Attack Report – OWASP Juice Shop

Threat Scenario

In this lab we are testing OWASP Juice Shop, which is a purposely vulnerable web application. The goal is to act like an attacker and try to break into the system. We selected the login page and admin functions as our target. The attack goal was to bypass authentication and get unauthorized access.

Attack 1: Administrator Page Access

Execution: We tried to open the administrator page directly by typing the URL http://localhost:3000/#/administration. Result: The page opened even without proper admin login. Evidence: Screenshot of the administration page visible without authentication. Impact: This shows broken access control. Sensitive admin page is not properly protected.

Attack 2: Weak Password Login

Execution: We attempted login with user admin@juice-sh.op and password admin123. Result: Login was successful. Evidence: Screenshot of successful login with weak password. Impact: This shows broken authentication. The system is using simple and guessable password for admin account.

Attack 3: SQL Injection

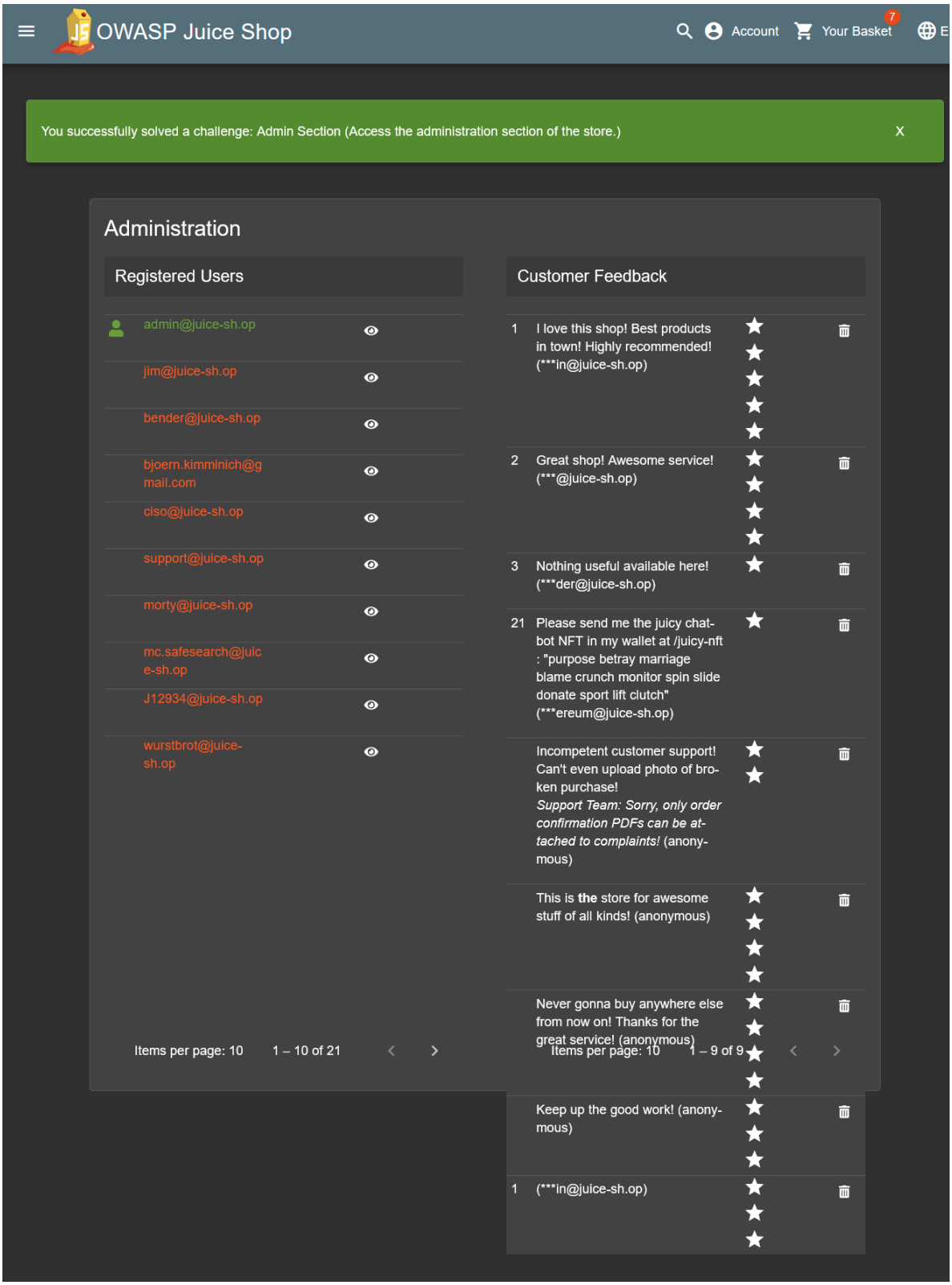
Execution: On the login page, in the email field we entered the payload ' OR 1=1--. In the password field we typed anything. Result: Login was successful without knowing the real password. Evidence: Screenshot of login page with payload and successful login. Impact: This shows SQL Injection vulnerability. The query is not sanitized and attacker can bypass login easily.

Tools and Commands Used

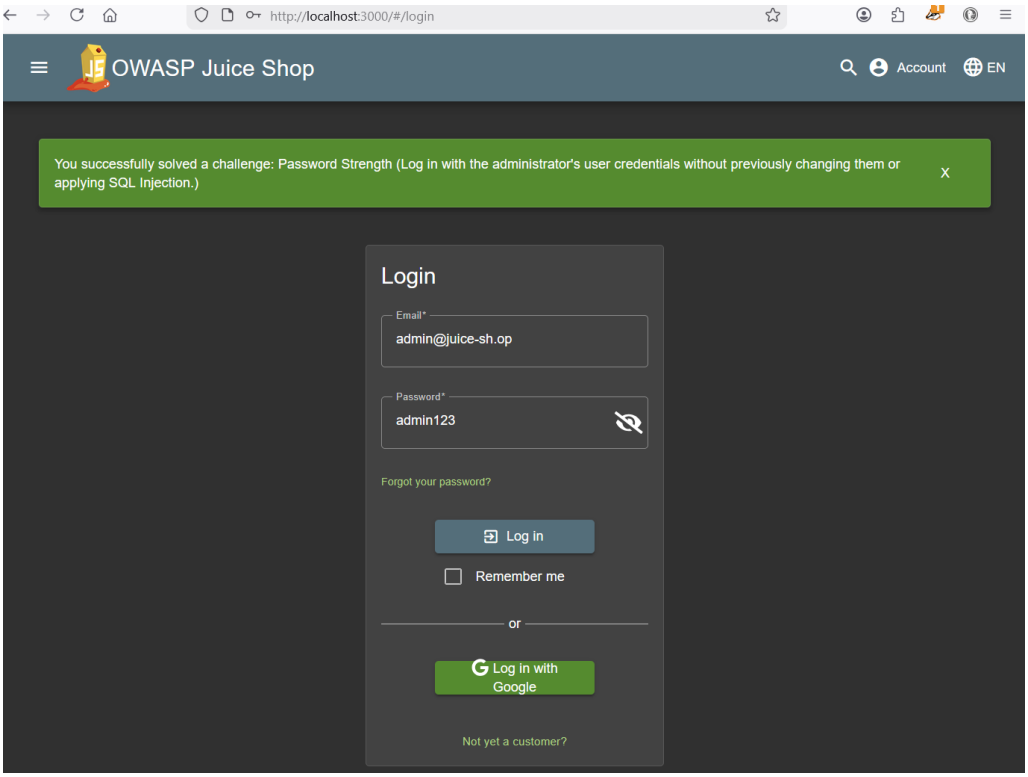
- Browser (Firefox/Chrome) for accessing Juice Shop.
- Simple payloads typed directly in login form.
- No special hacking tools were needed, only manual testing.

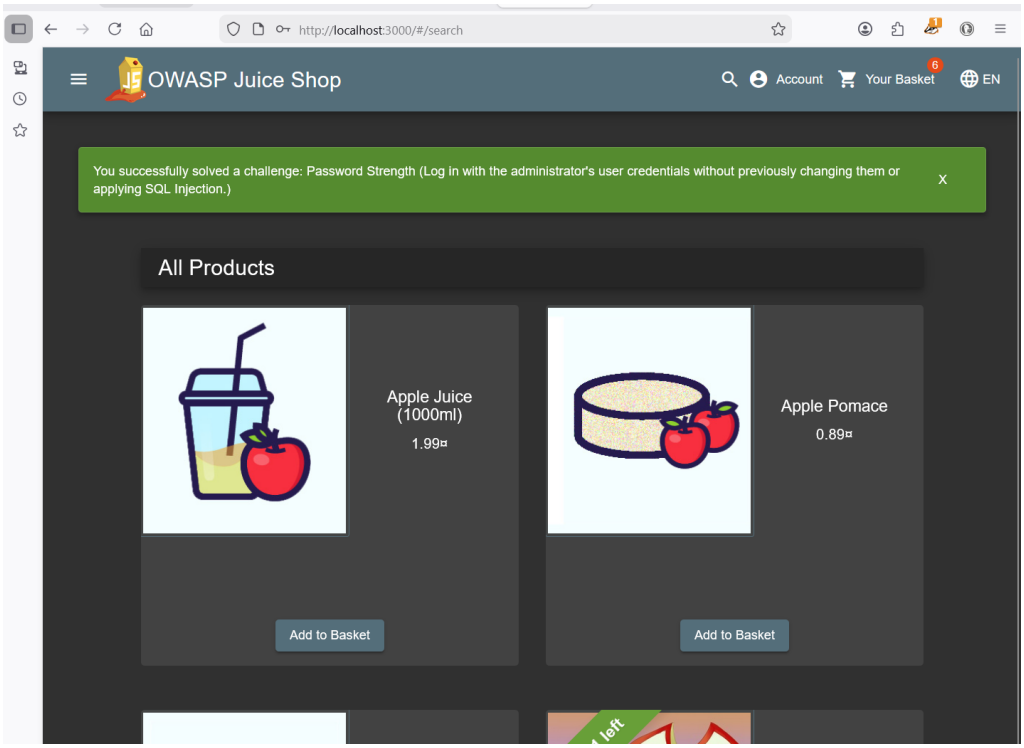
Evidence of Success

Screenshots of administrator page opened directly.

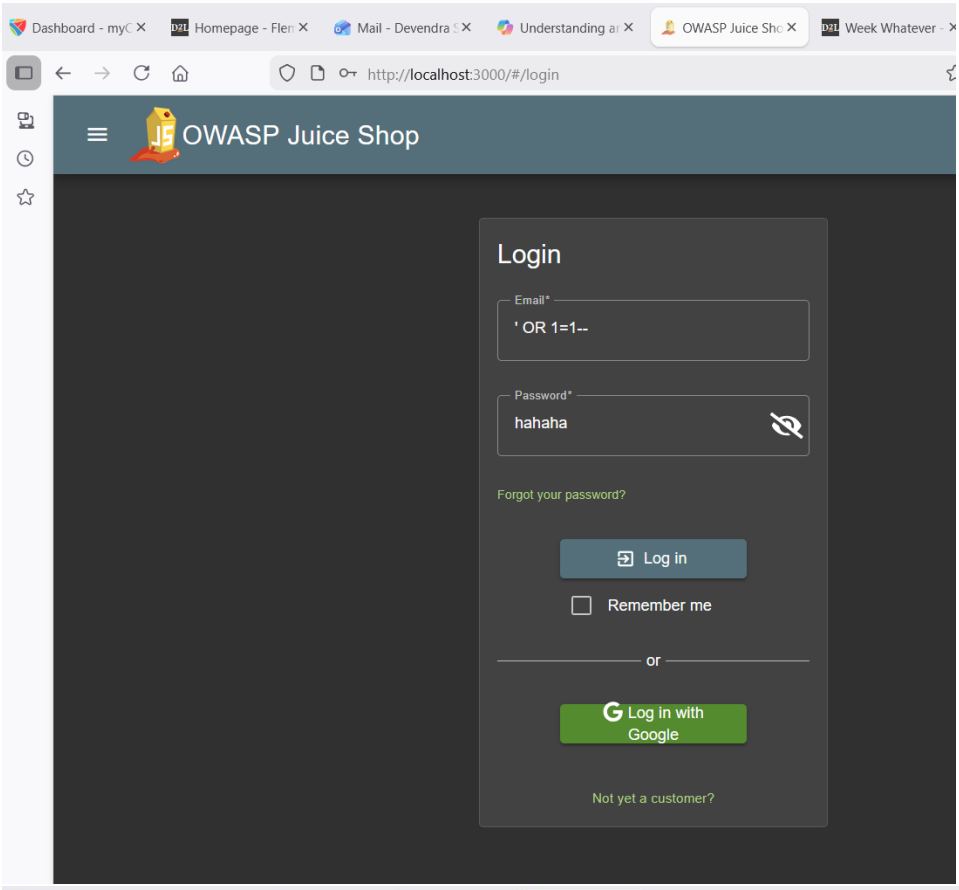


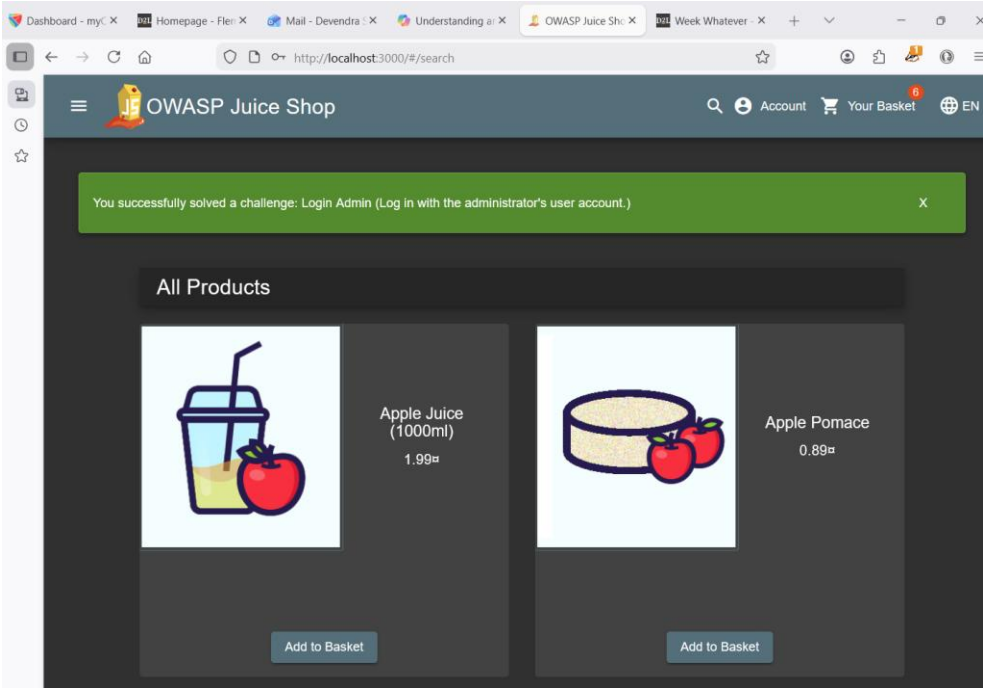
Screenshots of login with weak password admin123.





Screenshots of login bypass using ' OR 1=1--.





Conclusion

We performed three attacks on Juice Shop: direct administrator page access, weak password login, and SQL Injection. All three attacks were successful. This proves that Juice Shop is vulnerable and can be exploited easily. The next step will be to apply mitigation using Web Application Firewall and secure coding practices.