1. **Vulnerability Name:** Injection
   * **CWE:** CWE-89
   * **OWASP Category:** A1: Injection
   * **Description:**
     + **Overview:** Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query.
     + **Technical Details:** Attackers can manipulate input to execute malicious commands, leading to data breaches, unauthorized access, and potentially the takeover of the host system.
   * **Business Impact:**
     + **Risk:** High
     + **Consequences:** Data loss, unauthorized access, and potential legal and financial repercussions.
2. **Vulnerability Name:** Broken Authentication
   * **CWE:** CWE-306
   * **OWASP Category:** A2: Broken Authentication
   * **Description:**
     + **Overview:** Broken authentication occurs when attackers exploit flaws in the authentication process to gain unauthorized access to systems or data.
     + **Technical Details:** Common issues include weak password policies, session management problems, and exposed credentials.
   * **Business Impact:**
     + **Risk:** High
     + **Consequences:** Unauthorized access, data breaches, compromised user accounts.
3. **Vulnerability Name:** Sensitive Data Exposure
   * **CWE:** CWE-200
   * **OWASP Category:** A3: Sensitive Data Exposure
   * **Description:**
     + **Overview:** This vulnerability involves the exposure of sensitive data, such as financial information or personal details, due to weak encryption or insecure storage.
   * **Technical Details:** Attackers can intercept and exploit exposed data, leading to identity theft, fraud, or other malicious activities.
   * **Business Impact:**
     + **Risk:** High
     + **Consequences:** Loss of sensitive data, reputational damage, legal consequences.
4. **Vulnerability Name:** XML External Entity (XXE)
   * **CWE:** CWE-611
   * **OWASP Category:** A4: XML External Entity (XXE)
   * **Description:**
     + **Overview:** XXE occurs when an application processes XML input with external entity references, allowing attackers to disclose internal files, execute remote code, and perform other malicious actions.
   * **Technical Details:** Exploiting this vulnerability can lead to unauthorized access to internal files and data.
   * **Business Impact:**
     + **Risk:** Medium to High
     + **Consequences:** Unauthorized access to sensitive information, potential remote code execution.
5. **Vulnerability Name:** Broken Access Control
   * **CWE:** CWE-285
   * **OWASP Category:** A5: Broken Access Control
   * **Description:**
     + **Overview:** Broken access control occurs when users can perform actions or access data they shouldn't have permission for.
     + **Technical Details:** Attackers can exploit this to gain unauthorized access to sensitive areas or perform malicious actions.
   * **Business Impact:**
     + **Risk:** High
     + **Consequences:** Unauthorized access, data breaches, compromised system integrity.
6. **Vulnerability Name:** Security Misconfiguration
   * **CWE:** CWE-15
   * **OWASP Category:** A6: Security Misconfiguration
   * **Description:**
     + **Overview:** Security misconfiguration happens when security settings are not properly implemented or are left insecure.
     + **Technical Details:** Attackers can exploit these misconfigurations to gain unauthorized access or perform other malicious activities.
   * **Business Impact:**
     + **Risk:** Medium to High
     + **Consequences:** Unauthorized access, data breaches, service disruptions.
7. **Vulnerability Name:** Cross-Site Scripting (XSS)
   * **CWE:** CWE-79
   * **OWASP Category:** A7: Cross-Site Scripting (XSS)
   * **Description:**
     + **Overview:** XSS occurs when an application allows untrusted data to be included in web pages, potentially leading to the execution of malicious scripts in the context of a user's browser.
     + **Technical Details:** Attackers can use XSS to steal user data, deface websites, or perform other malicious actions.
   * **Business Impact:**
     + **Risk:** Medium to High
     + **Consequences:** Compromised user accounts, defaced websites, theft of sensitive information.
8. **Vulnerability Name:** Insecure Deserialization
   * **CWE:** CWE-502
   * **OWASP Category:** A8: Insecure Deserialization
   * **Description:**
     + **Overview:** Insecure deserialization occurs when untrusted data is used to abuse the logic of an application, leading to potentially harmful outcomes.
     + **Technical Details:** Attackers can exploit this vulnerability to execute arbitrary code, compromise the application, or launch other attacks.
   * **Business Impact:**
     + **Risk:** High
     + **Consequences:** Remote code execution, unauthorized access, compromised system integrity.
9. **Vulnerability Name:** Using Components with Known Vulnerabilities
   * **CWE:** CWE-840
   * **OWASP Category:** A9: Using Components with Known Vulnerabilities
   * **Description:**
     + **Overview:** This vulnerability involves the use of outdated or vulnerable software components in an application.
     + **Technical Details:** Attackers can exploit known vulnerabilities in components to compromise the security of the entire application.
   * **Business Impact:**
     + **Risk:** Medium to High
     + **Consequences:** Exploitation of known vulnerabilities, potential unauthorized access.
10. **Vulnerability Name:** Insufficient Logging and Monitoring
    * **CWE:** CWE-778
    * **OWASP Category:** A10: Insufficient Logging & Monitoring
    * **Description:**
      + **Overview:** Insufficient logging and monitoring can make it difficult to detect security incidents and respond in a timely manner.
      + **Technical Details:** Without proper logging and monitoring, attackers can operate undetected, increasing the likelihood of successful attacks.
    * **Business Impact:**
      + **Risk:** Medium to High
      + **Consequences:** Delayed detection of security incidents, increased impact of successful attacks.