INTRODUCTION TO WEB APPLICATION TESTING

MODULE 1 — Web Application Basics

1.1 What Is a Web Application?

A **web application** is software that runs on a server and is accessed through a browser using HTTP/HTTPS.

Examples:

- Ecommerce sites (Amazon)
- Banking portals
- Social media
- Admin dashboards
- APIs

A web app typically includes:

- **Frontend:** HTML, CSS, JS
- **Backend:** PHP, Python, Node.js, Java, .NET
- **Database:** MySQL, PostgreSQL, MongoDB
- **Server:** Apache, Nginx, IIS

1.2 How Web Applications Work (Technical + Simple)

🧠 Step-by-step:

1. User opens **browser**
2. Browser sends **HTTP request** to server
3. Server processes it using **backend logic**

4. Backend fetches data from **database**
5. Server responds with **HTML/JSON**
6. Browser renders it on screen

A pentester attacks **every step above**.

1.3 HTTP & HTTPS (Professional Explanation)

✔ HTTP Request Structure:

```
GET /login HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0
Cookie: sessionid=1234
```

✔ HTTP Response:

```
HTTP/1.1 200 OK
Server: Apache/2.4
Content-Type: text/html
```

Important Components:

- Methods: GET, POST, PUT, DELETE
- Headers: Authorization, Cookie, User-Agent
- Status Codes:
  - 200 → OK
  - 301 → Redirect
  - 401 → Unauthorized
  - 403 → Forbidden
  - 500 → Server error

1.4 OWASP TOP 10 Overview (Professional)

Most web attacks fall under OWASP categories:

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable Components
7. Identification & Authentication Issues
8. Software & Data Integrity Failures
9. Logging & Monitoring Failures
10. Server-Side Request Forgery (SSRF)

We will cover each thoroughly in later modules.