**security vulnerabilities**

|  |  |  |  |
| --- | --- | --- | --- |
| **OWASP Category** | **JPetStore** | **Why It Might Be Vulnerable** | **OWASP Reference** |
| **A01: Broken Access Control** | Typing URL /actions/Admin.action directly | If this page is not blocked for normal users, it gives access to admin-only content. | A01: Broken Access Control |
| **A02: Cryptographic Failures** | Login form uses http:// instead of https:// | Passwords sent over HTTP can be seen by attackers on the network. | A02: Cryptographic Failures |
| **A03: Injection** | Typing <script>alert (1) </script> in search bar | If the website shows the script result, it's vulnerable to XSS (cross-site scripting). | A03: Injection |
| **A04: Insecure Design** | Manually changing quantity in cart URL | Changing /updateCart?qty=1000 might let user buy 1000 items not available in stock. | A04: Insecure Design |
| **A05: Security Misconfiguration** | Missing headers in HTTP response (like X-Frame-Options) | Without headers, the site is open to attacks like clickjacking. | A05: Security Misconfiguration |
| **A06: Vulnerable Components** | . action in URL indicates Java Struts (old tech) | Older versions of Java frameworks may have known security holes. | A06: Vulnerable and Outdated Components |
| **A07: Auth Failures** | Unlimited login attempts without lockout | Allows brute-force attacks — attacker keeps guessing until correct. | A07: Identification and Authentication Failures |
| **A08: Integrity Failures** | External JS files loaded without integrity check | If an attacker changes the JS, users may run malicious code unknowingly. | A08: Software and Data Integrity Failures |
| **A09: Logging Failures** | Wrong passwords do not show warning or delay | No logs = admins don’t know if someone is attacking the site. | A09: Security Logging and Monitoring Failures |
| **A10: SSRF** | If app lets users enter URLs to fetch (e.g., image) | Malicious user could trick server into requesting internal/private systems. | A10: Server-Side Request Forgery |