目录

[Tenda ac23 版本V16.03.07.39\_cn 2](#_Toc126236603)

[fromSetSysTime->sub\_196104->strcpy((char \*)v6, s); timeZone参数存在栈溢出 2](#_Toc126236604)

[Tenda ac23 版本信息：V16.03.07.45\_cn 4](#_Toc126236605)

[formWifiBasicSet->sub\_451DF8->sub\_450EE4 ->v18； 4](#_Toc126236606)

[saveParentControlInfo函数存在字符串溢出 参数deviceId 5](#_Toc126236607)

[saveParentControlInfo->compare\_parentcontrol\_time函数存在栈溢出Time参数 6](#_Toc126236608)

[formSetPPTPServer->sub\_4781A4函数存在栈溢出 8](#_Toc126236609)

[fromSetRouteStatic->save\_staticroute\_data存在栈溢出漏洞 9](#_Toc126236610)

[formSetVirtualSer->save\_virtualser\_data 11](#_Toc126236611)

[mDMZSetCfg函数参数dmzIp存在栈溢出 12](#_Toc126236612)

[fromSetIpMacBind->sub\_48E668栈溢出 参数list->sub\_48E668中触发栈溢出 13](#_Toc126236613)

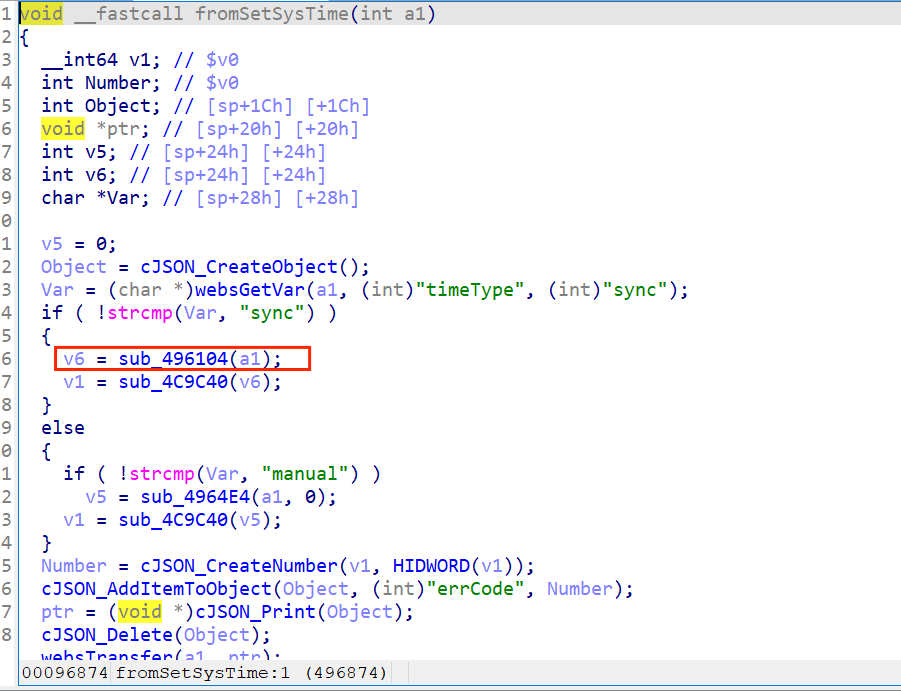
[formSetRebootTimer->sub\_497154栈溢出：参数rebootTime->sub\_497154触发栈溢出 15](#_Toc126236614)

[fromAdvSetMacMtuWan存在栈溢出漏洞 16](#_Toc126236615)

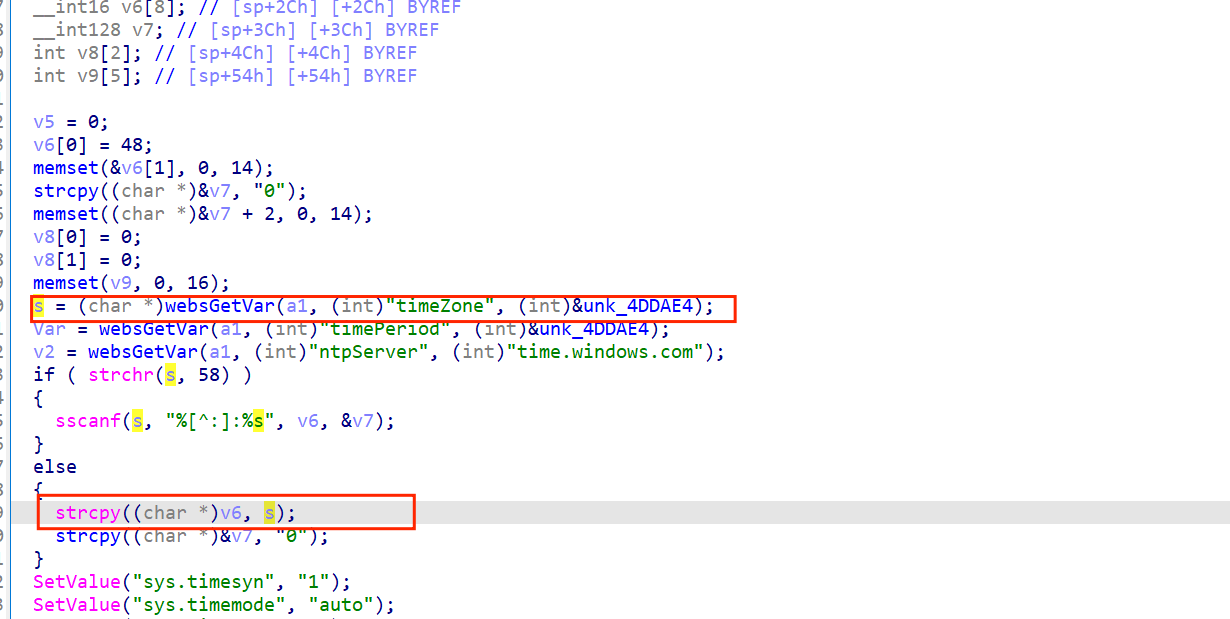
[formWifiBasicSet->sub\_451DF8->sub\_450EE4->sub\_450A4C 19](#_Toc126236616)

# Tenda ac23 版本V16.03.07.39\_cn

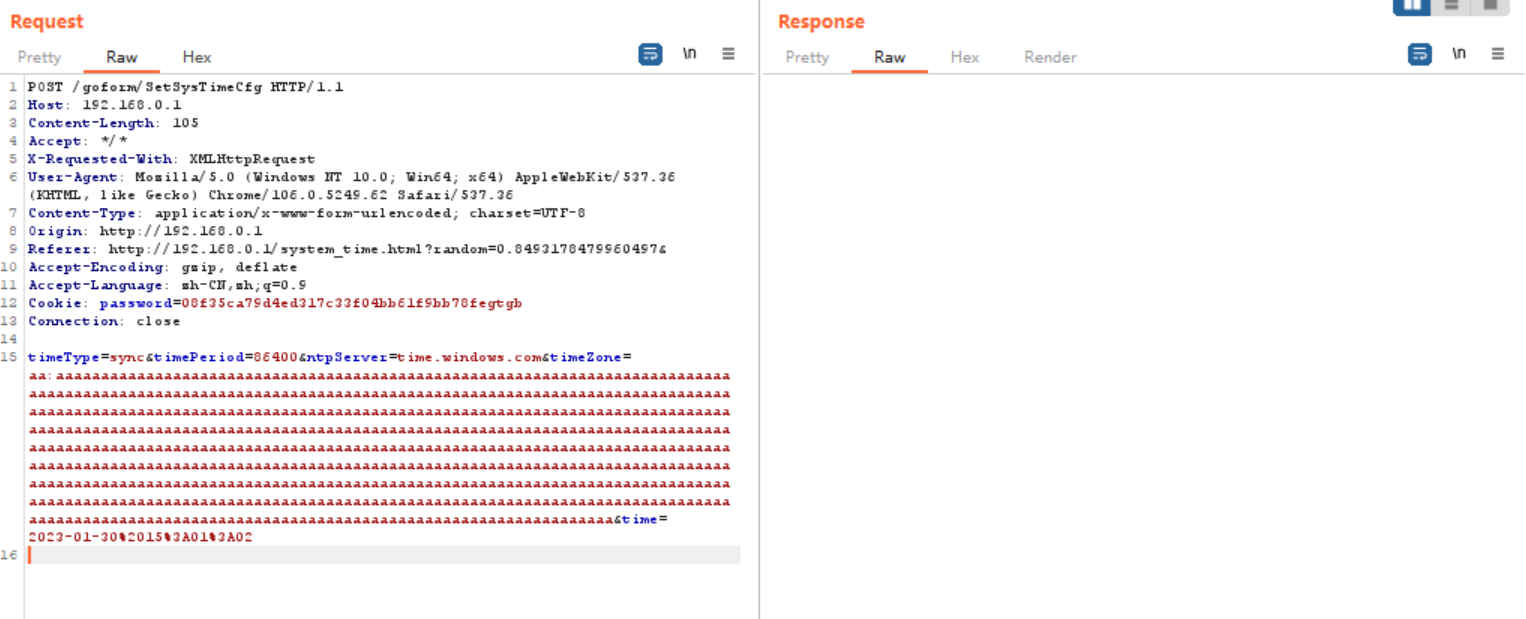
## fromSetSysTime->sub\_196104->strcpy((char \*)v6, s); timeZone参数存在栈溢出



由于v6只有8个字节，当传入过多时触发栈溢出。



Poc：



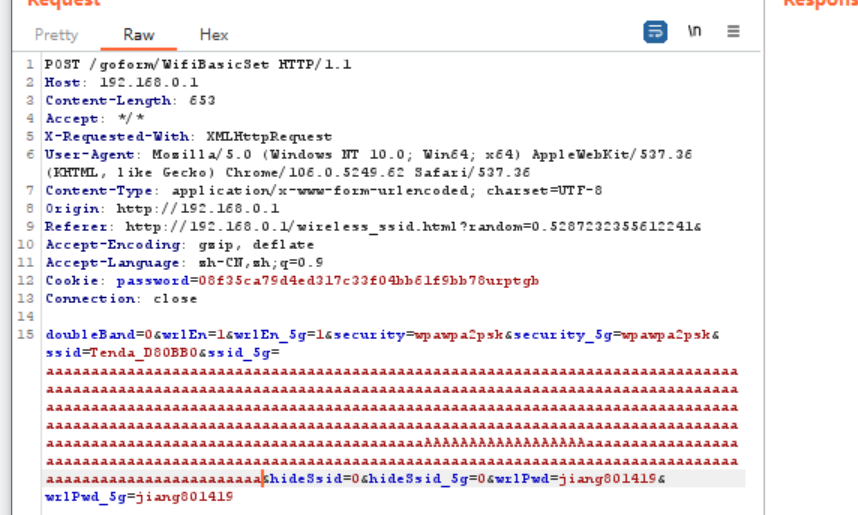
# Tenda ac23 版本信息：V16.03.07.45\_cn

## formWifiBasicSet->sub\_451DF8->sub\_450EE4 ->v18；

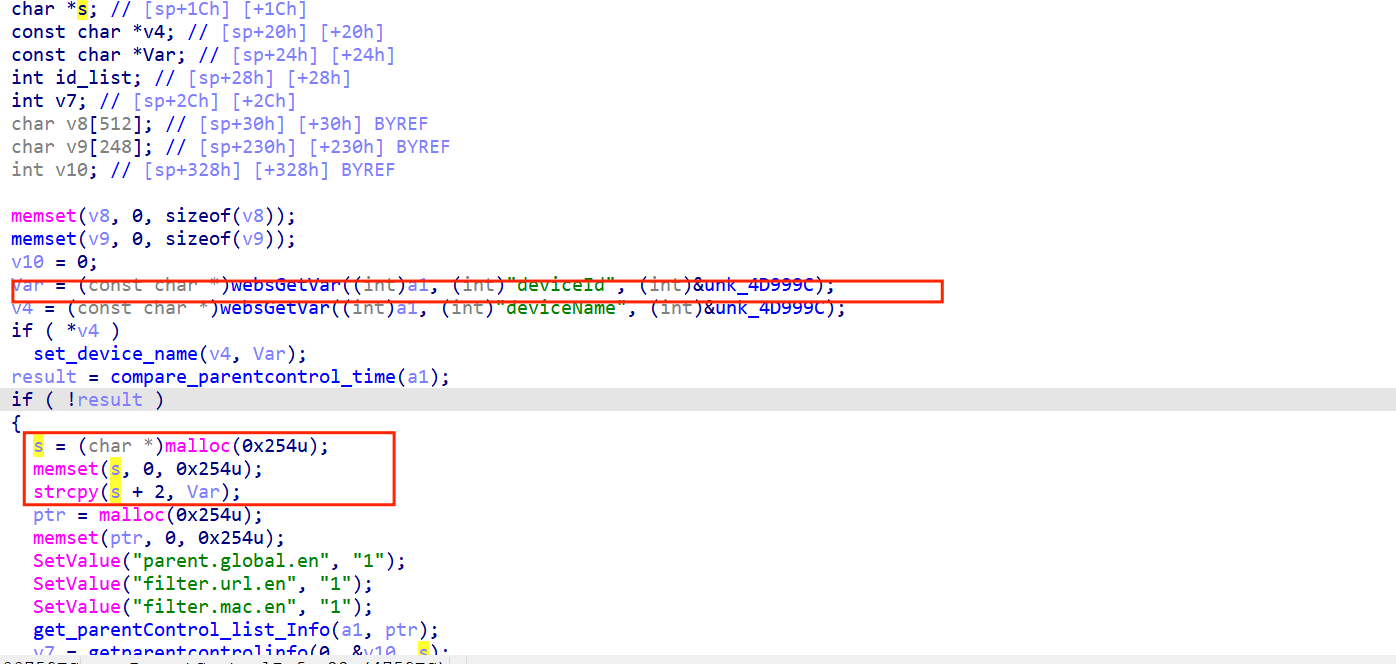
当用户提交参数长度过多时会导致set\_idx\_to\_mib给v18超出范围导致栈溢出



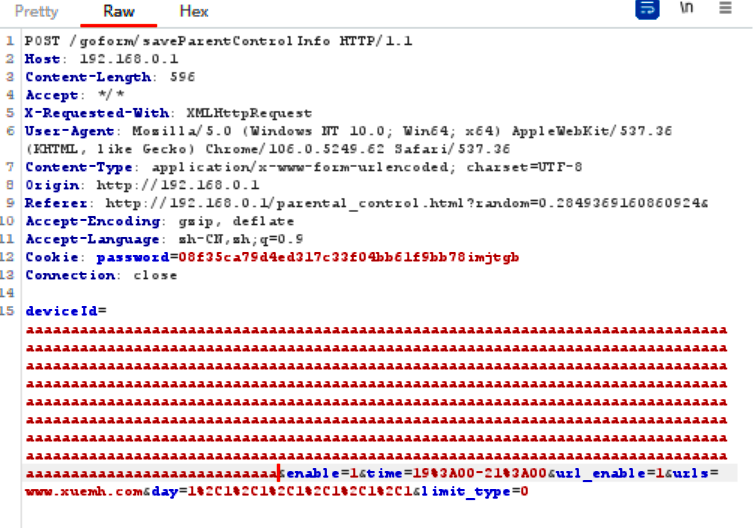
poc:



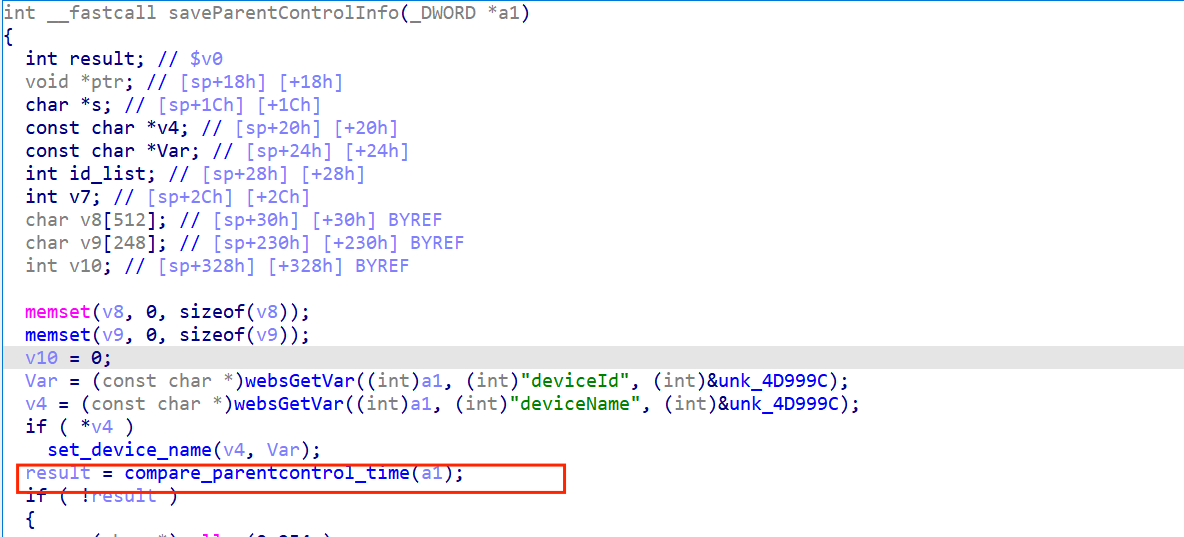
## saveParentControlInfo函数存在字符串溢出 参数deviceId

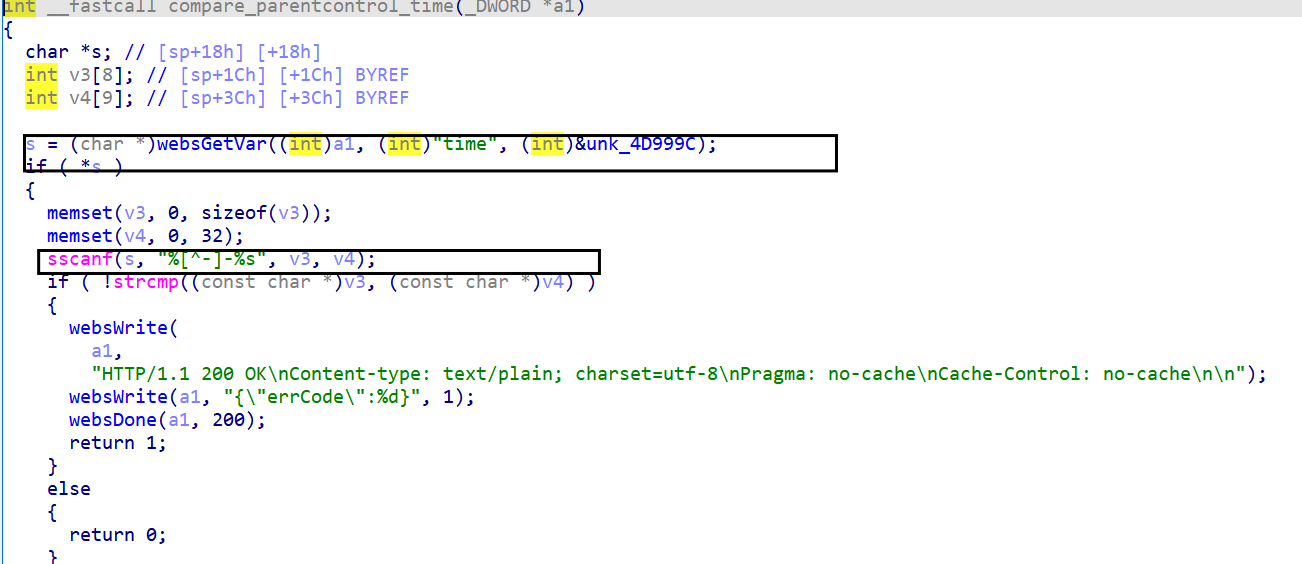


Poc：



## saveParentControlInfo->compare\_parentcontrol\_time函数存在栈溢出Time参数

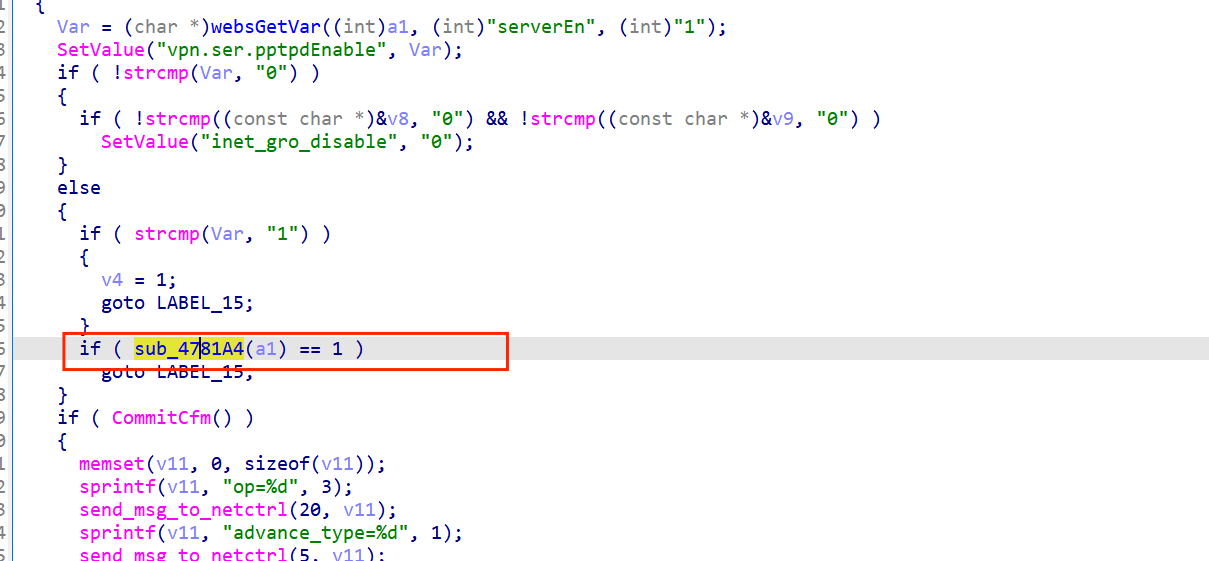




Poc:



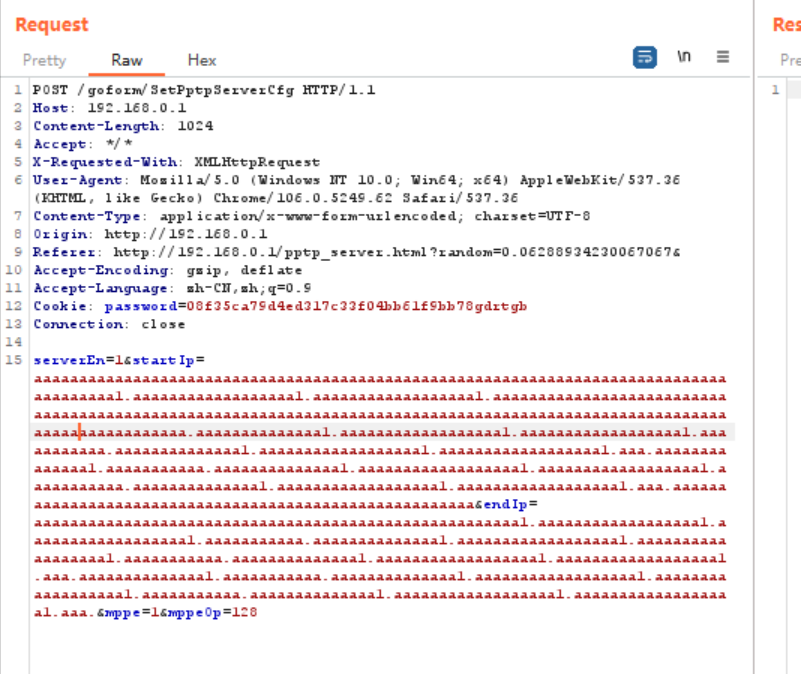
## formSetPPTPServer->sub\_4781A4函数存在栈溢出



Sub\_4781A4

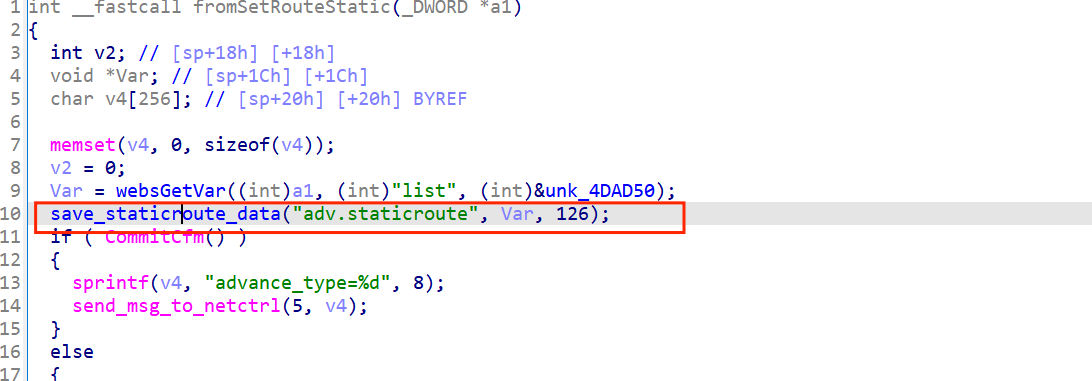


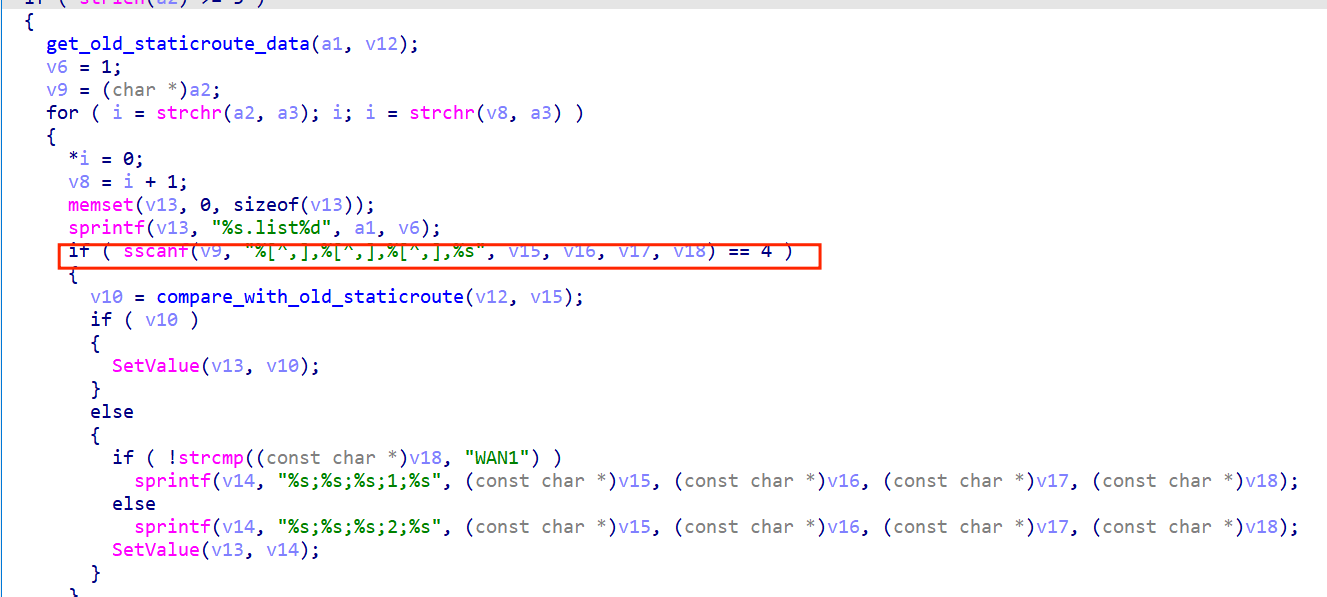
Poc：



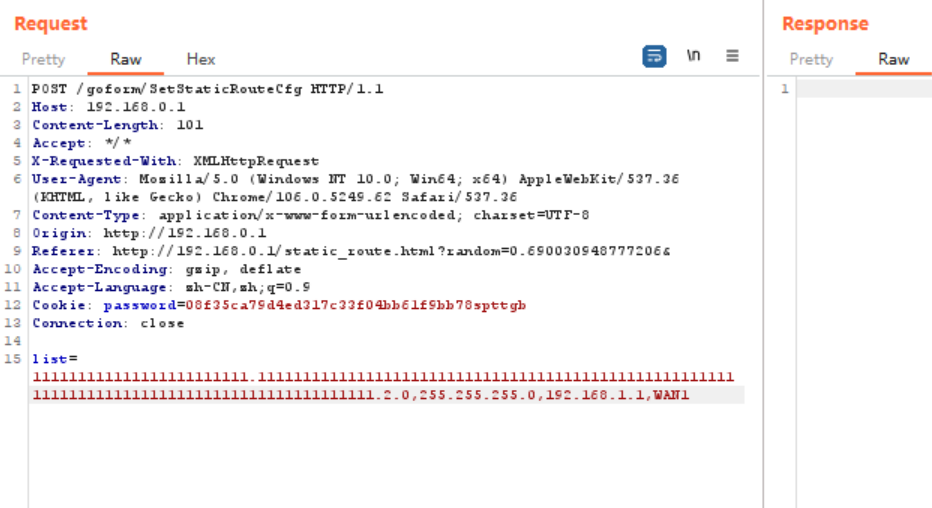
## fromSetRouteStatic->save\_staticroute\_data存在栈溢出漏洞

参数list传给save\_staticroute\_data 导致无限这复制从而栈溢出

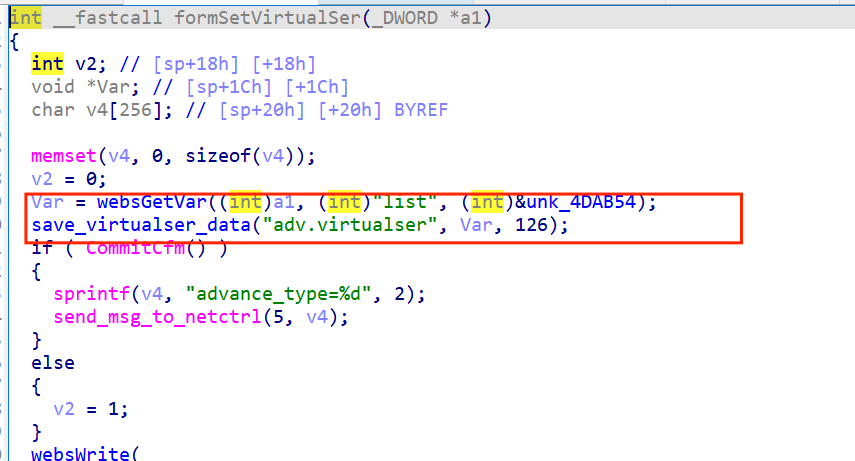


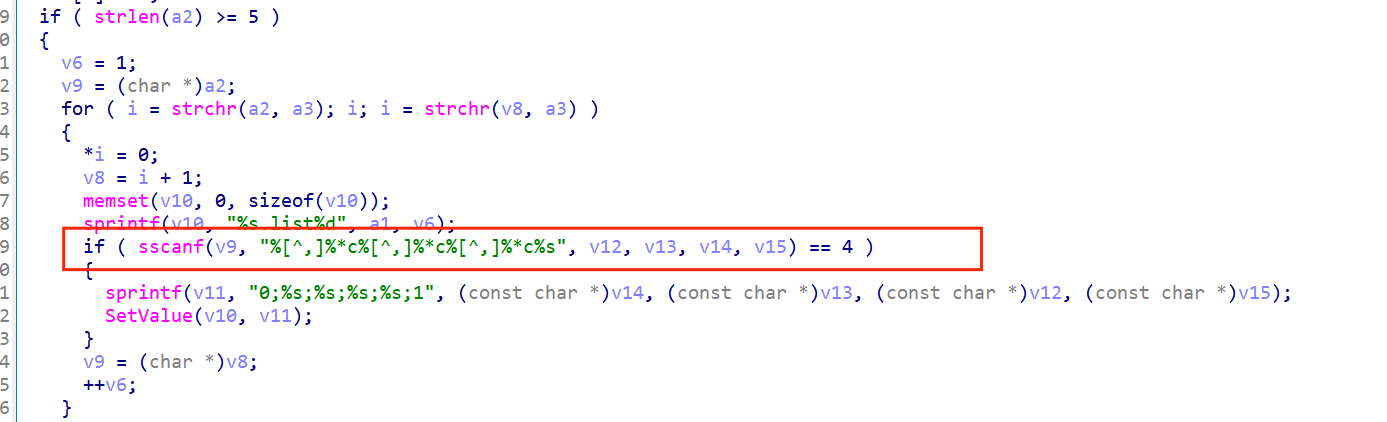


Poc：

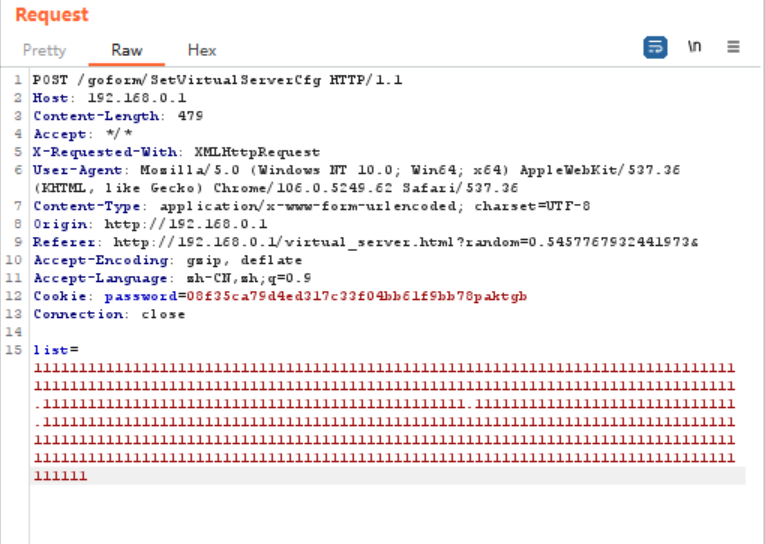


## formSetVirtualSer->save\_virtualser\_data

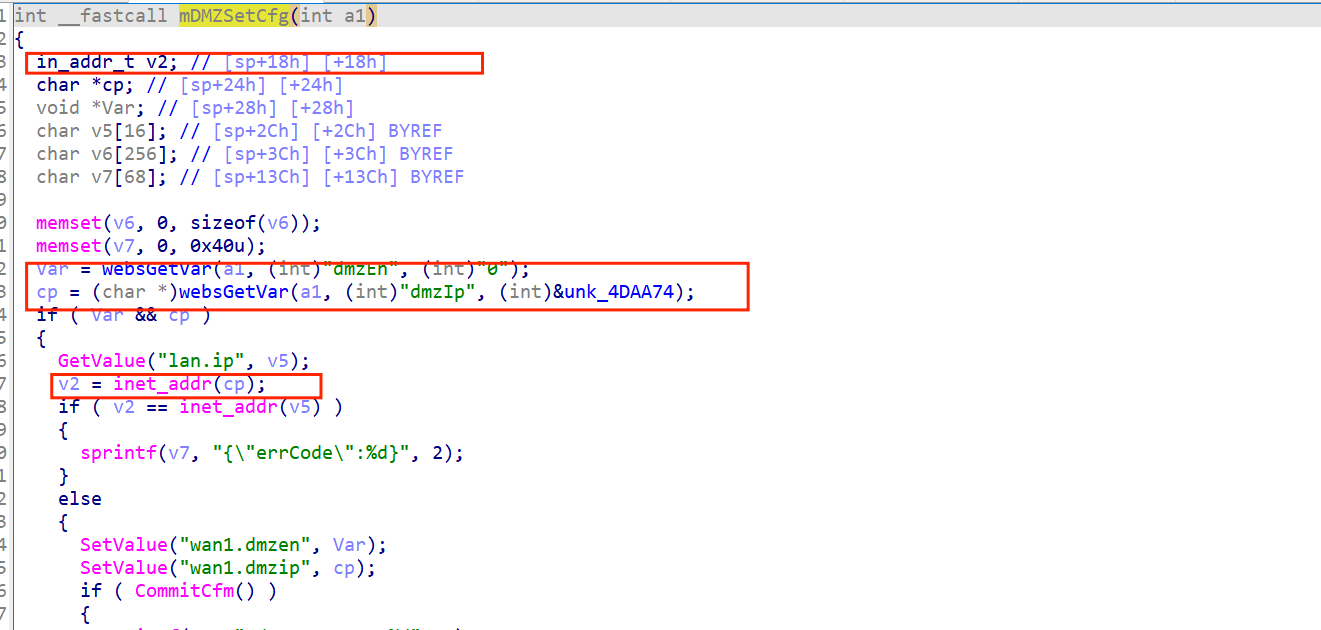


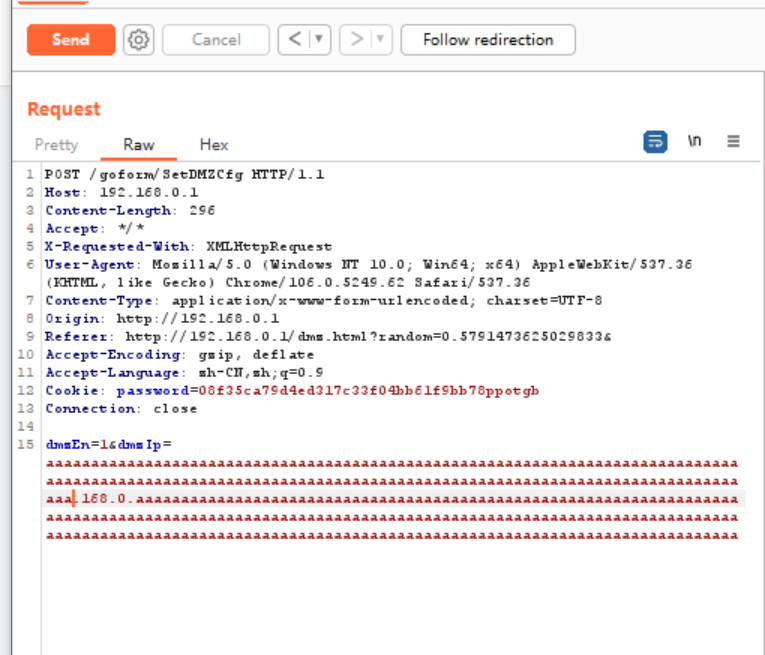


Poc:

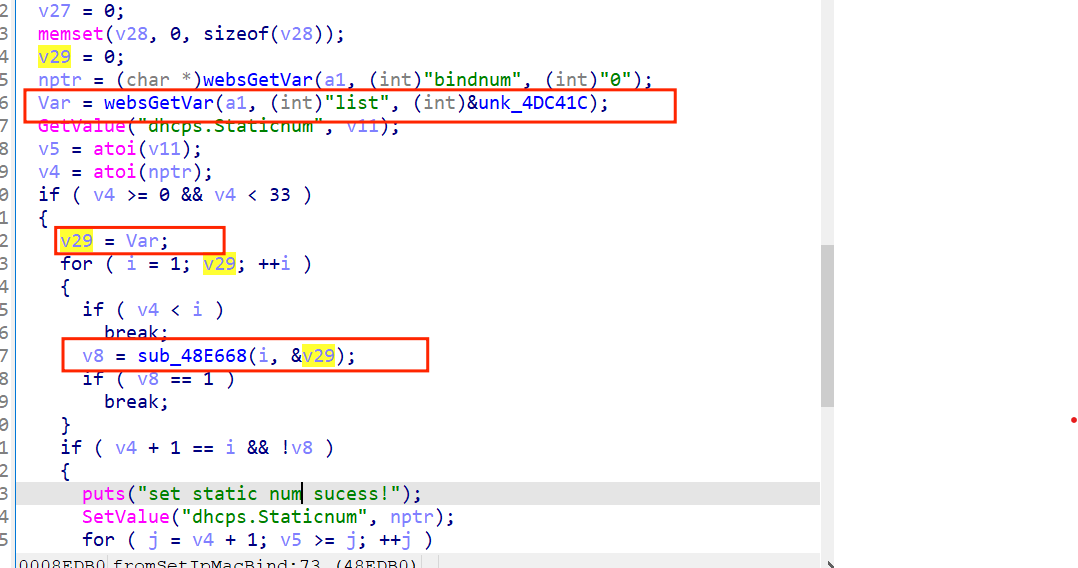


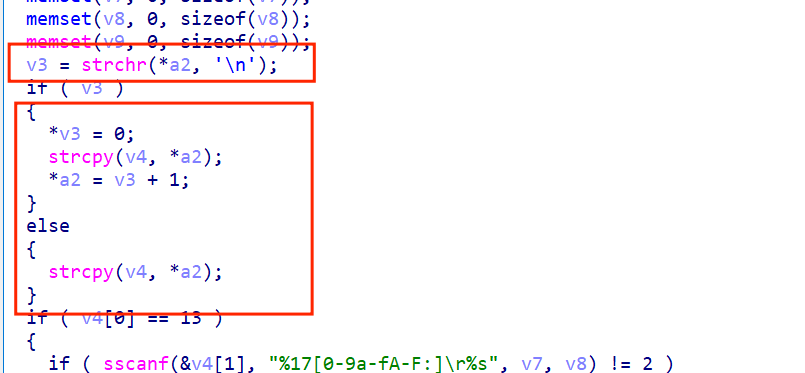
## mDMZSetCfg函数参数dmzIp存在栈溢出



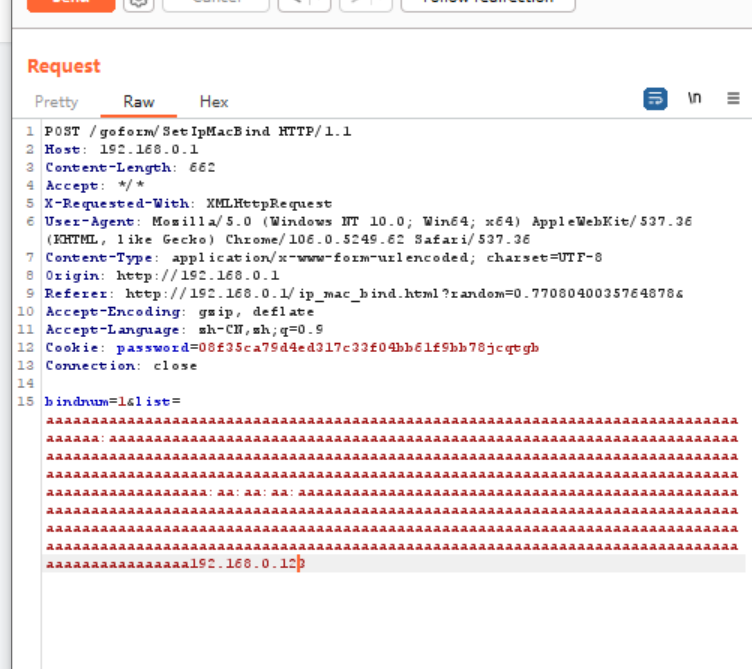


## fromSetIpMacBind->sub\_48E668栈溢出 参数list->sub\_48E668中触发栈溢出

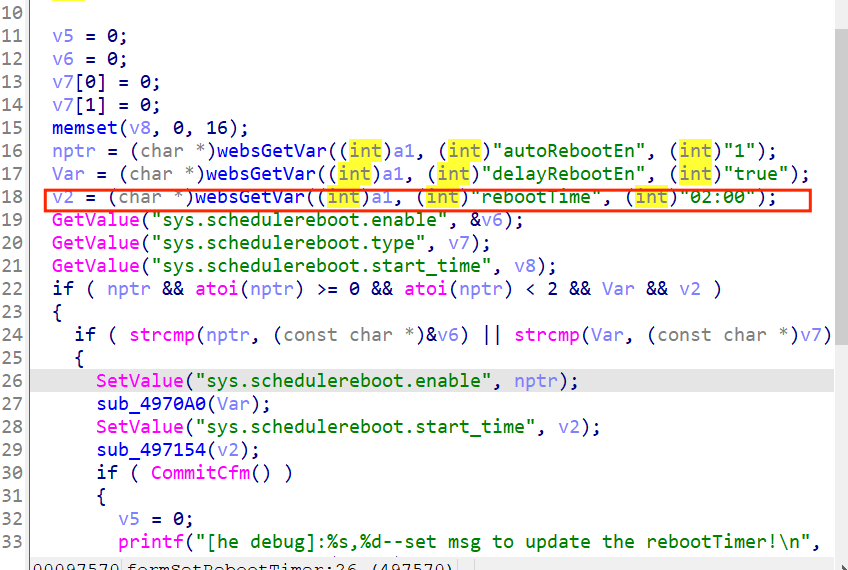


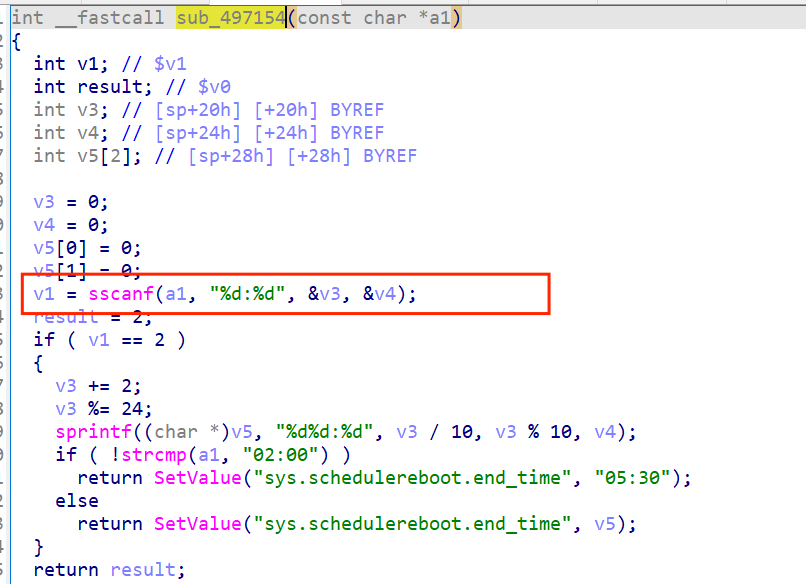


Poc

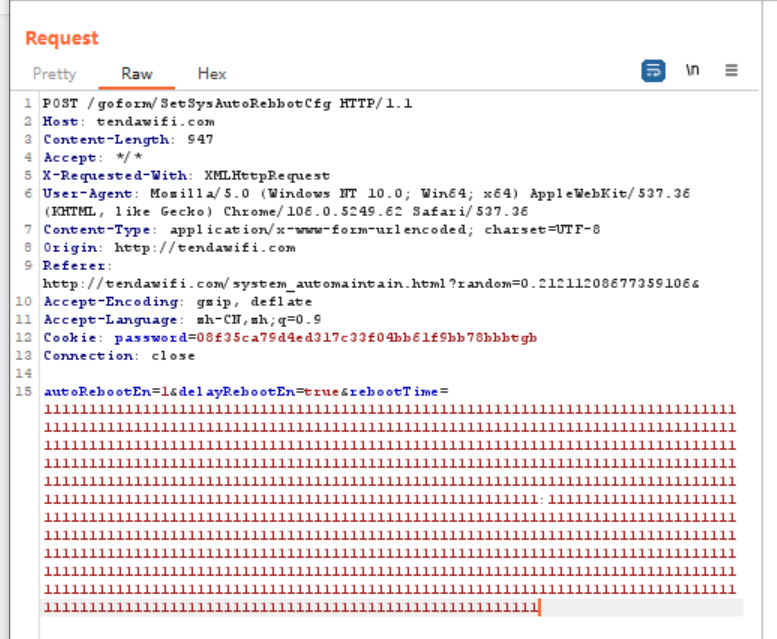


## formSetRebootTimer->sub\_497154栈溢出：参数rebootTime->sub\_497154触发栈溢出



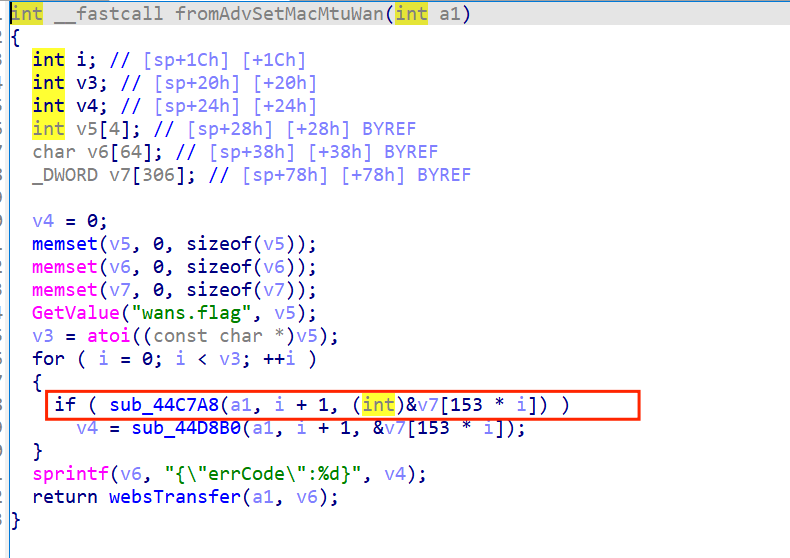


Poc：



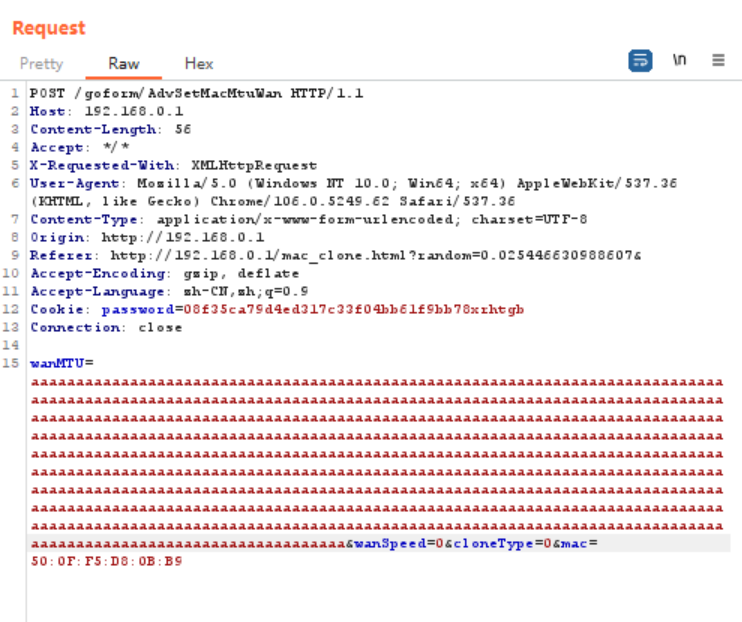
## fromAdvSetMacMtuWan存在栈溢出漏洞

触发函数sub\_44C7A8：





Poc：



## formWifiBasicSet->sub\_451DF8->sub\_450EE4->sub\_450A4C

