**Future\_CS\_01: Web Application Security Testing Report**  
**Submitted by:** Shravani Joshi  
**Internship Program:** Future Interns – Cybersecurity Track  
**Project Title:** Web Application Security Testing – A Hands-On Experience with Real Vulnerabilities  
**Date:** 13-05-25

**1. Objective**

The purpose of this project was to explore common web application vulnerabilities through practical testing in a safe and controlled environment. The focus was on identifying and exploiting vulnerabilities such as **SQL Injection (SQLi)** and **Cross-Site Scripting (XSS)** using industry-standard tools.

This exercise was conducted for educational purposes only, with ethical considerations in place. All testing was performed on intentionally vulnerable applications.

**2. Scope of the Project**

* Perform manual and automated vulnerability assessments
* Identify real vulnerabilities and simulate potential impacts
* Suggest appropriate mitigation techniques
* Document findings in a detailed security report

**3. Tools & Platforms Used**

* **OWASP ZAP**: Intercepting proxy and automated vulnerability scanner
* **Burp Suite Community Edition**: Manual testing of web application requests and responses
* **Altoro Mutual (by HCL)**: Deliberately vulnerable banking application for ethical testing
* **OWASP Juice Shop**: Widely used vulnerable app for XSS and client-side vulnerability testing

**4. Testing Methodology**

**4.1 SQL Injection (SQLi) – Altoro Mutual**

* **Tool Used:** OWASP ZAP
* **Approach:** Injected basic SQL queries in login fields and form inputs
* **Outcome:**
  + Successfully bypassed login and accessed admin dashboard
  + Viewed sensitive transaction histories
  + Modified user profiles
  + Simulated unauthorized money transfers
* **Impact:** Demonstrated the severity of improperly sanitized input fields and lack of backend validation.

**4.2 Cross-Site Scripting (XSS) – OWASP Juice Shop**

* **Tools Used:** OWASP ZAP and Burp Suite
* **Approach:** Inserted malicious scripts into comment fields and search parameters
* **Outcome:**
  + Successfully triggered script executions in the browser
  + Demonstrated potential for session hijacking and content manipulation
* **Impact:** Highlighted the ease of executing XSS in poorly protected input areas and emphasized the need for output encoding.

**5. Key Findings**

| **Vulnerability** | **Application** | **Severity** | **Potential Impact** |
| --- | --- | --- | --- |
| SQL Injection | Altoro Mutual | High | Account takeover, unauthorized transactions |
| XSS | OWASP Juice Shop | Medium | Data theft, session hijacking, defacement |

**6. Mitigation Recommendations**

* **Input Validation:** Sanitize all user inputs on both client and server sides
* **Parameterized Queries:** Use prepared statements to avoid SQL injection
* **Output Encoding:** Encode data before rendering it in the browser to prevent XSS
* **Content Security Policy (CSP):** Enforce strict content policies for browsers
* **Regular Security Testing:** Integrate vulnerability scanning into CI/CD pipelines

**7. Learning Outcomes**

* Gained hands-on experience in identifying and exploiting real-world web vulnerabilities
* Developed familiarity with OWASP’s top vulnerabilities and practical mitigation strategies
* Improved understanding of how seemingly minor gaps in validation can lead to critical system compromises
* Strengthened technical proficiency in using tools like ZAP and Burp Suite for ethical penetration testing

**8. Conclusion**

This project provided a realistic and impactful introduction to **Web Application Security Testing**. It reinforced the importance of secure coding practices, continuous vulnerability assessments, and a strong security-first development mindset. The exercise demonstrated how **real-world attacks are executed** and, more importantly, how they can be **prevented with proactive security measures**.

**9. Deliverables**

* Vulnerability Assessment Report (attached)
* Screenshots of successful injections (redacted for ethical reasons)
* List of mitigation strategies for each vulnerability identified

**10. Acknowledgments**

Special thanks to **Future Interns** for providing the environment and resources to conduct this project safely and ethically. This experience has greatly contributed to my understanding of application-level security and ethical hacking.