🌐 Web & Application Security

1. What is Web & Application Security?

Web and application security means protecting websites and apps from attacks, vulnerabilities, and unauthorized access.
Goal → Keep data safe, ensure availability, and prevent hacking.

---

2. Common Threats

🔷 Injection Attacks

- SQL Injection (malicious queries to databases).
- Command Injection.

🔷 Cross-Site Scripting (XSS)

- Injecting malicious scripts into webpages.

🔷 Cross-Site Request Forgery (CSRF)

- Forcing users to perform unwanted actions while logged in.

🔷 Broken Authentication & Session Hijacking

- Stolen cookies or weak sessions.

🔷 Insecure Direct Object Reference (IDOR)

- Accessing files/data by modifying URL or request.

🔷 Distributed Denial of Service (DDoS)

- Flooding servers to take apps offline.

🔷 Misconfiguration & Weak Security

- Default passwords, exposed APIs, outdated libraries.

---

3. Security Mechanisms

🔐 Authentication & Authorization

- Strong passwords, MFA, OAuth, JWT tokens.

🛡️ Input Validation & Sanitization

- Prevent SQL Injection & XSS.

📜 HTTPS / TLS Encryption

- Secure communication.

🔍 Secure Coding Practices

- Use parameterized queries, avoid hard-coded secrets.

🗄️ Session Management

- Secure cookies, session timeouts, token-based authentication.

🧱 Web Application Firewall (WAF)

- Blocks malicious traffic.

📦 Security Headers

- CSP (Content Security Policy), X-Frame-Options, HSTS.

---

4. OWASP Top 10 (Most Critical Web App Risks)

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