Internship Project Report

HTTP Login Credentials Interception Using Wireshark

Submitted by: Shashvat Singh

Date: June 20, 2025

Objective of the Project

The objective of this project is to demonstrate how unencrypted HTTP login forms can expose user credentials. Using Wireshark, we capture and analyze network packets to extract username and password fields submitted through a POST request.

Tools Used

- Wireshark

- Python HTTP Server

- Web Browser (Chrome)

- HTML Form

Step-by-Step Process

1. A simple HTML login form was created and hosted on a local Python HTTP server running on port 8080.

2. The form used the POST method to send username and password fields to the server.

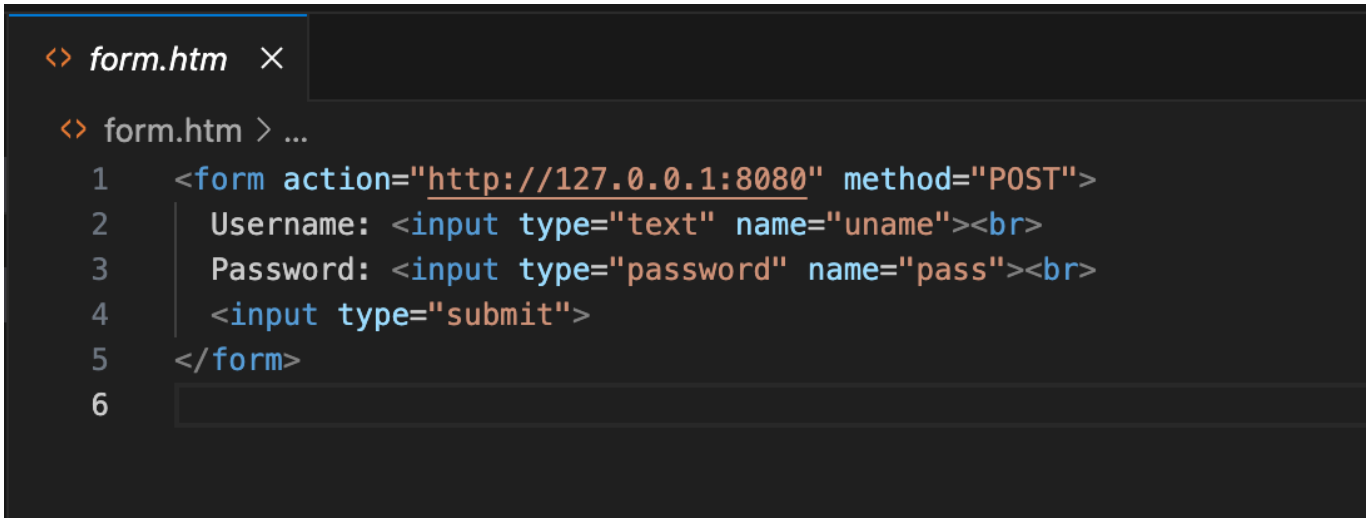
3. Wireshark was started with capture on the loopback interface (lo0).

4. The login form was submitted with credentials (both 'shashvat').

5. A filter (`http.request.method == "POST"`) was applied in Wireshark to isolate relevant packets.

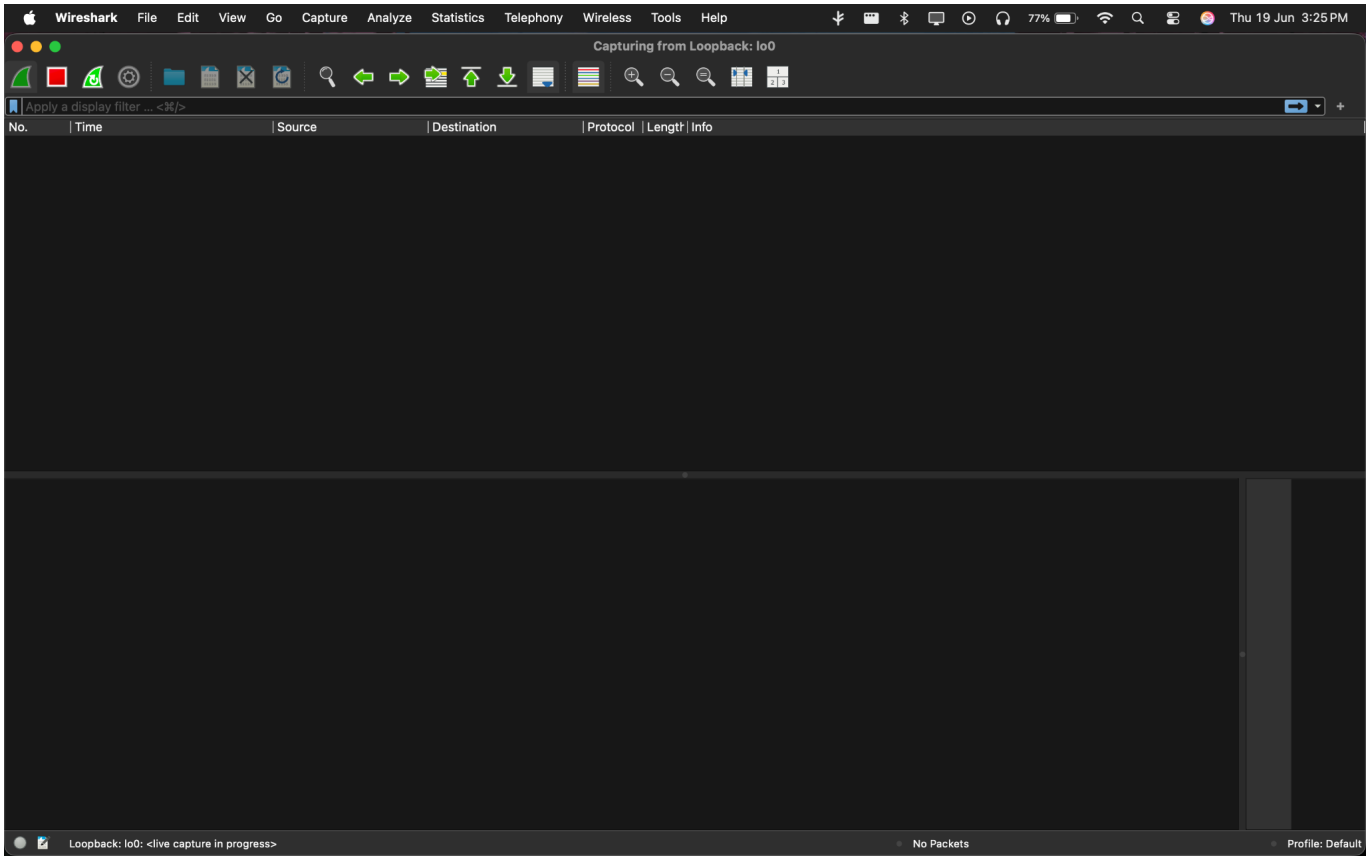
6. The POST packet payload was analyzed to extract the form data and demonstrate that credentials were sent in plaintext.

Login Form Displayed in Browser

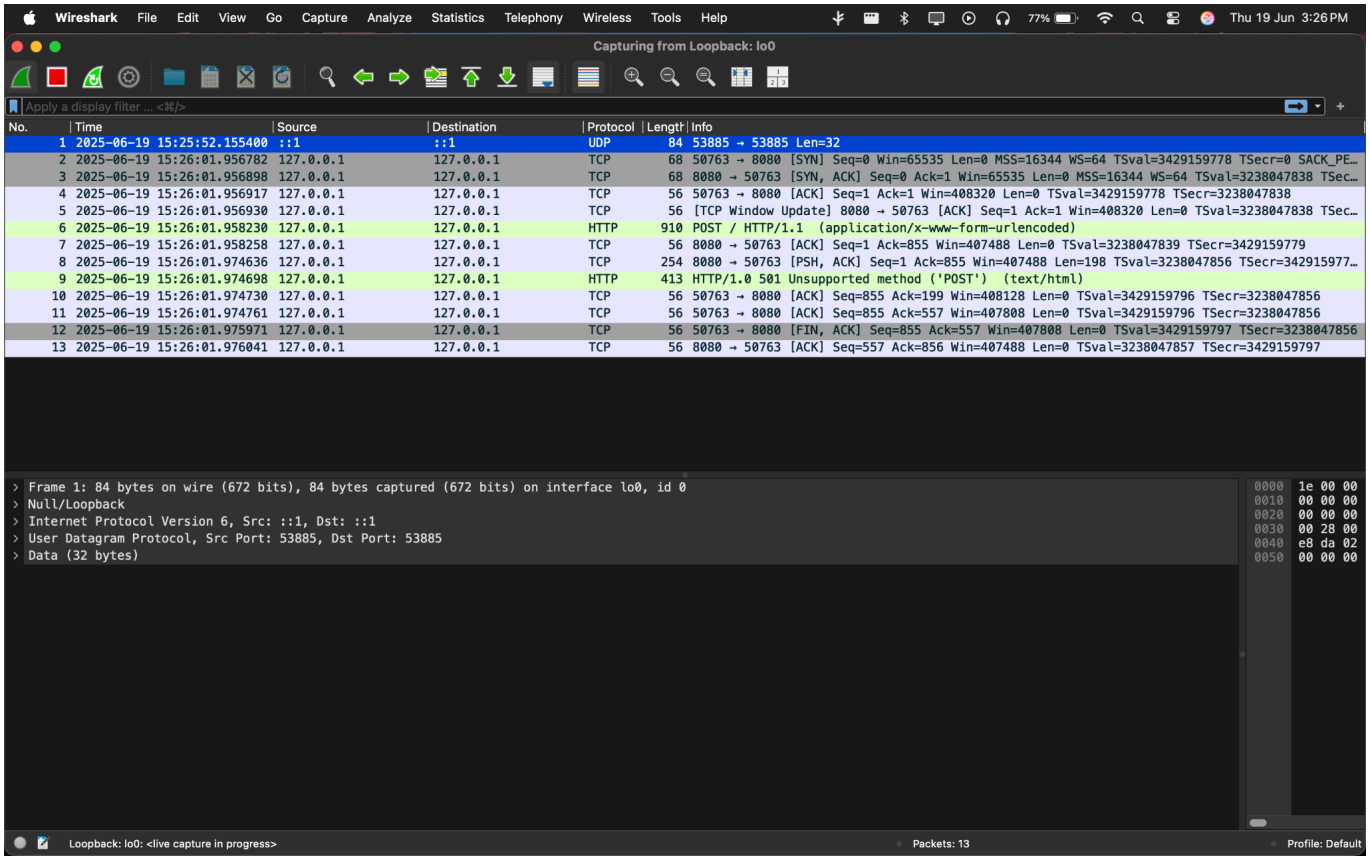


Wireshark Capturing Loopback Traffic

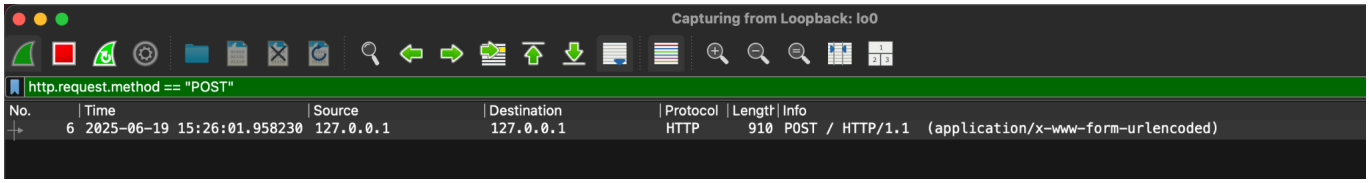
Captured POST Packet Containing Form Data



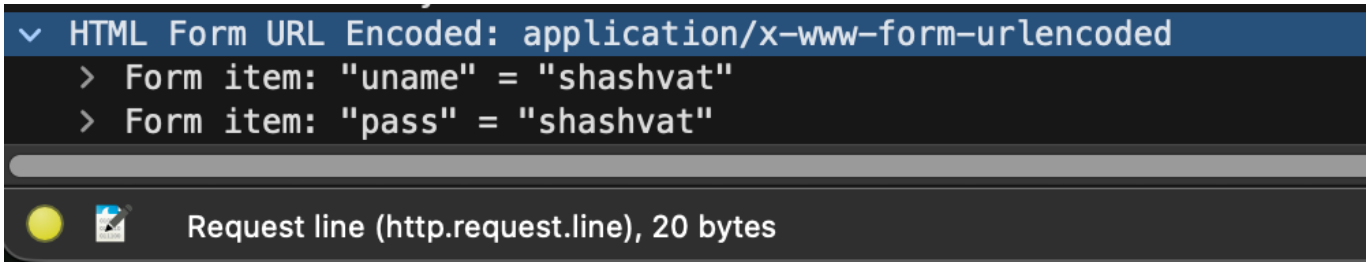
Filtered Display of HTTP POST Packets



Credentials Found Inside Packet Details



Decoded Form Fields with Username and Password



Conclusion

This project highlights the risks of transmitting sensitive information over unencrypted HTTP connections. Using Wireshark, it was clearly shown that login credentials submitted through a POST form can be intercepted and read in plain text. This demonstrates the critical need for using HTTPS to protect user data in transit.