Day 16 – Daily Diary
Date: 16/07/25**Topic:** Web Development and JavaScript-based Attacks
Session Summary:

Today in class, sir discussed **JavaScript and common web development-related attacks**. The session focused on how attackers can exploit client-side scripts to perform malicious actions and how developers can secure their applications.

🔍 Key Points Covered:

- **Introduction to JavaScript Vulnerabilities:**
  - JavaScript runs on the client side and is often a target for exploitation.
- **Common Web-Based Attacks using JavaScript:**
  1. **Cross-Site Scripting (XSS):**
     - Explained how attackers inject malicious scripts into websites.
     - Showed how XSS can be used to steal cookies, session tokens, or redirect users.
     - Discussed types: Stored XSS, Reflected XSS, and DOM-based XSS.
  2. **Cross-Site Request Forgery (CSRF):**
     - Described how JavaScript can be used to trick a user into performing actions unknowingly.
  3. **Clickjacking:**
     - Attackers use transparent frames to trick users into clicking on hidden elements.
  4. **Malicious JavaScript Injection in Forms and URLs.**
- **Brute Force and SQL Injection Recap:**
  - Though mainly discussed on previous days, sir briefly connected how JavaScript could be misused in tools for brute force login attempts or form automation.

🛡 Prevention Techniques Discussed:

- Validating and sanitizing user inputs
- Using Content Security Policy (CSP)
- Escaping output data before rendering
- Avoiding `eval()` and other insecure functions in JavaScript

✍ Assignment / Activity:

- Sir assigned us to **research a real-life case of an XSS attack** and suggest how it could have been prevented.
- We were encouraged to read OWASP guidelines on secure JavaScript coding.