# OWASP Top 10 – 2021

| Rank | Category | Explanation | Example |
| --- | --- | --- | --- |
| A01 | Broken Access Control | Improper restrictions allow attackers to access unauthorized data or functions. | A user changing their user ID in a URL to view another user's account. |
| A02 | Cryptographic Failures | Weak or missing encryption exposes sensitive data (formerly called *Sensitive Data Exposure*). | Storing passwords without hashing or transmitting credit card info over HTTP. |
| A03 | Injection | Untrusted data is sent to an interpreter (SQL, OS, LDAP, etc.) causing unwanted actions. | SQL Injection: admin' OR '1'='1 bypasses login. |
| A04 | Insecure Design | The application lacks secure architecture and design from the start. | No rate limiting in a login form allows brute force attacks. |
| A05 | Security Misconfiguration | Default settings, exposed error messages, or unnecessary services cause vulnerabilities. | Leaving admin interfaces open or using default credentials. |
| A06 | Vulnerable and Outdated Components | Using software with known flaws or unsupported versions. | Using jQuery 1.x with known XSS bugs in a web app. |
| A07 | Identification and Authentication Failures | Flaws in login, session management, or password reset mechanisms. | Weak session ID can be guessed or reused. |
| A08 | Software and Data Integrity Failures | The app doesn’t verify the integrity of software or data updates. | No signature check for plugins allows a malicious update. |
| A09 | Security Logging and Monitoring Failures | Inadequate logging or alerting delays detection of attacks. | No logs of failed logins or no alerts on suspicious activity. |
| A10 | Server-Side Request Forgery (SSRF) | Server makes unintended requests to internal systems on behalf of attacker. | Attacker tricks server into accessing http://localhost/admin. |