目录

[Tenda ac23 V16.03.07.45\_cn 2](#_Toc20882)

[1. formWifiBasicSet->sub\_451DF8->sub\_450EE4 ->v18； 2](#_Toc20249)

[2. The saveParentControlInfo function has a string overflow parameter deviceId.String overflow due to insufficient storage space allocation 3](#_Toc12341)

[3. The saveParentControlInfo->compare\_parentcontrol\_time function has a stack overflow time parameter 4](#_Toc17022)

[4. formSetPPTPServer->sub\_4781A4 function has a stackoverflow 6](#_Toc25274)

[5. fromSetRouteStatic->save\_staticroute\_data has a stack overflow vulnerability 8](#_Toc21741)

[6. formSetVirtualSer->save\_virtualser\_data function a stack overflow vulnerability triggered by the list parameter 9](#_Toc15630)

[7. The mDMZSetCfg function parameter dmzIp has a stack overflow is triggered by the list parameter 10](#_Toc25131)

[8.The stack overflow is triggered in the fromSetIpMacBind->sub\_48E668 stack overflow parameter list->sub\_48E668 11](#_Toc19780)

[9. formSetRebootTimer->sub\_497154 stack overflow: The parameter rebootTime->sub\_497154 triggers stack overflow 14](#_Toc25560)

[10. fromAdvSetMacMtuWan has a stack overflow vulnerability.Trigger function sub\_44C7A8 16](#_Toc8941)

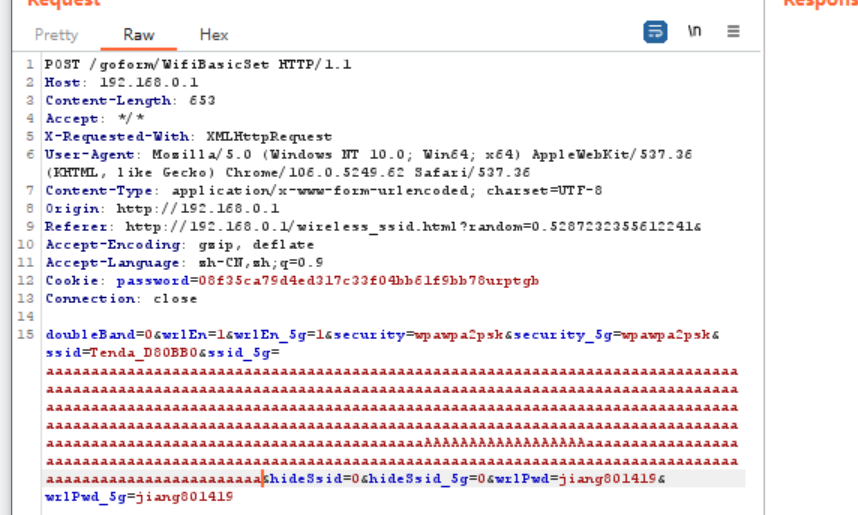
[11.formWifiBasicSet->sub\_451DF8->sub\_450EE4->sub\_450A4C 17](#_Toc32237)

# Tenda ac23 V16.03.07.45\_cn

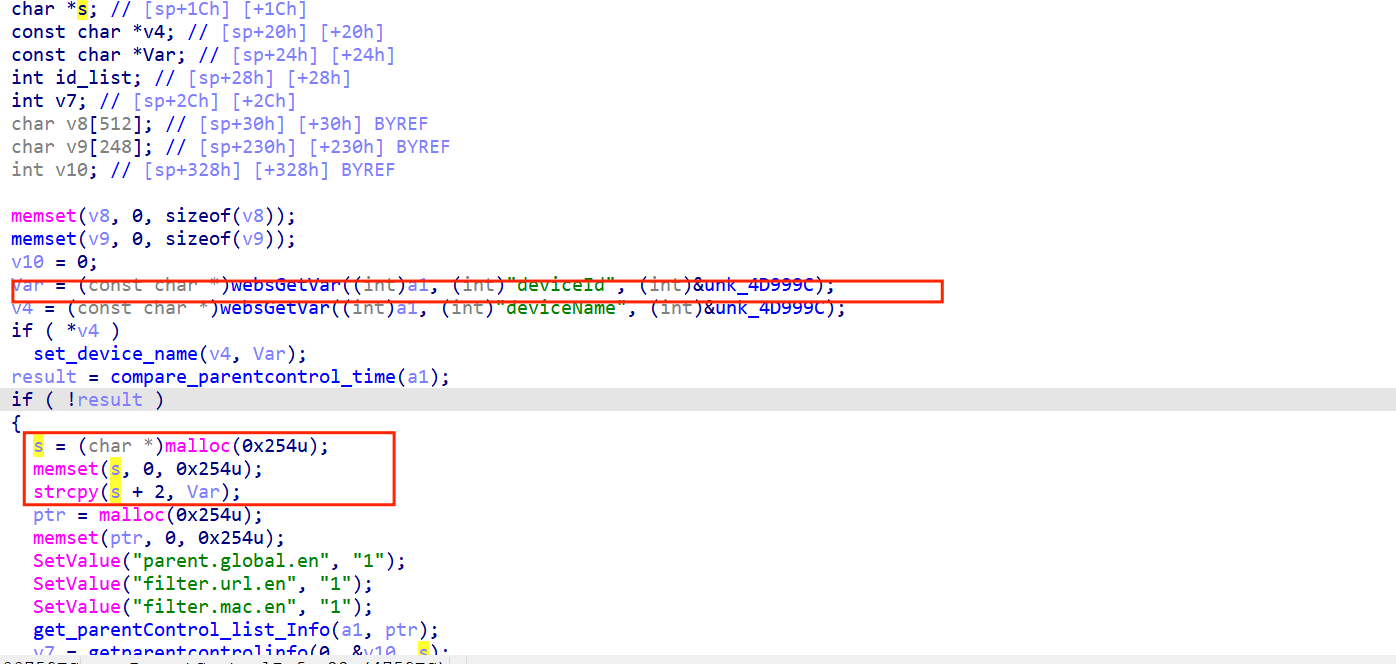
## 1. formWifiBasicSet->sub\_451DF8->sub\_450EE4 ->v18；

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. 

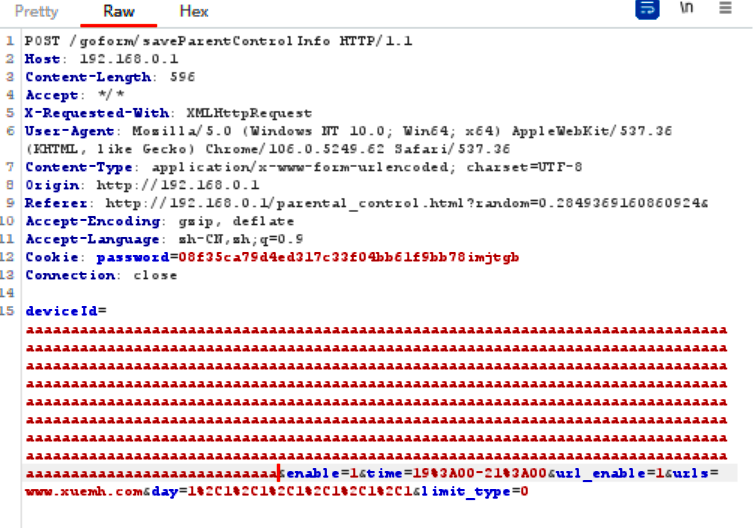
poc:



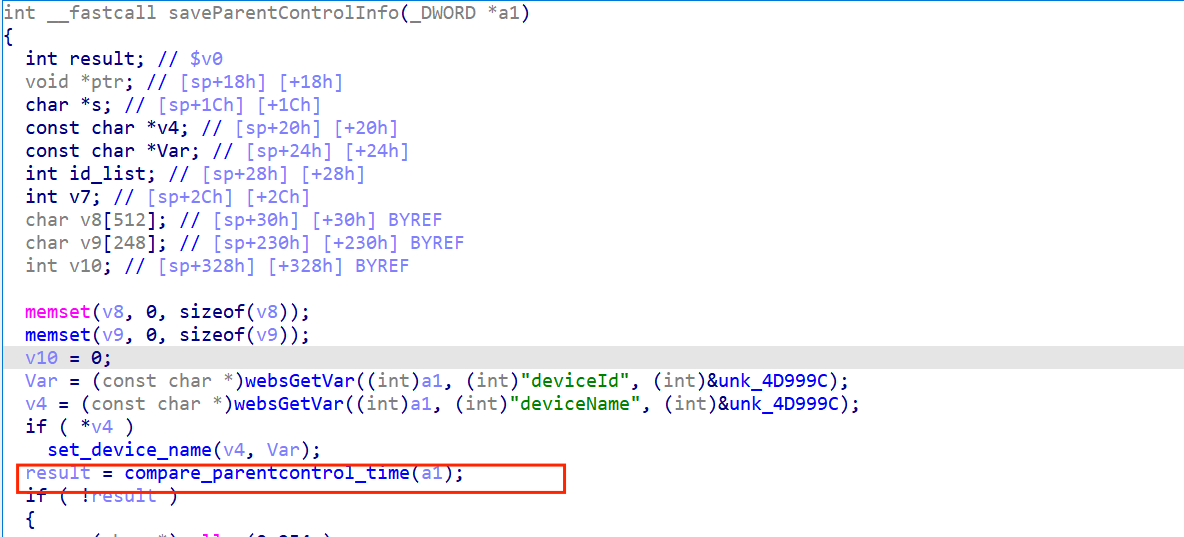
## 2. The saveParentControlInfo function has a string overflow parameter deviceId.String overflow due to insufficient storage space allocation

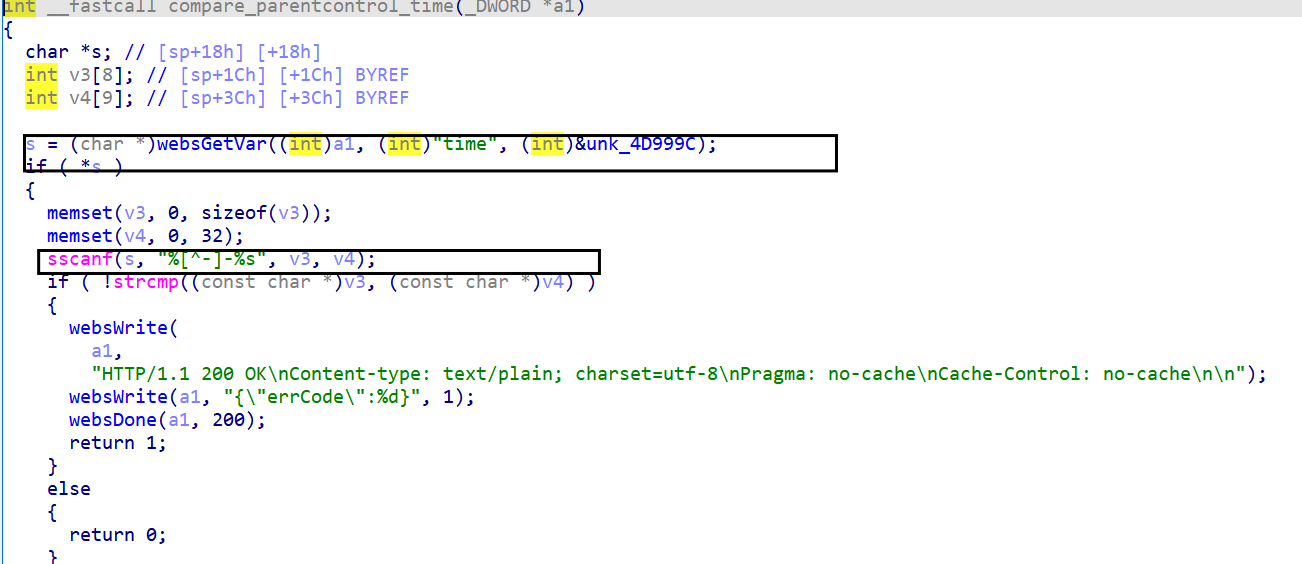


Poc：



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

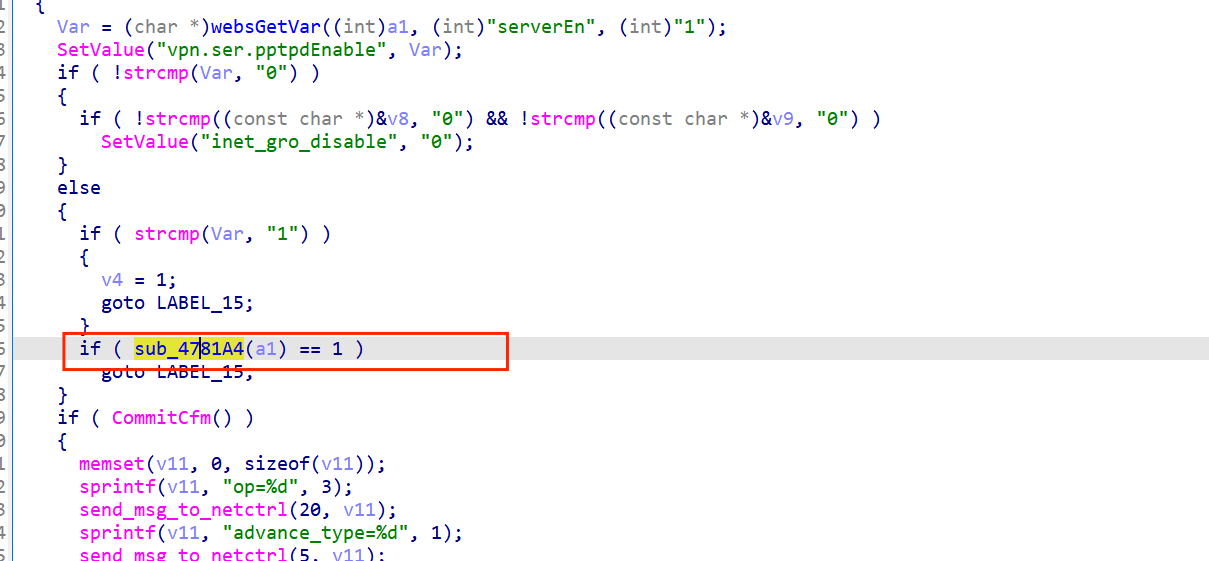




Poc:



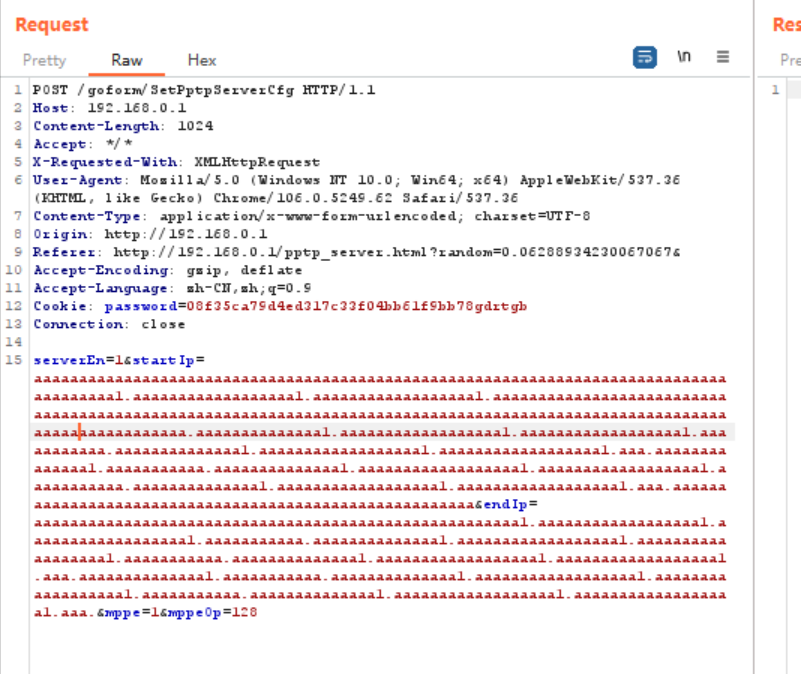
## 4. formSetPPTPServer->sub\_4781A4 function has a stackoverflow



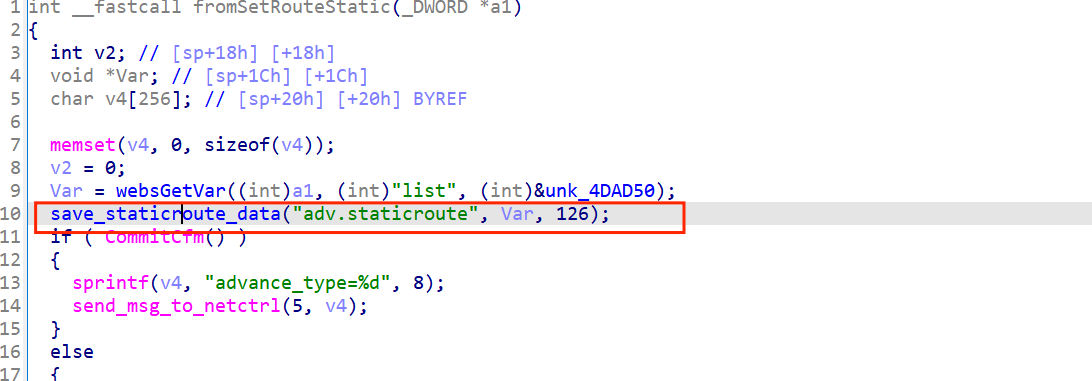
Sub\_4781A4

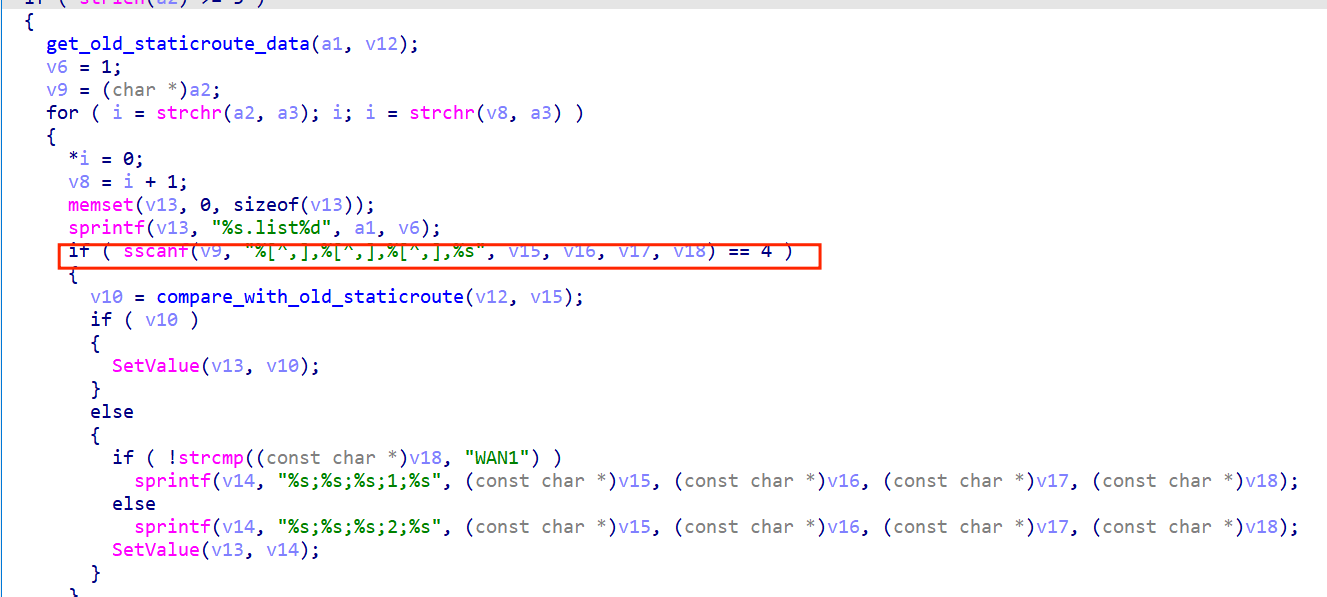


Poc：

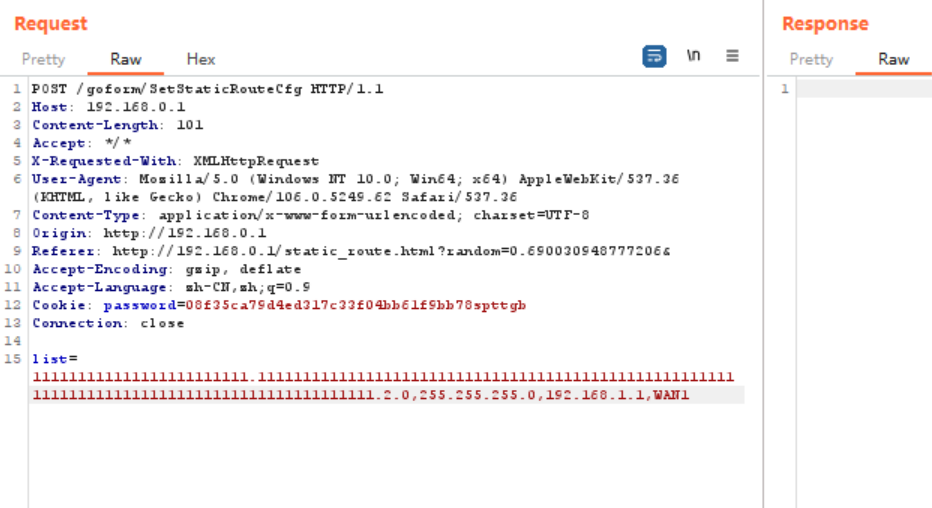


## 5. fromSetRouteStatic->save\_staticroute\_data has a stack overflow vulnerability

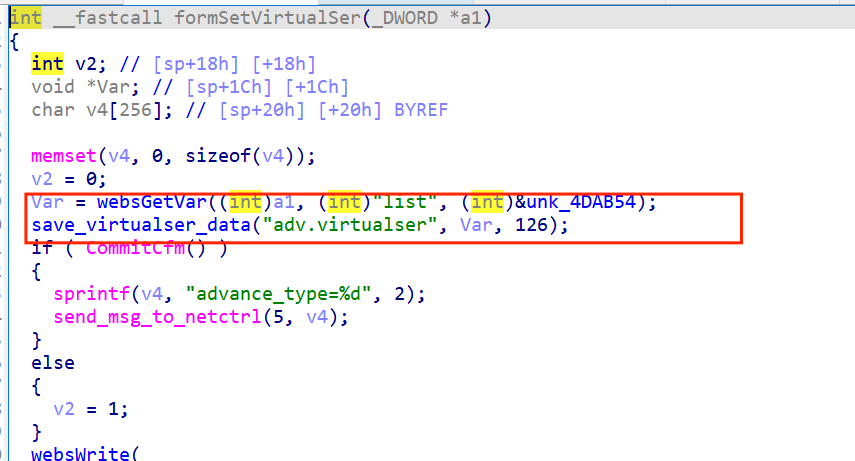
The parameter list is passed to save\_staticroute\_data causing this replication to be infinite, thus overflowing the stack 

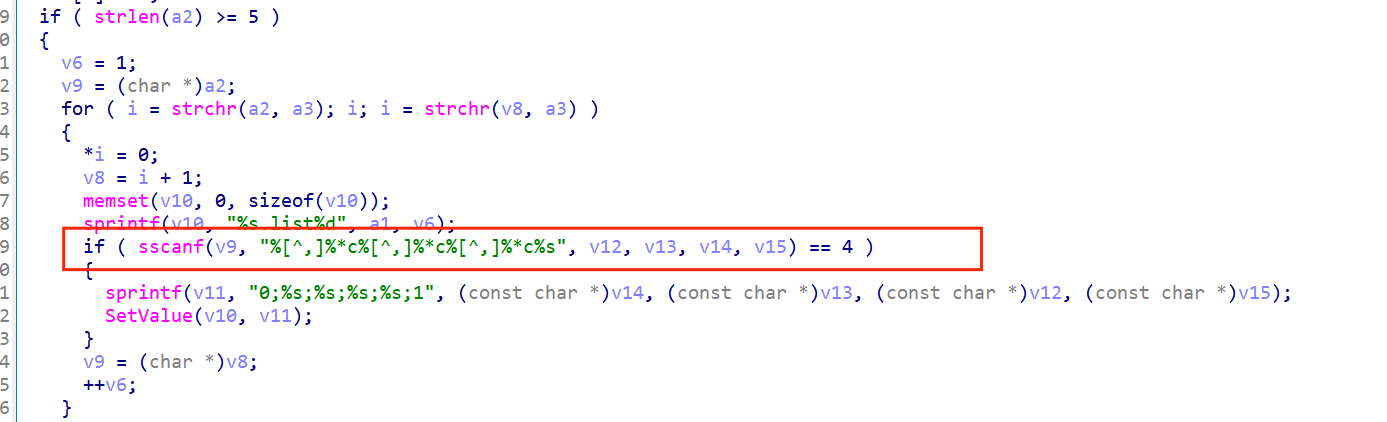


Poc：

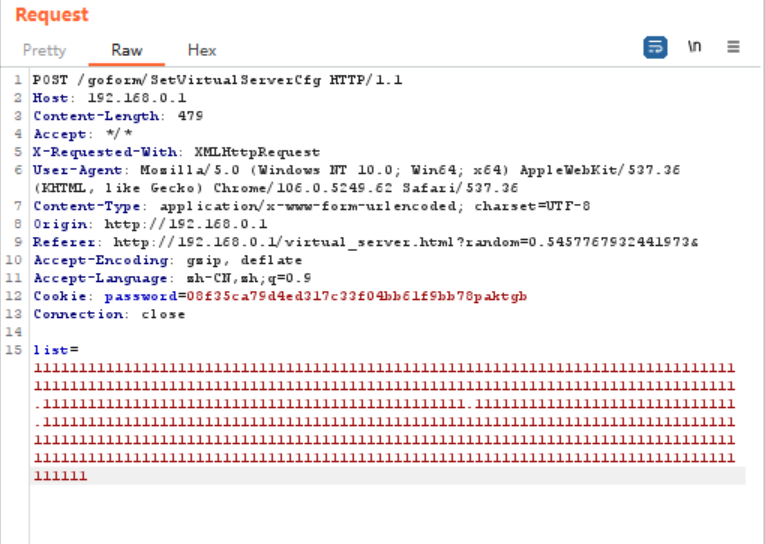


## 6. formSetVirtualSer->save\_virtualser\_data function a stack overflow vulnerability triggered by the list parameter

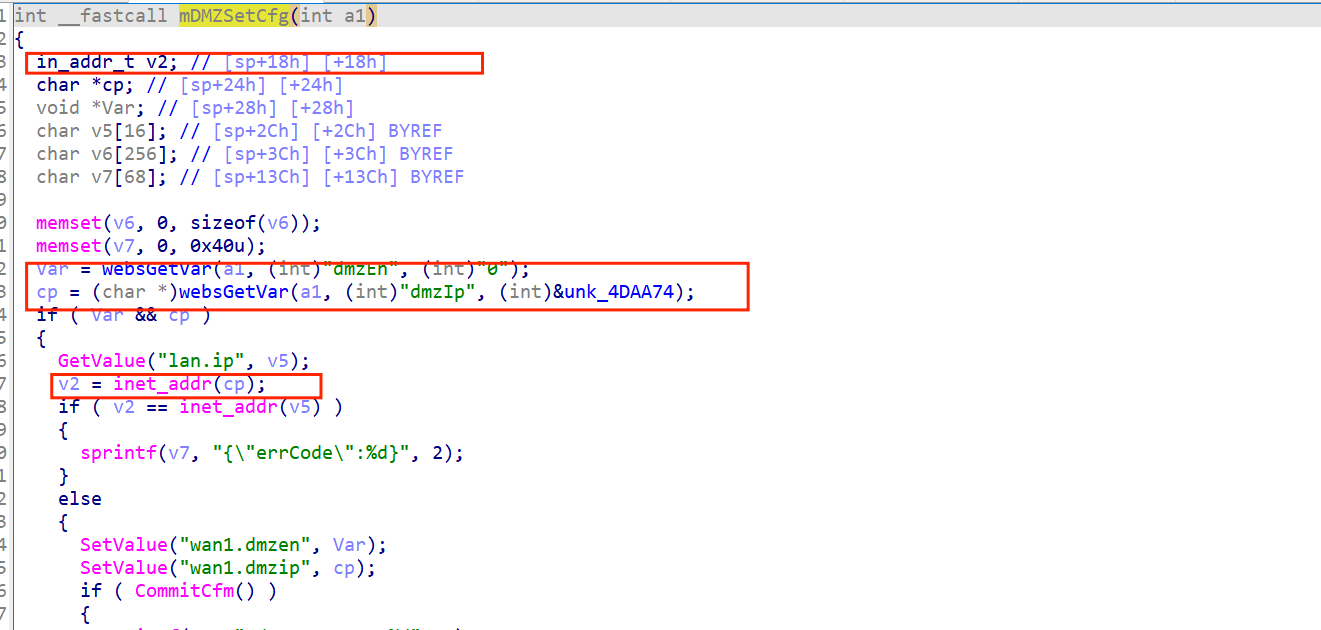


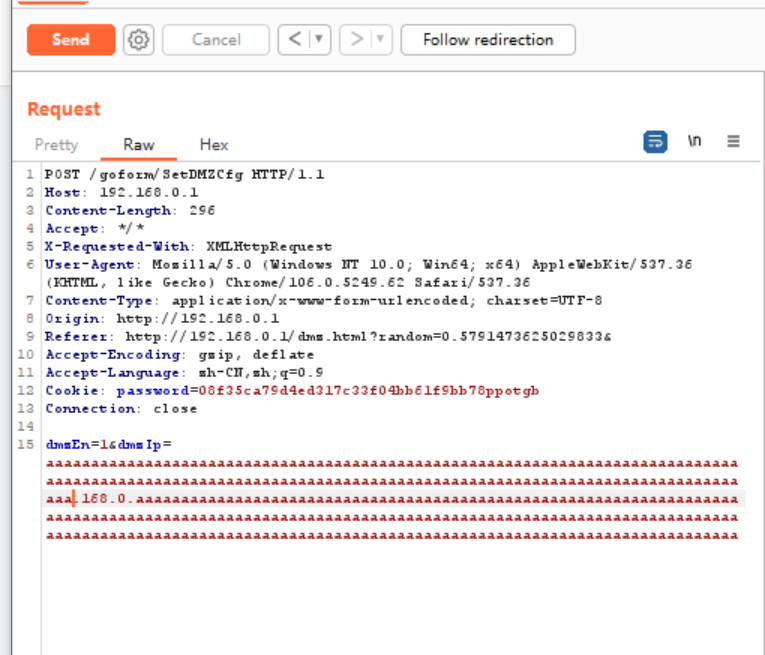


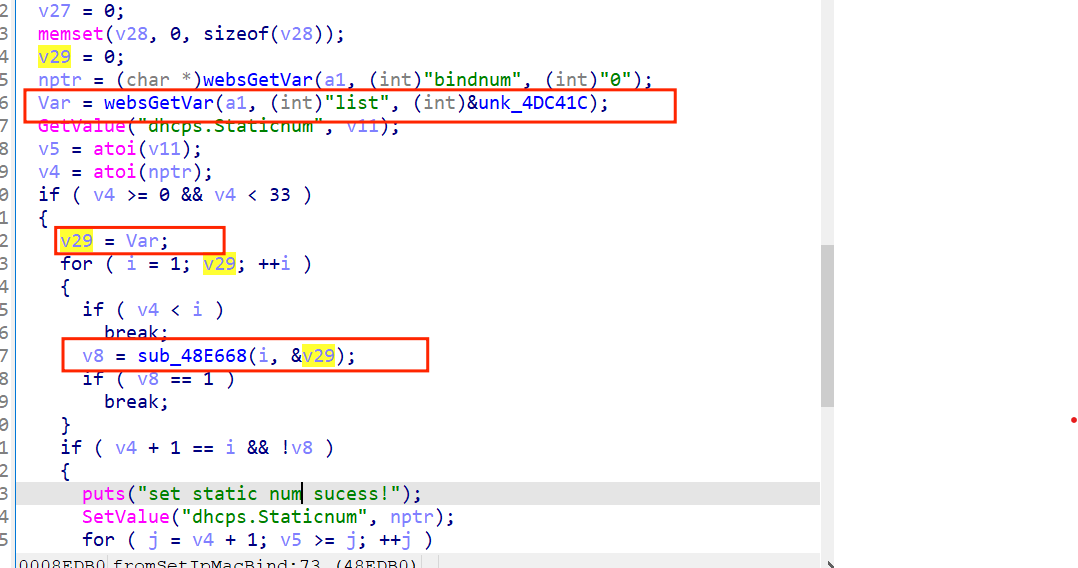
Poc:

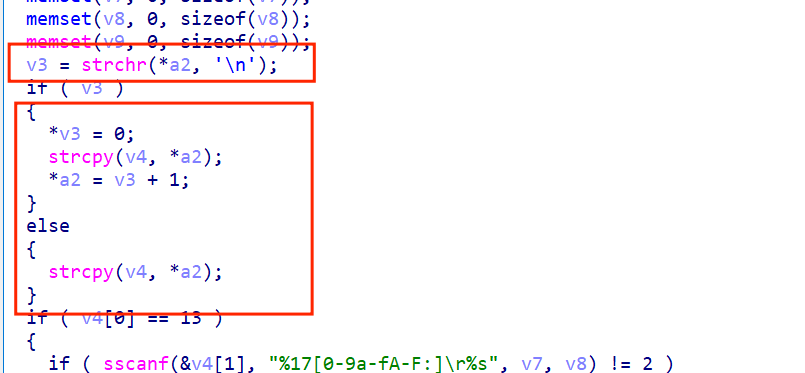


## 7. The mDMZSetCfg function parameter dmzIp has a stack overflow is triggered by the list parameter

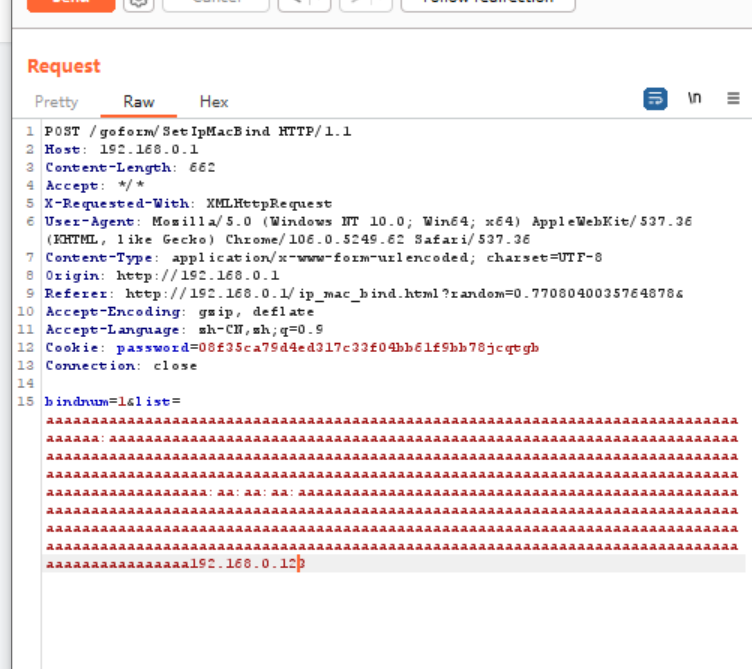




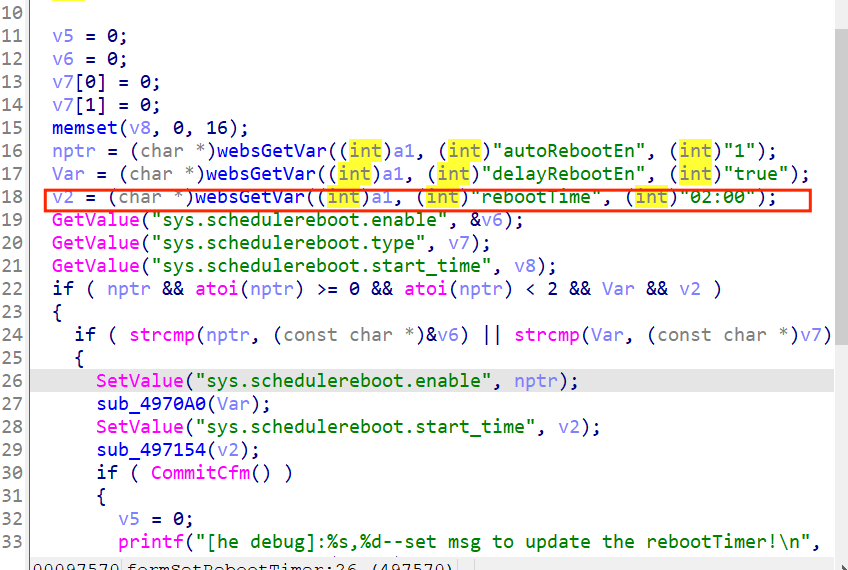
**8.The stack overflow is triggered in the fromSetIpMacBind->sub\_48E668 stack overflow parameter list->sub\_48E668** 

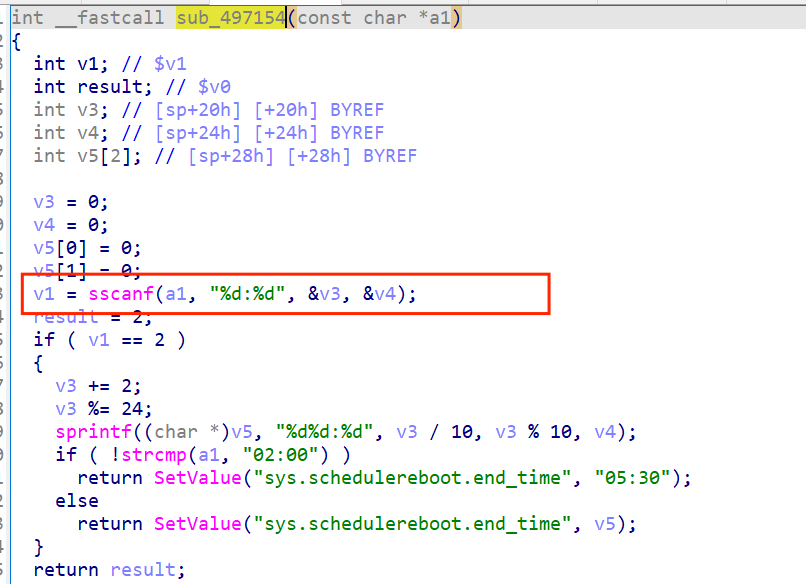


Poc:

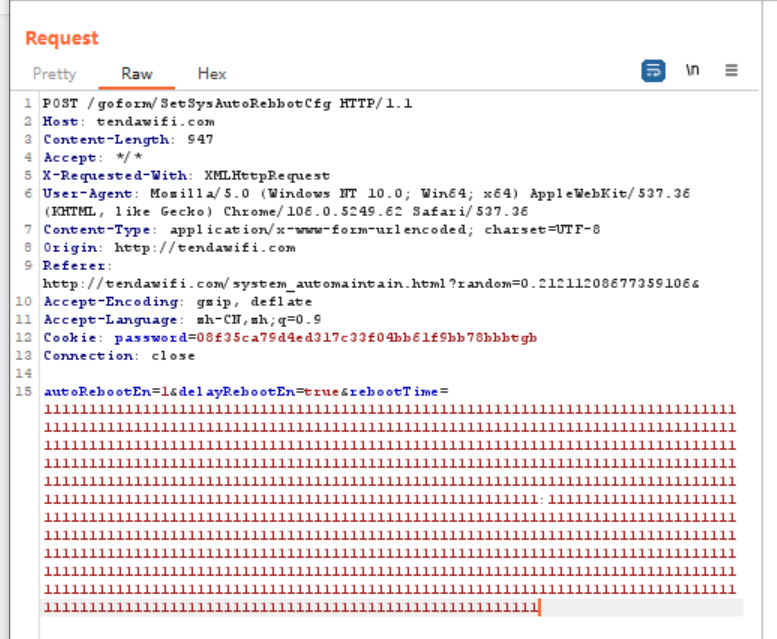


## 9. formSetRebootTimer->sub\_497154 stack overflow: The parameter rebootTime->sub\_497154 triggers stack overflow

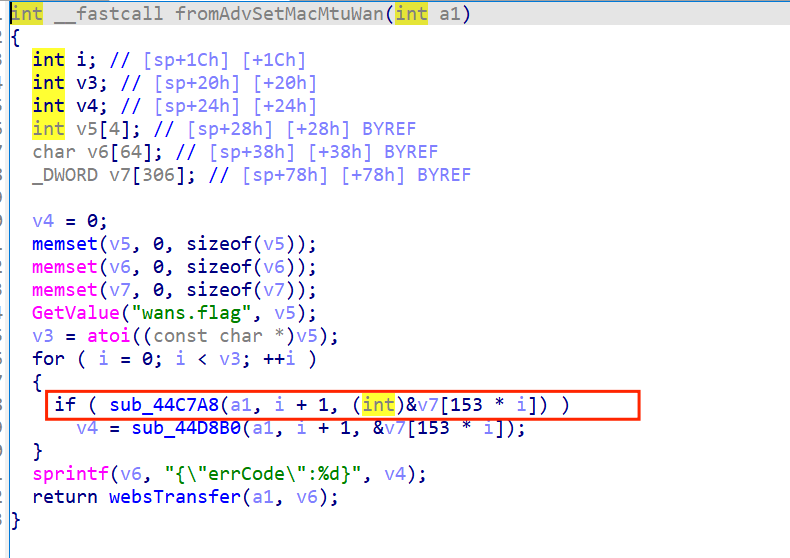




Poc：

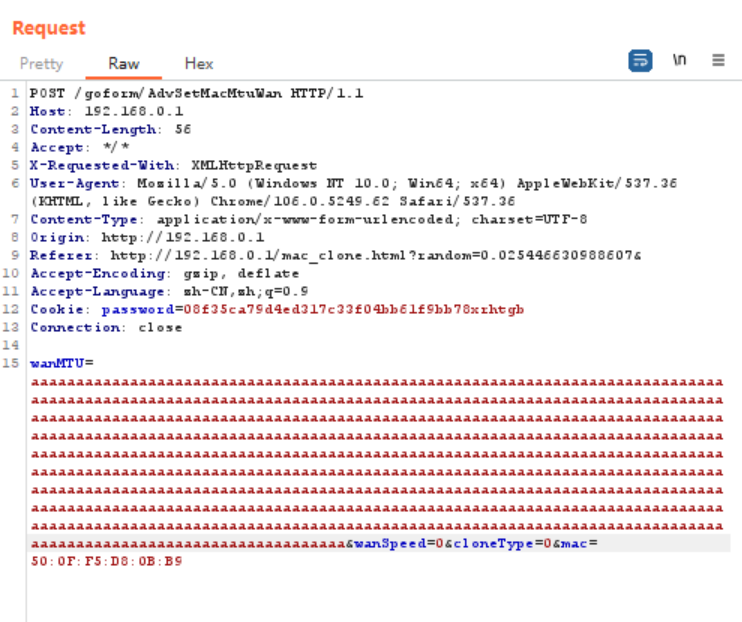


## 10. fromAdvSetMacMtuWan has a stack overflow vulnerability.Trigger function sub\_44C7A8





Poc：



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

