OWASP Top 10 – PetStore Application Vulnerability Mapping

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Name** | **Description** | **Example in PetStore Application** | **Mitigation** |
| A01:2021 | Broken Access Control | Unauthorized users gain access to restricted data or actions | Unauthenticated users may access sensitive catalog/cart URLs directly via browser address bar | Enforce strict access control rules on the backend; test URL access and privilege escalations |
| A02:2021 | Cryptographic Failures | Weak or missing encryption for sensitive data | Passwords may be transmitted without HTTPS or stored insecurely | Enforce HTTPS; hash passwords using secure algorithms like bcrypt; avoid transmitting plain data |
| A03:2021 | Injection | Untrusted input used in a command or query | Search field may allow SQL-like or script injection | Use parameterized queries, input validation, and context-aware output encoding |
| A04:2021 | Insecure Design | Security flaws due to poor architectural decisions | No validation on quantity input in cart allows negative values | Apply secure design principles; validate logic both on UI and server side |
| A05:2021 | Security Misconfiguration | Default settings, exposed error messages, or misconfigured headers | Missing HTTP security headers like Content-Security-Policy, X-Frame-Options | Harden server config; disable detailed error messages; add security headers |
| A06:2021 | Vulnerable and Outdated Components | Using libraries or software with known vulnerabilities | Outdated JavaScript/CSS libraries in front-end | Regularly update third-party libraries and monitor for CVEs |
| A07:2021 | Identification and Authentication Failures | Insecure login or session management | No CAPTCHA during login; sessions may not expire; password reset is not protected | Use secure login flows, CAPTCHA, MFA, strong password policies, and session timeouts |
| A08:2021 | Software and Data Integrity Failures | Code and data integrity not verified | External JS loaded without SRI; no verification of delivery channels | Use SRI, digital signatures, and secure CI/CD pipelines |
| A09:2021 | Security Logging and Monitoring Failures | Lack of alerting or insufficient logging for threats | Checkout errors or login attempts not logged | Enable centralized logging and monitoring; define alert thresholds for anomalies |
| A10:2021 | Server-Side Request Forgery (SSRF) | Server is tricked into making unauthorized requests | If API endpoints accept user-defined URLs, attacker could attempt internal access | Validate and sanitize all URLs and input; whitelist allowed domains |