1/10/2025

Amruthesh – 241059041

Web Application Security - Cybersecurity - msis

Assignment 1

Real-world Attacks of Web Application Security

**1. SQL Injection (SQLi)**

An attacker manipulates SQL queries to access or alter data in a database by injecting malicious input.

**Security Pillars Affected:**

**Confidentiality:** Access sensitive data like passwords or credit card info.

**Integrity:** Alter or delete data in the database.

**Availability:** Potential to crash the database or affect the app’s performance.

**Consequences:**

**Legal:** Violation of data protection laws (e.g., GDPR).

**Financial:** Costs from fines, compensations, and loss of business.

**Reputation:** Loss of customer trust.

**Prevention:** Use parameterized queries, validate and sanitize all inputs.

**Sources:** https://owasp.org/www-community/attacks/SQL\_Injection

**2. Cross-Site Scripting (XSS)**

Attackers inject malicious JavaScript into web pages that are viewed by other users, stealing cookies or redirecting them to malicious sites.

**Security Pillars Affected:**

**Confidentiality:** Steal sensitive information such as session cookies.

**Integrity:** Modify the content of a page or redirect users.

**Availability:** Rarely impacts availability directly.

**Consequences:**

**Legal:** User data theft leading to potential lawsuits.

**Financial:** Cleaning up, compensating affected users.

**Reputation:** Trust loss and negative press.

**Prevention:** Sanitize inputs, implement Content Security Policy (CSP), use HttpOnly cookies.

**Sources:** https://owasp.org/www-community/attacks/xss/

**3. Cross-Site Request Forgery (CSRF)**

Attackers trick users into performing actions they did not intend, such as changing account settings, by submitting unauthorized requests on their behalf.

**Security Pillars Affected:**

**Confidentiality:** No direct effect on confidentiality, but could lead to unauthorized actions.

**Integrity:** Unauthorized changes or actions.

**Availability:** Usually doesn’t impact availability.

**Consequences:**

**Legal:** Fraudulent transactions can lead to lawsuits.

**Financial:** Costs to reverse fraudulent actions.

**Reputation:** Damage to user confidence.

**Prevention:** Use anti-CSRF tokens, SameSite cookies, require re-authentication for sensitive actions.

**Sources:** https://owasp.org/www-community/attacks/csrf

**4. Distributed Denial-of-Service (DDoS)**

Attackers overwhelm a server with excessive traffic, making it unavailable to legitimate users.

Security Pillars Affected:

**Availability:** Disrupts the service by making it slow or unavailable.

**Confidentiality &** **Integrity:** Generally unaffected but can lead to further vulnerabilities.

**Consequences:**

**Legal:** Potential breach of service level agreements (SLA) with customers.

**Financial:** Mitigation costs, loss of business during downtime.

**Reputation:** Loss of customer trust due to downtime.

**Prevention:** Use DDoS protection services, traffic filtering, load balancing.

**Sources:** https://owasp.org/www-community/attacks/Denial\_of\_Service

**5. Insecure Direct Object References (IDOR)**

Attackers manipulate URLs or input parameters to access resources they are not authorized to, such as viewing other users' private files.

**Security Pillars Affected:**

**Confidentiality:** Unauthorized access to private data.

**Integrity:** Potential to modify or delete sensitive resources.

**Availability:** Rarely affects availability.

**Consequences:**

**Legal:** Breach of privacy laws, legal action.

**Financial:** Costs from compensating victims, possible fines.

**Reputation:** Damage to reputation from the data breach.

**Prevention:** Implement proper access control, use unpredictable resource identifiers, validate all parameters.

**Sources:** https://cheatsheetseries.owasp.org/cheatsheets/Insecure\_Direct\_Object\_Reference\_Prevention\_Cheat\_Sheet.html