Stage 1: Identifying Vulnerabilities in Cybersecurity

Cybersecurity vulnerabilities are weaknesses in software, hardware, or processes that attackers exploit to gain unauthorized access, disrupt operations, or steal sensitive information. Below are some of the most critical vulnerabilities that affect web applications, networks, and systems.

List of Vulnerabilities

| S.No | Vulnerability Name | CWE - No |
| --- | --- | --- |
| 1 | SQL Injection (SQLi) | CWE-89 |
| 2 | Cross-Site Scripting (XSS) | CWE-79 |
| 3 | Broken Authentication | CWE-287 |
| 4 | Insecure Direct Object References (IDOR) | CWE-639 |
| 5 | Security Misconfiguration | CWE-16 |
| 6 | Sensitive Data Exposure | CWE-200 |
| 7 | Server-Side Request Forgery (SSRF) | CWE-918 |
| 8 | XML External Entities (XXE) | CWE-611 |
| 9 | Unrestricted File Upload | CWE-434 |
| 10 | Cross-Site Request Forgery (CSRF) | CWE-352 |

Detailed Analysis of Vulnerabilities

1) SQL Injection (SQLi)

* CWE: CWE-89 (Improper Neutralization of Special Elements in SQL Commands)
* OWASP/SANS Category: OWASP Top 10 (A03:2021 - Injection) / SANS 25 (#1 - SQL Injection)
* Description: SQL Injection occurs when an application fails to sanitize user inputs in database queries. Attackers manipulate SQL statements to extract, modify, or delete sensitive data.
* Business Impact:
  + Unauthorized access to user data (passwords, financial records).
  + Database corruption leading to service disruptions.
  + Regulatory compliance violations (GDPR, CCPA).

2) Cross-Site Scripting (XSS)

* CWE: CWE-79 (Improper Neutralization of Input During Web Page Generation)
* OWASP/SANS Category: OWASP Top 10 (A07:2021 - Identification and Authentication Failures) / SANS 25 (#2 - XSS)
* Description: XSS vulnerabilities allow attackers to inject malicious scripts (JavaScript) into web pages viewed by other users, leading to data theft, phishing, and website defacement.
* Business Impact:
  + Session hijacking (stealing authentication cookies).
  + Phishing attacks leading to credential theft.
  + Damage to website integrity and reputation.

3) Broken Authentication

* CWE: CWE-287 (Improper Authentication)
* OWASP/SANS Category: OWASP Top 10 (A07:2021 - Identification and Authentication Failures) / SANS 25 (#3 - Broken Authentication)
* Description: Weak authentication mechanisms allow attackers to gain unauthorized access through brute-force attacks, session hijacking, and credential stuffing.
* Business Impact:
  + Account takeovers leading to identity theft.
  + Privilege escalation (attackers gaining admin rights).
  + Financial loss due to fraudulent transactions.

4) Insecure Direct Object References (IDOR)

* CWE: CWE-639 (Authorization Bypass Through User-Controlled Key)
* OWASP/SANS Category: OWASP A06:2021 (Vulnerable and Outdated Components)
* Description: IDOR occurs when an application exposes internal object references (like User IDs in URLs) without proper access controls. Attackers manipulate these references to gain unauthorized access to other users' data.
* Business Impact:
  + Leakage of confidential user records.
  + Unauthorized modification or deletion of critical data.
  + Compliance violations with data protection laws.

5) Security Misconfiguration

* CWE: CWE-16 (Configuration Issues)
* OWASP/SANS Category: OWASP Top 10 (A05:2021 - Security Misconfiguration)
* Description: Security misconfigurations happen due to default settings, exposed error messages, or improper permissions, making applications vulnerable to attacks.
* Business Impact:
  + Exposure of system architecture and internal errors.
  + Unintended access to administrative functionalities.
  + Increased risk of exploitation by automated attacks.

6) Sensitive Data Exposure

* CWE: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)
* OWASP/SANS Category: OWASP Top 10 (A02:2021 - Cryptographic Failures)
* Description: Applications that do not properly encrypt or protect sensitive information (e.g., passwords, credit card numbers) expose users to identity theft and fraud.
* Business Impact:
  + Unauthorized access to financial and personal data.
  + Non-compliance with legal and regulatory requirements.
  + Reputation damage due to data leaks.

7) Server-Side Request Forgery (SSRF)

* CWE: CWE-918 (Server-Side Request Forgery)
* OWASP/SANS Category: OWASP Top 10 (A10:2021 - Server-Side Request Forgery)
* Description: SSRF occurs when an application allows attackers to send malicious requests to internal services by manipulating input parameters.
* Business Impact:
  + Access to internal systems leading to data exfiltration.
  + Abuse of cloud services for unauthorized actions.
  + Increased risk of lateral movement in attacks.

8) XML External Entities (XXE)

* CWE: CWE-611 (Improper Restriction of XML External Entity Reference)
* OWASP/SANS Category: OWASP Top 10 (A04:2021 - Insecure Design)
* Description: XXE vulnerabilities occur when an application parses XML input without proper validation, allowing attackers to read files and execute remote code.
* Business Impact:
  + Exposure of sensitive internal files.
  + Server crashes due to malicious payload execution.
  + Potential Remote Code Execution (RCE).

9) Unrestricted File Upload

* CWE: CWE-434 (Unrestricted Upload of File with Dangerous Type)
* OWASP/SANS Category: OWASP Top 10 (A08:2021 - Software and Data Integrity Failures)
* Description: Applications that allow users to upload files without proper validation can be exploited to execute malicious scripts, deface websites, or spread malware.
* Business Impact:
  + Execution of malware and backdoors.
  + Server compromise leading to data theft.
  + Website defacement and reputational damage.

10) Cross-Site Request Forgery (CSRF)

* CWE: CWE-352 (Cross-Site Request Forgery)
* OWASP/SANS Category: OWASP Top 10 (A09:2021 - Security Logging and Monitoring Failures)
* Description: CSRF attacks trick authenticated users into unknowingly executing actions on a web application, such as changing passwords or transferring funds.
* Business Impact:
  + Unauthorized transactions or account changes.
  + Loss of user trust due to unintended actions.
  + Difficulty in tracking attacker activities.