

INFORMATION ASSURANCE AND SECURITY 2

TOPIC: BURP SUITE

By. Dr. Louie F. Agustin

Lecture: Introduction to Burp Suite

Overview:

Burp Suite is a comprehensive platform for web application security testing. Developed by PortSwigger, it offers a variety of tools integrated into a single environment to make the process of identifying web vulnerabilities more efficient and effective. This lecture will introduce you to the basics of Burp Suite, including its core components, and provide practical examples to get you started with web application penetration testing.

Burp Suite is a powerful tool for web application security testing, offering a wide range of features to identify, exploit, and report vulnerabilities. Through practical exercises and an understanding of its components, security professionals can significantly enhance their ability to secure web applications against potential threats.

Objectives:

By the end of this lecture, students should be able to:

1. Understand the fundamental concepts and components of Burp Suite.
2. Configure Burp Suite and set up a testing environment.
3. Perform basic web vulnerability assessments using Burp Suite tools.
4. Analyze and interpret the results of security tests.

Introduction to Burp Suite Components

Proxy

- Function: Intercepts HTTP/S traffic between your browser and the web servers. - Usage: Modifying requests and responses to test for vulnerabilities like SQL injection, XSS, etc.

1.2 Scanner

- Function: Automatically scans web applications for vulnerabilities.
- Usage: Identifying potential security weaknesses without manual testing.

1.3 Intruder

- Function: Automates custom attacks against web applications.
- Usage: Performing attacks such as brute force, credential stuffing, and parameter manipulation.

1.4 Repeater

- Function: Allows for manual reissuing of web requests to test for changes in responses. - Usage: Exploring and exploiting vulnerabilities like authentication flaws and logical errors.

1.5 Sequencer

- Function: Tests the randomness of session tokens.

- Usage: Assessing the strength of tokens that are meant to be unpredictable.

INFORMATION ASSURANCE AND SECURITY 2

TOPIC: BURP SUITE

By. Dr. Louie F. Agustin

Setting Up Burp Suite

Installation

- Step-by-Step Guide: Download Burp Suite from the official PortSwigger website and follow the installation instructions for your operating system.

Configuration

- Proxy Setup: Configure your browser to route traffic through Burp Suite's proxy listener. - HTTPS Interception: Install Burp's CA certificate to intercept HTTPS traffic without security warnings.

Practical Examples:

Example 1: Using the Proxy to Intercept Requests

1. Objective: Capture and modify a login request.
2. Steps:
 - Configure your browser to use Burp's proxy.
 - Navigate to a login page of a test application.
 - Enter credentials and intercept the request in Burp Suite.
 - Modify the request parameters and forward it to observe the behavior.

Example 2: Conducting a Brute Force Attack with Intruder

1. Objective: Test for weak passwords in login forms.
2. Steps:
 - Capture a login request using the Proxy.
 - Send this request to Intruder.
 - Set the position for the password parameter.
 - Load a list of common passwords into the payload options.
 - Start the attack and analyze the responses for successful logins.

Example 3: Identifying Cross-Site Scripting (XSS) with Scanner

1. Objective: Automatically scan for XSS vulnerabilities.
2. Steps:
 - Navigate to the target web application through Burp Suite.
 - Right-click on the target from the site map and select "Scan".
 - Review the scan results for potential XSS vulnerabilities.

Analyzing Results:

- Understanding the Output: Learn how to interpret the results provided by Burp Suite, including severity ratings and potential impact.
- Reporting: Use Burp Suite's reporting features to generate comprehensive reports of your findings.