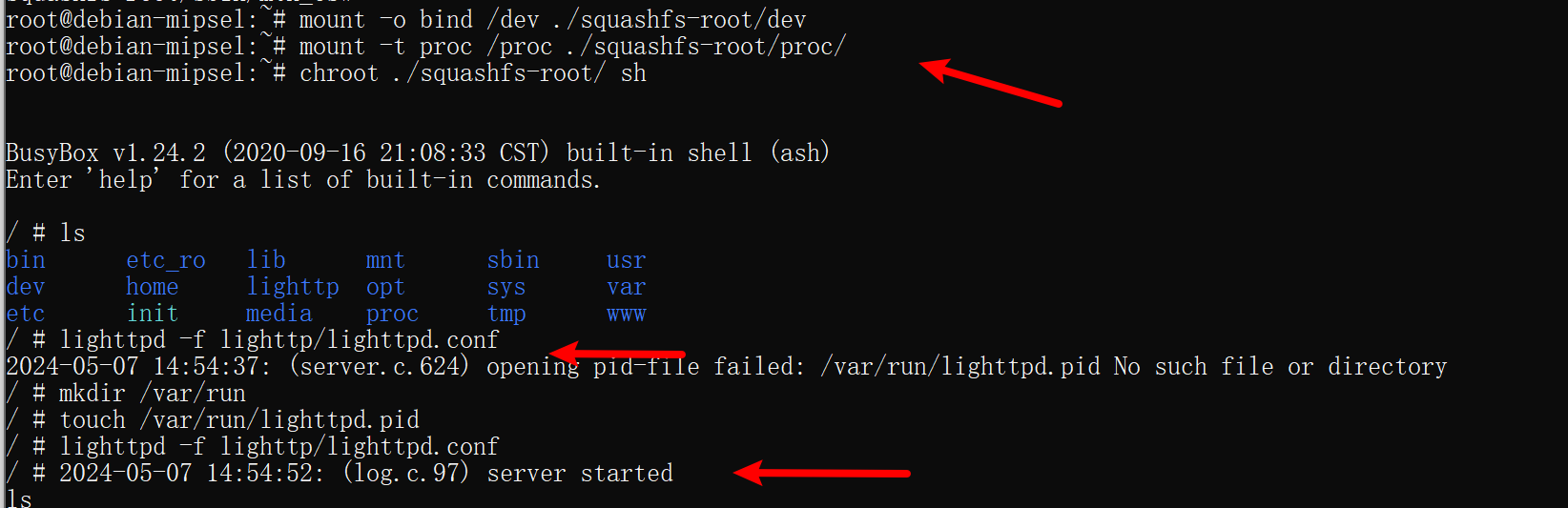
V9.3.5u.6095\_B20200916版本的固件

## 漏洞证明与分析

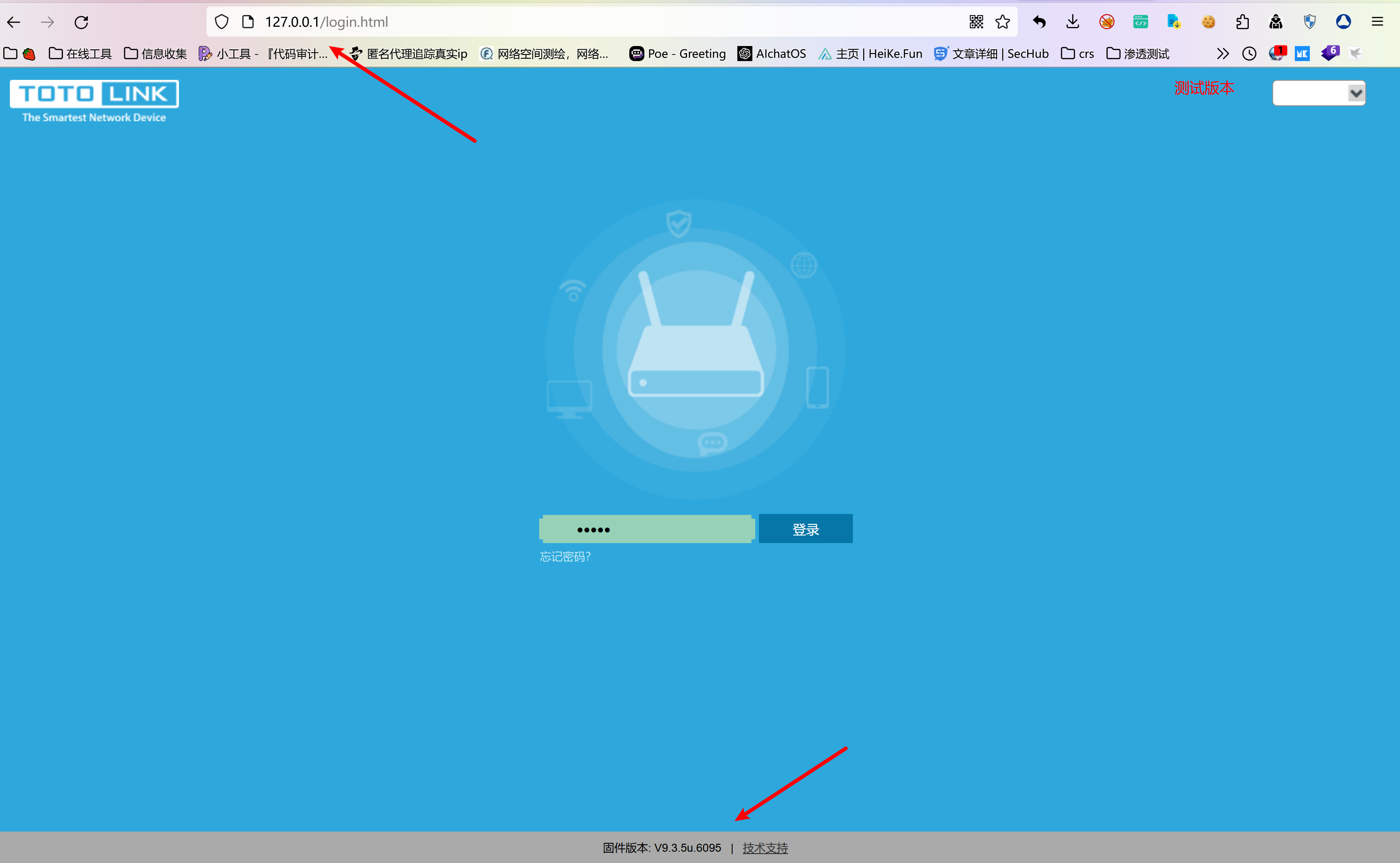
截图如下：

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



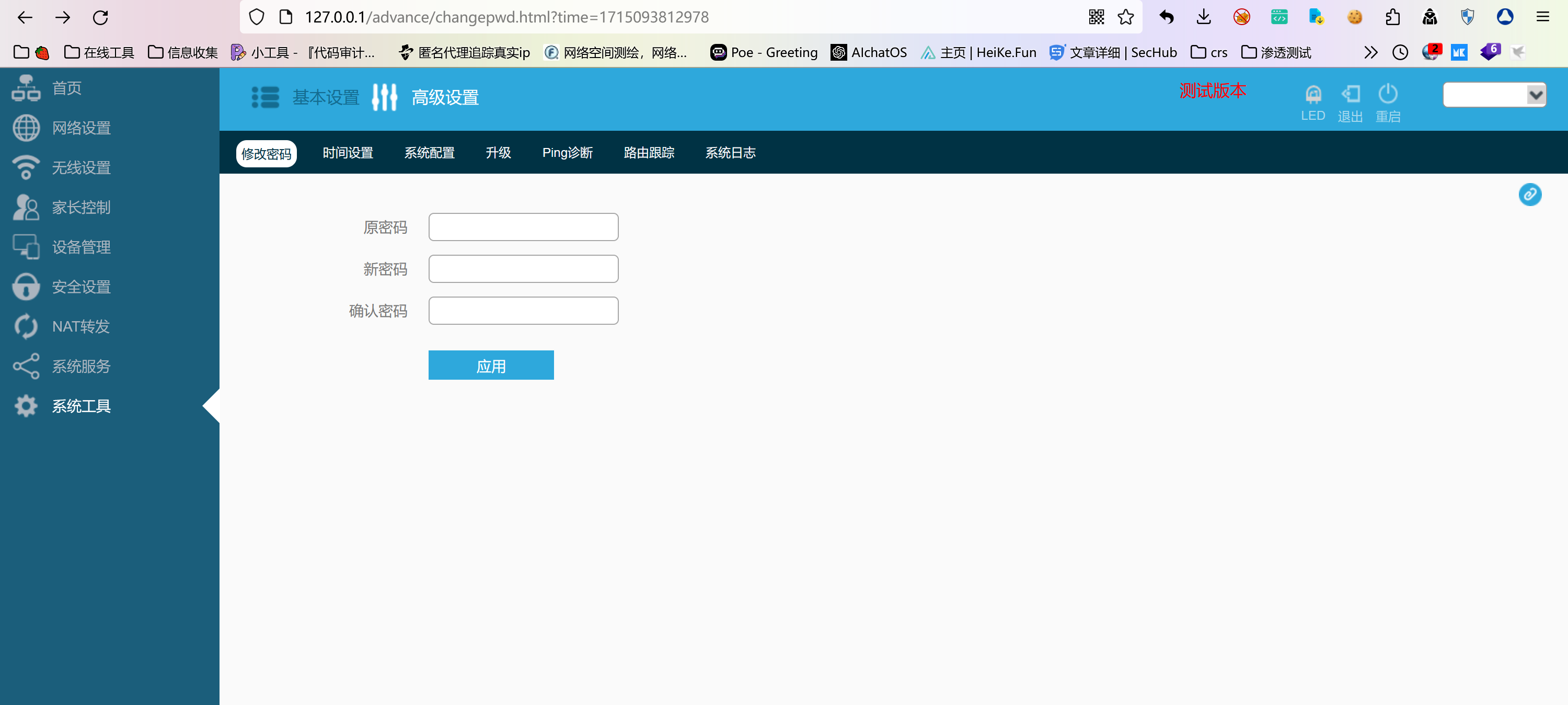
开启的web服务证明如下，可以看到下方是V9.3.5u.6095的版本。



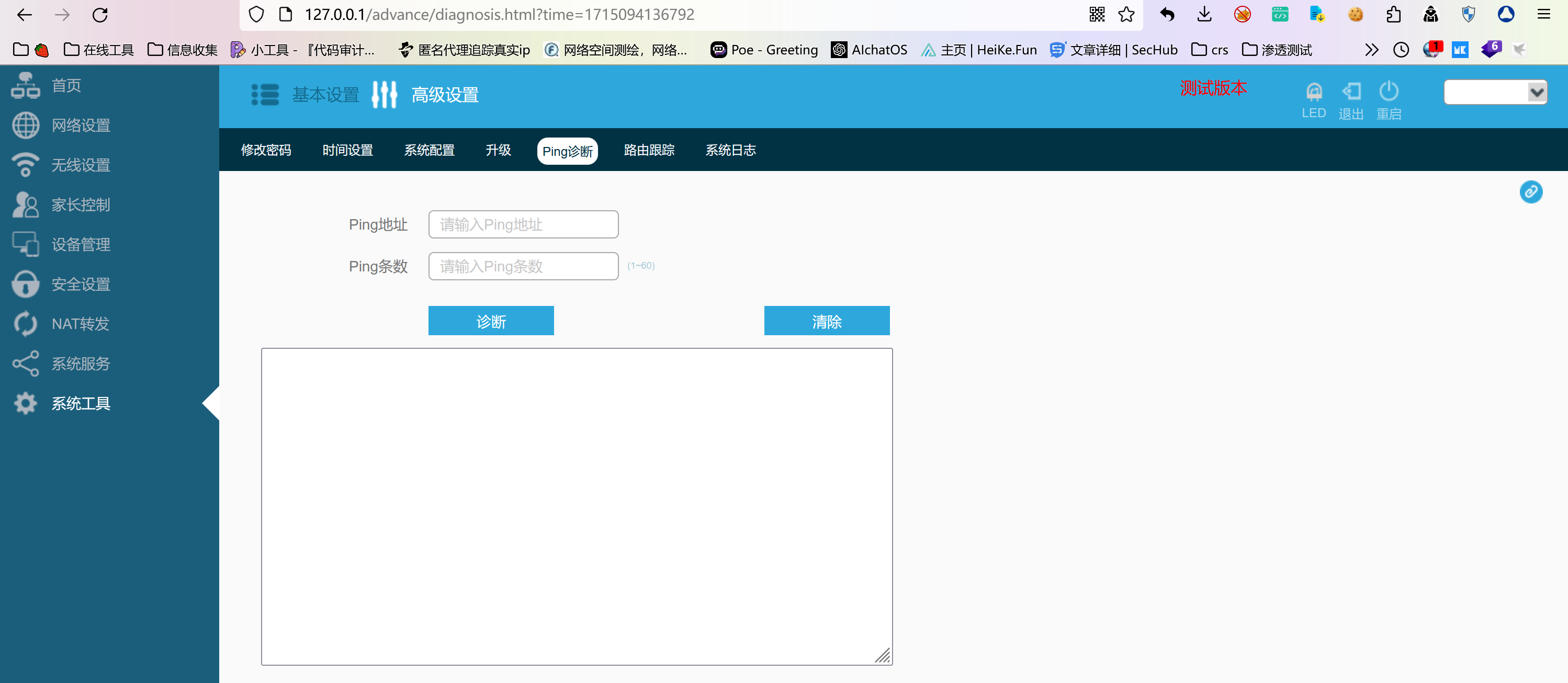
### 命令执行漏洞

访问<http://127.0.0.1/advance/changepwd.html?time=1715093812978>

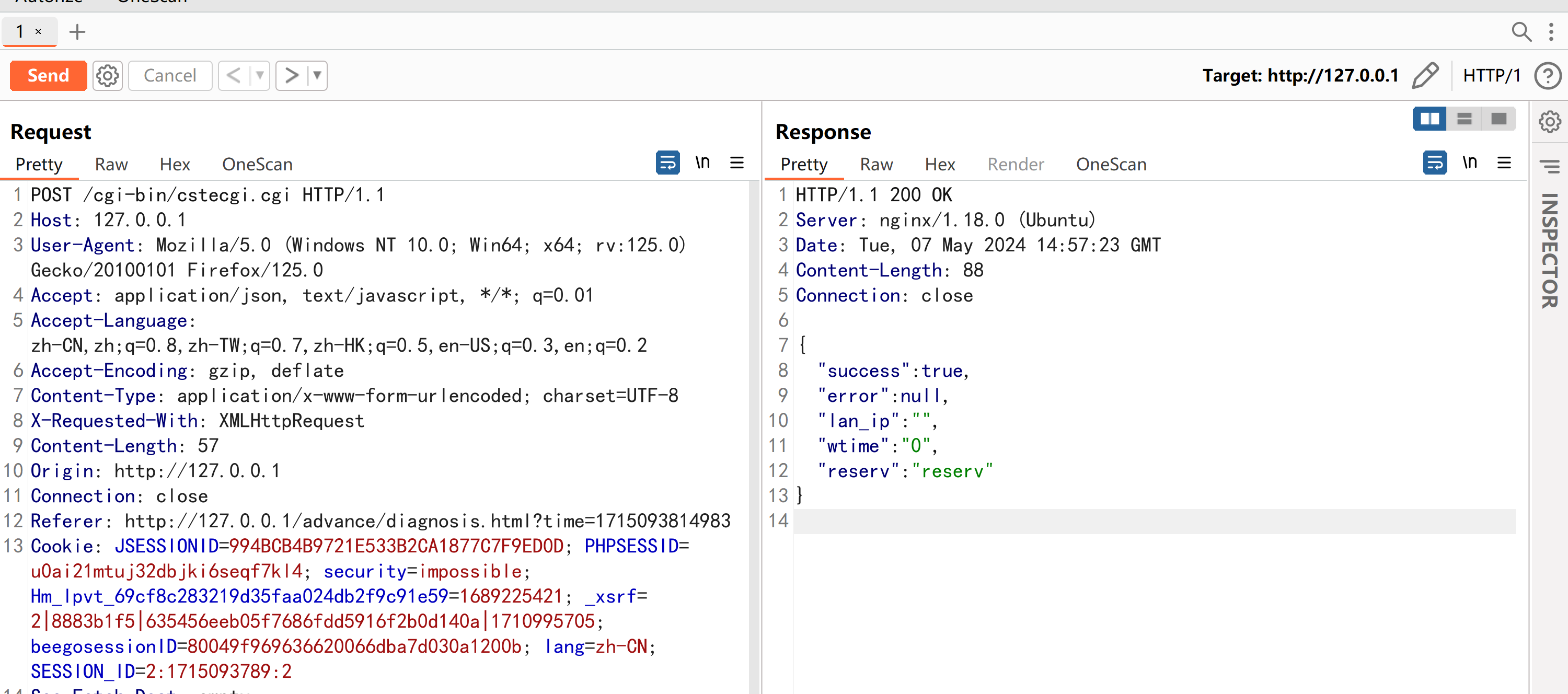
*进入后台页面*

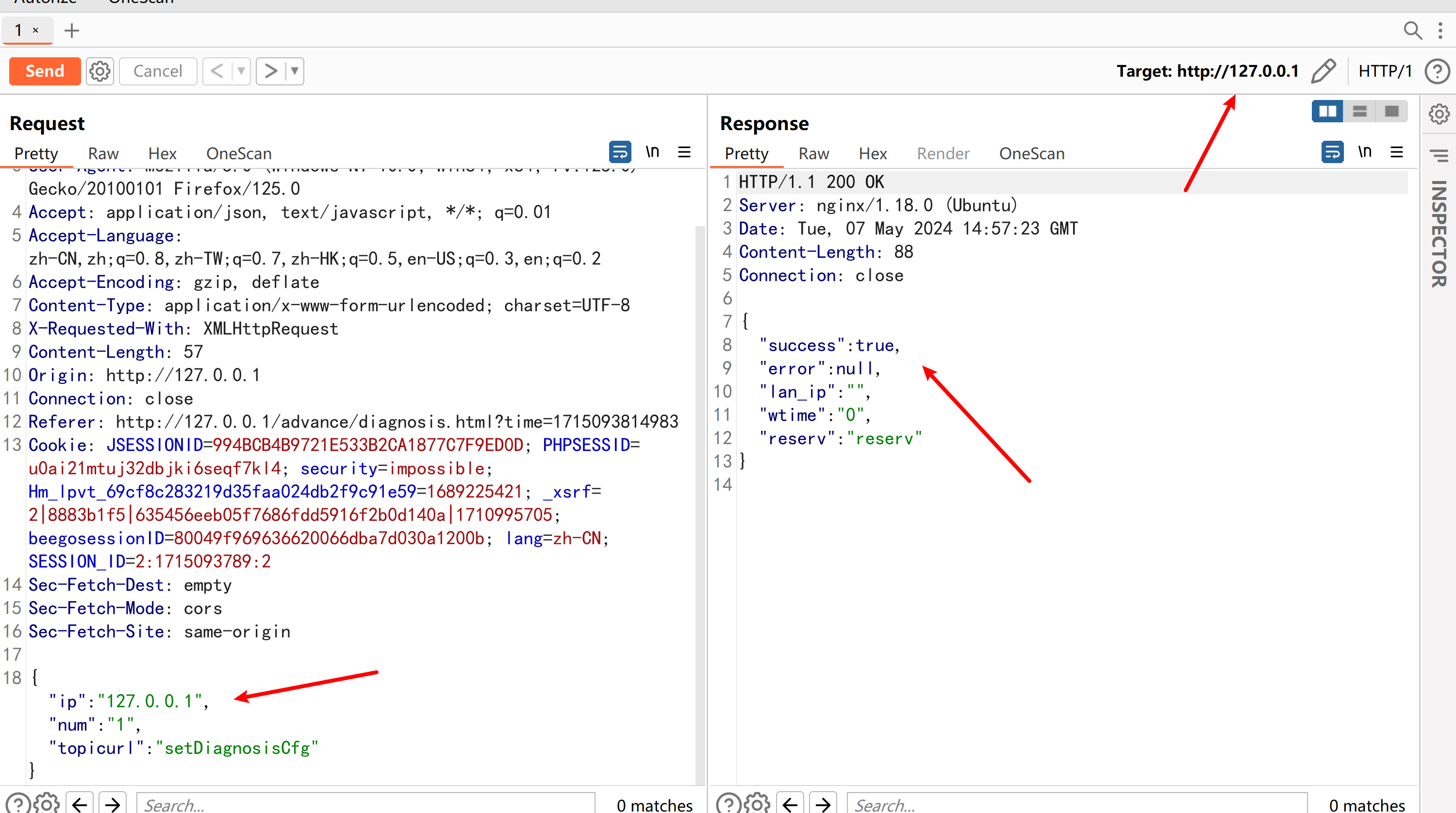


系统工具里有个ping诊断：



输入127.0.0.1 1条数抓包，点击发包

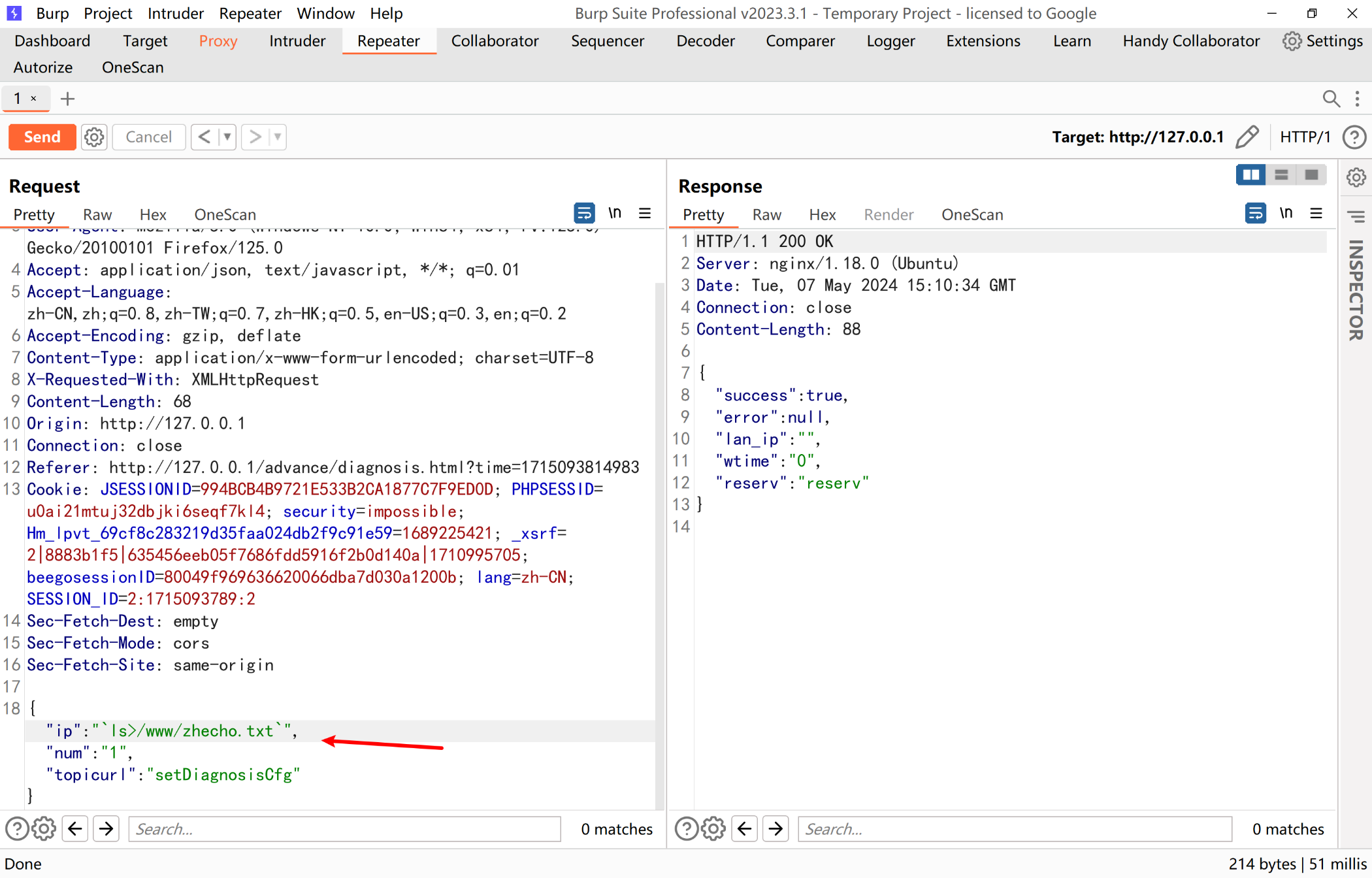




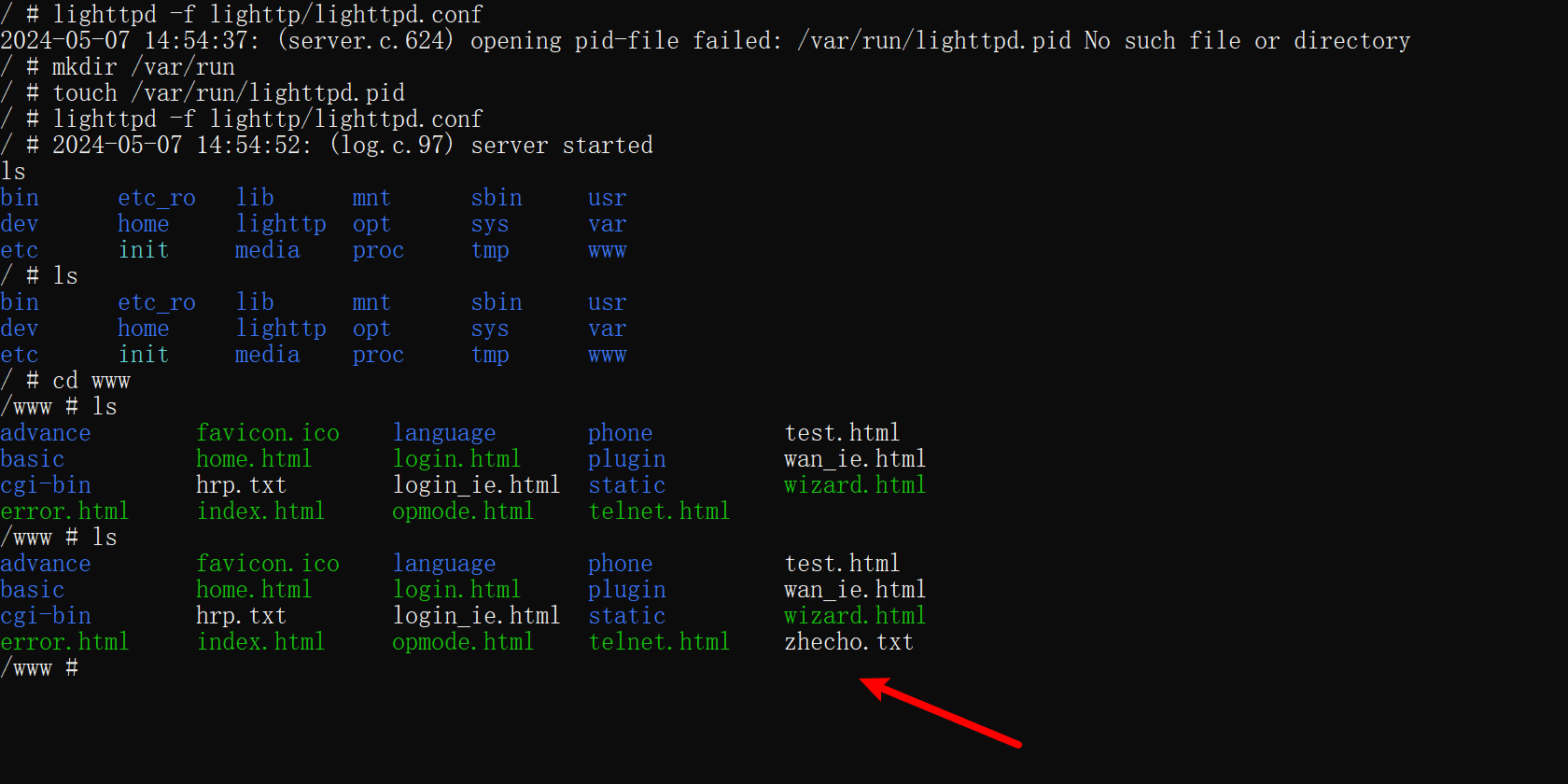
发现成功发送ping命令测试语句。

这里将payload进行修改，修改恶意命令为可以任意写入文件到服务器：

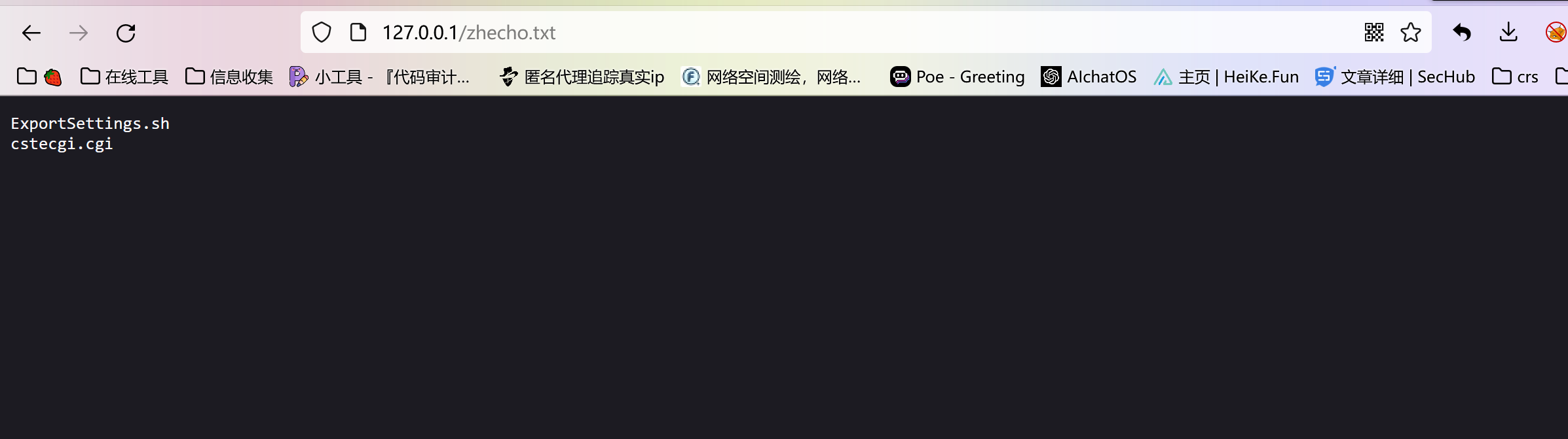
{"ip":"`ls>/www/zhecho.txt`","num":"1","topicurl":"setDiagnosisCfg"}



发包成功，接着到固件系统查ls命令查看，发现成功创建该zhecho.txt文件：



访问下：



可以看到成功创建了zhecho.txt文件，命令执行成功。