Burp Suite Practical Implementation Report

Prepared By: Pratik Bhaskar Sumbe

Objective

To demonstrate hands-on implementation of web application security testing using Burp Suite in a controlled lab environment, focusing on identification of SQL Injection (Tautology-Based Authentication Bypass).

Tools Used

1. Burp Suite Professional / Community
2. Web Browser (Firefox/Chrome)
3. Deliberately Vulnerable Web Application (Lab Environment)

Methodology

1. Configured browser proxy to route traffic through Burp Suite.
2. Captured HTTP request using Intercept feature.
3. Analyzed login request parameters.
4. Modified input with a tautology-based payload to test authentication bypass.
5. Forwarded modified request to the server and observed response.

Result

The modified request demonstrated how improper input validation can alter SQL query logic and potentially bypass authentication in vulnerable systems.

Key Learning Outcomes

1. Understanding of HTTP request interception and modification.
2. Awareness of SQL Injection vulnerability mechanics.
3. Importance of parameterized queries and input validation.
4. Practical experience with Burp Suite Proxy and Repeater tools.

Ethical Use Statement

All testing activities were conducted in a controlled, legal, and educational lab environment. No unauthorized systems were targeted.