NEW YORK INSTITUTE
OF TECHNOLOGY

Lab 4 – Web Application Vulnerabilities

Lab Overview

This lab is designed to test your ability to identify, exploit, and analyze security vulnerabilities commonly found in web applications.

Your mission is to uncover **hidden flags** and get at least **125 points by** exploiting weaknesses in the system using tools like Burp Suite. Each task presents a different security flaw, ranging from information leakage to SQL injection.

Requirements:

- Burp Suite (Community or Pro)
- Web browser with proxy settings configured for Burp Suite
- Target vulnerable web application

Task 1: Important Page Leakage via robots.txt (5 points)

Task Description:

An important page is being leaked in the robots.txt file. Identify the disallowed paths and determine what sensitive pages are being restricted. One of these pages contains a sensitive file that holds a **flag**.

Task 2: Become a Millionaire & Buy the Red Button (10 points)

Task Description:

There is a way to manipulate the price of an item and increase your budget unfairly. Can you modify the request to become a millionaire **and** purchase the red button?

Task 3: Check Cart of Mike (10 points)

Task Description:

Find a way to view the **shopping cart** of a user named "Mike" without having access to his account.

Task 4: Stored XSS to Redirect to URI in Variable "gg" (15 points)

Task Description:

Insert a malicious payload into the review section that, when triggered, redirects users to a URI stored in variable **gg**.

Task 5: Editing Review of User "Chad" (15 points)

Task Description:

A user named "Chad" left a hostile review about the webpage on fake airpods product. Can you find a way to **edit his review** without proper authorization?

Task 6: Change Email of User "CryptoBro419" (20 points)

Task Description:

Modify the **email** of the user CryptoBro419 from crypto@notascam.com to crypto@scammer.com. Identify where email updates are being processed and exploit any weaknesses.

Task 7: Hijack Account of "Evil_user" (25 points)

Task Description:

Find a way to **hijack** the account of a user named "Evil_user" by exploiting vulnerabilities in the authentication or session management process.

Task 8: Visit Admin Dashboard Without Logging in as Admin (25 points)

Task Description:

Access the **admin dashboard** without using admin credentials. Investigate whether the dashboard is protected by authentication or if there are ways to bypass restrictions.

Task 9: Blind SQL Injection to Get Admin (administrator_745) Password (30 points)

Task Description:

Using **blind SQL** injection techniques, extract the admin password from the database without directly seeing the response.

Lab Deliverables

To successfully complete this lab, you must:

- Get at least 125 out of 155 points and store all the flags in a single file (flags.txt).
- Submit a detailed report explaining each exploit, including:
  - Steps taken to find and exploit the vulnerability.
  - Screenshots of relevant Burp Suite requests and responses.
  - Observations and challenges encountered.
- Ensure that all screenshots clearly showcase the attack process and obtained flags.
- Upload both flags.txt and the final report as part of your submission.

This lab manual provides hands-on experience with common web vulnerabilities. Use ethical hacking principles and test only in controlled environments. Have fun and good luck!