# NETWORK TRAFFIC SNIFFING USING WIRESHARK

By Sidhima (2023A7R011)
CSE - Cybersecurity

# SNIFFING

- Sniffing is the process of monitoring and capturing data packets that travel across a network.
- It helps in analyzing network traffic to detect vulnerabilities, leaked data, or unauthorized access.
- Hackers can misuse it to steal passwords, cookies, or other sensitive data over unencrypted connections.

# WIRESHARK

- Wireshark is a free, open-source packet analyzer used to inspect network traffic in real-time.
- It’s widely used by network administrators, security analysts, developers, and ethical hackers.
- Wireshark captures and decodes packets, helping users understand protocols and spot vulnerabilities.

# OBJECTIVES

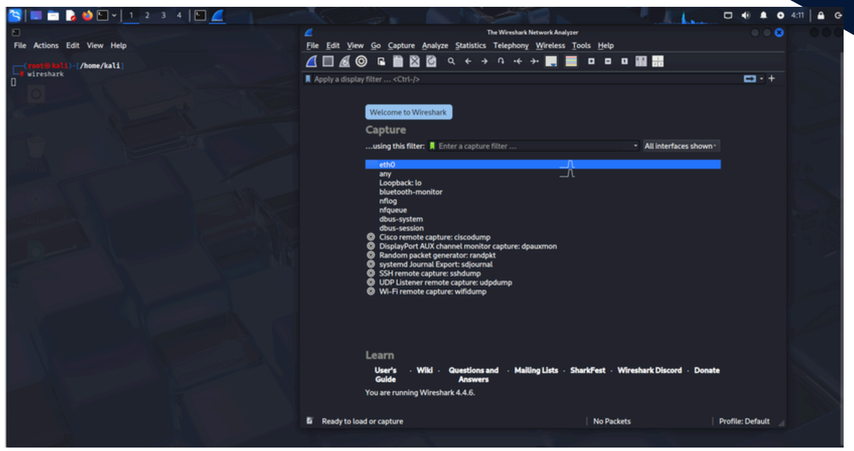
- Capture unencrypted traffic from a browser to a test web server.
- Use Wireshark on Kali Linux for network sniffing.
- Identify encrypted vs. unencrypted data.
- Demonstrate security concerns in transmitting sensitive info without encryption.

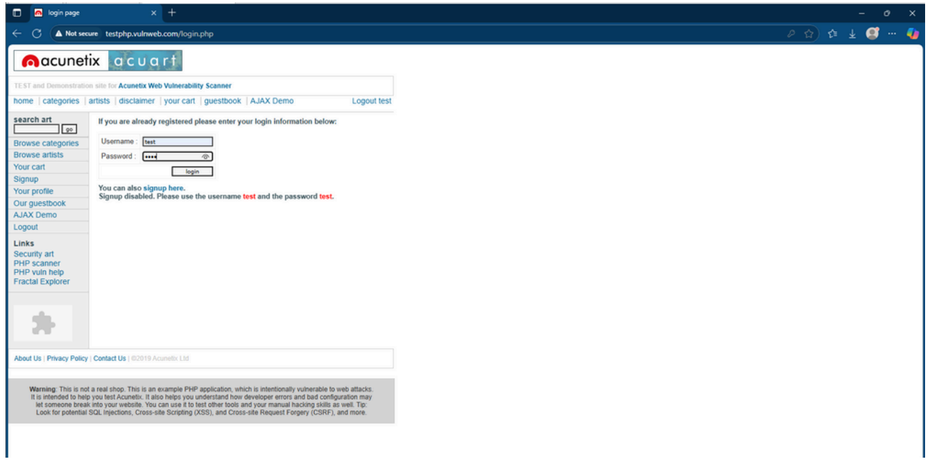
# TOOLS & TECHNIQUES

- Sniffing Tool: Wireshark
- Test Machine: Windows (Browser used to access the website)
- Website: testphp.vulnweb.com (unsecured site)

# Capturing Unencrypted Traffic

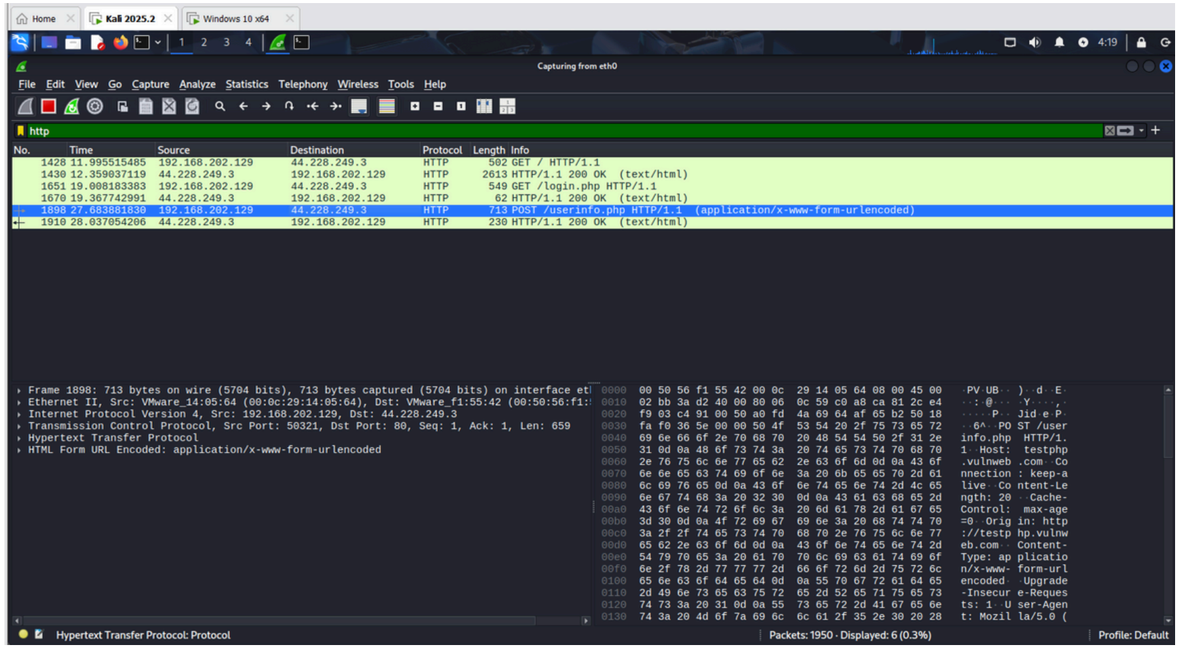
- Start Wireshark on Kali Linux.
- Select the correct network interface (e.g., eth0 or wlan0).
- Begin capturing packets.
- On the Windows browser, access http://testphp.vulnweb.com.
- Wireshark captures HTTP requests and responses in plain text.



# Filtering Encrypted Traffic

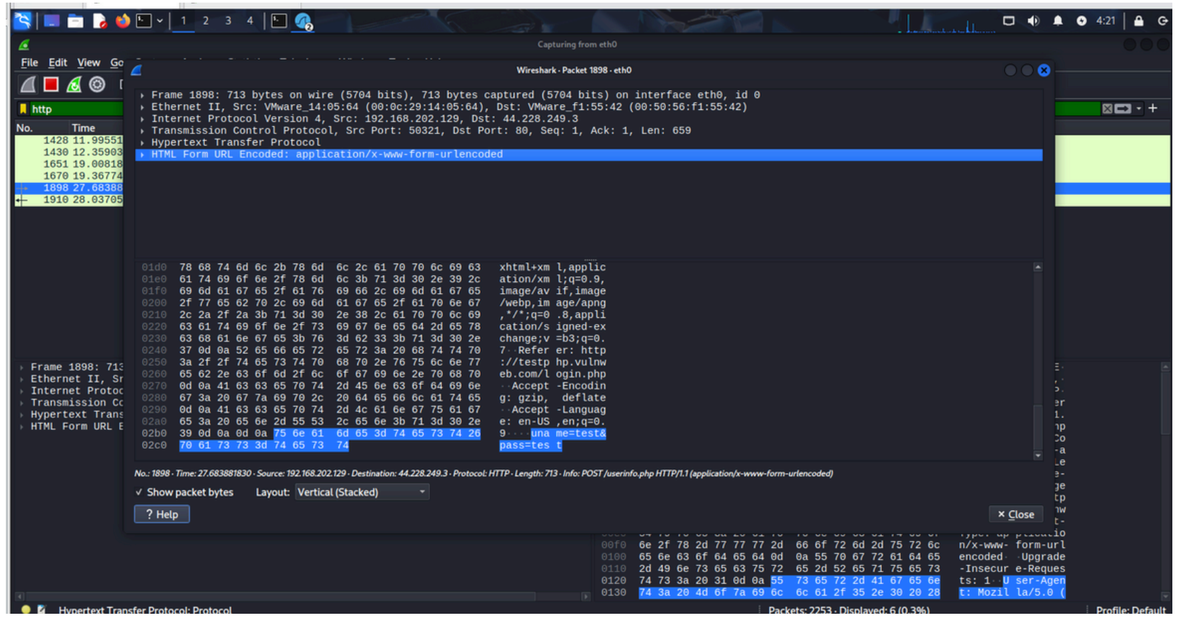
- Apply filters to separate traffic:
  For unencrypted HTTP: http
- Observe that HTTP data (like login details, cookies) is visible.
- HTTPS traffic appears encrypted—no readable content.



# Viewing and Analyzing Data

- Decrypted Usernames & Passwords: Clearly showing how sensitive data can be exposed.

- Sensitive Data Exposed: A strong warning about the implications of such captures.



# Conclusion & Security Recommendations

- Unencrypted (HTTP) traffic is easily sniffed and read.
- Encrypted (HTTPS) traffic protects data in transit.
- Always use HTTPS for login, transactions, and sensitive communications.
- Tools like Wireshark are powerful—ethical use only