Day 26

"CLOUD SECURITY"

OWASP Top 10 Cloud Application Vulnerabilities & Risks:

1. **Injection (SQL/NoSQL/OS/LDAP)**
    a. Attackers inject untrusted data into interpreters → execute unintended commands or access unauthorized data.
2. **Broken Authentication**
    a. Flaws in login/session handling → attackers steal credentials, tokens, or impersonate users.
3. **Sensitive Data Exposure**
    a. Weak protection of PII/financial/health data → stolen via lack of encryption (at rest/in transit).
4. **XML External Entities (XXE)**
    a. Poorly configured XML processors allow external entities → file disclosure, SSRF, DoS, remote code execution.
5. **Broken Access Control**
    a. Failure to enforce permissions → attackers escalate privileges, access accounts, or modify data.
6. **Security Misconfiguration**
    a. Default/incomplete configs, open storage, misconfigured headers, verbose errors → easy exploitation.
7. **Cross-Site Scripting (XSS)**
    a. Unvalidated input in webpages → malicious scripts run in users' browsers, session hijacking, redirects.
8. **Insecure Deserialization**
    a. Unsafe handling of serialized objects → remote code execution, replay, injection, privilege escalation.
9. **Using Components with Known Vulnerabilities**
    a. Exploitable libraries/frameworks run with app privileges → may lead to server takeover or data loss.
10. **Insufficient Logging & Monitoring**
    a. Poor detection & response → breaches go unnoticed (~200 days avg), attackers persist and escalate.

Cloud-Specific Risks:

1. **Data Breaches**
   Unauthorized access to sensitive/confidential data (e.g., PII, financial).
2. **Weak Identity, Credential & Access Management**
   Risks from weak passwords, missing MFA, poor key rotation → easier compromise.
3. **Insecure Interfaces & APIs**
   Cloud APIs (management, provisioning) can be exploited if insecure → unauthorized control.
4. **System & Application Vulnerabilities**
   Exploitable bugs allow data theft, system takeover, or service disruption.

5. **Account Hijacking**
   Stolen credentials → attackers eavesdrop, manipulate data, redirect clients.
6. **Malicious Insiders**
   Authorized employees/partners misuse access → compromise CIA (confidentiality, integrity, availability).
7. **Advanced Persistent Threats (APTs)**
   Long-term stealthy attacks to exfiltrate data & IP from cloud infrastructure.
8. **Data Loss**
   Accidental deletion, disasters, or no backups → permanent data loss risk.
9. **Insufficient Due Diligence**
   Rushed cloud adoption without assessing legal, technical, compliance risks.
10. **Abuse & Nefarious Use of Cloud Services**
    Free trials/fraudulent sign-ups → attackers misuse cloud (botnets, malware hosting).
11. **Denial of Service (DoS)**
    Flooding/overloading cloud services → downtime & disruption.
12. **Shared Technology Issues**
    Multitenant isolation failures (IaaS, PaaS, SaaS) → data leakage, side-channel attacks.

Scope of Cloud Application Security

Developing secure cloud applications requires diverse skills and roles. The scope covers the following areas:

1. **Secure Software Development Lifecycle (SSDLC)**

   - Integrates security assurance into all SDLC phases: architecture analysis, code review, penetration testing.
   - Ensures applications are secured from **design to deployment**.
   - Addresses cloud-specific security concerns at each stage.

2. **Design and Architecture**

   - Focuses on designing cloud apps to mitigate known threats.
   - Incorporates best practices and secure patterns to enhance app protection.

3. **DevOps & CI/CD**

   - Continuous Integration/Continuous Deployment automates testing and integration.
   - Embeds **security controls** in development pipelines to strengthen cloud app security.
   - Supports faster, secure deployment through DevOps best practices.

--The End--