Burp Suite Task Report

Student Name: Ammar Yasser Mohamed
Course: ITI-Cybersecurity-Summer-2025

Date: August 3, 2025

1. Intercepting Requests Using Burp Suite

- Open Burp Suite and go to the **Proxy** – **Intercept** tab.
- Ensure **Intercept is on**.
- Configure your browser to use Burp's proxy at `127.0.0.1:8080`, or use Burp's embedded browser.
- Visit any website – the HTTP request will appear in the Intercept tab.
- You can choose to:
  - **Forward** – send the request to the server.
  - **Drop** – discard the request.
  - **Edit** – modify the request before forwarding.
- Requests can be sent to **Repeater** or **Intruder** for further testing.

2. Repeater vs Intruder

- **Repeater**: Used for manual testing of individual requests.
- **Intruder**: Used for automated attacks on specific parameters.
- Repeater gives full manual control over each request and response.
- Intruder allows faster testing by sending many modified requests automatically.
- Repeater is ideal for tasks like parameter tampering or manual XSS testing.

- Intruder is used for brute force attacks, fuzzing, and login enumeration.

3. Intruder Attack Types

a. Sniper

- Attacks one parameter at a time.
- Useful for testing XSS, SQL Injection, or input validation.
- Replaces one variable with payloads individually.

b. Battering Ram

- Sends the same payload to all defined positions.
- Good for using a single payload list for multiple fields.

c. Pitchfork

- Sends different payloads to each position in parallel.
- Each payload list is synchronized line-by-line.
- Ideal for testing username and password lists together.

d. Cluster Bomb

- Sends all possible combinations of multiple payload sets.
- Most time-consuming but very thorough.
- Used for complete brute-force testing (e.g., all usernames $\times$ all passwords).