Here's a summarized table of the [OWASP Top 10 Web Application Security Risks (2021 edition)](https://owasp.org/www-project-top-ten/), representing the most critical vulnerabilities:

|  |  |  |
| --- | --- | --- |
| **Rank** | **Vulnerability Name** | **Description** |
| A01 | Broken Access Control | Failures allowing users to act outside their intended permissions. |
| A02 | Cryptographic Failures | Weak or improper encryption that can expose sensitive data. |
| A03 | Injection | Code injection flaws like SQL, NoSQL, OS, and LDAP injection. |
| A04 | Insecure Design | Security flaws rooted in poor application design and architecture. |
| A05 | Security Misconfiguration | Improperly configured settings, servers, or software components. |
| A06 | Vulnerable and Outdated Components | Usage of libraries or frameworks with known vulnerabilities. |
| A07 | Identification and Authentication Failures | Issues with login mechanisms, session handling, or identity validation. |
| A08 | Software and Data Integrity Failures | Trusting data or software without verification, e.g., unsigned updates. |
| A09 | Security Logging and Monitoring Failures | Lack of visibility into attacks or system misuse due to weak monitoring. |
| A10 | Server-Side Request Forgery (SSRF) | Server is tricked into making requests to unintended destinations. |