OWASP Juice Shop Security Findings Report

Project / Task: Day 3 – Security Basics
Application: OWASP Juice Shop
Date: 30-08-2025
Tester: Khadija

---

1. Summary

During exploration of the OWASP Juice Shop demo, several security issues were identified including input validation flaws, weak authentication, and broken access control. These findings are documented below with steps to reproduce, severity, and recommended mitigation measures.

---

2. Findings Table

#	Issue / Vulnerability	Type	Steps to Reproduce	Severity	Notes / Recommendations
1	Weak Password Acceptance	Authentication	1. Go to Sign Up 2. Enter `email: test@gmail.com` 3. Enter `password: 12345` 4. Submit	Medium	Enforce strong password policy (min length + complexity)
2	XSS in Product Review	Input Validation	1. Go to any product 2. Enter `<script>alert('XSS')</script>` in review field 3. Submit	High	Sanitize inputs and encode output to prevent JS execution
3	Access to Admin Features	Broken Access Control	1. Navigate to `/admin` URL without logging in 2. Observe access to admin page	High	Restrict pages to authorized roles only
4	Sensitive Data in Error Message	Information Disclosure	1. Submit invalid login 2. Observe stack trace or detailed error	Medium	Customize error messages to avoid revealing internal logic

---

3. Observations / Additional Notes

- Modules allow invalid data formats
- Application shows overly verbose error messages in some flows.
- Many issues are intentional for learning purposes.

---

4. Conclusion

The OWASP Juice Shop intentionally exposes multiple vulnerabilities for learning purposes. Critical issues include XSS, broken access control, and weak authentication. Mitigation strategies involve proper input validation, role-based access control and password policy enforcement.