# OWASP Top 10 (2021) — Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| OWASP Top 10 | Vulnerability | Description | Common Example |
| A01:2021 | Broken Access Control | Restrictions on authenticated users are not properly enforced. Attackers can act as users or admins without proper authorization. | URL tampering to access another user’s account |
| A02:2021 | Cryptographic Failures | Sensitive data exposure due to insecure cryptography or lack of encryption. | Sending sensitive data (e.g., passwords) over HTTP instead of HTTPS |
| A03:2021 | Injection | Untrusted data is sent to an interpreter, leading to unintended commands or data leakage. | SQL Injection — manipulating SQL queries via input fields |
| A04:2021 | Insecure Design | Flaws in design that compromise security even before coding starts. | No rate limiting on login attempts, enabling brute force attacks |
| A05:2021 | Security Misconfiguration | Incorrect configurations or incomplete setups expose vulnerabilities. | Default admin accounts left enabled, error messages leaking stack traces |
| A06:2021 | Vulnerable and Outdated Components | Using components (libraries, frameworks) with known vulnerabilities. | Using an old version of jQuery with known security issues |
| A07:2021 | Identification and Authentication Failures | Weak authentication mechanisms that allow attackers to compromise passwords, keys, or session tokens. | Session fixation or weak password policies |
| A08:2021 | Software and Data Integrity Failures | Code and infrastructure do not protect against integrity violations. | Unsigned software updates, using plugins from untrusted sources |
| A09:2021 | Security Logging and Monitoring Failures | Insufficient logging and monitoring delay detection and response to breaches. | No logging of failed login attempts, making breach investigations difficult |
| A10:2021 | Server-Side Request Forgery (SSRF) | The server is tricked into sending requests to unintended locations, including internal services. | Attacker tricks a server into accessing internal metadata URLs |