DATAFORTE ACADEMY

DEPARTMENT: CYBERSECURITY

INSTRUCTOR: MR SEUN

PROJECT GROUP: DATAFORTE PROTOCOL PIONEERS - GROUP 5

PROJECT TITLE:

UNCOVERING INSECURE COMMUNICATIONS: USING WIRESHARK TO CAPTURE HTTP CREDENTIALS AND RAISE CYBERSECURITY AWARENESS.

PARTICIPANTS:

- CHINEDU ABEL
- ADEBAYO OLUWASEUN
- ADETUNJI DAYO
- RASAQ LUQMAN
- SAMUEL TONY
- OLADEJI OLAJIDE
- OGO MARTINS
- AMOO OLUDARE
- PATRICIA EKPENYONG

This project demonstrates the importance of browsing the internet through websites that use encryption for communication.

TOOLS:

Wireshark, Acunetix website (http://testphp.vulnweb.com)

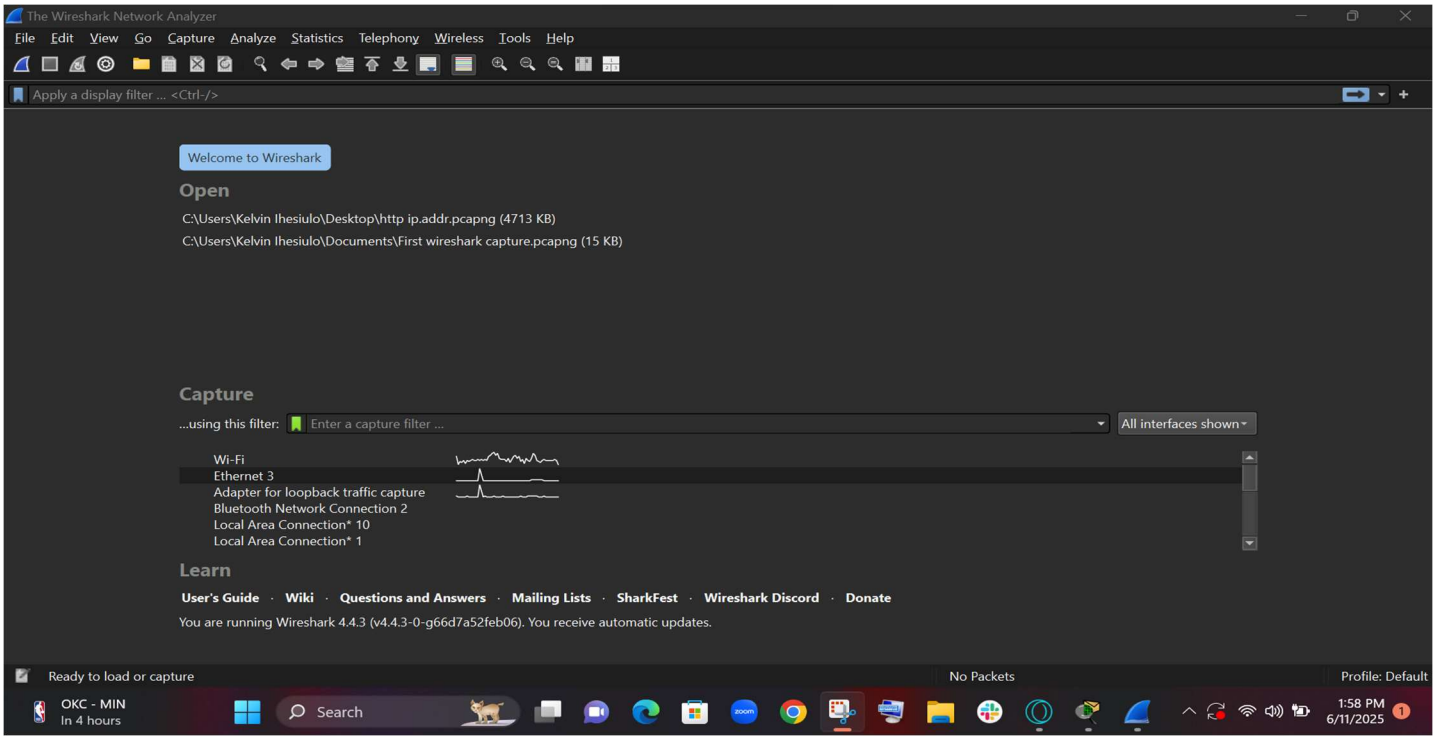
METHOD DESCRIPTION IN STEPS:

- We downloaded Wireshark from https://www.wireshark.org/download

- We Installed it on a designated computer

- We connected the computer to the internet and opened Wireshark.

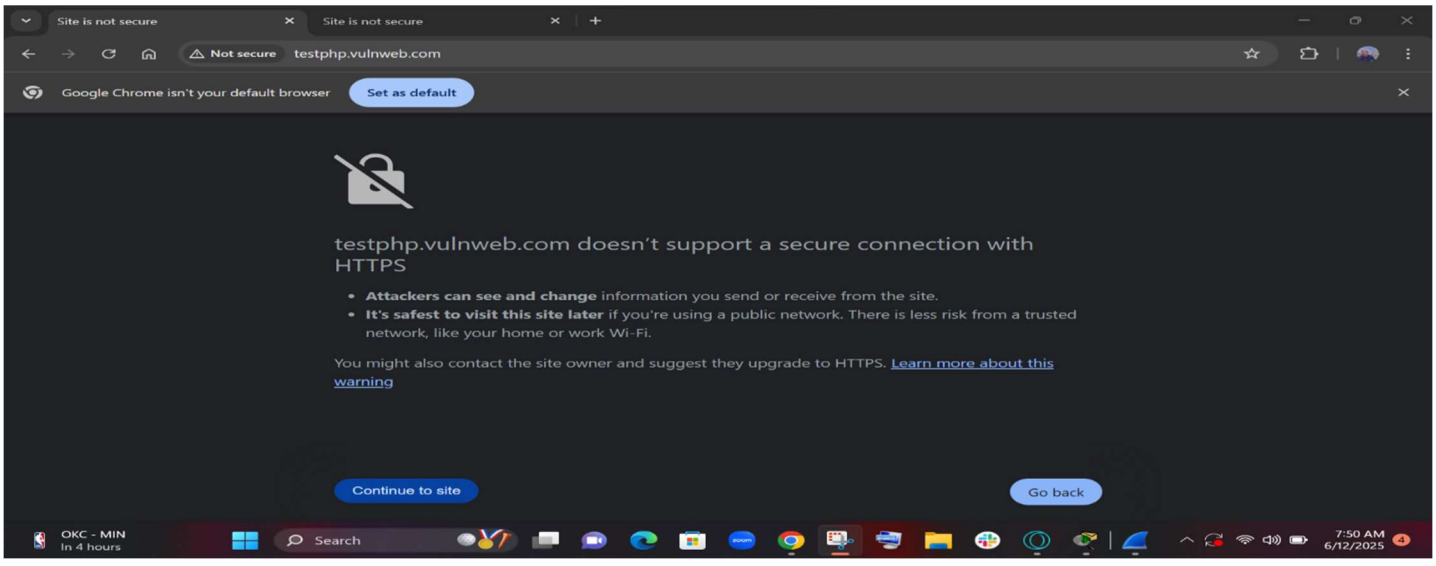
Here, Wireshark homepage is active displaying network from which data can be captured.



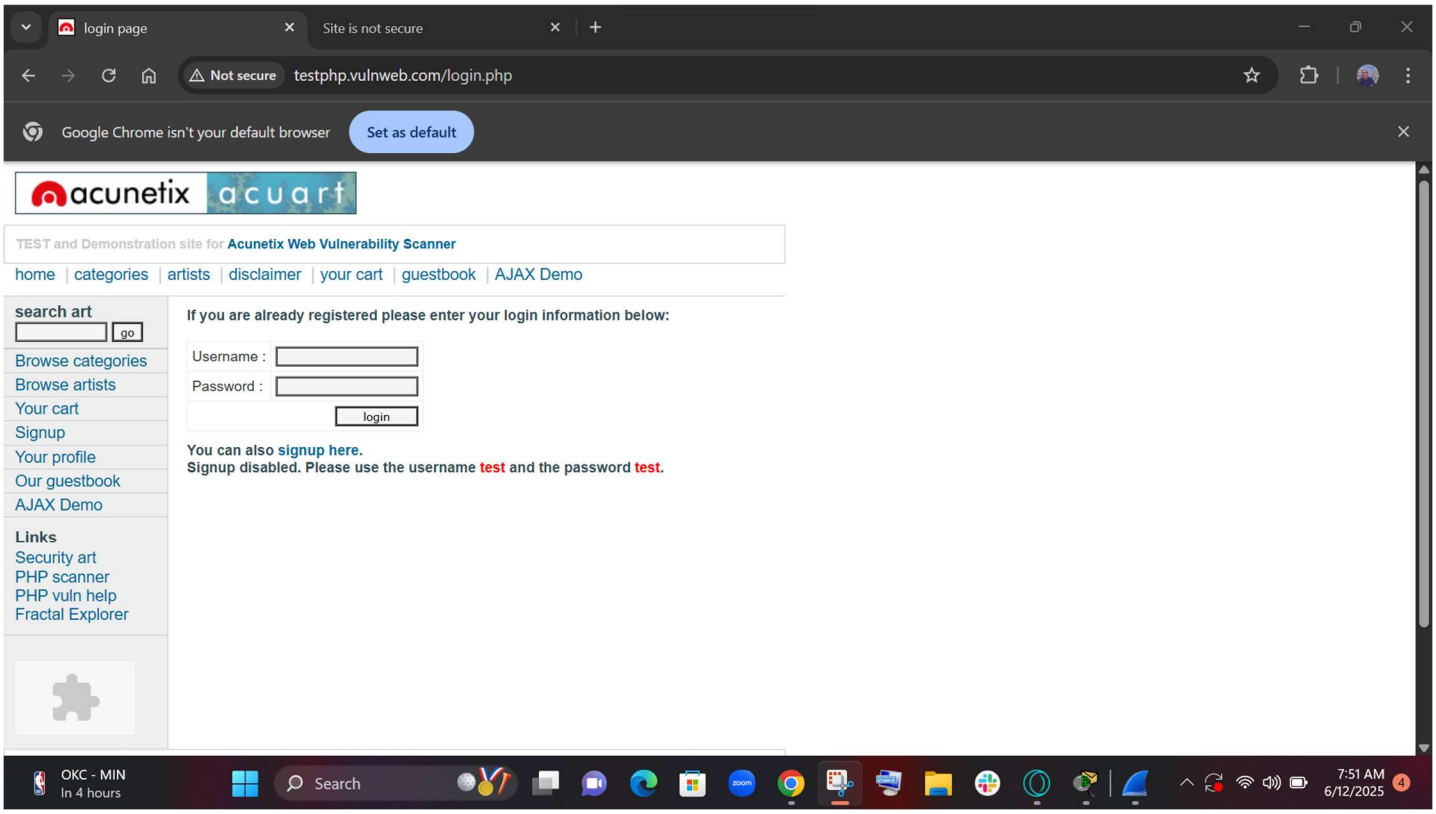
We selected wi-fi so that data packets capture can begin.

-We then visited http://testphp.vulnweb.com

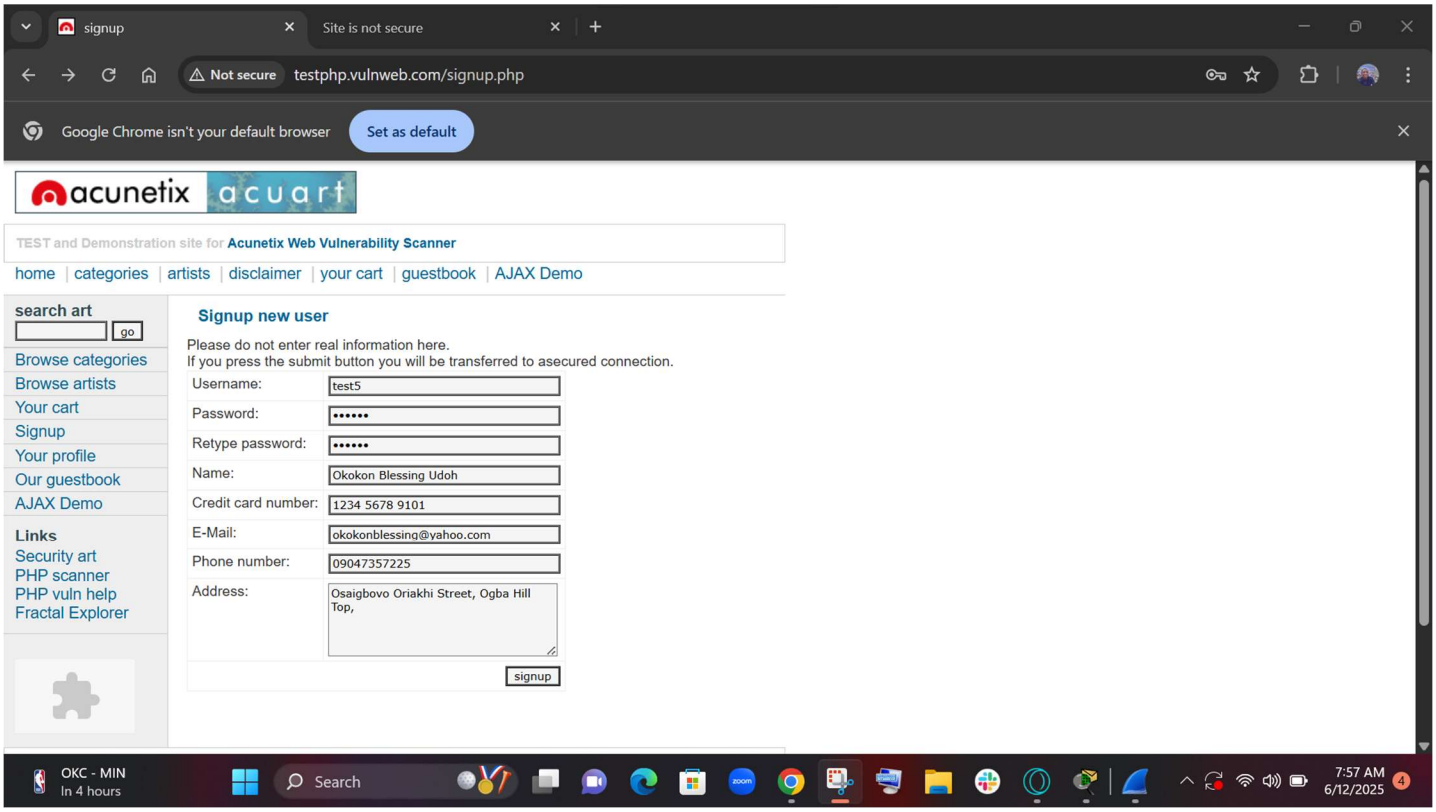
Here the browser displays a warning that the website is unsafe



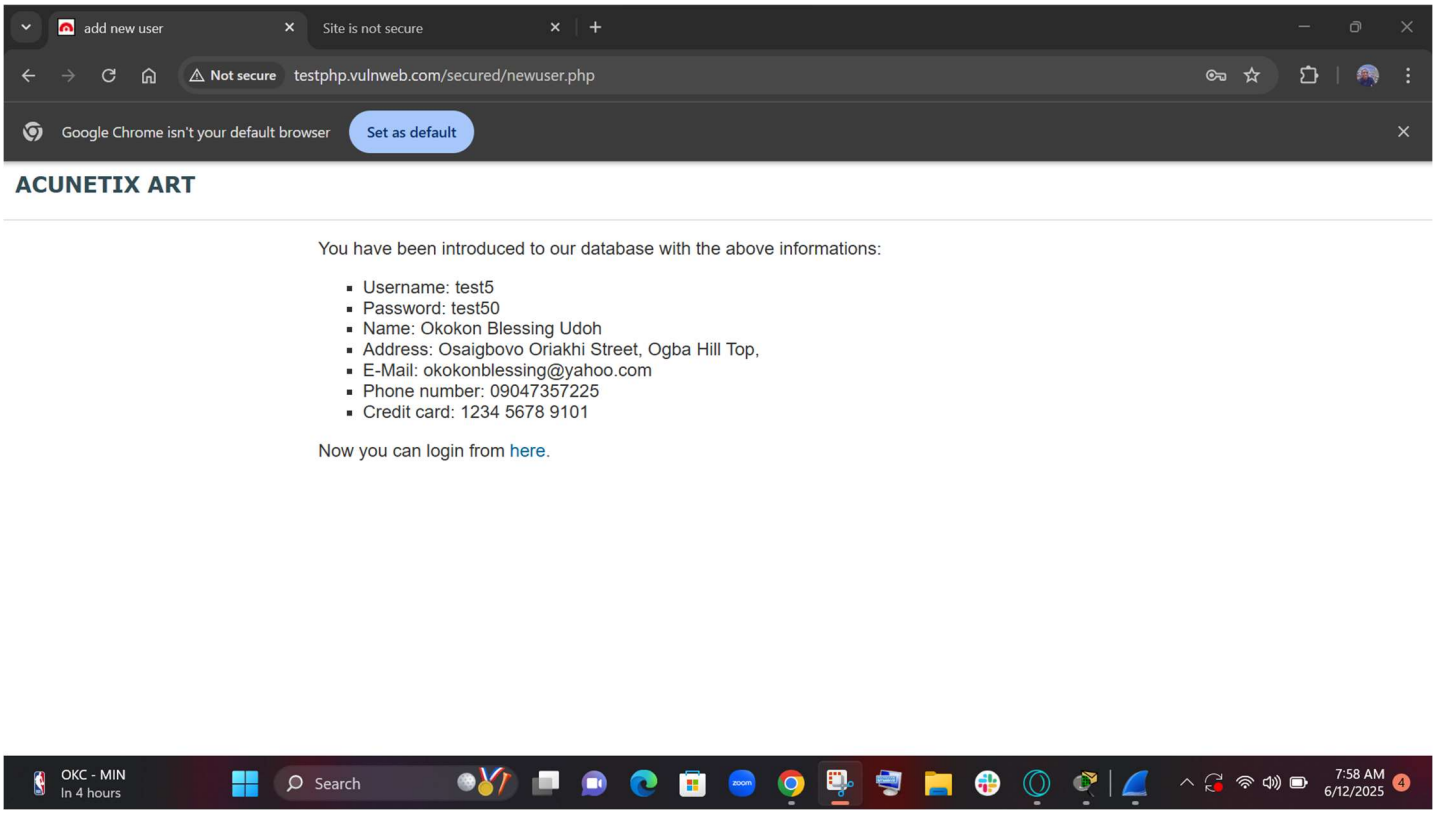
We continued to the site and here, the homepage opened.



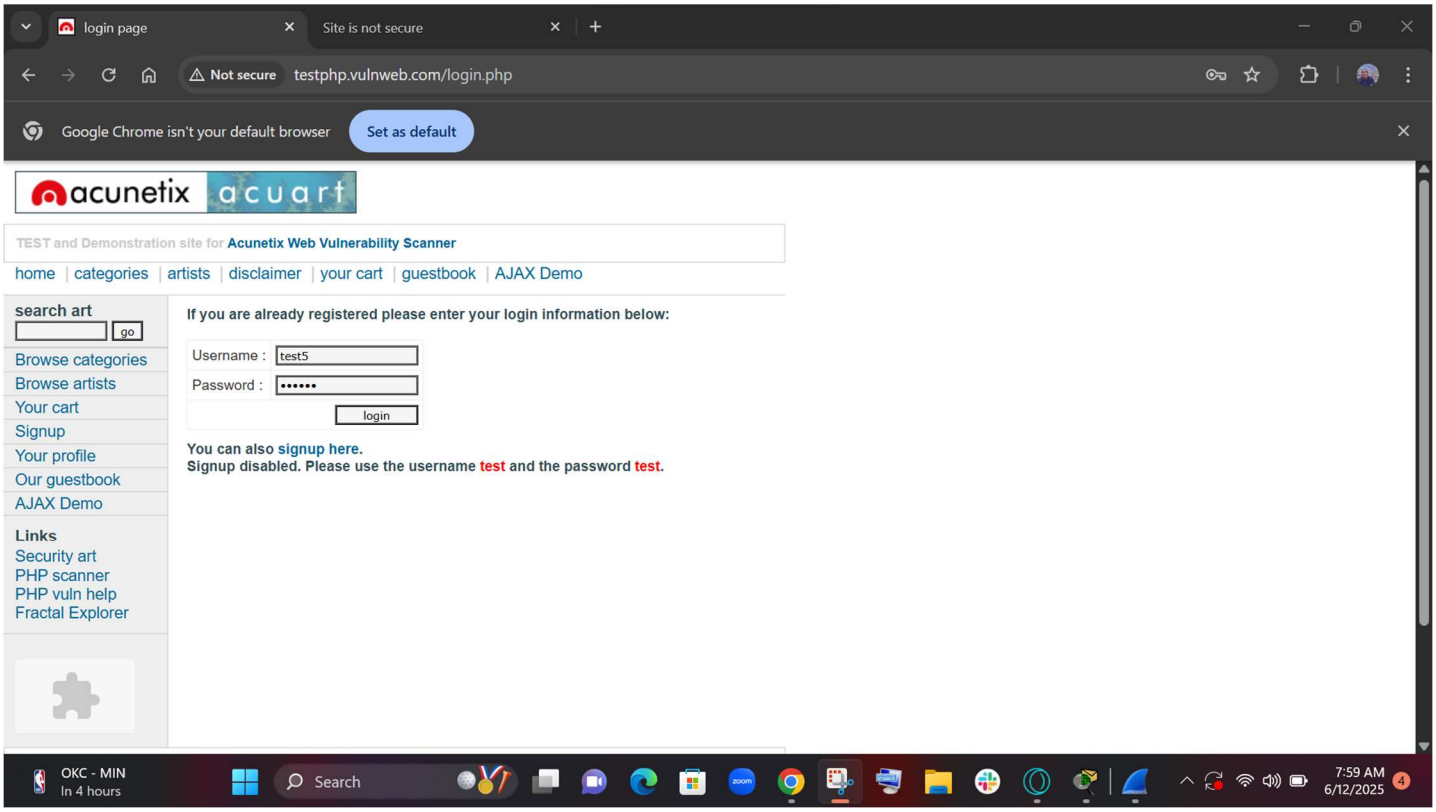
We proceeded to the sign up page to sign up an account with the personal information below.



We successfully opened an account on the Acunetix web platform

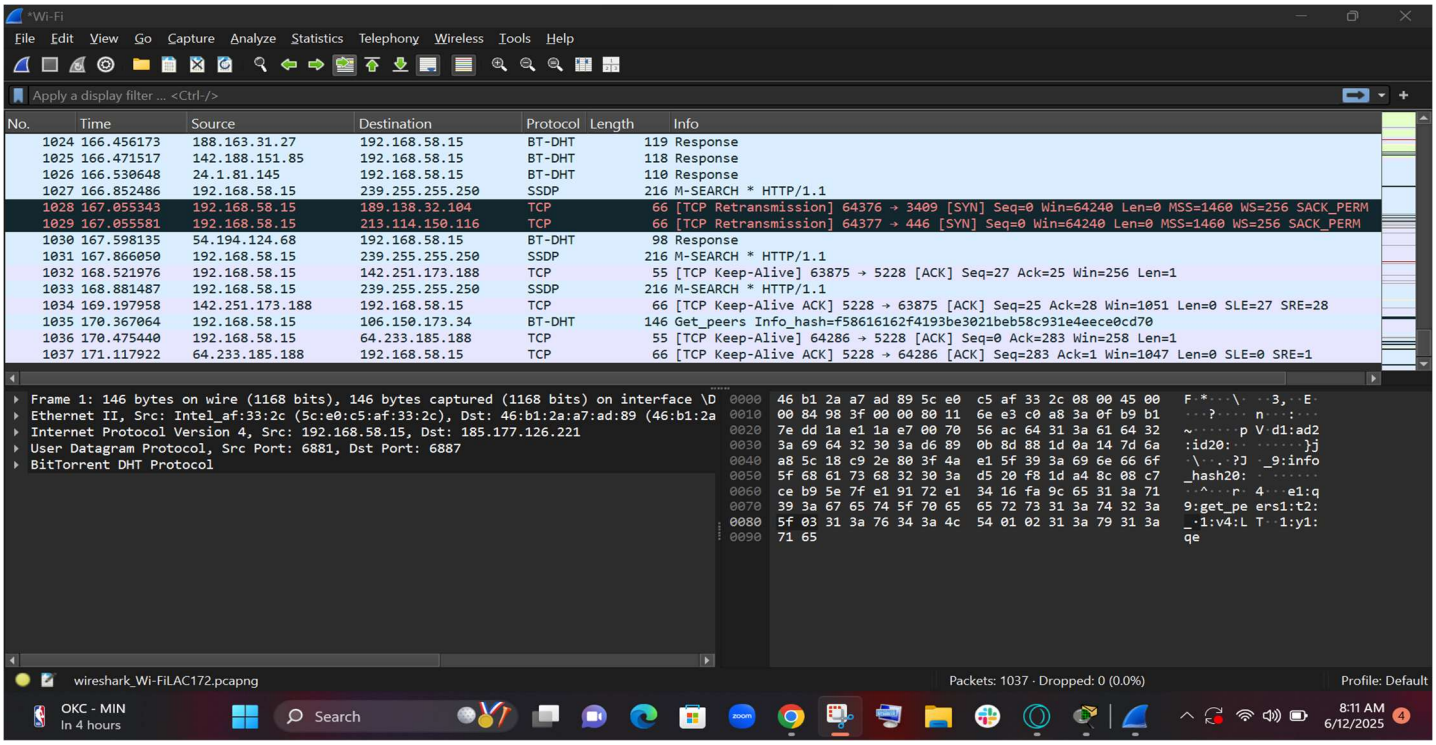


- Then we proceeded to login into the account we created.



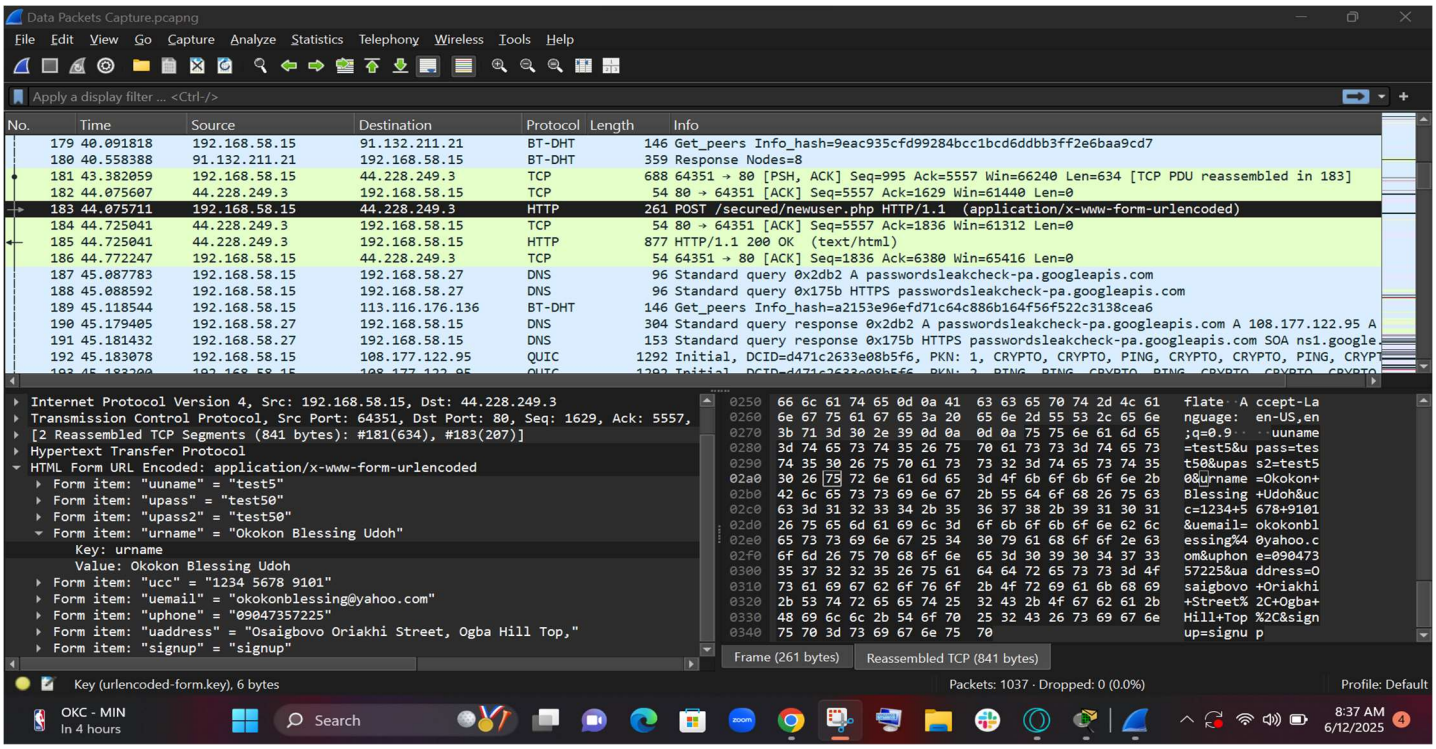
- We went back to Wireshark which has been busy capturing all the data traffic between us and the server hosting the Acunetix website, and we stopped the capture process.

- We then saved the captured data.



- Then we opened the captured data and began to analyse it.

- We started seeing information in plain text containing the credentials we inputed as we were creating the account. This can be seen at the bottom left of the image below.



WHY THIS DEMONSTRATION MATTERS:

In this demonstration we have highlighted that using a web platform that uses http instead of https will expose our data because http does not encrypt data before sending them across a network. The risk associated with this is that our sensitive personal information such as passwords and usernames, or banking information such as credit/debit card details will be viewed by malicious actors who could use them to steal from us or cause other type of harm.

In order to use the internet safely and prevent malicious actors from seeing our sensitive information, there are steps we must follow. One of such steps is to make sure any websites we are visiting is using HTTPS (Hyper Text Transfer Protocol Secured) and not just HTTP (Hyper Text Transfer Protocol).

HTTP transmits information over a network in plain text, making it easy for anyone who captures the data to read it.

HTTPS, on the other hand, uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to encrypte the information before sending them across the network. That way, whoever captures the data will not be able to read it because it's encrypted.

When using the internet therefore there two things one must look out for to be sure he/she is browsing safely;

1. Look for HTTPS in the URL
2. A padlock icon in the address bar

   The padlock icon is a security badge from the browser confirming that the website is safe