### OWASP Top 10 Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| # | Vulnerability | Description | Example |
| A01 | Broken Access Control | Users can access data or actions they're not supposed to (like editing someone else’s account). | Changing user ID in URL to access another user's data. |
| A02 | Cryptographic Failures | Sensitive data is not encrypted properly during storage or transmission. | Sending passwords over HTTP instead of HTTPS. |
| A03 | Injection | Attacker sends malicious input to execute unintended commands. | SQL Injection: OR '1'='1' in login forms. |
| A04 | Insecure Design | Poor application design with no secure defaults or threat modeling. | Lack of rate-limiting allows brute-force attacks. |
| A05 | Security Misconfiguration | Unsafe default settings or unnecessary features enabled. | Directory listing is turned on in production. |
| A06 | Vulnerable and Outdated Components | Using old or unpatched libraries/software. | Using an old jQuery version with known XSS issues. |
| A07 | Identification and Authentication Failures | Weak login, session management, or MFA problems. | Reusing session IDs or no account lockout after many login attempts. |
| A08 | Software and Data Integrity Failures | Using untrusted sources for code updates or plugins. | Loading a script from an external source without verifying integrity. |
| A09 | Security Logging and Monitoring Failures | Poor logging allows attacks to go unnoticed. | No alert triggered when a user tries 100 failed logins. |
| A10 | Server-Side Request Forgery (SSRF) | Server can be tricked into making requests to internal systems. | Image upload feature fetches metadata from internal server IPs. |