**APPLICATION AND WEB SECURITY**

**Assignment 1:**

Title: **HTTP Request and Response Observation**

Task:

* Open browser developer tools.
* Visit a website (e.g., <http://example.com>).
* Observe and write down details of:
  + - Request Method
    - URL
    - Status Code
    - Response Headers
    - Cookies (if any)
* Outcome: Understanding of HTTP protocol (Unit 2)

**Assignment 2:**

Title: **Identify Web Security Flaws in a Login Page**  
Task:

* Analyze a sample HTML/PHP login.
* Identify what can go wrong (e.g., SQL Injection, weak password policy).
* Suggest two methods to secure the page.
* **Outcome:** Understanding of authentication flaws (Unit 4)

#### Case Study 1:

**Title:** **Facebook Breach (2019): Session Token Leak**  
**Task:**

* Students research the Facebook breach due to session tokens being exposed.
* Write:
  + What was the vulnerability?
  + What caused it?
  + How could it have been prevented?

#### Case Study 2:

**Title:** **SQL Injection in Real Life – Example from a Bank or E-commerce App  
Task:**

* Analyze a publicly documented SQL Injection attack (e.g., Heartland breach).
* Explain the entry point, exploit, and damage caused.
* Mention the countermeasures.