目录

[Tenda ac23 版本V16.03.07.39\_cn 2](#_Toc126258643)

[1. fromSetSysTime->sub\_196104->strcpy((char \*)v6, s); There is a stack overflow in the timeZone parameter 2](#_Toc126258644)

[Tenda ac23 版本信息：V16.03.07.45\_cn 4](#_Toc126258645)

[1. formWifiBasicSet->sub\_451DF8->sub\_450EE4 ->v18； 4](#_Toc126258646)

[2. The saveParentControlInfo function has a string overflow parameter deviceId.String overflow due to insufficient storage space allocation 5](#_Toc126258647)

[3. The saveParentControlInfo->compare\_parentcontrol\_time function has a stack overflow time parameter 6](#_Toc126258648)

[4. formSetPPTPServer->sub\_4781A4 function has a stackoverflow 7](#_Toc126258649)

[5. fromSetRouteStatic->save\_staticroute\_data has a stack overflow vulnerability 8](#_Toc126258650)

[6. formSetVirtualSer->save\_virtualser\_data function a stack overflow vulnerability triggered by the list parameter 10](#_Toc126258651)

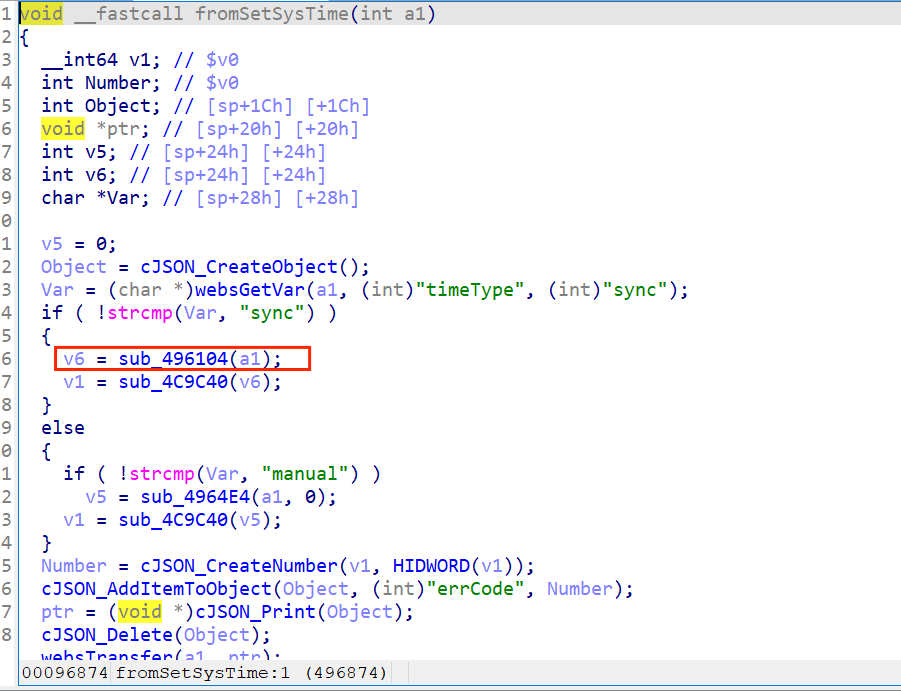
[7. The mDMZSetCfg function parameter dmzIp has a stack overflow is triggered by the list parameter 11](#_Toc126258652)

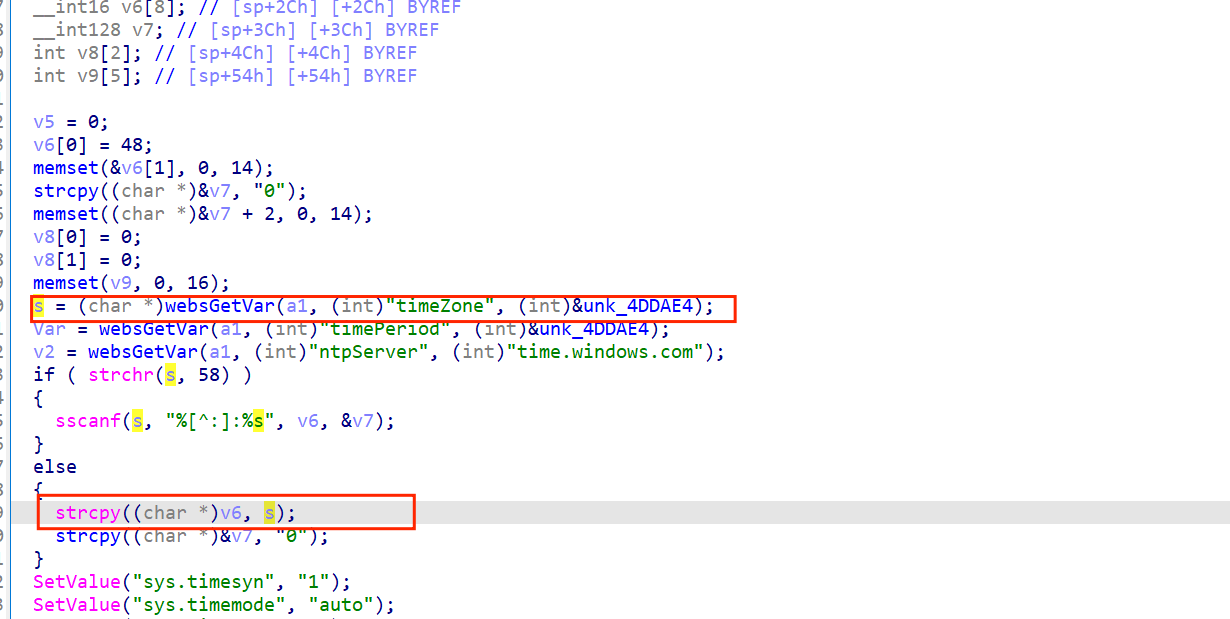
[8. formSetRebootTimer->sub\_497154 stack overflow: The parameter rebootTime->sub\_497154 triggers stack overflow 13](#_Toc126258653)

[9. fromAdvSetMacMtuWan has a stack overflow vulnerability.Trigger function sub\_44C7A8 15](#_Toc126258654)

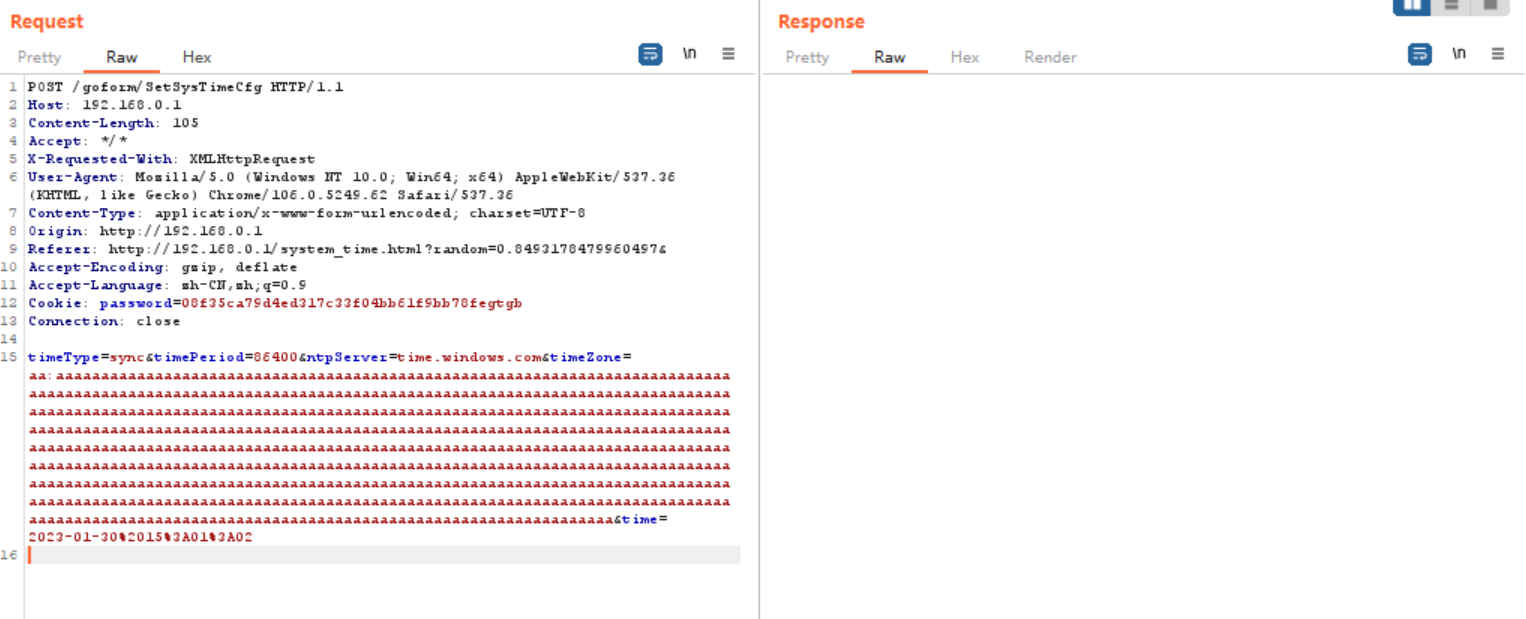
# Tenda ac23 版本V16.03.07.39\_cn

## 1. fromSetSysTime->sub\_196104->strcpy((char \*)v6, s); There is a stack overflow in the timeZone parameter





Poc：

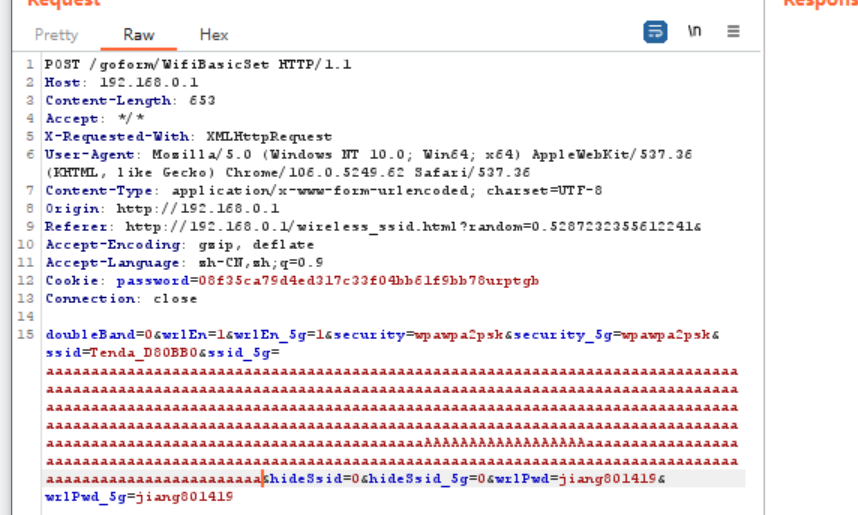


# Tenda ac23 版本信息：V16.03.07.45\_cn

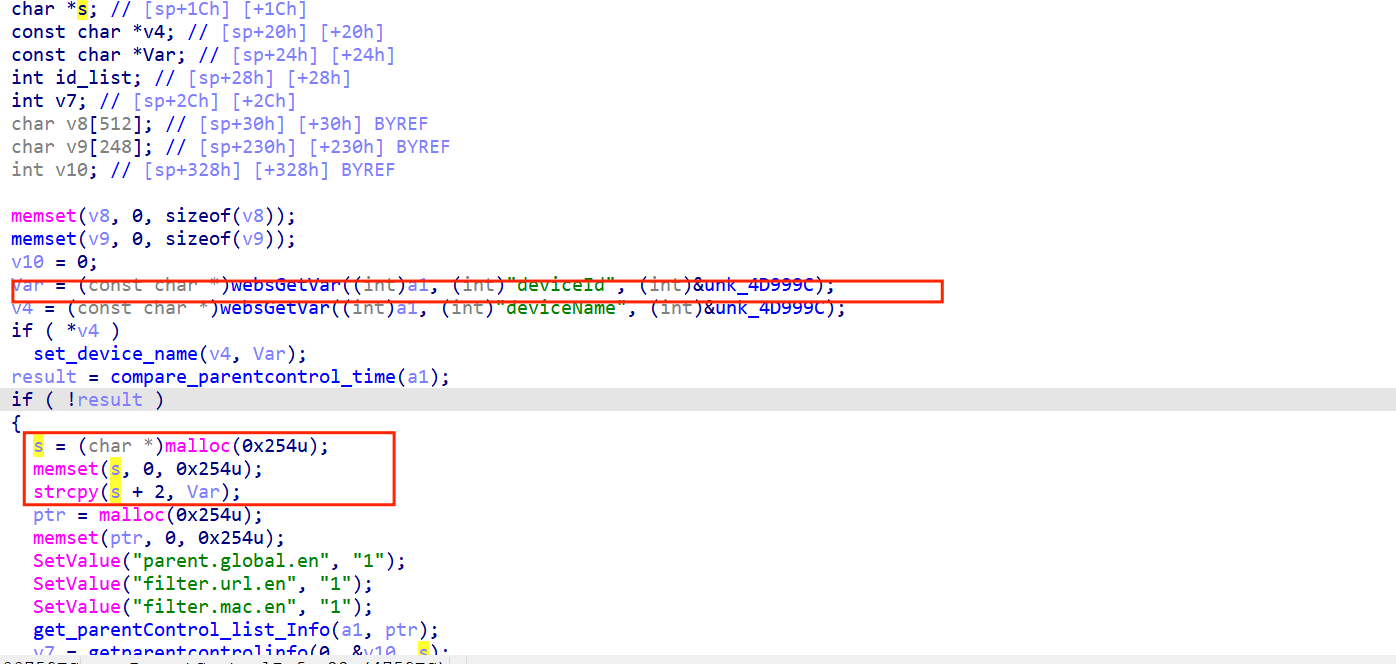
## 1. formWifiBasicSet->sub\_451DF8->sub\_450EE4 ->v18；

When the user submits too many parameters, it will cause the function to set\_idx\_to\_mib v18 beyond the preset range, resulting in stack overflow.

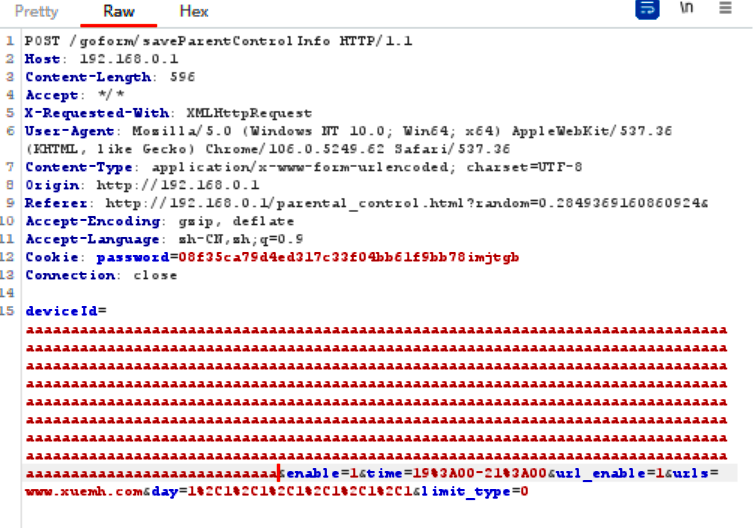
poc:



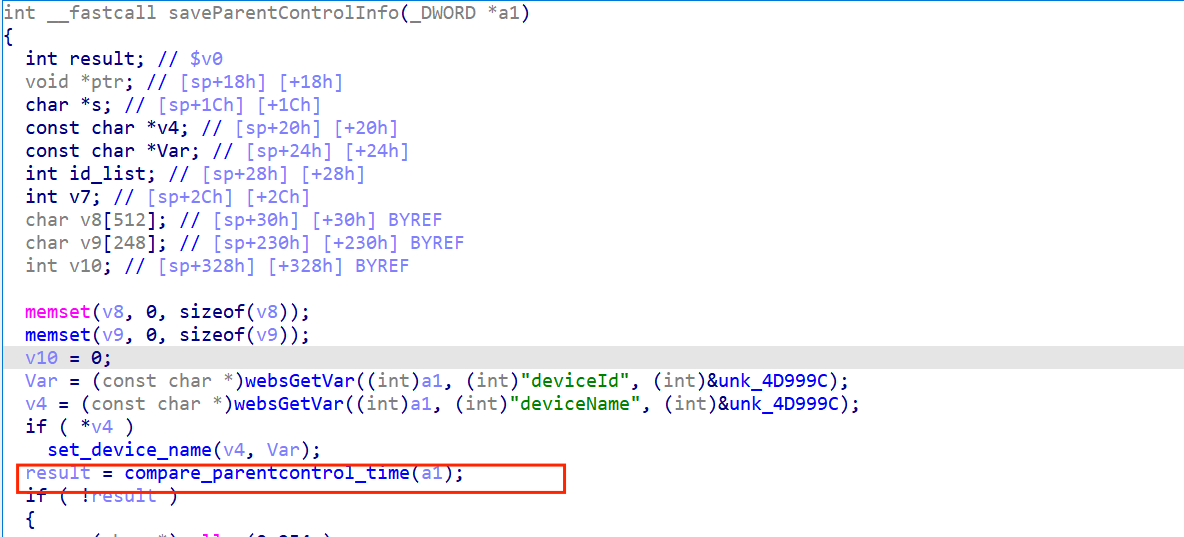
## 2. The saveParentControlInfo function has a string overflow parameter deviceId.String overflow due to insufficient storage space allocation

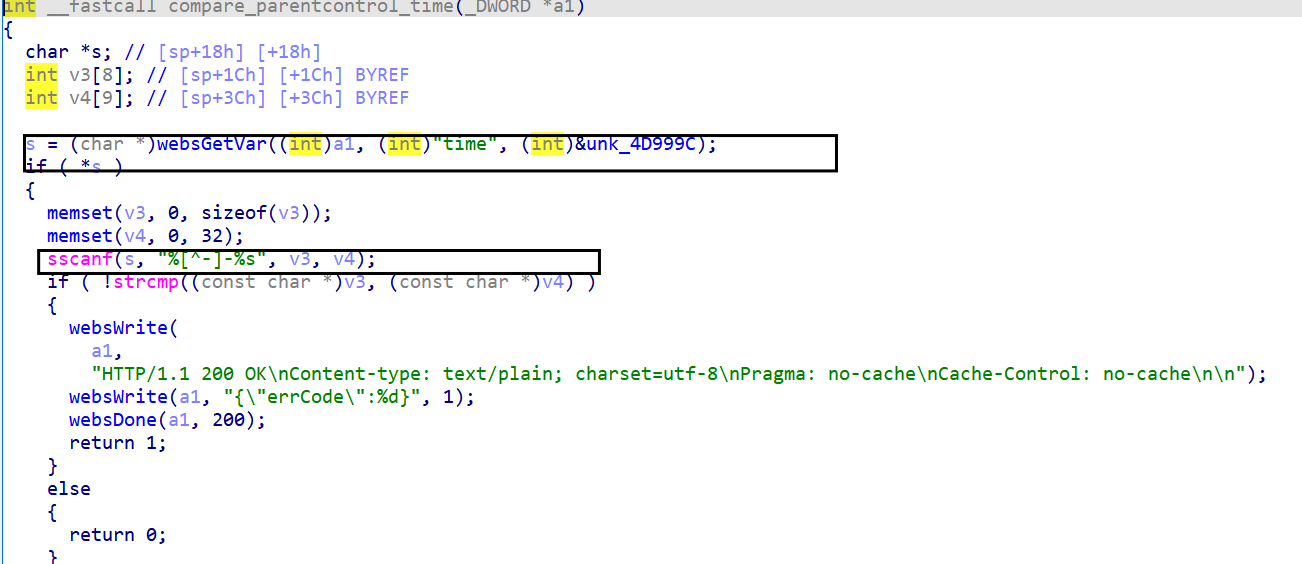


Poc：



## 3. The saveParentControlInfo->compare\_parentcontrol\_time function has a stack overflow time parameter

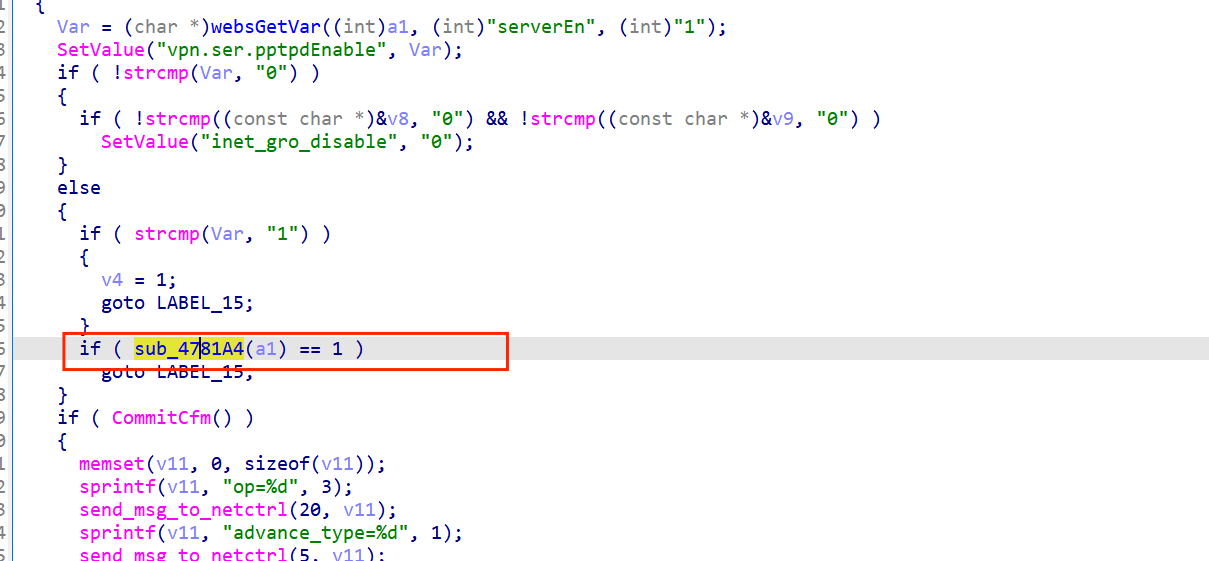




Poc:



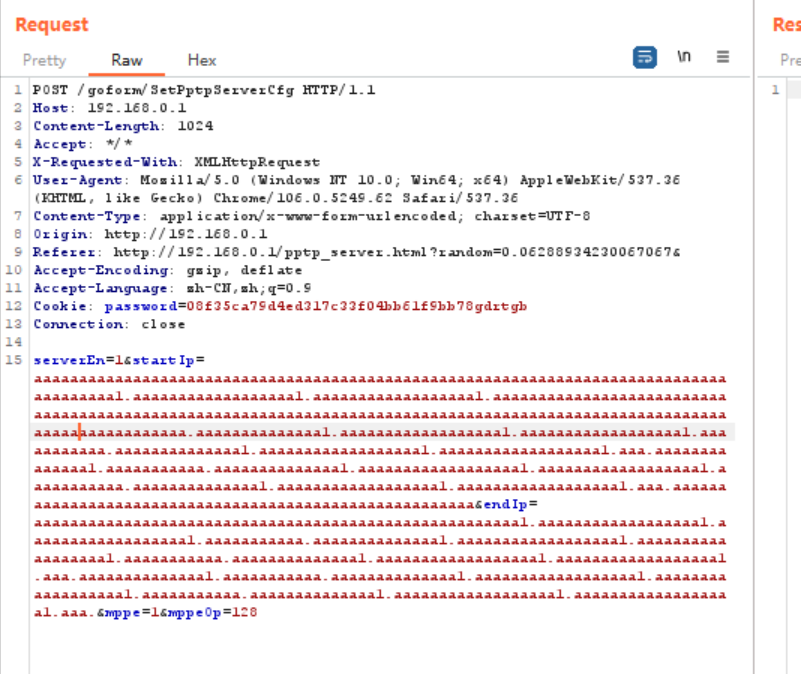
## 4. formSetPPTPServer->sub\_4781A4 function has a stackoverflow



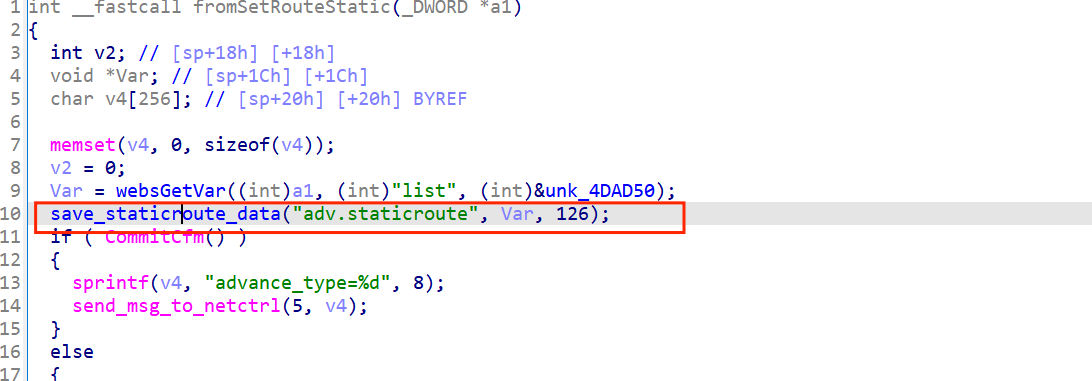
Sub\_4781A4

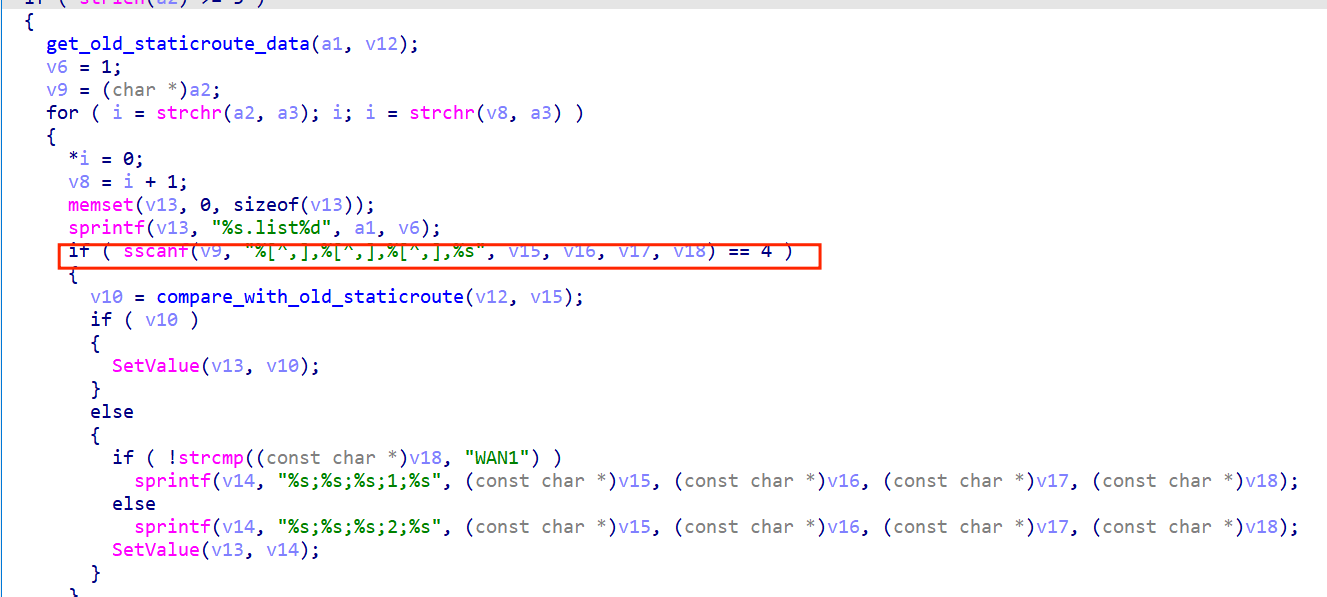


Poc：

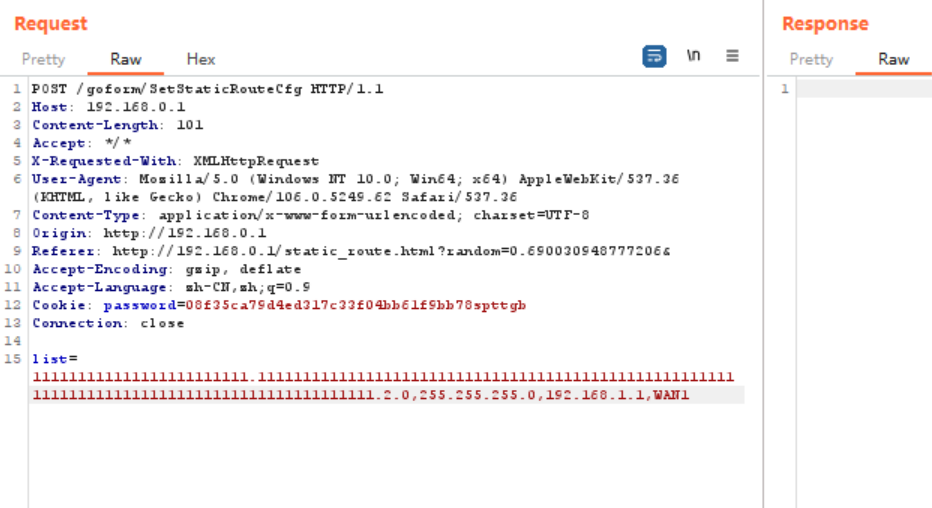


## 5. fromSetRouteStatic->save\_staticroute\_data has a stack overflow vulnerability

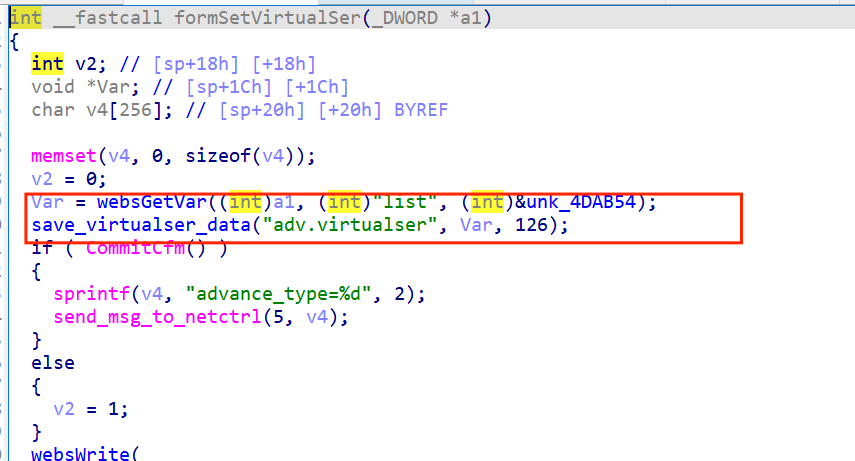
The parameter list is passed to save\_staticroute\_data causing this replication to be infinite, thus overflowing the stack 

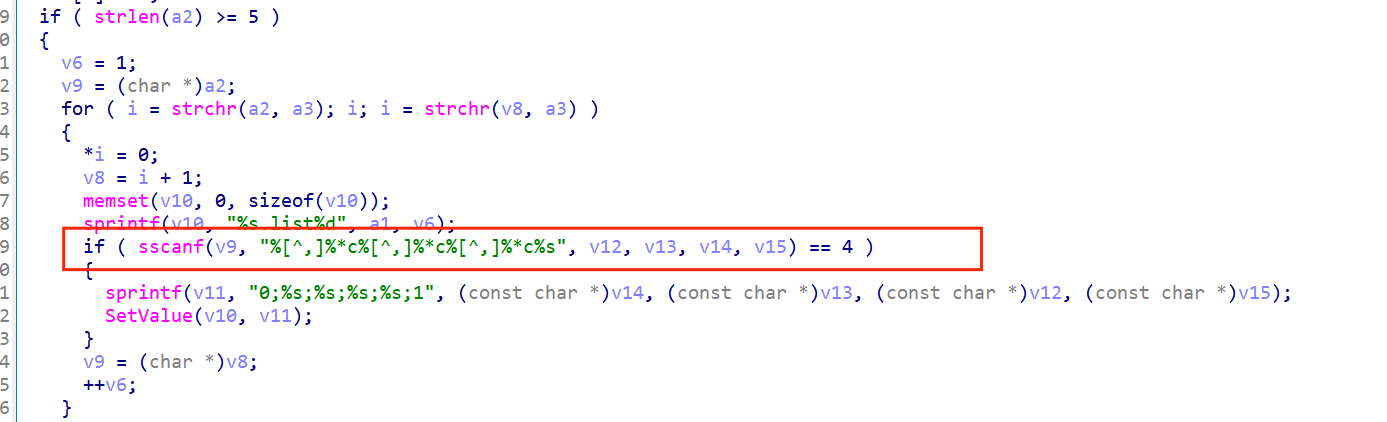


Poc：

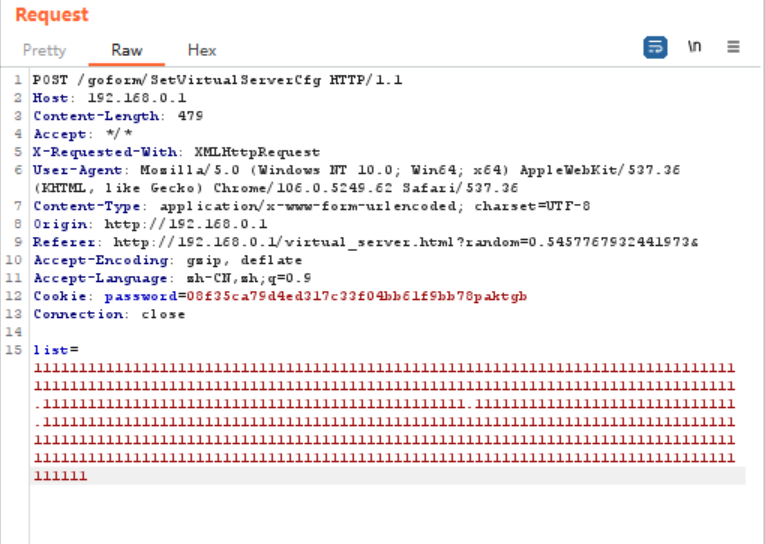


## 6. formSetVirtualSer->save\_virtualser\_data function a stack overflow vulnerability triggered by the list parameter

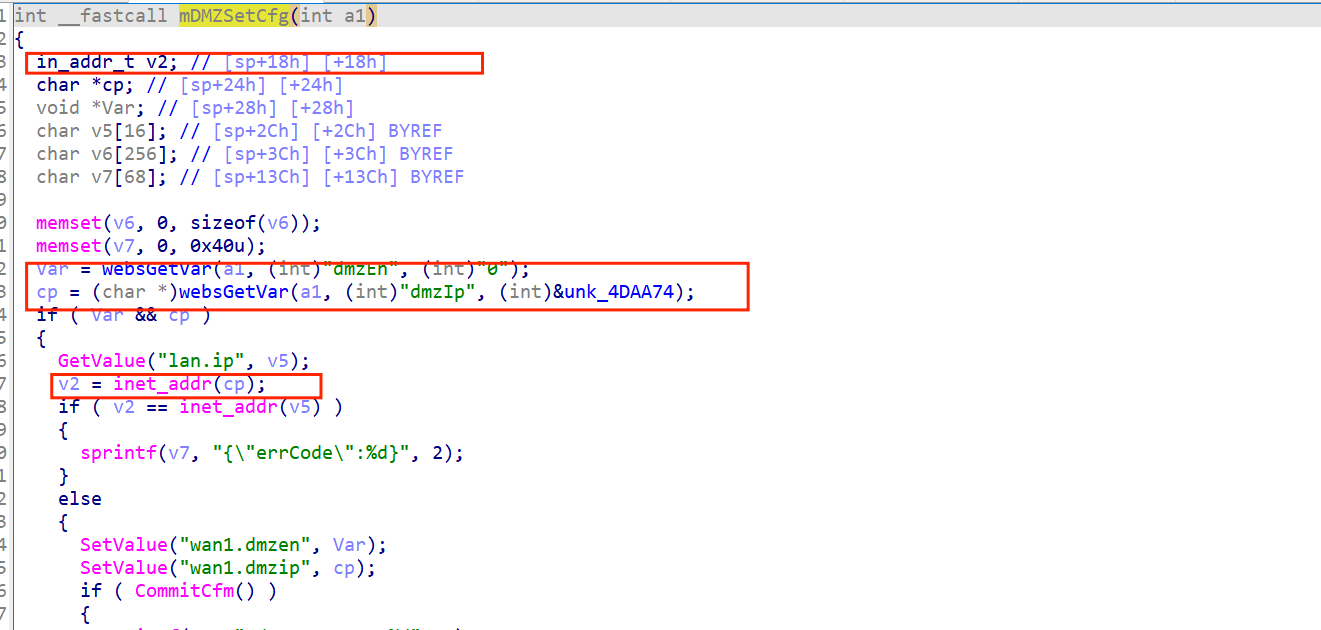


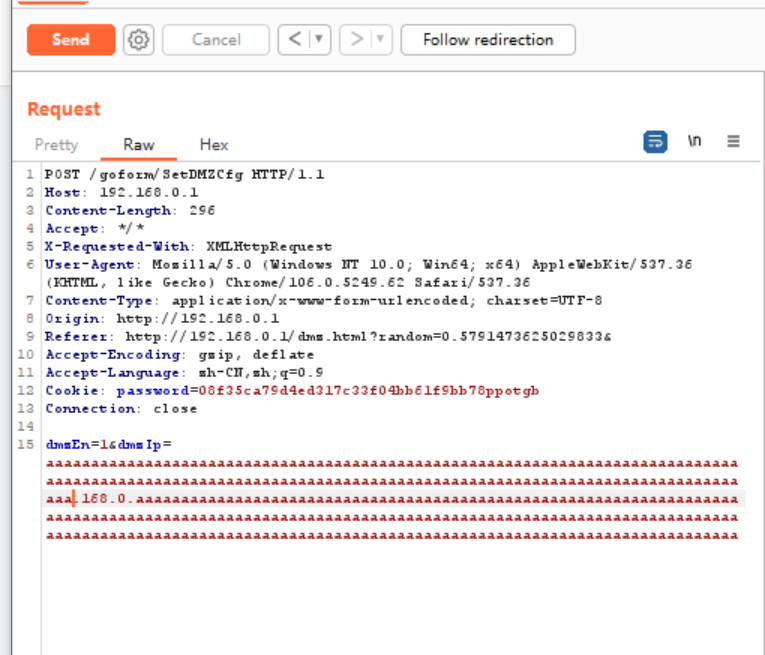


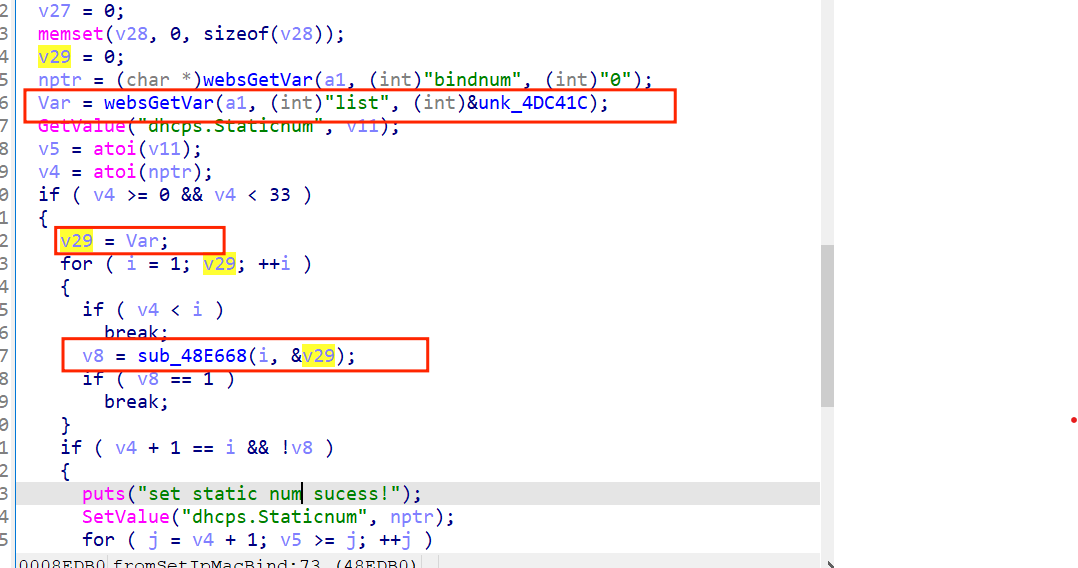
Poc:

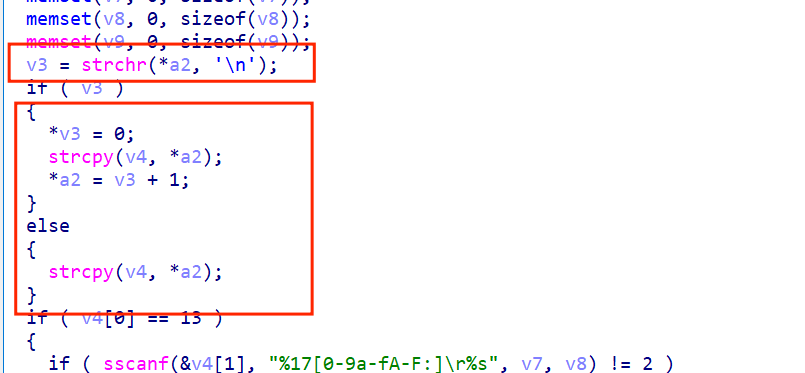


## 7. The mDMZSetCfg function parameter dmzIp has a stack overflow is triggered by the list parameter

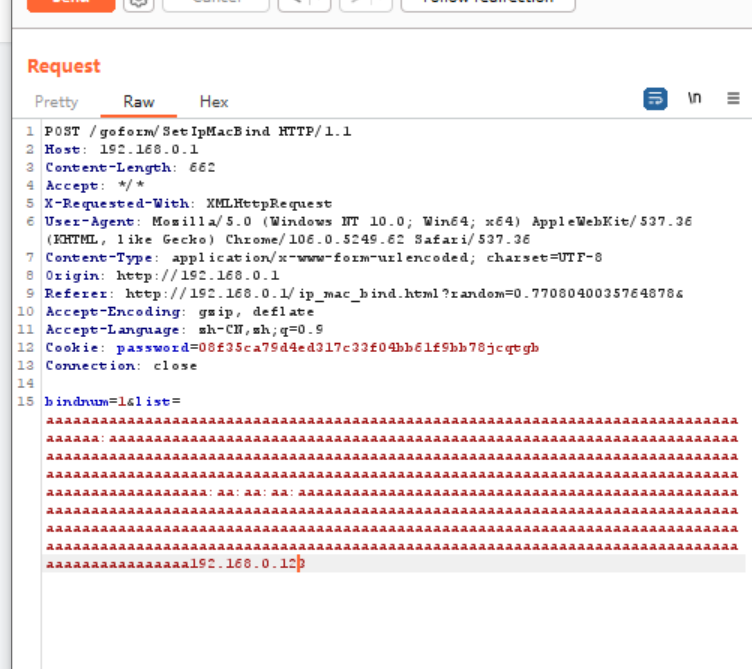




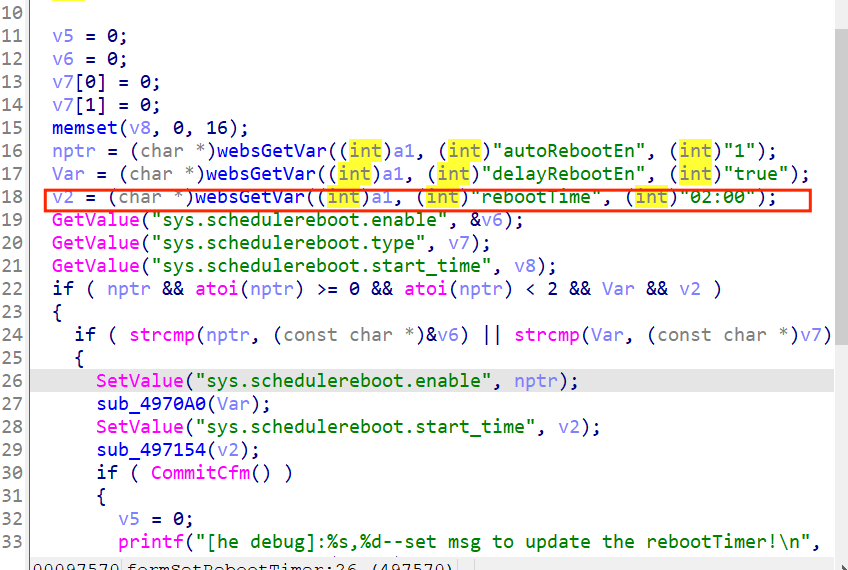
The stack overflow is triggered in the fromSetIpMacBind->sub\_48E668 stack overflow parameter list->sub\_48E668 

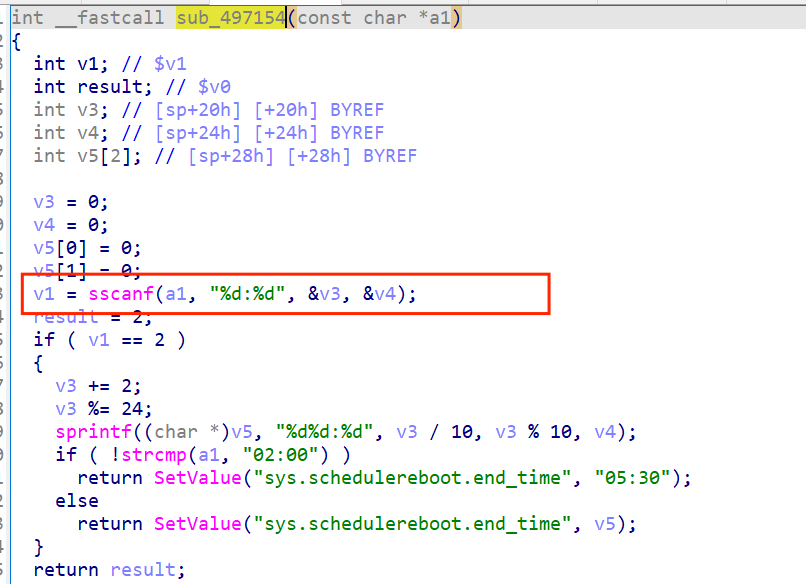


Poc:

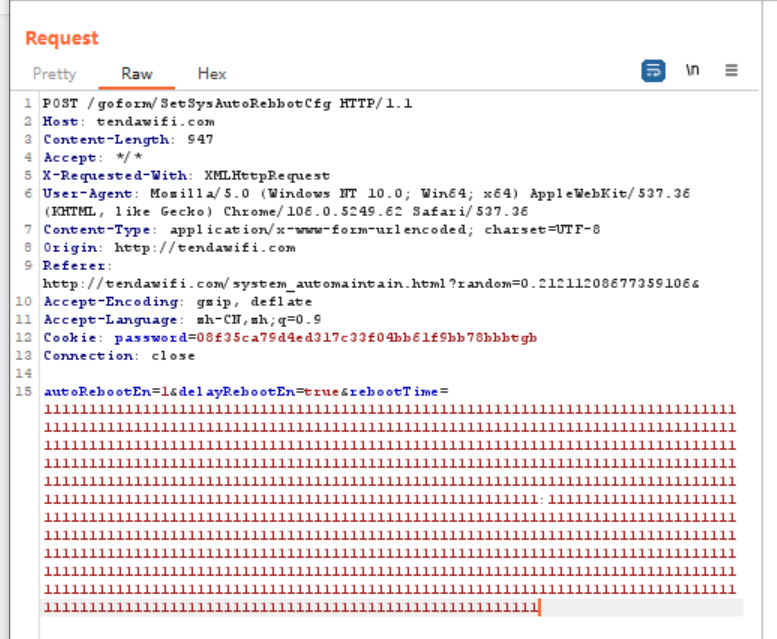


## 8. formSetRebootTimer->sub\_497154 stack overflow: The parameter rebootTime->sub\_497154 triggers stack overflow

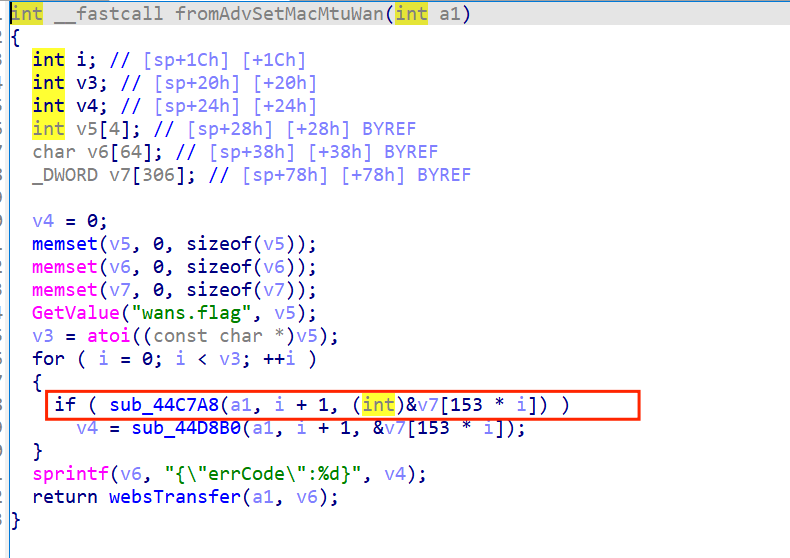




Poc：

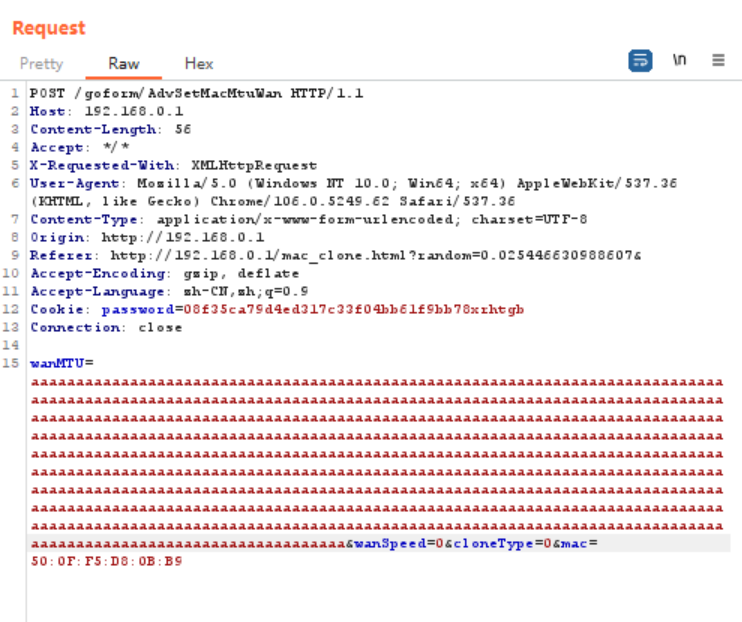


## 9. fromAdvSetMacMtuWan has a stack overflow vulnerability.Trigger function sub\_44C7A8





Poc：



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

