By following the steps below an ARP spoofing attack will take place between the web server created in the Raspberry Pi and any mobile user. The web server(Raspberry Pi), web client(mobile user) and the Attacker(another system) should be present in the same network. Here, the important point is the Raspberry Pi is also the 6lbr of the WSN formed using slip radio and sensor tag. Let’s look at the steps now.

Step 1: apache server installation on Raspberry Pi

1. Open terminal in Raspberry Pi
2. sudo apt update && sudo apt upgrade -y
3. sudo apt install apache2 -y
4. cd /var/www/html
5. ls -al
   1. You should have an *index.html* file in that folder.
6. hostname -I
   1. You will find the IP address
7. You can type “localhost” or the “IP” in the browser to find the home directory of Apache

Step 2: PhP installation on Raspberry pi

1. sudo apt install php -y
2. sudo service apache2 restart

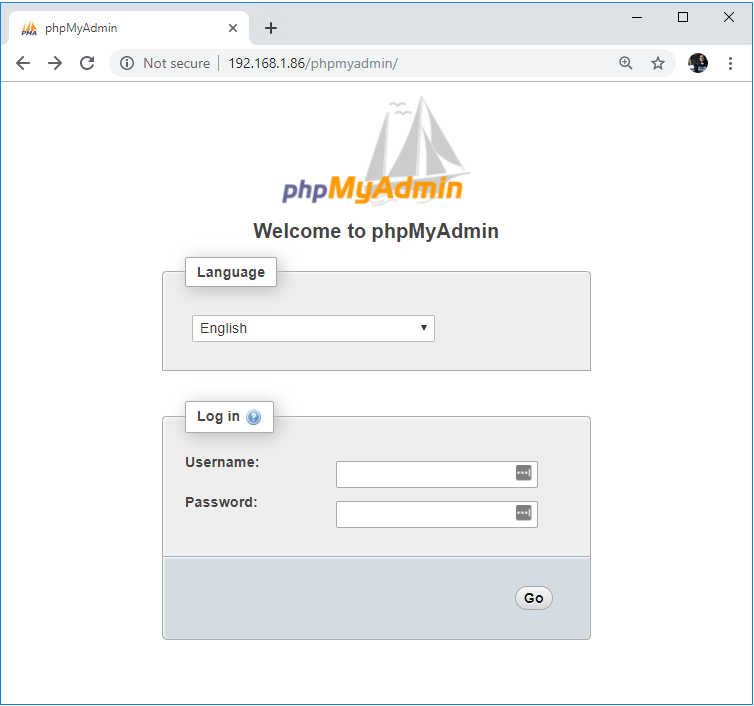
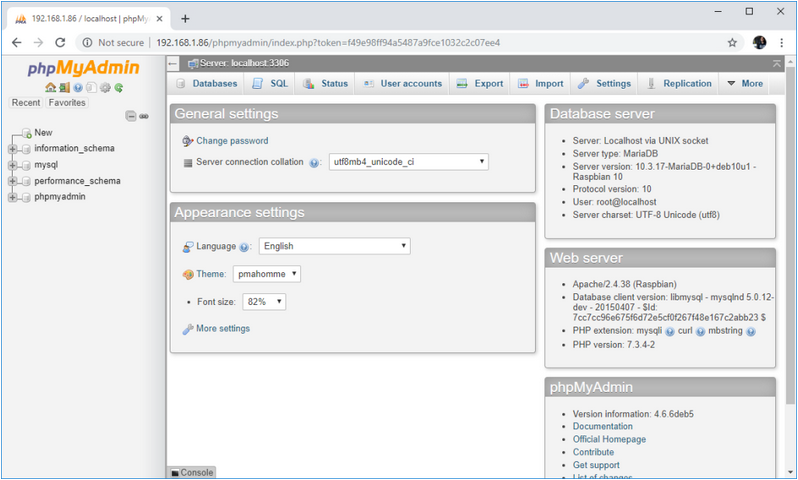
Step 3: MySQL (Maria DB) server installation on Raspberry Pi

1. sudo apt install mariadb-server php-mysql -y
2. sudo service apache2 restart
3. sudo mysql\_secure\_installation
   1. You will be asked Enter **current password for root** (type a secure password): press Enter
   2. Type in **Y** and press **Enter** to Set root password
   3. Type in a password at the New password: prompt, and press Enter. Important: remember this root password, as you will need it later
   4. Type in **Y** to Remove anonymous users
   5. Type in **Y** to Disallow root login remotely
   6. Type in **Y** to Remove test database and access to it
   7. Type in **Y** to Reload privilege tables now
4. sudo mysql --user=root --password
   1. > create user admin@localhost identified by '*your\_password*';
   2. > grant all privileges on \*.\* to admin@localhost;
   3. > FLUSH PRIVILEGES;
   4. > exit;

Step 4: PhPMyAdmin installation on Raspberry Pi

1. sudo apt install phpmyadmin -y
   1. Select **Apache2** when prompted and press the **Enter** key
   2. Configuring **phpmyadmin**? **OK**
   3. Configure database for phpmyadmin with **dbconfig-common**? **Yes**
   4. Type your **password** and press **OK**
2. sudo phpenmod mysqli
3. sudo ln -s /usr/share/phpmyadmin /var/www/html/phpmyadmin
4. sudo service apache2 restart
5. Go to browser and search <http://localhost/phpmyadmin>

Step 5: creation of Database of users and table creation

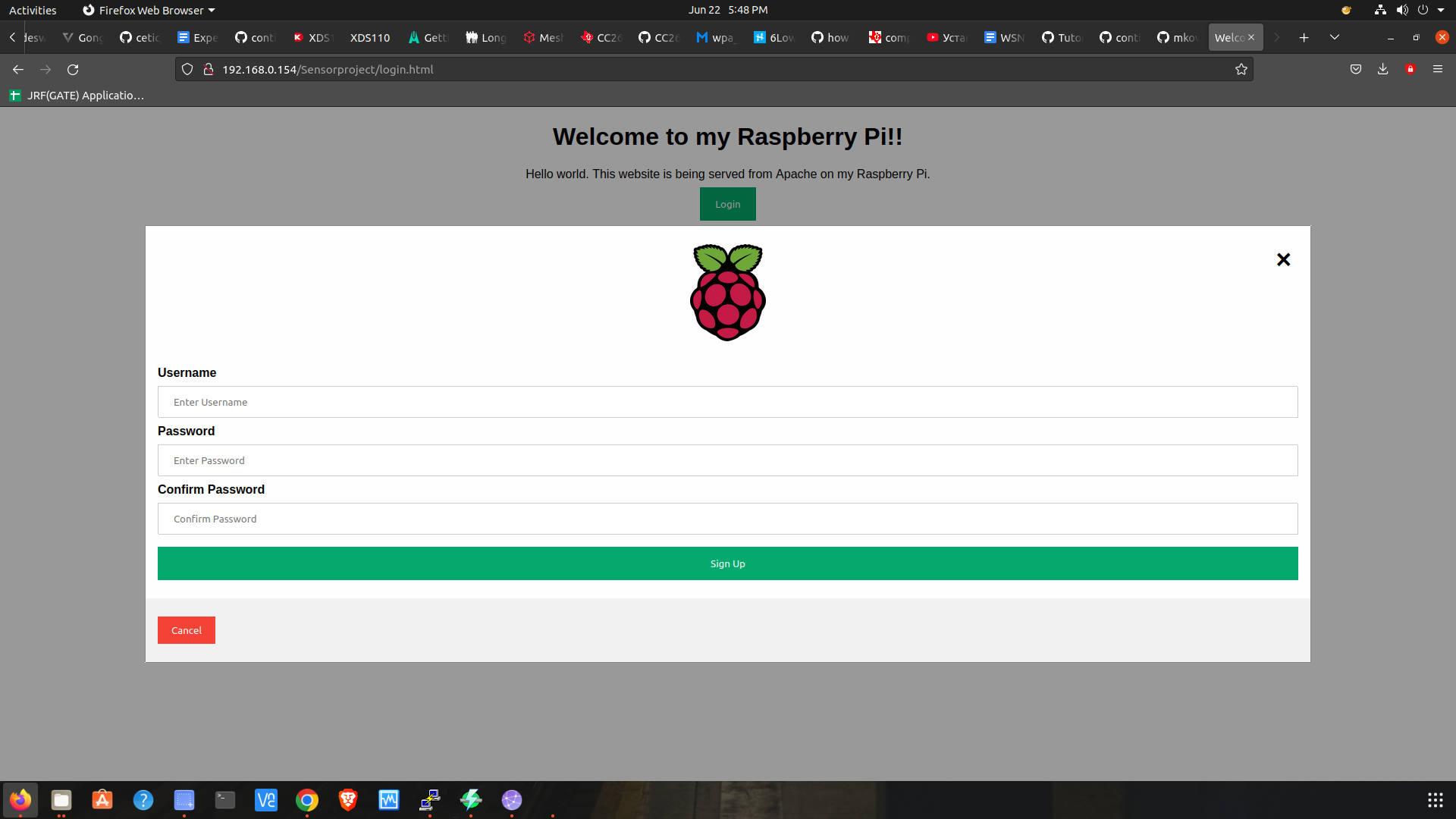
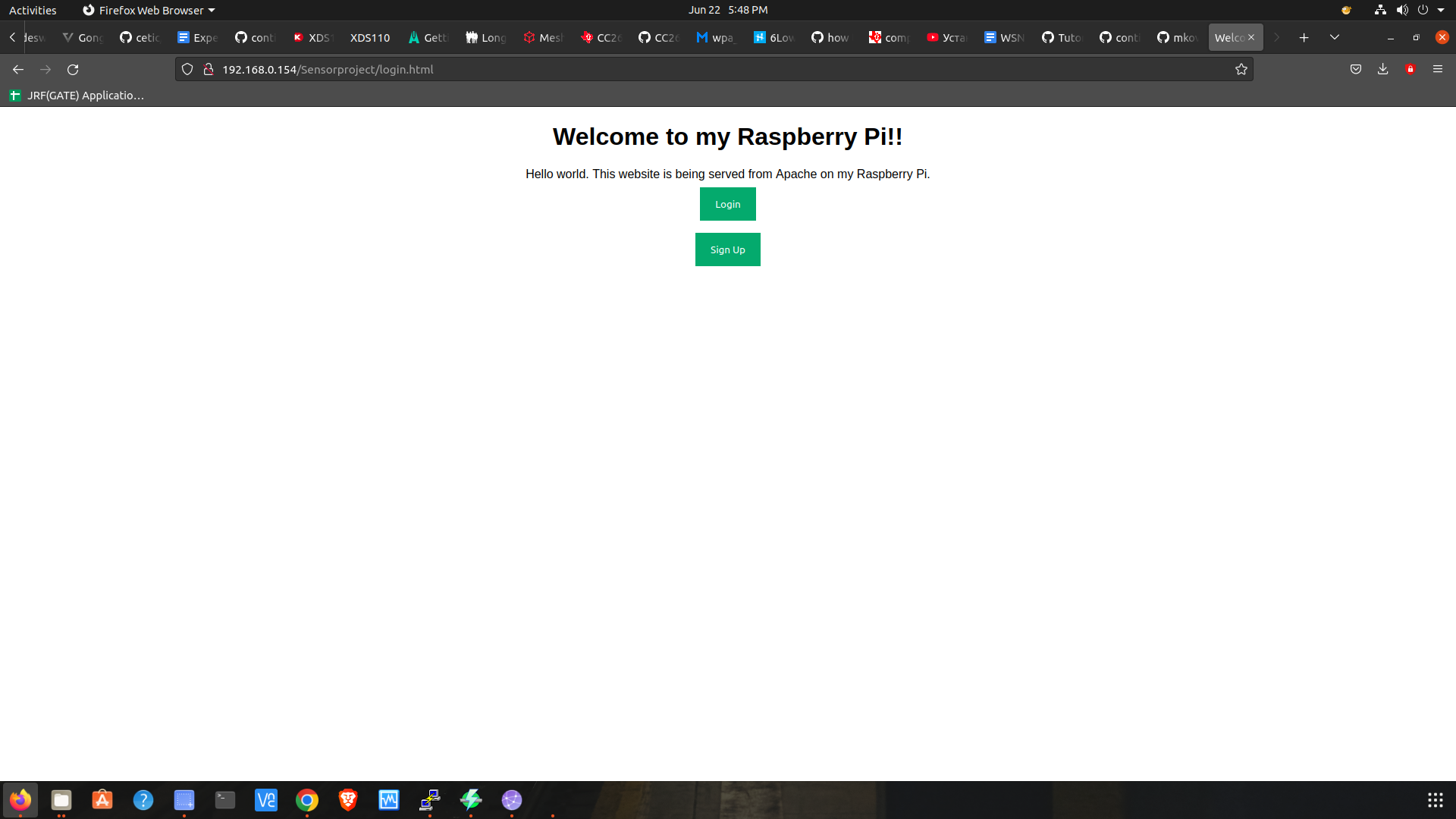
1. You shall see the following screen at <http://localhost/phpmyadmin>
2. Type admin in the Username field and *your\_password* in the Password field
3. You will find the following page after clicking on Go
4. Click on New to create a database and give it the name “demo”
5. After creating the database there will be two tables need to be created by running the following SQL queries:
   1. CREATE TABLE `loginform`( `id` INT(10) NOT NULL PRIMARY KEY AUTO\_INCREMENT), `user` VARCHAR(40) NOT NULL, `pass` VARCHAR(40), status INT(2));
   2. CREATE TABLE `loginform\_token`( `id` INT(10) NOT NULL PRIMARY KEY AUTO\_INCREMENT), `user` VARCHAR(40) NOT NULL, `token` VARCHAR(40), status INT(2));

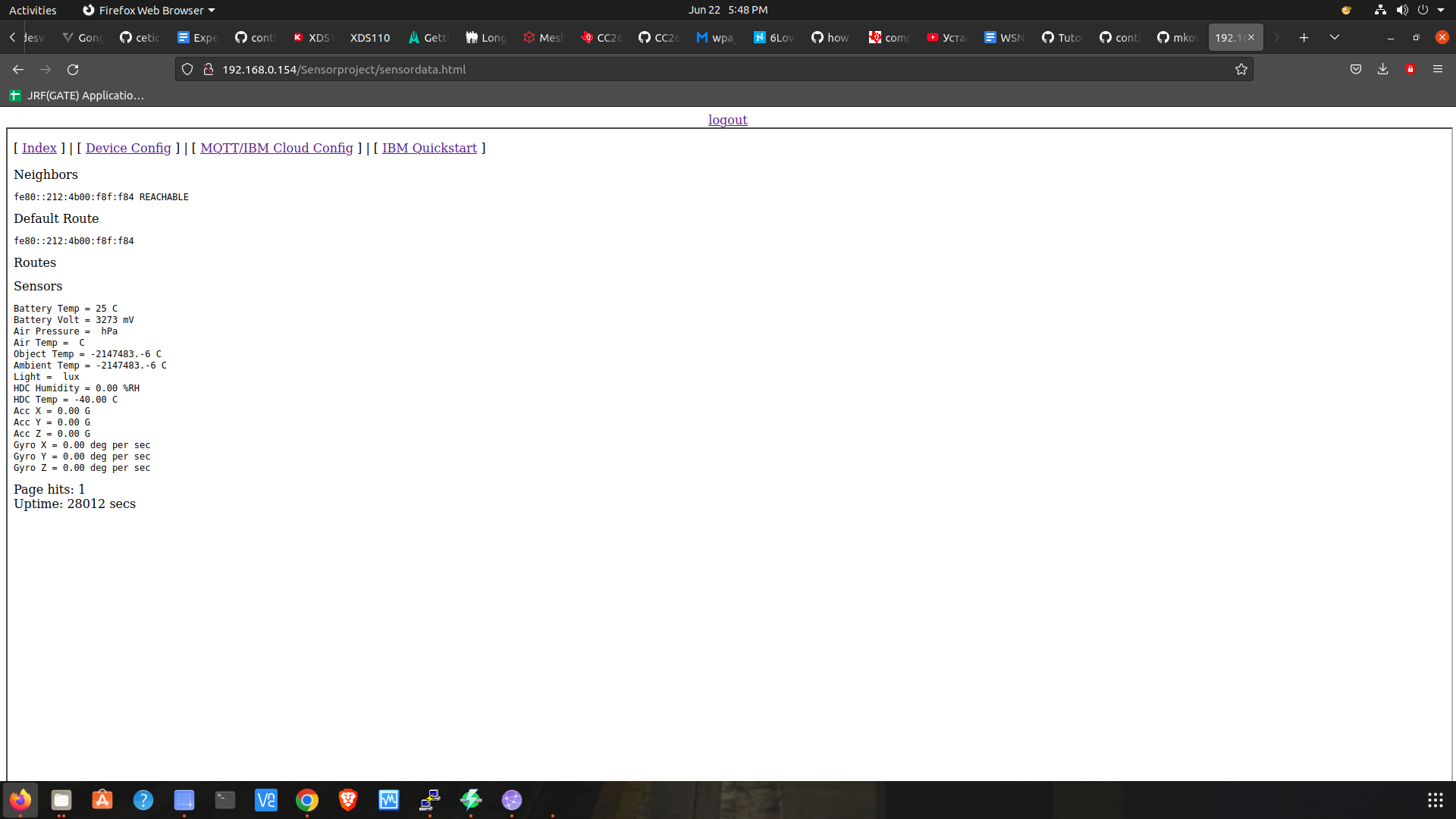
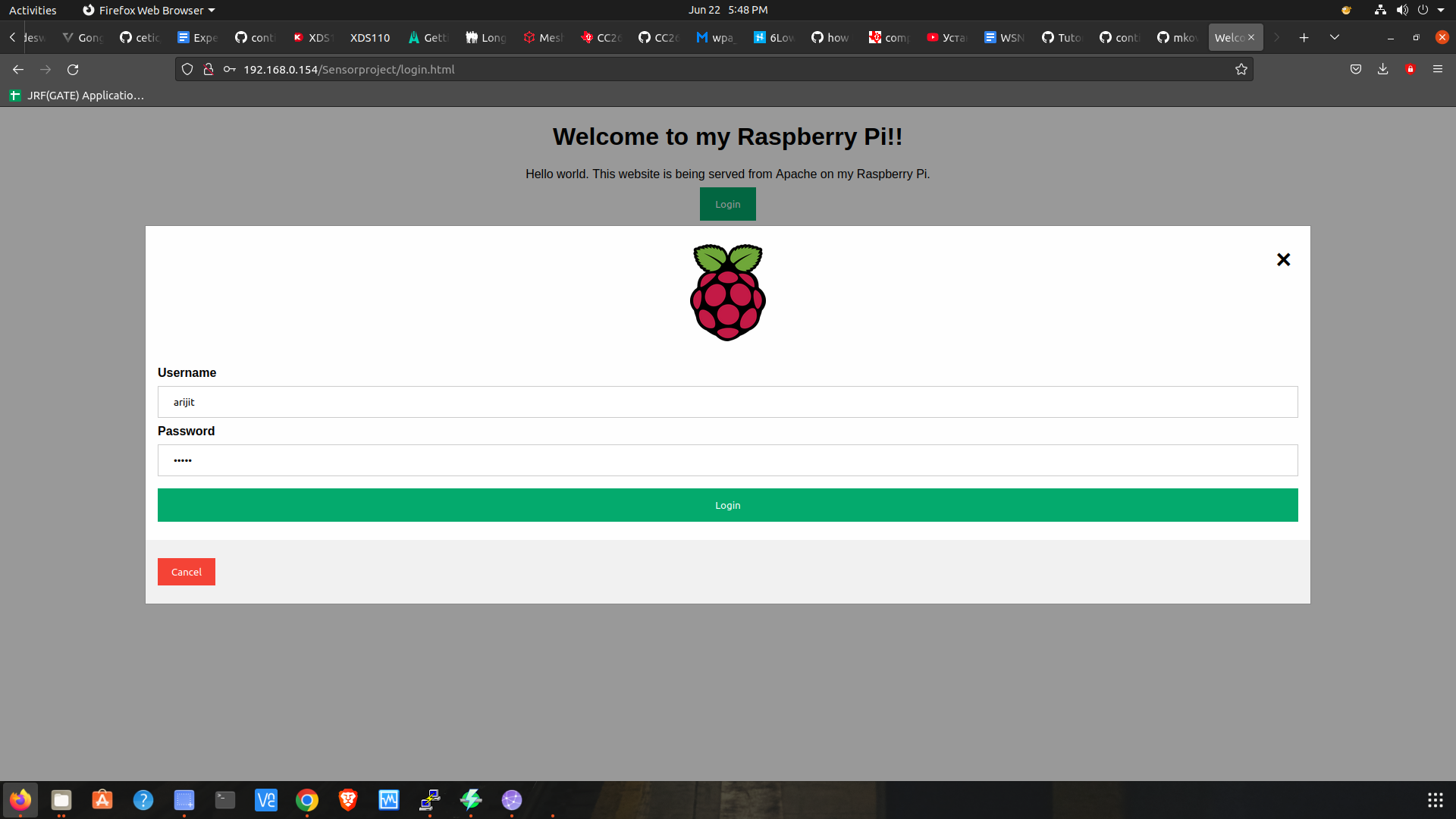
Step 6: Implementing web server in the raspberry pi

1. Download the [MITM Project](https://drive.google.com/drive/folders/12pk92gNw-TGr8n7Nrm0J-9bWGmVl65AM?usp=sharing)
2. Unizip the folder
3. cd /Downloads
4. cp Sensorproject /var/www/html
5. cd /var/www/html/Sensorproject
6. Edit the following:
   1. Change the IP addresses mentioned as 192.168.0.154 in the following files:
      1. signup.php
      2. check.php
      3. Logout.php
   2. Change the web address [fd00::212:4b00:1204:cbd1] with the web address of the web page opened to see the sensortag data in WSN

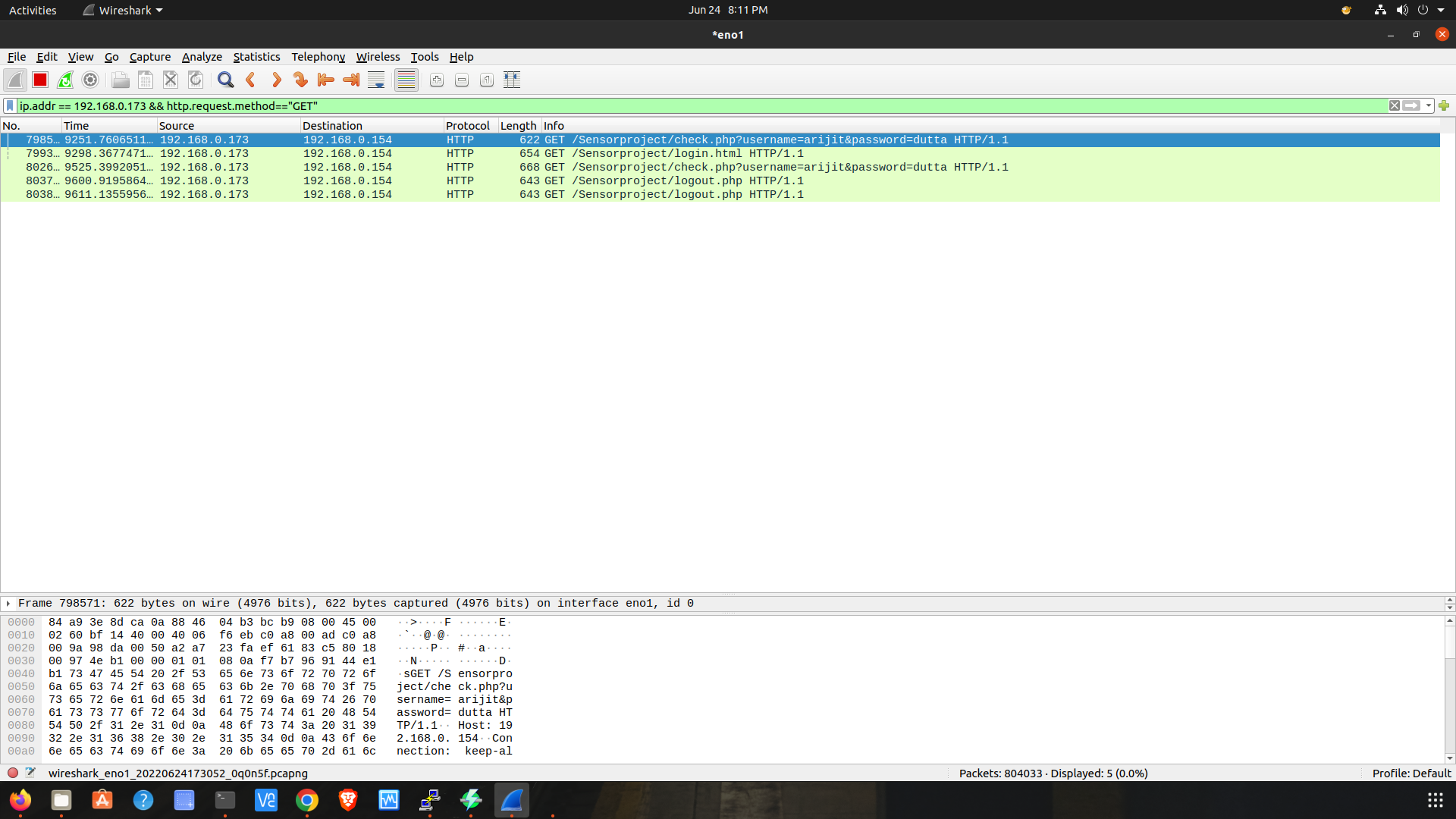
Step 7: Login to check the data as a legitimate user

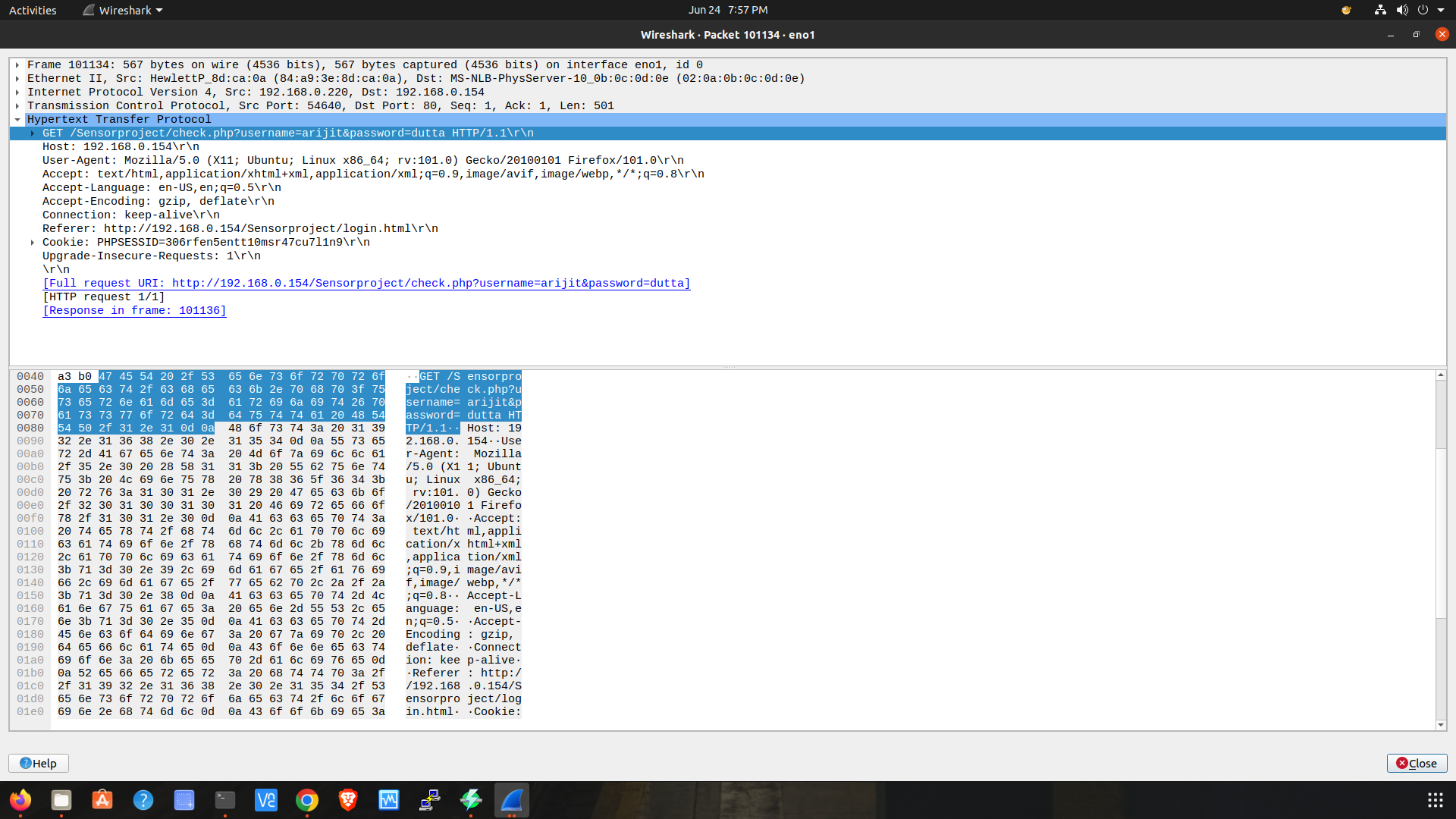
1. As a mobile user login to the [http://*your\_IP\_address/*Sensorproject/login.html](http://your_ip_address/Sensorproject/login.html)
2. Sign up and then login to see the sensor data

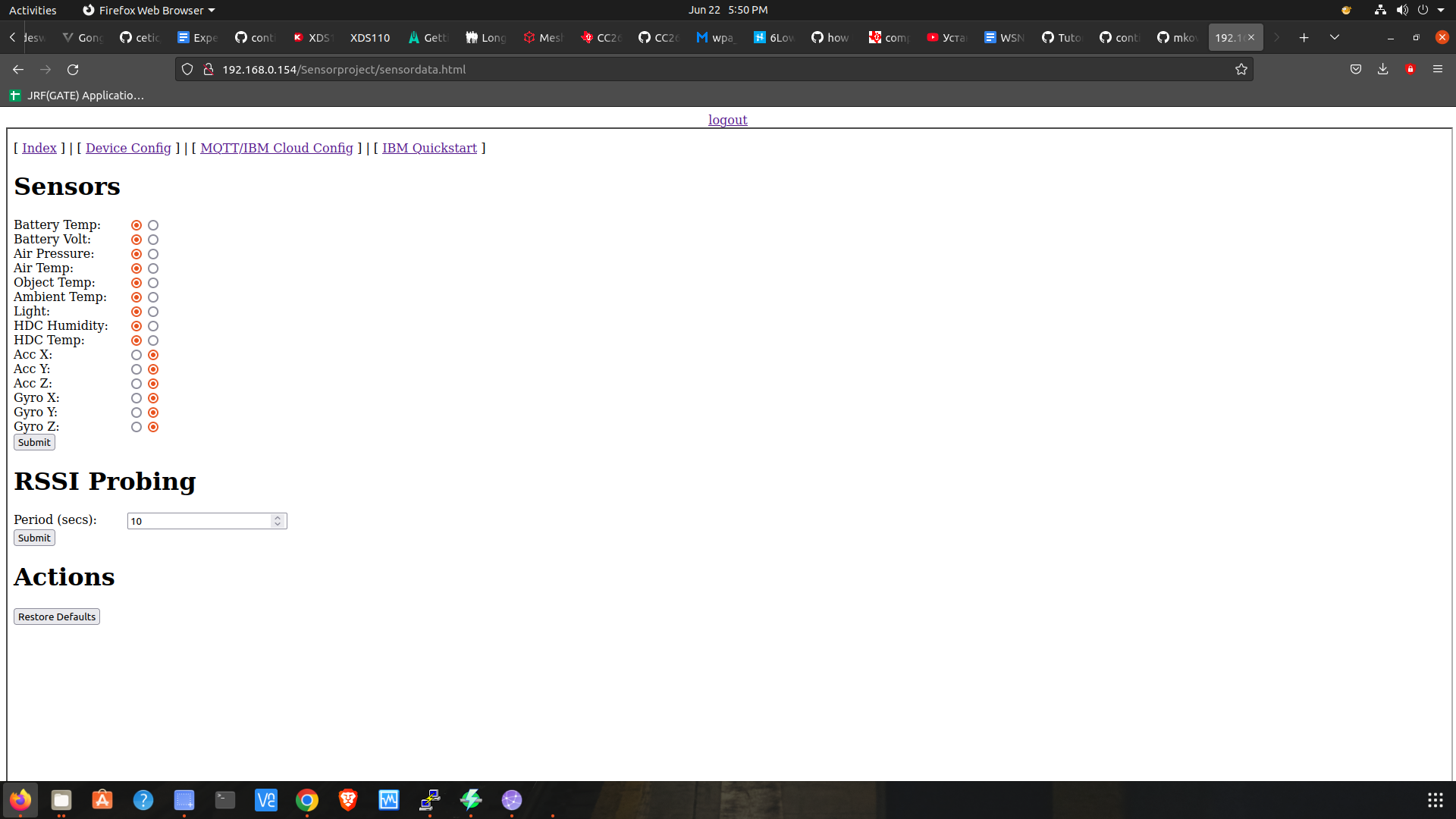




Step 8: Performing the ARP spoof attack

1. Connect the attacker’s system(Linux), mobile user and the Raspberry Pi in the same LAN.network. (Connect the LANs of these devices through a common router)
2. Now In the attacker system install python3 and scapy library using following commands:
   1. sudo apt install python3
   2. sudo pip3 install scapy
3. Now download the following [python script](https://drive.google.com/file/d/1aawoWb6iavskykIztpbZ4qCpcDf2M7Mf/view?usp=sharing) to make arpspoof attack
4. Execute the command in the terminal of attacker system
   1. echo 1 > /proc/sys/net/ipv4/ip\_forward
5. Find out the IP addresses of the mobile user(client) and the Raspberry Pi(server) using any IP scanning tool.
6. Execute the program the following way:
   1. cd ~/Downloads
   2. sudo python3 arpspoof.py
      1. Enter the client ID
      2. Enter the server ID
      3. Attack started
7. Install and open Wireshark software
8. Click on the “eno1” interface to sniff the packets
   1. Type ip.addr == *mobile\_user\_IP\_address* && http.request.method=="GET" in the filter bar

* 1. An http packet will be received as shown in the following picture  
       
       
       
       
       
       
       
       
       
     

1. The user ID and password as plaintext can be read by double clicking on the selected data packet and stop the program by pressing Control+c
2. Now use the same user ID and password to login to the web server as legitimate client and make the alteration in the device configuration and press submit button as follows:

1. The data in the mobile user will start showing as follows:

