Security Assessment Report

Project Title: Wireshark Analysis – HTTP vs HTTPS Credential Exposure
Prepared By: Swarupa Pawbake
Date: 30 July 2025

1. Executive Summary

The purpose of this project was to analyze the security differences between **HTTP and HTTPS traffic** using Wireshark. The test demonstrated that credentials submitted via HTTP are transmitted in **plain text**, making them vulnerable to interception, while HTTPS encrypts traffic, ensuring confidentiality and compliance with security standards such as **PCI-DSS and GDPR**.

2. Objective

- Capture and analyze login traffic over HTTP and HTTPS.
- Identify security risks in HTTP communication.
- Recommend measures to enforce secure communication in web applications.

3. Tools & Environment

- **Tools Used:** Wireshark
- **Test Environment:** Personal Laptop + Browser
- **Websites Used:**
  HTTP: http://testphp.vulnweb.com/login.php
  HTTPS: https://example.com

4. Methodology

Step 1: HTTP Capture

- Accessed http://testphp.vulnweb.com/login.php.
- Entered test credentials:
  - Username: test
  - Password: password3388
- Captured packets in Wireshark.

Step 2: HTTP Analysis

- Applied filter:
- Located **POST request** → Followed HTTP Stream.
- Observed credentials in plain text:

POST /login.php HTTP/1.1
Host: testphp.vulnweb.com
Username=test&Password=password3388

Step 3: HTTPS Capture

- Accessed https://example.com.
- Performed a basic request.
- Captured packets in Wireshark.

Step 4: HTTPS Analysis

- Applied filter:
- Observed only encrypted packets:

Application Data
Length: 902
Encrypted application data

- No credentials visible.

5. Findings

Protocol	Observation	Risk Level
HTTP	Credentials transmitted in clear text.	🔴 High
HTTPS	Data encrypted; credentials unreadable.	🟢 Low

6. Impact

- HTTP traffic allows attackers using packet sniffers to steal usernames and passwords.
- Could lead to **account compromise, data breaches, and compliance violations**.

7. Recommendations

- Enforce **HTTPS (TLS 1.2 or higher)** for all login and sensitive pages.
- Enable **HTTP Strict Transport Security (HSTS)**.
- Configure **secure cookie attributes** (HttpOnly, Secure, SameSite).
- Regularly test with Wireshark to ensure no sensitive data leaks.

8. Conclusion

The Wireshark analysis clearly demonstrates the **critical risks of using HTTP** for credential transmission. Implementing HTTPS with strong TLS enforcement is essential for maintaining **data confidentiality, compliance, and user trust**.

9. Screenshots (to attach in final PDF)

- **HTTP Capture:** Credentials in plain text.
- **HTTPS Capture:** Encrypted TLS packets.