Penetration Testing Report

# 📋 Executive Summary

This penetration testing assessment was conducted on the intentionally vulnerable website http://testphp.vulnweb.com/ to demonstrate how credentials transmitted via an unencrypted channel (HTTP) can be intercepted using network analysis tools. The purpose of this report is to present my findings to the stakeholders, showcasing a real-world example of sensitive data exposure over insecure channels.  
  
The exercise successfully demonstrated that both username and password are transferred in plain text during login. This highlights a critical security flaw that, if found in a production environment, would pose a high risk of user account compromise.

# 🎯 Objective

As part of a controlled cybersecurity simulation, my objective was to:  
- Intercept and analyze real-time traffic from a login page  
- Identify if user credentials were exposed  
- Present evidence of vulnerabilities related to data transmission

# 🔧 Tools & Environment

|  |  |
| --- | --- |
| Tool/Platform | Description |
| Wireshark | For packet capture and analysis |
| Web Browser (Chrome) | Used to submit login credentials |
| Windows 10 | Test system |
| Network Interface | Wi-Fi (local network monitoring) |

# 🧪 Methodology (My Step-by-Step Process)

Step 1: Capturing Network Traffic

I launched Wireshark, selected the Wi-Fi interface, and started live packet capturing. Applied the HTTP filter to focus on unsecured web traffic.

Step 2: Logging into the Website

Navigated to: http://testphp.vulnweb.com/  
Accessed the login page: http://testphp.vulnweb.com/login.php  
Entered test credentials:  
 - Username: admin  
 - Password: password1234  
Clicked Login, generating a POST request.

Step 3: Analyzing Packets in Wireshark

Switched back to Wireshark and filtered for: http  
Located the request: POST /login.php HTTP/1.1  
Packet Metadata:  
 - Source IP: 10.8.143.99  
 - Destination IP: 44.228.249.3

Step 4: Extracting the Sensitive Data

By expanding the HTTP layer in Wireshark, I was able to observe:  
uname=admin&pass=password1234  
Credentials captured:  
 - uname: admin  
 - pass: password1234

# 🔍 Key Findings

|  |  |
| --- | --- |
| Vulnerability | Details |
| Insecure Transmission | Login credentials were transmitted in cleartext over HTTP. |
| No Encryption (No SSL/TLS) | The connection was not encrypted—making it easy to sniff. |
| Data Interception Risk | Anyone with access to the same network can intercept login credentials. |

# 📉 Risk Assessment

|  |  |
| --- | --- |
| Factor | Assessment |
| Risk Level | Critical |
| Impact | Account Takeover, Credential Theft |
| Likelihood | High (on unsecured/public networks) |
| Exposure Scope | All users logging in without HTTPS protection |

# 🔐 Recommendations

1. Enforce HTTPS Across All Pages  
 - Implement SSL/TLS to encrypt data in transit.  
 - Force HTTP to redirect to HTTPS automatically.  
  
2. Secure Authentication Practices  
 - Avoid using GET/POST parameters for sensitive information without encryption.  
 - Encourage password complexity and implement multi-factor authentication.  
  
3. User Education  
 - Notify users to avoid entering credentials on non-secure (HTTP) pages.  
 - Display browser security indicators and enforce secure session management.  
  
4. Infrastructure Hardening  
 - Disable HTTP access altogether.  
 - Monitor login endpoints for suspicious requests and brute-force attacks.

# ✅ Conclusion

This simulation confirms that plaintext transmission of credentials over HTTP poses an immediate and critical risk. As a SOC Analyst and Security Tester, I have successfully demonstrated how this vulnerability can be exploited using Wireshark, and presented actionable remediation steps to improve data protection in web applications.

# 📎 Appendix: Raw Packet Example

POST /login.php HTTP/1.1  
Host: testphp.vulnweb.com  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 29  
  
uname=admin&pass=password1234

Report Prepared By:

Samuel Adeduntan  
Cybersecurity Analyst   
📧 adedunsam220@gmail.com | ☎️ +234-8152278751  
🔗 https://www.linkedin.com/in/samueladeduntan