1. Broken Access Control

Severity	Example Issues
Critical	Privilege Escalation (e.g., user accessing admin panel)
High	Horizontal Privilege Escalation (e.g., user accessing other users' data)
Medium	IDOR (Insecure Direct Object Reference) without sensitive data exposure
Low	Lack of Role-Based Access Control Enforcement
Informational	Unused roles or permissions present

---

2. Cryptographic Failures

Severity	Example Issues
Critical	No encryption on sensitive data (Passwords, Credit Cards)
High	Use of weak/hardcoded encryption keys
Medium	Outdated TLS/SSL versions in use (SSLv2, SSLv3, TLS 1.0)
Low	Missing HSTS header
Informational	Lack of encryption for non-sensitive data (like public images)

---

3. Injection (SQL, OS, LDAP, etc.)

Severity	Example Issues
Critical	SQL Injection leading to RCE or DB Dump
High	Command Injection allowing OS-level control
Medium	Reflected XSS or Blind SQL Injection without critical impact
Low	Email Header Injection without exploitation potential
Informational	Input fields accepting unsanitized input without impact

---

4. Insecure Design

Severity	Example Issues
Critical	Absence of security controls by design
High	No input validation or threat modeling
Medium	Lack of secure password policies
Low	Inadequate error handling revealing stack traces
Informational	No documentation of security requirements

---

5. Security Misconfiguration

Severity	Example Issues
Critical	Admin interfaces exposed publicly without authentication
High	Default credentials still enabled
Medium	Directory Listing enabled
Low	Verbose error messages
Informational	Commented sensitive information in source code

---

6. Vulnerable and Outdated Components

Severity	Example Issues
Critical	Use of components with known RCE vulnerabilities
High	Critical CVEs in use without patch
Medium	Medium-severity CVEs without mitigation
Low	Components nearing End-of-Life (EOL)

Severity	Example Issues
Informational	Outdated components with no known vulnerabilities

---

7. Identification and Authentication Failures

Severity	Example Issues
Critical	Authentication bypass (logic flaws)
High	Brute-force attack possible due to no rate-limiting
Medium	Weak password policy
Low	Username enumeration possible via error messages
Informational	Missing MFA recommendations

---

8. Software and Data Integrity Failures

Severity	Example Issues
Critical	Unsigned/Unverified software updates leading to RCE
High	Integrity check missing for important config/data files
Medium	Weak or predictable hash algorithms (MD5, SHA1)
Low	Lack of Subresource Integrity (SRI) in scripts
Informational	No code signing in non-critical components

---

9. Security Logging and Monitoring Failures

Severity	Example Issues
Critical	No logging of security-relevant events (logins, privilege changes)
High	Logs not protected, allowing tampering

Severity	Example Issues
Medium	Lack of monitoring on critical assets
Low	Generic error messages without context
Informational	No centralized logging implemented

---

10. Server-Side Request Forgery (SSRF)

Severity	Example Issues
Critical	SSRF allowing internal network pivot or metadata access
High	SSRF leading to sensitive data leakage
Medium	SSRF exploitable only on specific endpoints
Low	SSRF with restricted outbound requests
Informational	URL parsing logic vulnerable but with no practical exploit