🧪 Sniffing Attack using Wireshark

📌 Objective

The goal of this experiment is to demonstrate how credentials (username and password) submitted over an unencrypted HTTP website can be captured using **Wireshark**. The test is performed legally on a publicly available vulnerable web application.

🌐 Target Website

URL: http://testphp.vulnweb.com
Page Used: /login.php

🛠️ Tools Used

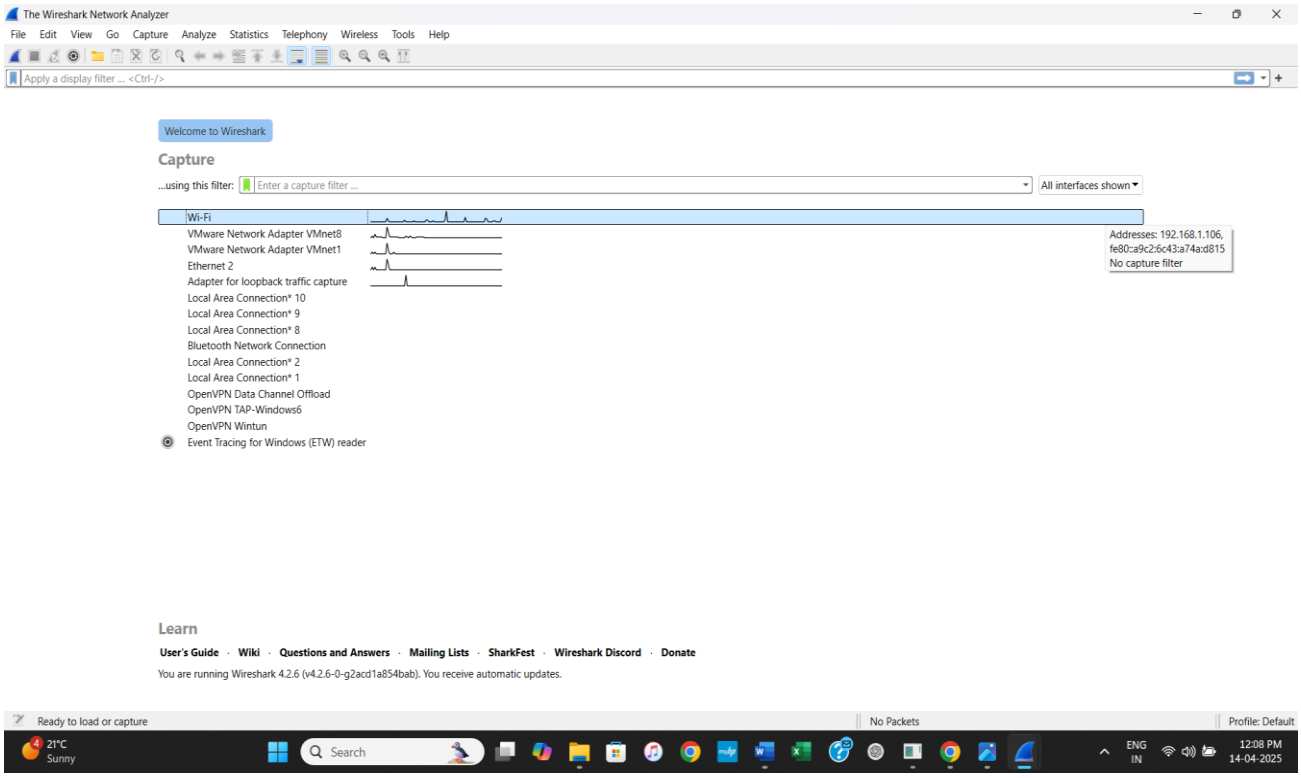
Tool	Purpose
Wireshark	Packet capture and protocol analysis
Web Browser	Used to simulate login
OS	Windows / Linux (any supported OS)

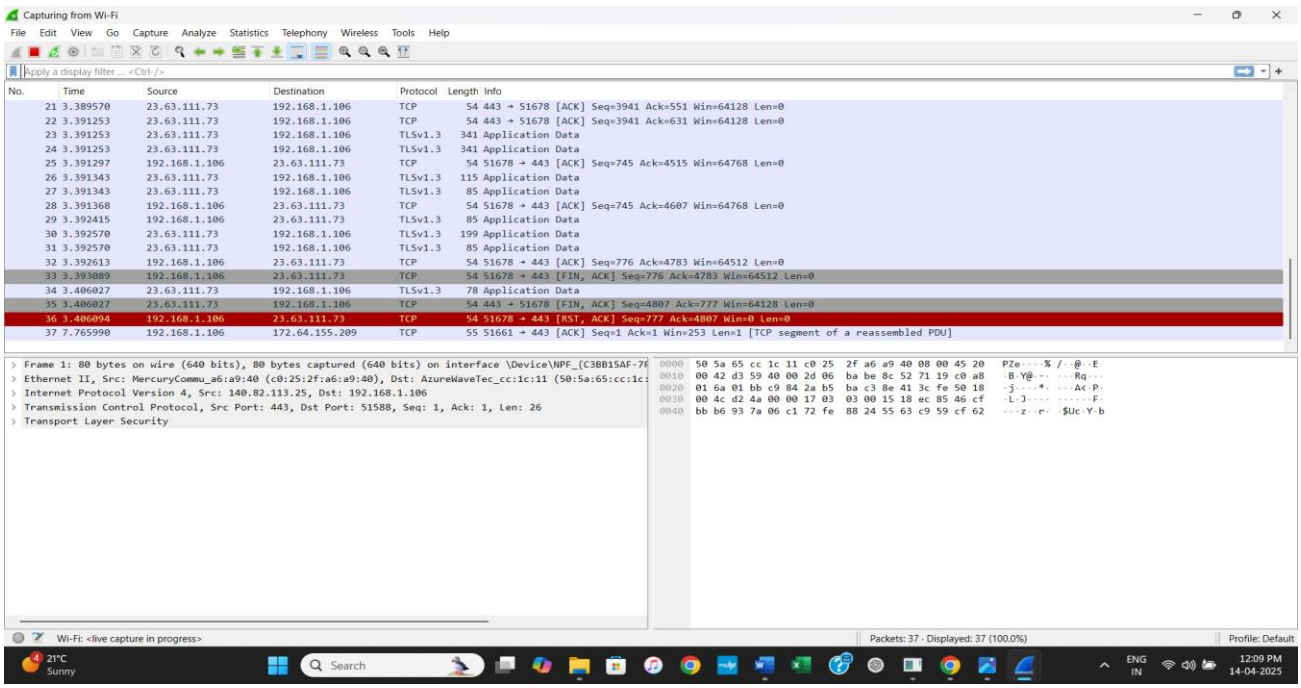
✅ Procedure

---

1. Start Wireshark

- Open Wireshark on your computer.
- Select your active network interface (e.g., Wi-Fi or Ethernet).
- Click **Start** to begin capturing packets.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
OpenVPN Data Channel Offload
OpenVPN TAP-Windows6
OpenVPN Wintun
Event Tracing for Windows (ETW) reader
Addresses: 192.168.1.106, fe80::a9c2:6c43:a74a:d815
No capture filter
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.6 (v4.2.6-0-g2acd1a854bab). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
21°C Sunny
Search
ENG IN
12:08 PM 14-04-2025


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
21 3.389570 23.63.111.73 192.168.1.106 TCP 54 443 → 51678 [ACK] Seq=3941 Ack=551 Win=64128 Len=0
22 3.391253 23.63.111.73 192.168.1.106 TCP 54 443 → 51678 [ACK] Seq=3941 Ack=631 Win=64128 Len=0
23 3.391253 23.63.111.73 192.168.1.106 TLSv1.3 341 Application Data
24 3.391253 23.63.111.73 192.168.1.106 TLSv1.3 341 Application Data
25 3.391297 192.168.1.106 23.63.111.73 TCP 54 51678 → 443 [ACK] Seq=745 Ack=4515 Win=64768 Len=0
26 3.391343 23.63.111.73 192.168.1.106 TLSv1.3 115 Application Data
27 3.391343 23.63.111.73 192.168.1.106 TLSv1.3 85 Application Data
28 3.391368 192.168.1.106 23.63.111.73 TCP 54 51678 → 443 [ACK] Seq=745 Ack=4607 Win=64768 Len=0
29 3.392415 192.168.1.106 23.63.111.73 TLSv1.3 85 Application Data
30 3.392570 23.63.111.73 192.168.1.106 TLSv1.3 199 Application Data
31 3.392570 23.63.111.73 192.168.1.106 TLSv1.3 85 Application Data
32 3.392613 192.168.1.106 23.63.111.73 TCP 54 51678 → 443 [ACK] Seq=776 Ack=4783 Win=64512 Len=0
33 3.393089 192.168.1.106 23.63.111.73 TCP 54 51678 → 443 [FIN, ACK] Seq=776 Ack=4783 Win=64512 Len=0
34 3.406027 23.63.111.73 192.168.1.106 TLSv1.3 78 Application Data
35 3.406027 23.63.111.73 192.168.1.106 TCP 54 443 → 51678 [FIN, ACK] Seq=4807 Ack=777 Win=64128 Len=0
36 3.406094 192.168.1.106 23.63.111.73 TCP 54 51678 → 443 [RST, ACK] Seq=777 Ack=4807 Win=0 Len=0
37 7.765990 192.168.1.106 172.64.155.209 TCP 55 51661 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{C3BB15AF-7E
Ethernet II, Src: MercuryCommu_a6:a9:40 (c0:25:2f:a6:a9:40), Dst: AzureWaveTec_cc:1c:11 (50:5a:65:cc:1c:
Internet Protocol Version 4, Src: 140.82.113.25, Dst: 192.168.1.106
Transmission Control Protocol, Src Port: 443, Dst Port: 51588, Seq: 1, Ack: 1, Len: 26
Transport Layer Security
0000 50 5a 65 cc 1c 11 c0 25 2f a6 a9 40 08 00 45 20 PZe····% /··@··E
0010 00 42 d3 59 40 00 2d 06 ba be 8c 52 71 19 c0 a8 ·B·Y@·-· ···Rq···
0020 01 6a 01 bb c9 84 2a b5 ba c3 8e 41 3c fe 50 18 ·j····*· ···A<·P·
0030 00 4c d2 4a 00 00 17 03 03 00 15 18 ec 85 46 cf ·L·J···· ·····F·
0040 bb b6 93 7a 06 c1 72 fe 88 24 55 63 c9 59 cf 62 ···z··r· ·$Uc·Y·b
Wi-Fi: <live capture in progress>
Packets: 37 · Displayed: 37 (100.0%)
Profile: Default
21°C Sunny
Search
ENG IN
12:09 PM 14-04-2025

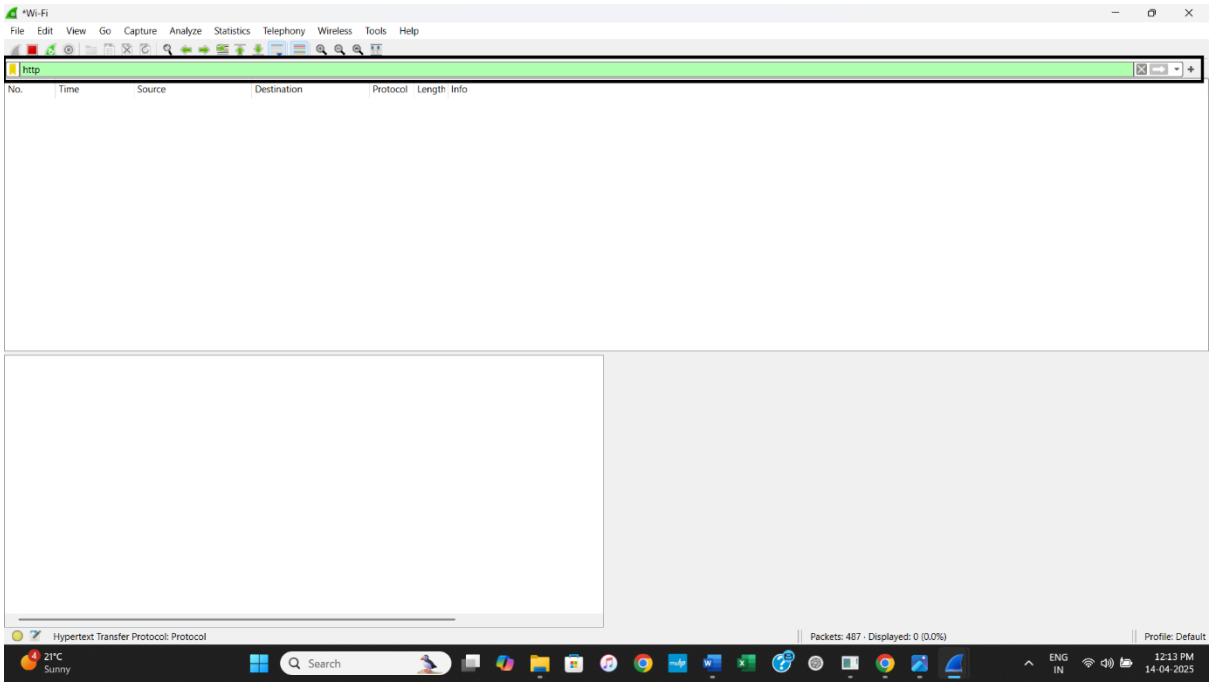
2. Apply Filter (Optional)

To only show HTTP traffic, apply the display filter:

- **http**

To focus on login attempts:

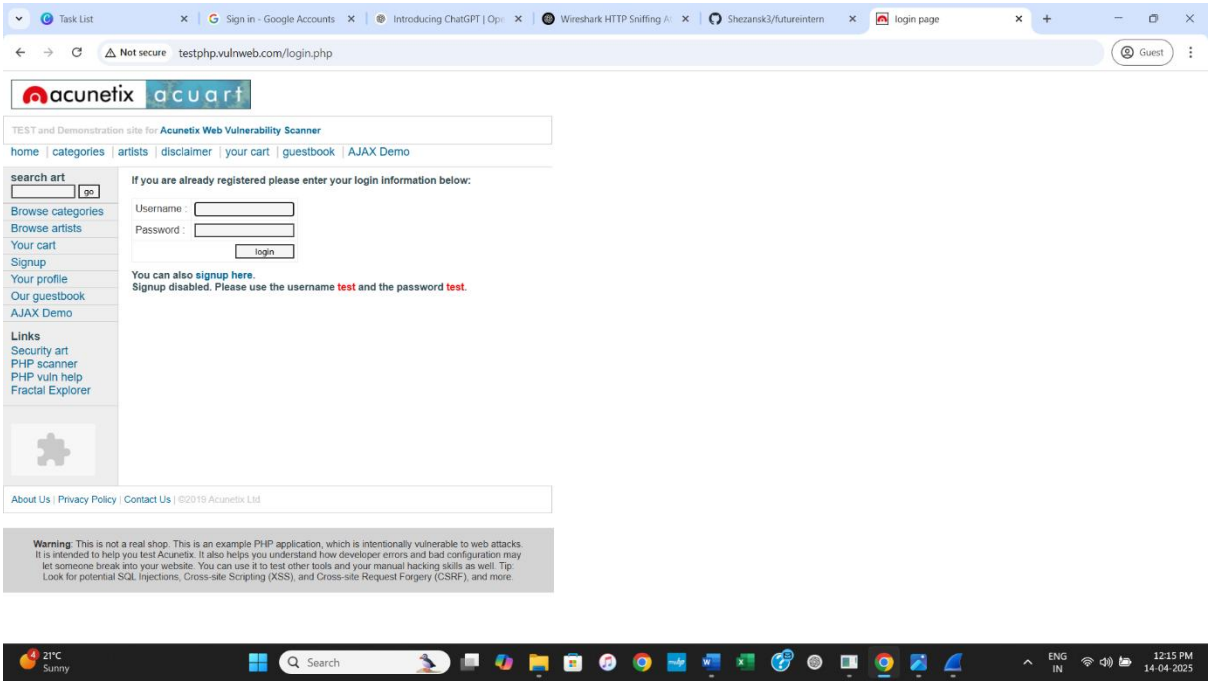
- **http.request.method == "POST"**



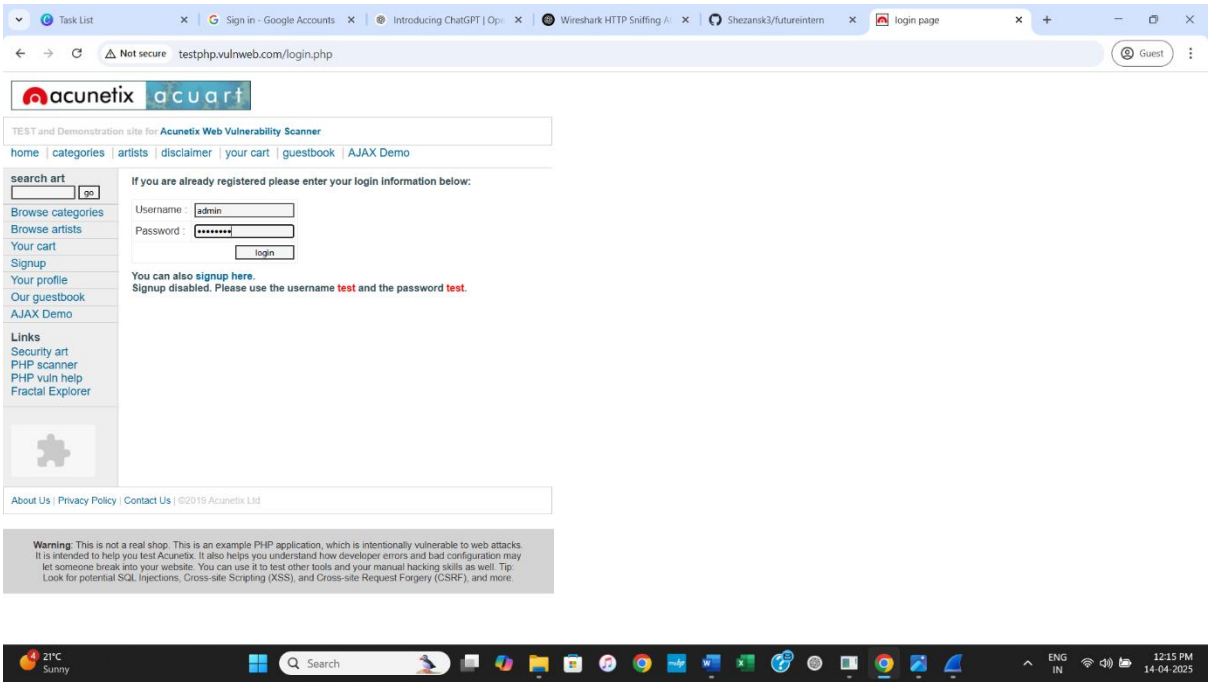
---

3. Perform Login on Target Site

- Open your web browser.
- Navigate to: http://testphp.vulnweb.com/login.php



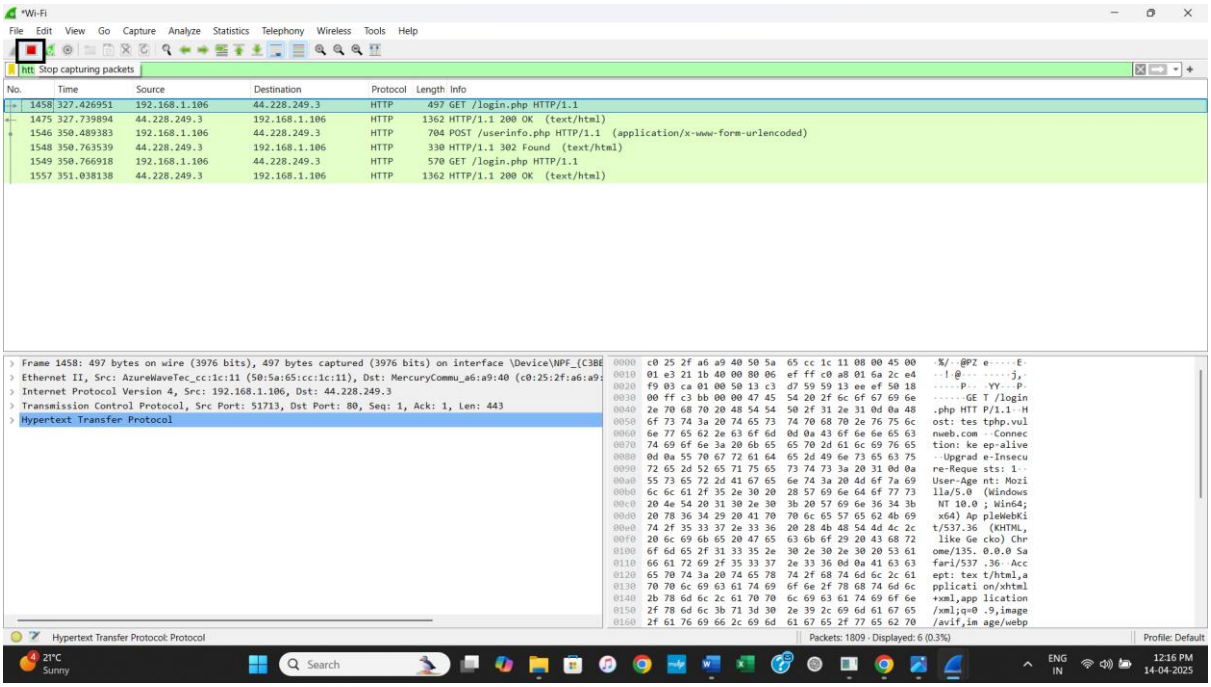
- Enter the following credentials:
    - **Username:** admin
    - **Password:** admin123
- Click the **Login** button.



---

4. Stop Packet Capture

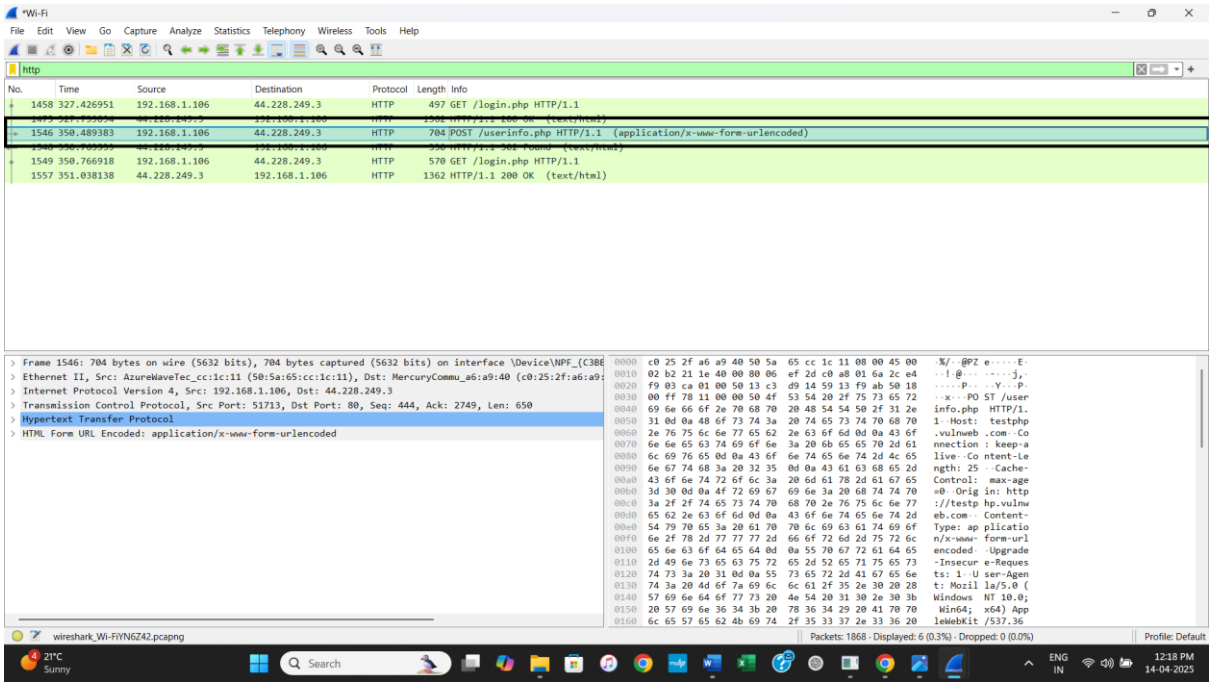
- Return to Wireshark.
- Click the **Stop** button (red square) to end the capture.



---

5. Locate and Follow the POST Request

- Find the HTTP POST request to /login.php.
- Right-click on the packet → Select **Follow** → **HTTP Stream**.



---

6. Analyze the Captured Data

You should see data like this:

- **POST /login.php HTTP/1.1**

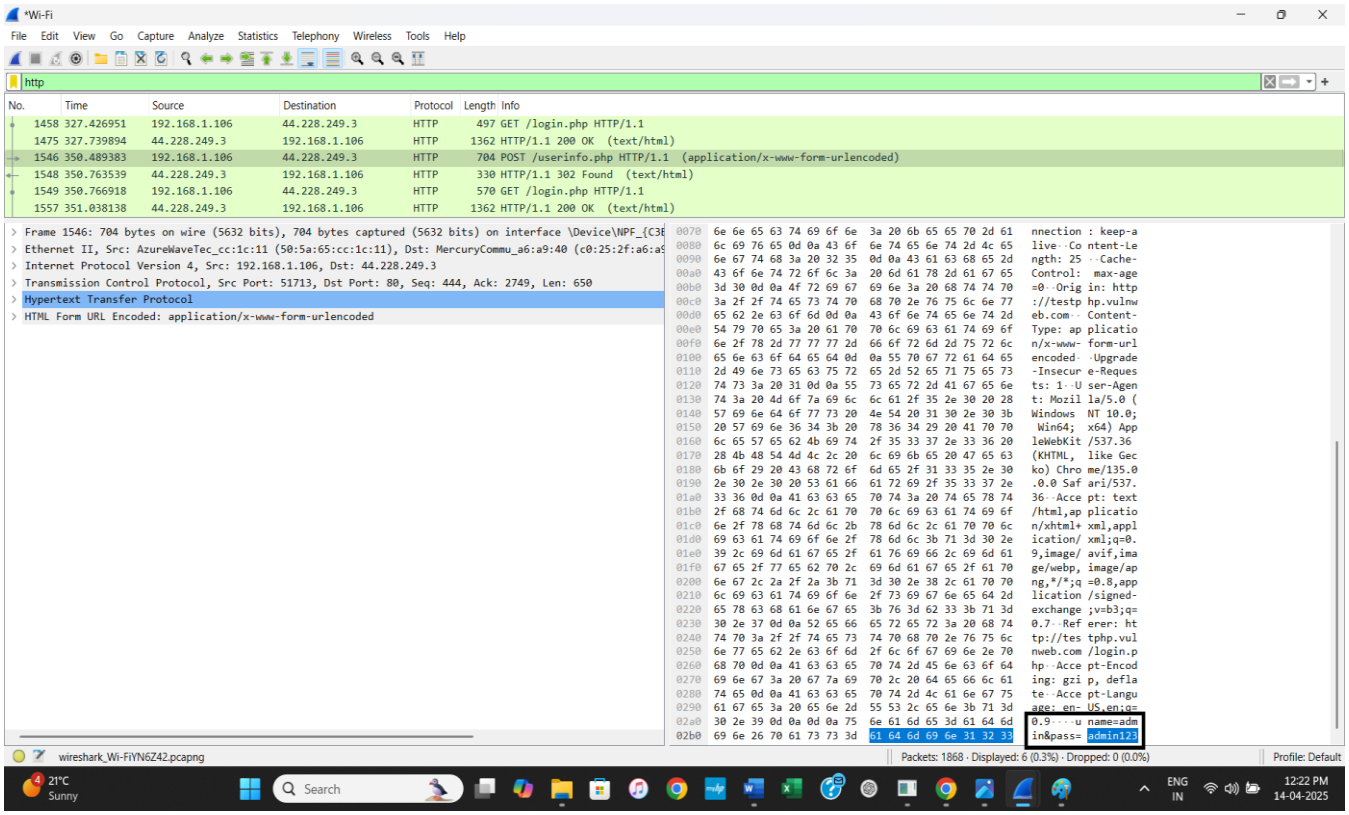
Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 ...

Content-Type: application/x-www-form-urlencoded

Content-Length: ...

- **uname=admin&pass=admin123&login=login**



Captured Information

Field	Value
Username	admin
Password	admin123