

Experiment-6

AIM: Finding a Remote Code Execution in IoTFirmware.

Step 1: First, we have to download the firmware name for that we have to visit the Netgear website.

Step 2: To download WNAP320-Firmware follow the below link.

- http://wwwdownloads.netgear.com/files/GDC/WNAP320/WNAP320_V3.7.11.4.zip

Step 3: In firmware WNAP320 we have to use the WNAP320-Firmware-Version-3-7-11-4 version.

The screenshot shows a web browser window with the URL <https://kb.netgear.com/000060419/WNAP320-Firmware-Version-3-7-11-4>. The page content includes:

- Enable/Disable Business central (Cloud Enabled) option resets the AP to factory default but retains IP, DNS and management VLAN settings
- In the following scenarios AP is expected to reboot automatically for the configuration to take effect:
 1. Country/Region change
 2. Firmware upgrade
 3. Restore Configuration
 4. Reset factory defaults
 5. Business central enable/disable

In all the other conditions AP is not supposed to reboot automatically.

To Install

1. Download the new software and save it to a convenient folder location.
Download link : http://wwwdownloads.netgear.com/files/GDC/WNAP320/WNAP320_V3.7.11.4.zip
2. Login to the access point web management GUI.
3. Take back-up of the current configuration and save it at a secure place.
4. Select **Maintenance > Upgrade > Firmware Upgrade**.
5. Click Browse and browse to the location of the software upgrade file that you just downloaded and click APPLY button.
Warning: When uploading software, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload might fail, corrupt the software, and render this AP completely inoperable.

Step 4: Open terminal & write ls/ cd tools/ ls firmware – analysis-toolkit Enter into cd tools for use of firmware analysis toolkit.

```

root@attifyos:/home/iot# ls
Arduino    Downloads  ghidra_scripts  package.json      sketchbook
bin        esp        go             package-lock.json  Templates
Desktop   esp32      Music          Pictures         tools
Documents ex.txt    node_modules   Public          Videos
root@attifyos:/home/iot# cd tools/
root@attifyos:/home/iot/tools# ls
arduino              gr-gsm           ook-decoder
baudrate            gr-paint          openocd
bdaddr               hackrf            qiling
bettercap            inspectrum       radare2
buildroot-2019.02.9 jadx              rfcat_150225
burpsuite.jar       kalibrate-rtl   routersploit
create_ap            killerbee        rtl_433
Cutter               libbtbb-2018-12-R1 rtl-sdr
drivers              libmpsse          scapy
dspectrumgui        liquid-dsp       spectrum_painter
dump1090             LTE-Cell-Scanner ubertooh-2018-12-R1
firmware-analysis-toolkit nmap            urh
ghidra_9.1.2_PUBLIC  node_modules
root@attifyos:/home/iot/tools# cd firmware-analysis-toolkit/
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# ls
binwalk      firmadyne    README.md  'WNAP320 Firmware Version 2.0.3.zip'
fat.config   LICENSE     reset.py

```

Step 5: Enter into the firmware analysis toolkit we can show a list of directories in the firmware analysis toolkit. After that enters into fat.config file with the help of the cat command. After that,we can see sudo_password in fat.config

cat fat. Config

```

root@attifyos:/home/iot/tools# cd firmware-analysis-toolkit/
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# ls
binwalk      firmadyne    README.md  'WNAP320 Firmware Version 2.0.3.zip'
fat.config   LICENSE     reset.py
fat.py       qemu-builds  setup.sh
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# cat fat.config
[DEFAULT]
sudo_password=attify
firmadyne_path=/home/iot/tools/firmware-analysis-toolkit/firmadyne
root@attifyos:/home/iot/tools/firmware-analysis-toolkit# ls
binwalk      firmadyne    README.md  'WNAP320 Firmware Version 2.0.3.zip'
fat.config   LICENSE     reset.py
fat.py       qemu-builds  setup.sh

```

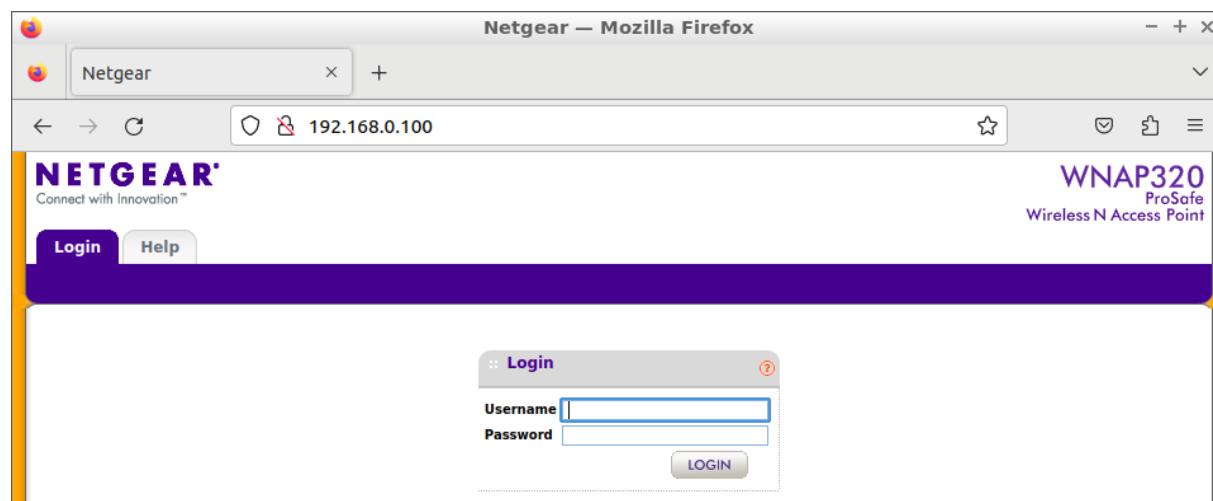
Step 6: Then enter into the ./fat.py file to see so many files are in the ./fat.py file. this file is used to gain the device to be accessible for all files & perform activities in the device.This fat creates an IP address to emulate the device.

./fat.py ‘file path’

Step 7: After performing fat create that is create an IP address to emulate IoT devices.

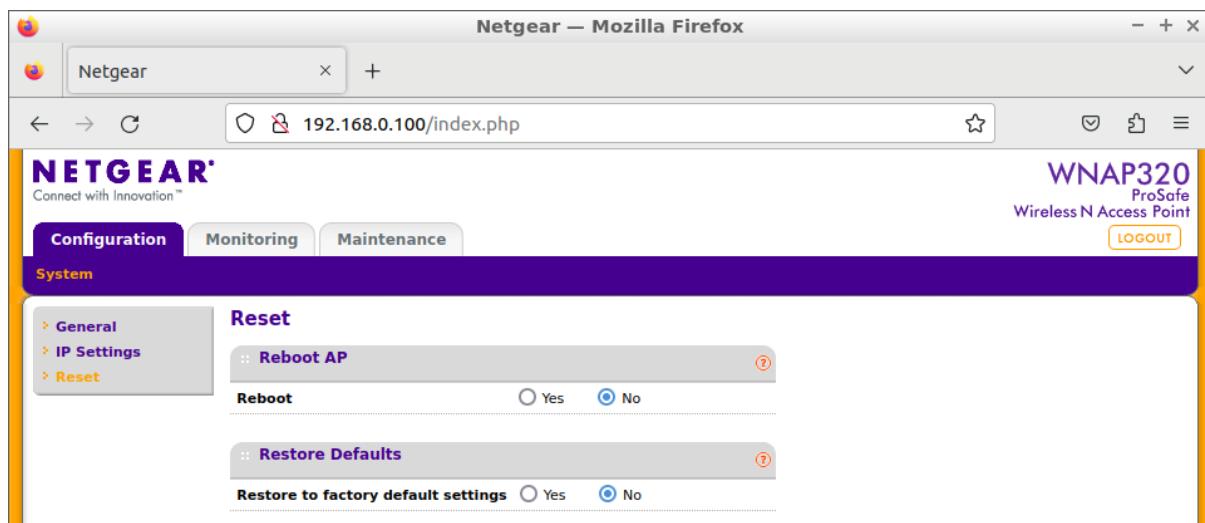
This IP address runs into a browser that can show a login page of the DIR-300 device.

After entering login credentials like Username & password. Username & password shows in emulating process use of FAT.



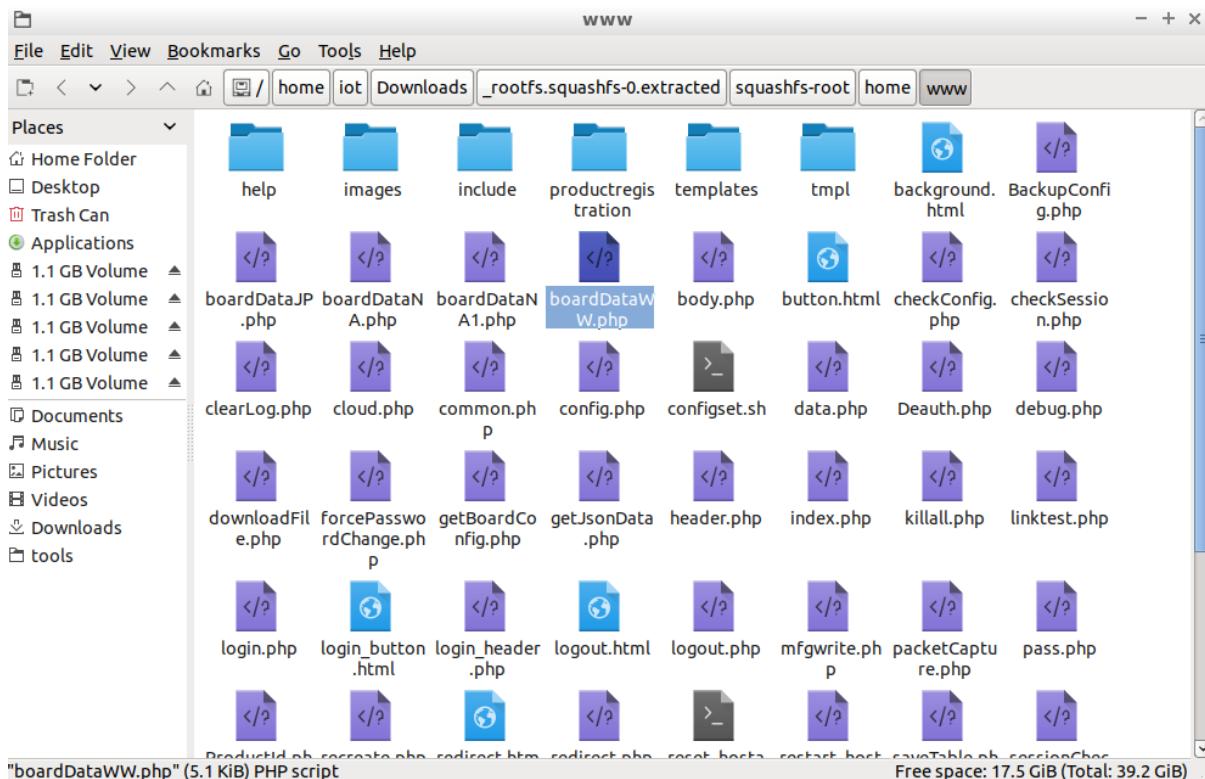
Step 8: After entering the Username & password we can redirect to the page of this device for emulating that's IoT device. we can access files & perform any activity on this device.

We can change or modify the data of this device.



Step 9: Then we have to check their php files for remote access. then we can find the boardDataWW.php vulnerable file.

Path : rootfs.squashfs-root/squashfs-root/home/www/boardDataWW.php



Step 10: We have to open file & find a vulnerable code in file.

```

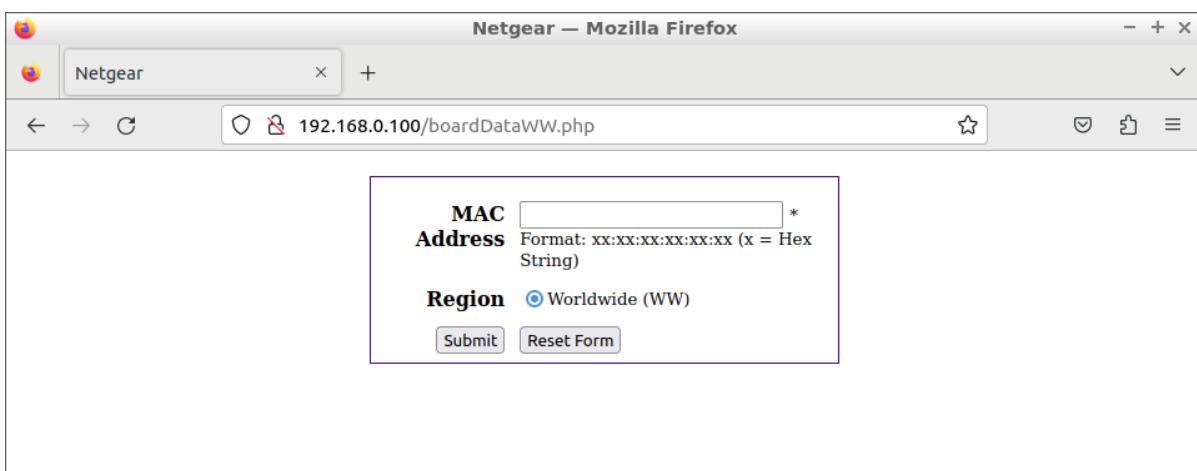
$flag=false;
$msg="";
function validateCommandArg($mac_address, $region){
    if (array_search($region,Array('WW'=>'0','NA'=>'1','JP'=>'2'))!==false && ereg("/^
        return true;
    else
        return false;
}
if (!empty($_POST['writeData'])) {
    $macAddress = escapeshellcmd($_POST['macAddress']);
    $reginfo = escapeshellcmd($_POST['reginfo']);
    if (!empty($macAddress) && !empty($reginfo)) {
        //echo "test ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'];
        //exec("wr_mfg_data ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'],
        if(validateCommandArg($macAddress,$reginfo))
            exec("wr_mfg_data -m ".$macAddress." -c ".$reginfo,$dummy,$res);

        if ($res==0) {
            conf_set_buffer("system:basicSettings:apName netgear".substr($_POST
            conf_save();
            $msg = 'Update Success!';
            $flag = true;
}

```

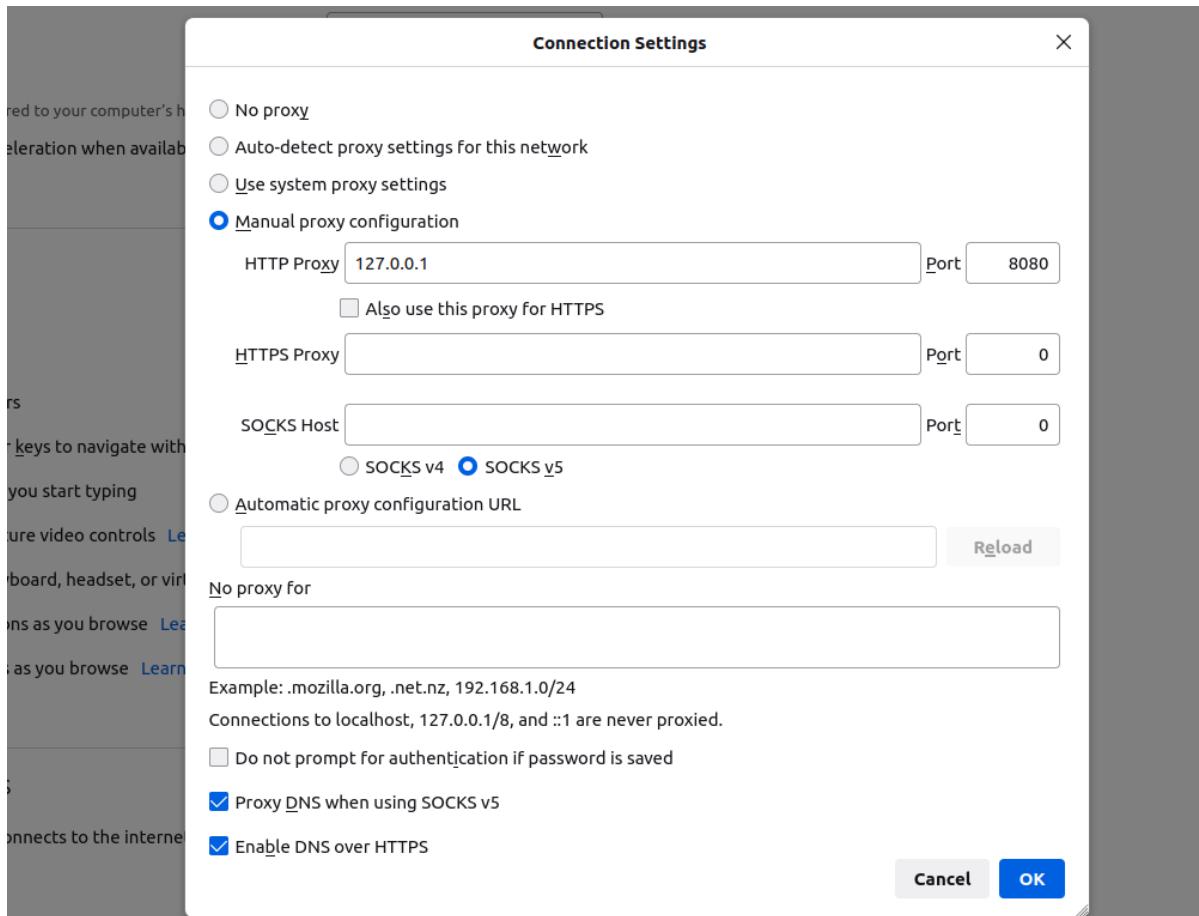
Step 11: After find vulnerable file we have go to website & write

192.168.0.100/boardDataWW.php so we can see the boardDataWW page.



Step 12: We have to do proxy settings for the exploit website. We have to go manual proxy settings.

- Path : Mozilla Firefox/ preferences/network setting/manual proxy configuration
- HTTP proxy : 127.0.0.1
- Port : 8080



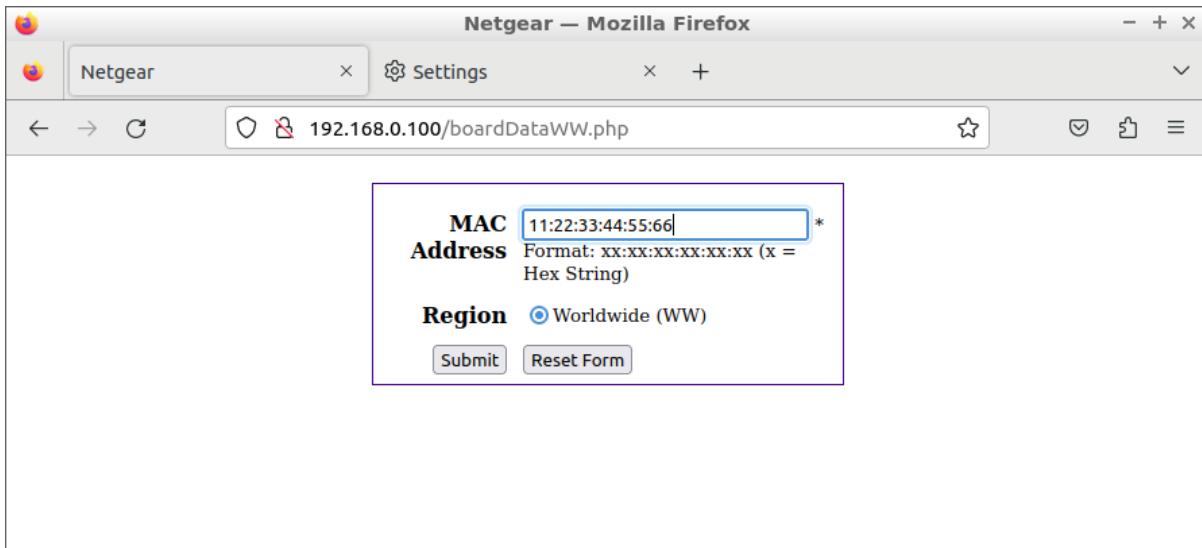
Step 13: We have to open burpsuite for intercept website . we have to write command `java -jar burpsuite.jar` in terminal .

java -jar burpsuite.jar

```
root@attifyos: /home/iot/tools 66x24
Welcome to fish, the friendly interactive shell
iot@attifyos ~> sudo su
[sudo] password for iot:
root@attifyos:/home/iot# cd tools/
root@attifyos:/home/iot/tools# ls
arduino          gr-gsm      ook-decoder
baudrate         gr-paint    openocd
bdaddr           hackrf      qiling
bettercap        inspectrum radare2
buildroot-2019.02.9 jadx       rfcat_150225
burpsuite.jar  kalibrate-rtl routersploit
create_ap        killerbee   rtl_433
Cutter           libbbtbb-2018-12-R1 rtl-sdr
drivers          libmpsse    scapy
dspectrungui    liquid-dsp  spectrum_painter
dump1090         LTE-Cell-Scanner ubertoooth-2018-12-R
1
firmware-analysis-toolkit nmap      urh
ghidra 9.1.2_PUBLIC node_modules
root@attifyos:/home/iot/tools# java -jar burpsuite.jar ■
```

```
root@attifyos: /home/iot/tools/firmware-analysis-toolkit 70x24
root@attifyos: /home/iot/tools/firmware-analysis-toolkit 70x24
[ 138.200000] Code: 00000000 00000000 00000000 <90830000> 90a20000
24840001 14600003 24a50001 03e00008
[ 138.224000] hostapd_tr/5034: potentially unexpected fatal signal 11
.
[ 138.224000]
[ 138.224000] Cpu 0
[ 138.224000] $ 0 : 00000000 00000001 00000004 00000000
[ 138.236000] $ 4 : 00000004 0041b178 00000000 00000001
[ 138.236000] $ 8 : 2ab25004 004300b8 00000031 ffffff0
[ 138.236000] $12 : 8f151eb0 000000234 06ca3695 2aad9578
[ 138.236000] $16 : 7ff21470 7ff21300 7f905104 ffffffff
[ 138.236000] $20 : 7ff213c4 00401a08 00000001 00401bc0
[ 138.248000] $24 : 00000000 2aaafc810
[ 138.248000] $28 : 00437080 7ff20d50 7ff20d50 00417768
[ 138.256000] Hi : 00000005
[ 138.256000] Lo : 19999999
[ 138.256000] epc : 2aaafc810 0x2aaafc810
[ 138.256000] Not tainted
[ 138.256000] ra : 00417768 0x417768
[ 138.256000] Status: 0000a413 USER EXL IE
[ 138.256000] Cause : 10800008
[ 138.256000] BadVA : 00000004
[ 138.256000] PrId : 00019300 (MIPS 24Kc)
```

Step 14: After that intercept off of burp suite. Go to website, enter a MAC Address on it then on intercept in burp suite. So we can see MAC address in a proxy. Then select a whole code & send it to repeater .



Step 15: After send a code to repeater , we can see MAC address which we can enter into website page. With use of this code we can get remote code execution of website.

- We can change a MAC address into malicious script or code. With use of this malicious script or code we can gain remote access of website.

The screenshot shows the Burp Suite Community Edition interface. The target is set to `http://192.168.0.100`. The Request tab shows a POST request to `/boardDataWW.php` with the following raw data:

```

1 POST /boardDataWW.php HTTP/1.1
2 Host: 192.168.0.100
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 93
9 Origin: http://192.168.0.100
10 Connection: close
11 Referer: http://192.168.0.100/boardDataWW.php
12 Cookie: PHPSESSID=374c2c502f7108485b64a0715f6d7987
13 Upgrade-Insecure-Requests: 1
14
15 macAddress=11%3A22%3A33%3A44%3A55%3A66&regInfo=0&writeData=Submit|

```

The Response tab shows the following raw HTTP response:

```

1 HTTP/1.1 302 Found
2 Connection: close
3 Status: 302 Moved Temporarily
4 X-Powered-By: PHP/5.6.36
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 location: index.php
9 Content-type: text/html; charset=UTF-8
10 Date: Fri, 14 Feb 2025 13:44:57 GMT
11 Server: lighttpd/1.4.18
12 Content-Length: 0
13
14

```

Conclusion: By using the burp suite we can exploit this vulnerable code but we can't do it due to the security perspective. We can perform remote code access with the use of WNAP320 firmware, Netgear website & burp suite.