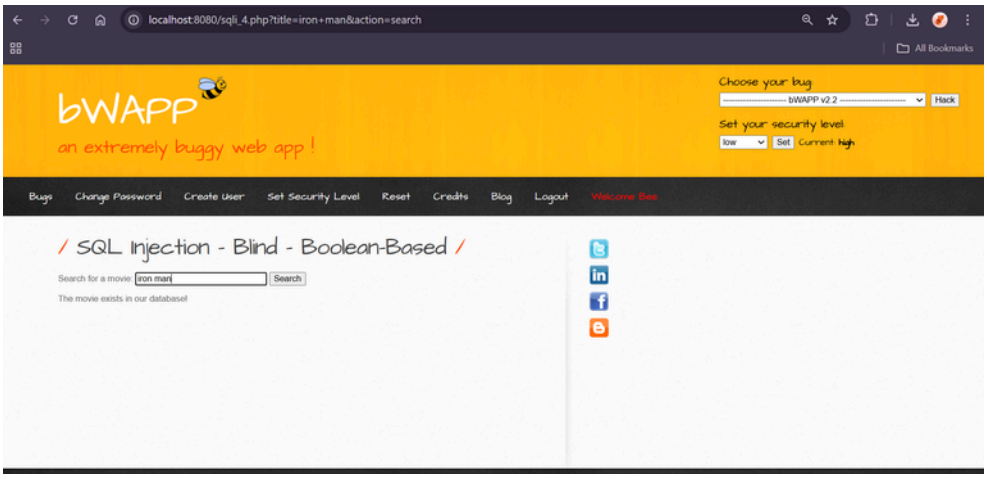
bWAPP Security Report

This report summarizes the security assessment performed on the bWAPP application. It documents the vulnerabilities discovered, their impact, proof of concept, and recommended mitigation steps. The assessment aligns with the OWASP Top 10 framework.

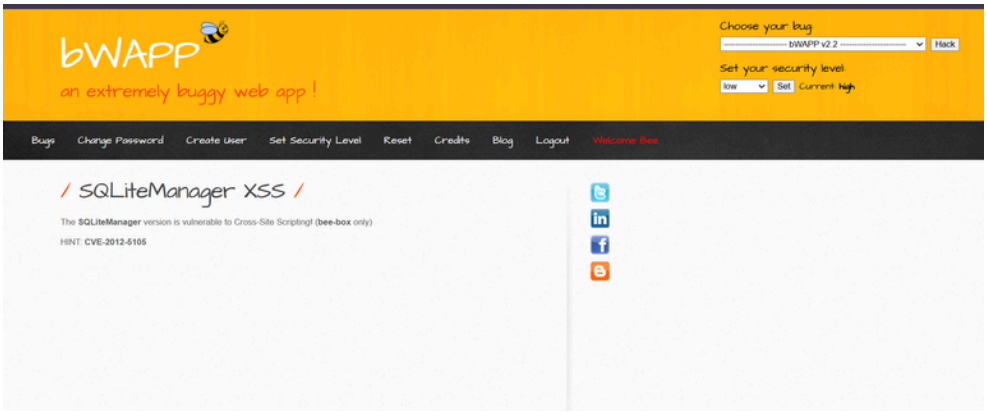
1. SQL Injection

Description: The application fails to properly sanitize user input in SQL queries, allowing attackers to extract or manipulate database contents. **Impact:** High - Can lead to data leakage, credential theft, or complete database compromise. **Mitigation:** Use parameterized queries (prepared statements), apply input validation, and implement least privilege for database users.



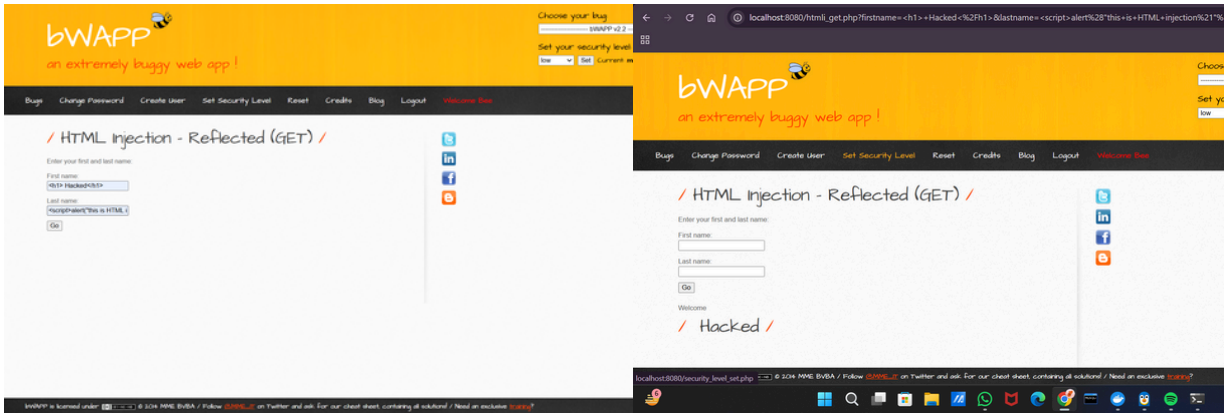
2. Cross-Site Scripting (XSS)

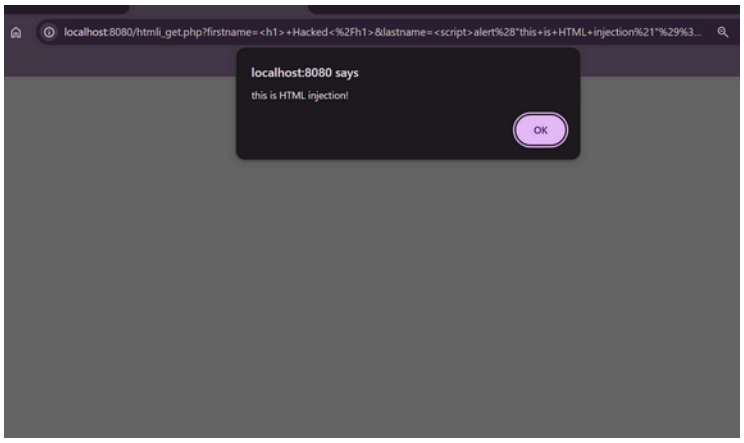
Description: User input is directly reflected on the webpage without proper sanitization, enabling execution of malicious JavaScript.
Impact: Medium - Can result in session hijacking, phishing, or redirection to malicious websites.
Mitigation: Sanitize and encode all user inputs, use Content Security Policy (CSP), and validate data on both client and server sides.



3. HTML Injection

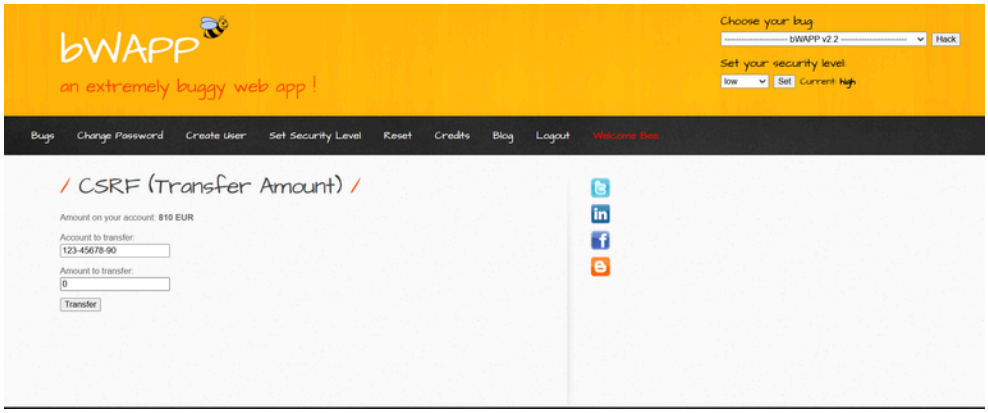
Description: The application allows raw HTML tags to be injected into forms, altering the webpage's structure and misleading users. **Impact:** Medium - Can modify webpage layout, deface the application, or trick users into submitting sensitive data. **Mitigation:** Escape and encode HTML characters, sanitize input, and implement strict content validation.

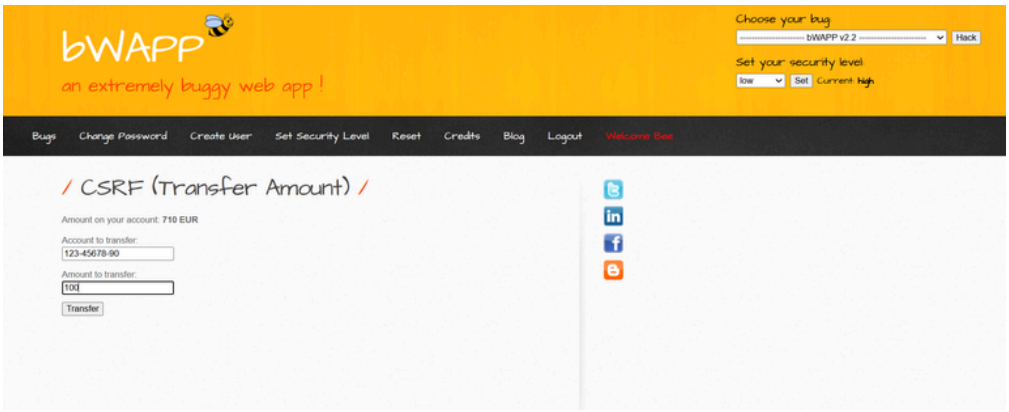




4. Cross-Site Request Forgery (CSRF)

Description: The application does not implement anti-CSRF tokens, allowing attackers to trick users into performing unintended actions.
Impact: High - Can result in unauthorized actions on behalf of authenticated users.
Mitigation: Use unique CSRF tokens for each request, validate the origin of requests, and implement same-site cookies.





OWASP Top 10 Mapping

Vulnerability	OWASP Category
SQL Injection	A03: Injection
Cross-Site Scripting (XSS)	A03: Injection
HTML Injection	A03: Injection
Cross-Site Request Forgery (CSRF)	A05: Security Misconfiguration