

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.

The screenshot shows the OWASP Juice Shop administration interface. At the top, there's a green banner stating "You successfully solved a challenge: Admin Section (Access the administration section of the store.)". Below this, the main content area is divided into two sections: "Registered Users" and "Customer Feedback".

Registered Users:

- admin@juice-sh.op
- jim@juice-sh.op
- bender@juice-sh.op
- bjoern.kimminich@g mail.com
- ciso@juice-sh.op
- support@juice-sh.op
- morty@juice-sh.op
- mc.safesearch@juic e-sh.op
- J12934@juice-sh.op
- wurstbrot@juice sh.op

Customer Feedback:

- 1 I love this shop! Best products in town! Highly recommended! (**in@juice-sh.op)
★★★★★
- 2 Great shop! Awesome service! (**@juice-sh.op)
★★★★★
- 3 Nothing useful available here! (**der@juice-sh.op)
★★★★★
- 21 Please send me the juicy chat-bot NFT in my wallet at /juicy-nft : "purpose betray marriage blame crunch monitor spin slide donate sport lift clutch"
(**ereum@juice-sh.op)
Incompetent customer support!
Can't even upload photo of bro-
ken purchase!
Support Team: Sorry, only order confirmation PDFs can be attached to complaints! (anony-
mous)
- This is the store for awesome stuff of all kinds! (anonymous)
★★★★★
- Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)
Items per page: 10 1 – 10 of 21 < >
Items per page: 10 1 – 9 of 9 < >
★★★★★
- Keep up the good work! (anony-
mous)
★★★★★
- 1 (**in@juice-sh.op)
★★★★★

Screenshots of login with weak password admin123.

The screenshot shows the OWASP Juice Shop login interface. At the top, there is a green notification bar with the text: "You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)". Below this is the login form with fields for Email* (admin@juice-sh.op) and Password* (admin123). There is also a "Forgot your password?" link, a "Log in" button, a "Remember me" checkbox, and a "Log in with Google" button. A "Not yet a customer?" link is at the bottom.

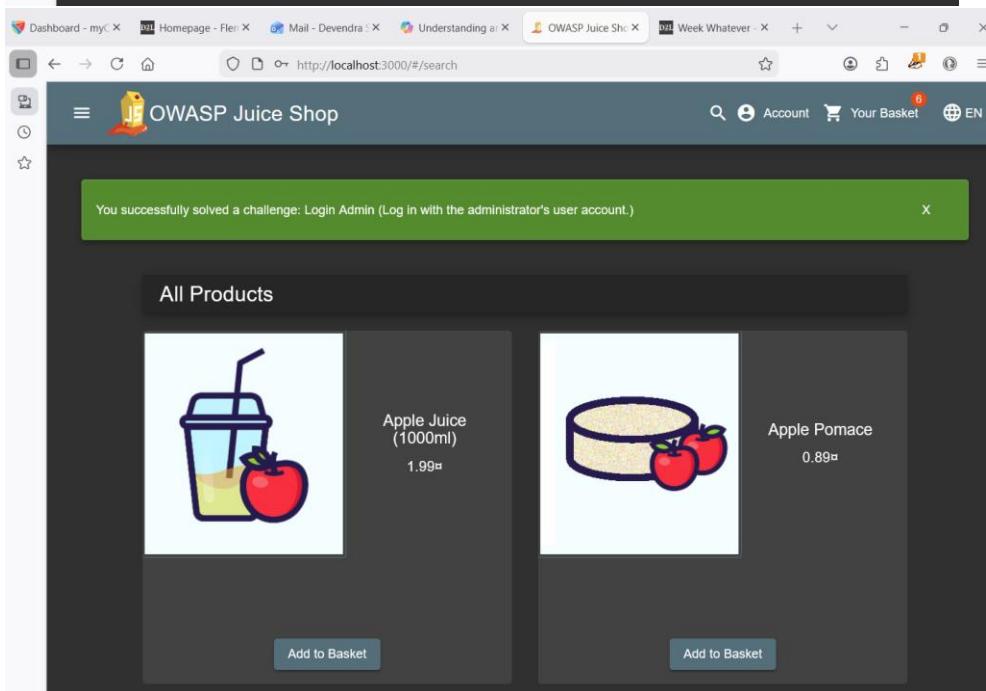
The screenshot shows the OWASP Juice Shop "All Products" page. At the top, there is a green notification bar with the same challenge completion message. Below it, the page displays two product items: "Apple Juice (1000ml)" priced at 1.99 and "Apple Pomace" priced at 0.89. Each item has a thumbnail image, a product name, a price, and an "Add to Basket" button. The footer features a navigation bar with links like "left", "right", and "home".

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

The screenshot shows a browser window with the URL <http://localhost:3000/#/login>. The page title is "OWASP Juice Shop". The login form has the following fields:

- Email*: ' OR 1=1--
- Password*: hahaha

Below the form are links for "Forgot your password?", "Log in" (with a key icon), "Remember me" (unchecked), and "Log in with Google". At the bottom is a link "Not yet a customer?".



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.