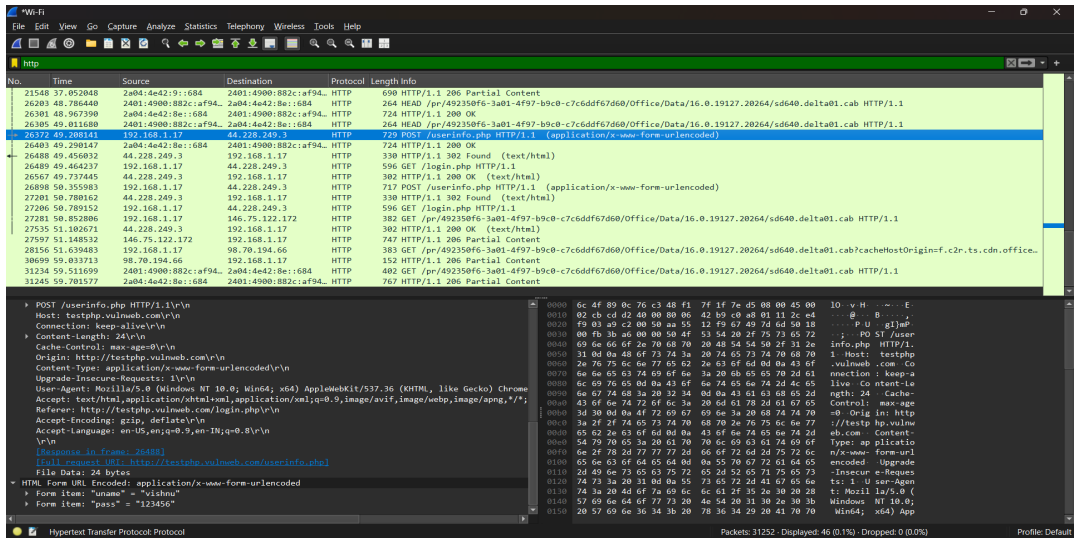


Wireshark Network Traffic Analysis Report

This report provides an analysis of captured network traffic using Wireshark. The following screenshot and details highlight observed HTTP traffic where sensitive information such as usernames and passwords were transmitted in plaintext, indicating a potential security risk.

Captured Traffic Screenshot:



Key Findings: 1. A POST request was made to *userinfo.php* at host *testphp.vulnweb.com*. 2. The HTTP request used **application/x-www-form-urlencoded** content type. 3. User credentials were transmitted in plaintext: - Username: **vishnu** - Password: **123456** 4. The connection was unencrypted (HTTP instead of HTTPS), exposing sensitive data. 5. Potential attacker could intercept traffic and extract login details.

Security Implications: Transmitting login credentials over HTTP is a major security vulnerability. Any attacker with access to the network can capture packets and retrieve sensitive data, leading to unauthorized access, identity theft, and further exploitation.

Recommendations: 1. Implement HTTPS (TLS/SSL) to encrypt all communication between clients and servers. 2. Avoid transmitting sensitive data in plaintext. 3. Educate developers and administrators on secure authentication practices. 4. Use strong password policies and multi-factor authentication (MFA). 5. Regularly monitor network traffic for suspicious activities.

Conclusion: The captured Wireshark traffic highlights the risks of using unencrypted HTTP for authentication. To ensure confidentiality, integrity, and security of user data, organizations must enforce HTTPS and follow secure coding practices.