**Stage – 1:**

**List of Vulnerability Table ➖**

|  |  |  |
| --- | --- | --- |
| **S.no** | **Vulnerability Name** | **CWE - No** |
| **1**  **2**  **3**  **4**  **5** | SQL Injection  Cross-Site Scripting (XSS)  Broken Authentication  Sensitive Data Exposure  Security Misconfiguration | CWE-89  CWE-79  CWE-287  CWE-200  CWE-16 |

**REPORT:-**

**1) Vulnerability Name :-** SQL Injection (SQLi)

**CWE :-** CWE-89 (Improper Neutralization of Special Elements in SQL Commands)

**OWASP/SANS Category :-** OWASP Top 10 (A03:2021 - Injection) / SANS 25 (#1 - SQL Injection)

**Description :-** bWAPP contains vulnerable input fields that do not properly sanitize user input, allowing attackers to inject malicious SQL queries. Attackers can retrieve or modify sensitive database information by manipulating SQL statements.

**Business Impact** :-

* Unauthorized access to user data (passwords, payment details).
* Potential data breach and compliance violations (GDPR, CCPA).
* Database corruption or deletion, leading to service disruption.

**2) Vulnerability Name :-** Cross-Site Scripting (XSS)

**CWE :-** CWE-79 (Improper Neutralization of Input During Web Page Generation)

**OWASP/SANS Category :-** OWASP Top 10 (A07:2021 - Identification and Authentication Failures) / SANS 25 (#2 - XSS)

**Description :-** bWAPP does not properly sanitize or escape user input, allowing attackers to inject JavaScript into web pages. This enables session hijacking, phishing attacks, and defacement of web pages.

**Business Impact** :-

* Session hijacking leading to account takeovers.
* Data theft (stealing cookies, personal information).
* Reputation damage if malicious scripts alter website content.

**3) Vulnerability Name :-** Broken Authentication

**CWE :-** CWE-287 (Improper Authentication)

**OWASP/SANS Category :-** OWASP Top 10 (A07:2021 - Identification and Authentication Failures) / SANS 25 (#3 - Broken Authentication)

**Description :-** Weak authentication mechanisms allow brute-force attacks, credential stuffing, and session hijacking. bWAPP lacks multi-factor authentication (MFA) and uses weak session management, making it vulnerable.

**Business Impact** :-

* User account compromise, leading to identity theft.
* Privilege escalation, allowing attackers to gain admin access.
* Financial and reputational loss due to unauthorized transactions.

**4) Vulnerability Name :-** Insecure Direct Object References (IDOR)

**CWE :-** CWE-639 (Authorization Bypass Through User-Controlled Key)

**OWASP/SANS Category :-** OWASP A06:2021 (Vulnerable and Outdated Components)

**Description :-** bWAPP exposes object references in URLs, allowing attackers to manipulate IDs to access unauthorized data. Attackers can view or modify records belonging to other users.