

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

<> form.htm ✕

<> form.htm > ...

```
1  <form action="http://127.0.0.1:8080" method="POST">
2    Username: <input type="text" name="uname"><br>
3    Password: <input type="password" name="pass"><br>
4    <input type="submit">
5  </form>
6
```

Wireshark Capturing Loopback Traffic

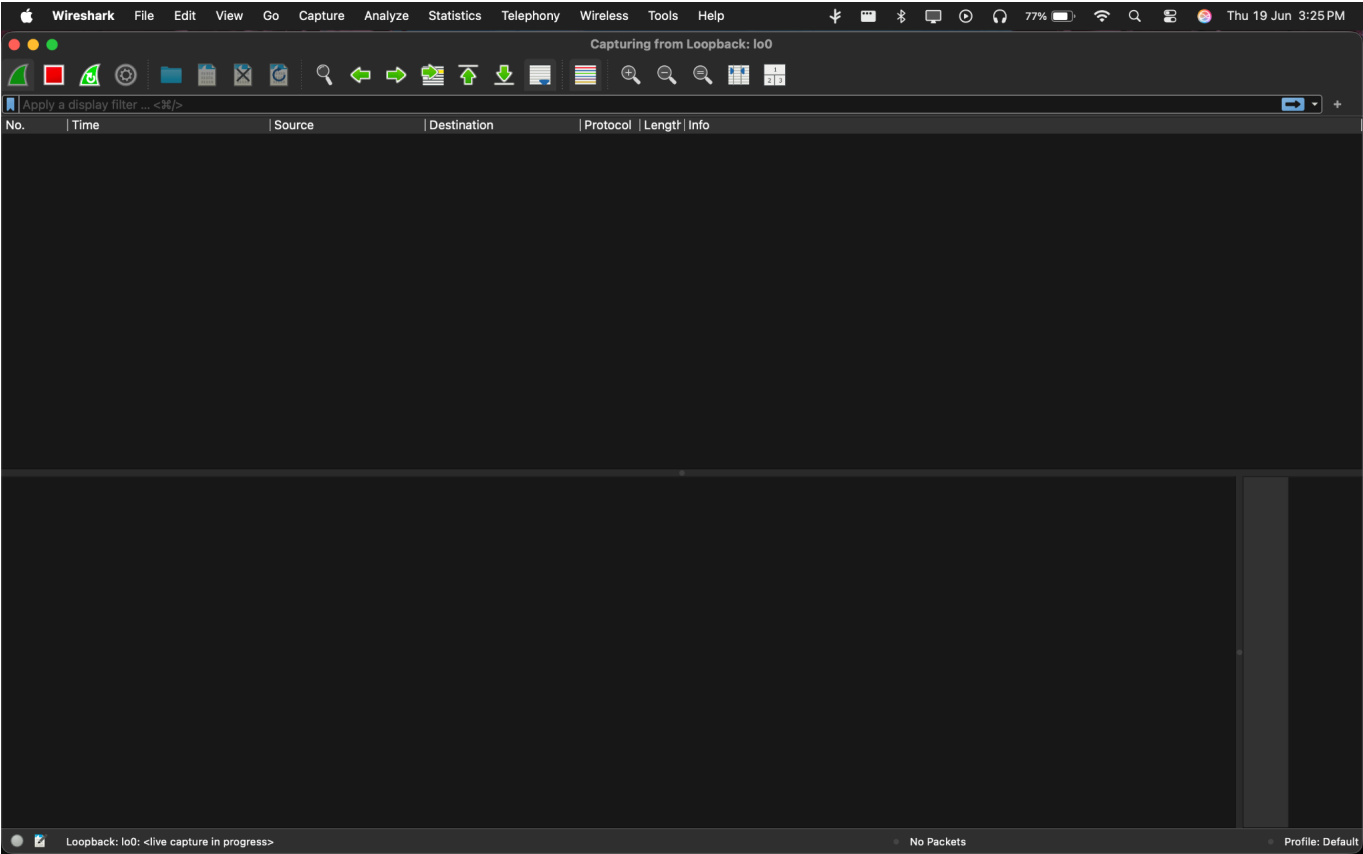
i http://127.0.0.1:8080/form.htm

Username:

Password:

Submit

Captured POST Packet Containing Form Data



Filtered Display of HTTP POST Packets

Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capturing from Loopback: lo0

Apply a display filter ... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2025-06-19 15:25:52.155400	:::1	:::1	UDP	84	53885 → 53885 Len=32
2	2025-06-19 15:26:01.956782	127.0.0.1	127.0.0.1	TCP	68	50763 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=3429159778 TSecr=0 SACK_PE...
3	2025-06-19 15:26:01.956898	127.0.0.1	127.0.0.1	TCP	68	8080 → 50763 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=3238047838 TSecr=...
4	2025-06-19 15:26:01.956917	127.0.0.1	127.0.0.1	TCP	56	50763 → 8080 [ACK] Seq=1 Ack=1 Win=408320 Len=0 TSval=3429159778 TSecr=3238047838
5	2025-06-19 15:26:01.956930	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 8080 → 50763 [ACK] Seq=1 Ack=1 Win=408320 Len=0 TSval=3238047838 TSecr=...
6	2025-06-19 15:26:01.958230	127.0.0.1	127.0.0.1	HTTP	910	POST / HTTP/1.1 (application/x-www-form-urlencoded)
7	2025-06-19 15:26:01.958258	127.0.0.1	127.0.0.1	TCP	56	8080 → 50763 [ACK] Seq=1 Ack=855 Win=407488 Len=0 TSval=3238047839 TSecr=3429159779
8	2025-06-19 15:26:01.974636	127.0.0.1	127.0.0.1	TCP	254	8080 → 50763 [PSH, ACK] Seq=1 Ack=855 Win=407488 Len=198 TSval=3238047856 TSecr=342915977...
9	2025-06-19 15:26:01.974698	127.0.0.1	127.0.0.1	HTTP	413	HTTP/1.0 501 Unsupported method ('POST') (text/html)
10	2025-06-19 15:26:01.974730	127.0.0.1	127.0.0.1	TCP	56	50763 → 8080 [ACK] Seq=855 Ack=199 Win=408128 Len=0 TSval=3429159796 TSecr=3238047856
11	2025-06-19 15:26:01.974761	127.0.0.1	127.0.0.1	TCP	56	50763 → 8080 [ACK] Seq=855 Ack=557 Win=407808 Len=0 TSval=3429159796 TSecr=3238047856
12	2025-06-19 15:26:01.975971	127.0.0.1	127.0.0.1	TCP	56	50763 → 8080 [FIN, ACK] Seq=855 Ack=557 Win=407808 Len=0 TSval=3429159797 TSecr=3238047856
13	2025-06-19 15:26:01.976041	127.0.0.1	127.0.0.1	TCP	56	8080 → 50763 [ACK] Seq=557 Ack=856 Win=407488 Len=0 TSval=3238047857 TSecr=3429159797

> Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface lo0, id 0

> Null/Loopback

> Internet Protocol Version 6, Src: ::1, Dst: ::1

> User Datagram Protocol, Src Port: 53885, Dst Port: 53885

> Data (32 bytes)

0000 1e 00 00

0010 00 00 00

0020 00 00 00

0030 00 28 00

0040 e8 da 02

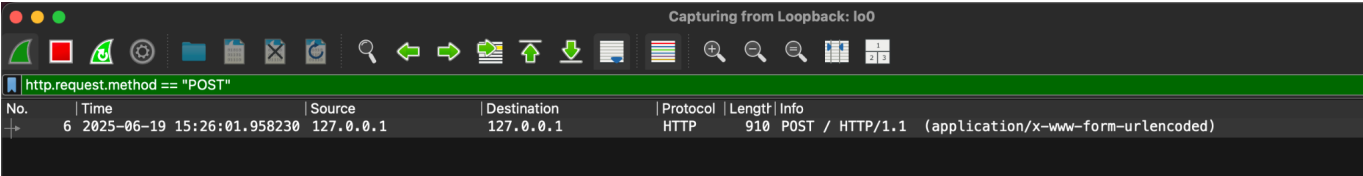
0050 00 00 00

Loopback: lo0: <live capture in progress>

Packets: 13

Profile: Default

Credentials Found Inside Packet Details



Decoded Form Fields with Username and Password

✓ HTML Form URL Encoded: application/x-www-form-urlencoded

> Form item: "uname" = "shashvat"

> Form item: "pass" = "shashvat"



Request line (http.request.line), 20 bytes

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.