🛡️ Wireshark Packet Capture Report – Credential Leak Analysis

1. 🔍 Objective:

To analyze HTTP network traffic using Wireshark and identify sensitive information (username/password) transmitted in plain text, useful for SOC analyst interviews.

---

2. 🖥️ Lab Setup:

- **OS:** macOS (M2)
- **Target Website:** testphp.vulnweb.com
- **Browser Used:** Firefox
- **Action Performed:** Opened login page to observe packet flow
- **Wireshark Filter:** http

3. 📡 Captured HTTP Request (GET):

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15)
Accept: text/html
Connection: keep-alive
```

4. 📫 Captured HTTP Response (200 OK):

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Content-Type: text/html
Content-Encoding: gzip
```

Inside the response body:

```
If you are already registered please enter your login information below:
<form method="post" action="userinfo.php">
Username: test
Password: test
```

🟢 This confirms **login credentials were visible over plain-text HTTP**.

---

5. ⚠️ Key Observation:

- The login form transmits credentials **without encryption**.
- Vulnerable to **Man-in-the-Middle (MITM)** attacks on public/shared

networks.

---

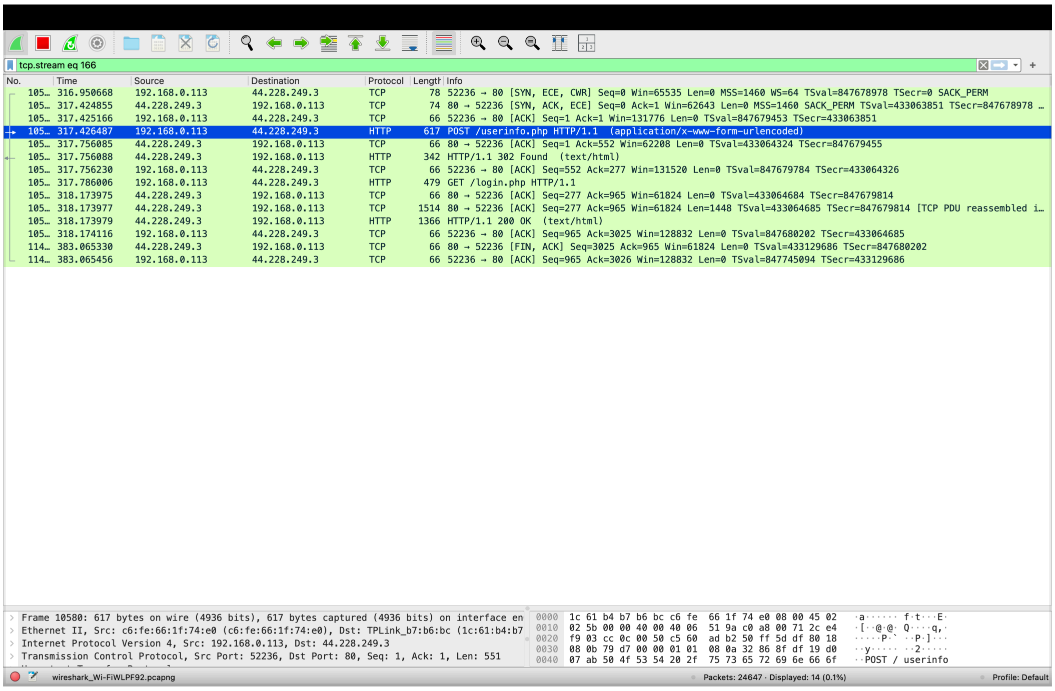
6. ✅ Conclusion :

This capture demonstrates a **real-world security gap** — unencrypted login forms. It shows ability to:

- Use Wireshark to analyze real traffic
- Filter & extract HTTP data
- Understand implications of insecure data transmission

📷 Attachments:

- Screenshot of HTTP POST packet
- Full TCP Stream view



[redacted]

```
tcp.stream eq 166

No.     Time        Source         Destination    Protocol Length Info
  105…  316.950668  192.168.0.113  44.228.249.3   TCP        78 52236 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=847678978 TSecr=0 SACK_PERM
  105…  317.424855  44.228.249.3   192.168.0.113  TCP        74 80 → 52236 [SYN, ACK, ECE] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM TSval=433063851 TSecr=847678978 …
  105…  317.425166  192.168.0.113  44.228.249.3   TCP        66 52236 → 80 [ACK] Seq=1 Ack=1 Win=131776 Len=0 TSval=847679453 TSecr=433063851
  105…  317.426487  192.168.0.113  44.228.249.3   HTTP      617 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  105…  317.756085  44.228.249.3   192.168.0.113  TCP        66 80 → 52236 [ACK] Seq=1 Ack=552 Win=62208 Len=0 TSval=433064324 TSecr=847679455
  105…  317.756088  44.228.249.3   192.168.0.113  HTTP      342 HTTP/1.1 302 Found  (text/html)
  105…  317.756230  192.168.0.113  44.228.249.3   TCP        66 52236 → 80 [ACK] Seq=552 Ack=277 Win=131520 Len=0 TSval=847679784 TSecr=433064326
  105…  317.786006  192.168.0.113  44.228.249.3   HTTP      479 GET /login.php HTTP/1.1
  105…  318.173975  44.228.249.3   192.168.0.113  TCP        66 80 → 52236 [ACK] Seq=277 Ack=965 Win=61824 Len=0 TSval=433064684 TSecr=847679814
  105…  318.173977  44.228.249.3   192.168.0.113  TCP      1514 80 → 52236 [ACK] Seq=277 Ack=965 Win=61824 Len=1448 TSval=433064685 TSecr=847679814 [TCP PDU reassembled i…
  105…  318.173979  44.228.249.3   192.168.0.113  HTTP     1366 HTTP/1.1 200 OK  (text/html)
  105…  318.174116  192.168.0.113  44.228.249.3   TCP        66 52236 → 80 [ACK] Seq=965 Ack=3025 Win=128832 Len=0 TSval=847680202 TSecr=433064685
  114…  383.065330  44.228.249.3   192.168.0.113  TCP        66 80 → 52236 [FIN, ACK] Seq=3025 Ack=965 Win=61824 Len=0 TSval=433129686 TSecr=847680202
  114…  383.065456  192.168.0.113  44.228.249.3   TCP        66 52236 → 80 [ACK] Seq=965 Ack=3026 Win=128832 Len=0 TSval=847745094 TSecr=433129686
```

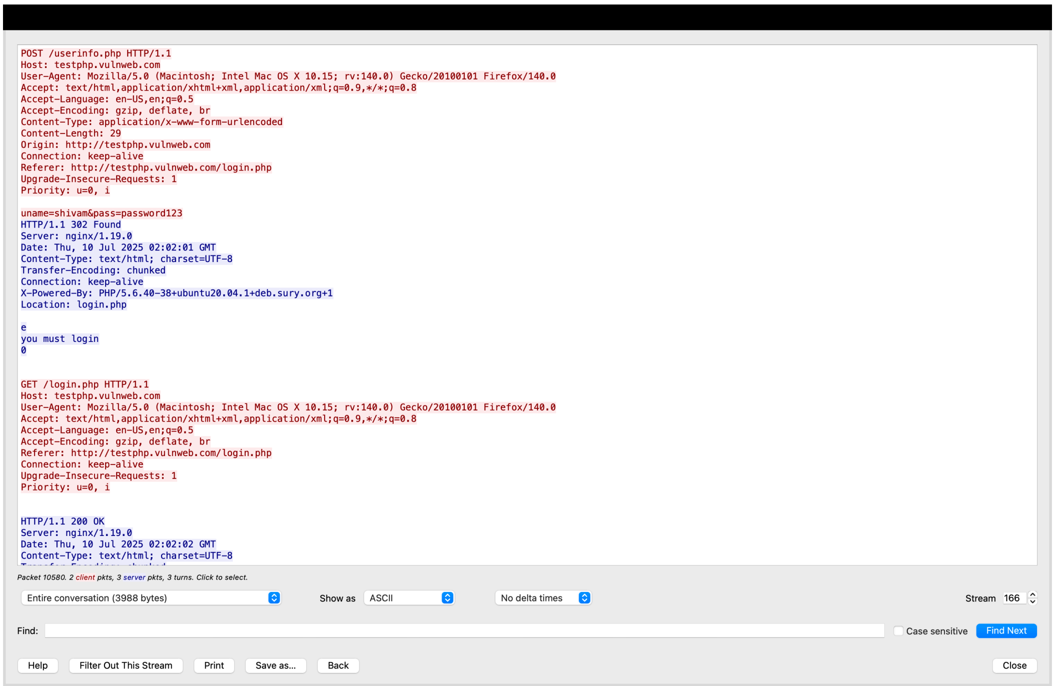
```
> Frame 10580: 617 bytes on wire (4936 bits), 617 bytes captured (4936 bits) on interface en
> Ethernet II, Src: c6:fe:66:1f:74:e0 (c6:fe:66:1f:74:e0), Dst: TPLink_b7:b6:bc (1c:61:b4:b7
> Internet Protocol Version 4, Src: 192.168.0.113, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 52236, Dst Port: 80, Seq: 1, Ack: 1, Len: 551
```

```
0000  1c 61 b4 b7 b6 bc c6 fe  66 1f 74 e0 08 00 45 02   ·a······ f·t···E·
0010  02 5b 00 00 40 00 40 06  51 9a c0 a8 00 71 2c e4   ·[··@·@· Q····q,·
0020  f9 03 cc 0c 00 50 c5 60  ad b2 50 ff 5d df 80 18   ·····P·` ··P·]···
0030  08 0b 79 d7 00 00 01 01  08 0a 32 86 8f df 19 d0   ··y····· ··2·····
0040  07 ab 50 4f 53 54 20 2f  75 73 65 72 69 6e 66 6f   ··POST / userinfo
```

wireshark_Wi-FiWLPF92.pcapng

Packets: 24647 · Displayed: 14 (0.1%)

Profile: Default



[redacted]

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=shivam&pass=password123
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Thu, 10 Jul 2025 02:02:01 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php

e
you must login
0


GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i


HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 10 Jul 2025 02:02:02 GMT
Content-Type: text/html; charset=UTF-8
```

Packet 10580. 2 client pkts, 3 server pkts, 3 turns. Click to select.

Entire conversation (3988 bytes)

Show as: ASCII

No delta times

Stream: 166

Find:

□ Case sensitive