https://owasp.org/www-project-top-ten/#

Learn More about the top 10 vulnerabilities and try to capture this in a table format.

|  |  |  |
| --- | --- | --- |
| **No** | **Vulnerabilities** | **Description** |
| A01 | Broken Access Control | Broken Access Control moves up to #1. This refers to failures in enforcing proper access controls, allowing unauthorized users to access data or functionality. |
| A02 | Cryptographic Failures | This vulnerability focuses on failures related to cryptography, often leading to sensitive data exposure or system compromise. Previously called Sensitive Data Exposure. |
| A03 | Injection | Injection flaws such as SQL, OS, or LDAP injection. These are caused when untrusted data is sent to an interpreter, leading to unintended actions being performed. |
| A04 | Insecure Design | A new category for 2021 that highlights design flaws. It emphasizes the importance of using threat modeling, secure design patterns, and secure reference architectures. |
| A05 | Security Misconfiguration | Security misconfigurations refer to incomplete or improper configuration settings in software or servers, leading to vulnerabilities. |
| A06 | Vulnerable and Outdated Components | Refers to the use of outdated or insecure software components that may contain known vulnerabilities. This category had previously been titled Using Components with Known Vulnerabilities. |
| A07 | Identification and Authentication Failures | Previously "Broken Authentication", now focusing on identification failures. It deals with issues where attackers can bypass or compromise the authentication process. |
| A08 | Software and Data Integrity Failures | This new category deals with software and data integrity issues, especially with assumptions about updates, critical data, and CI/CD pipelines without verifying integrity. |
| A09 | Security Logging and Monitoring Failures | This includes insufficient logging and monitoring, affecting the ability to detect incidents. This failure hampers visibility, alerting, and forensic investigation. |
| A10 | Server-Side Request Forgery (SSRF) | SSRF attacks occur when an attacker can make the server send requests to unintended locations, often leading to data leakage or other attacks, despite low occurrence rates. |