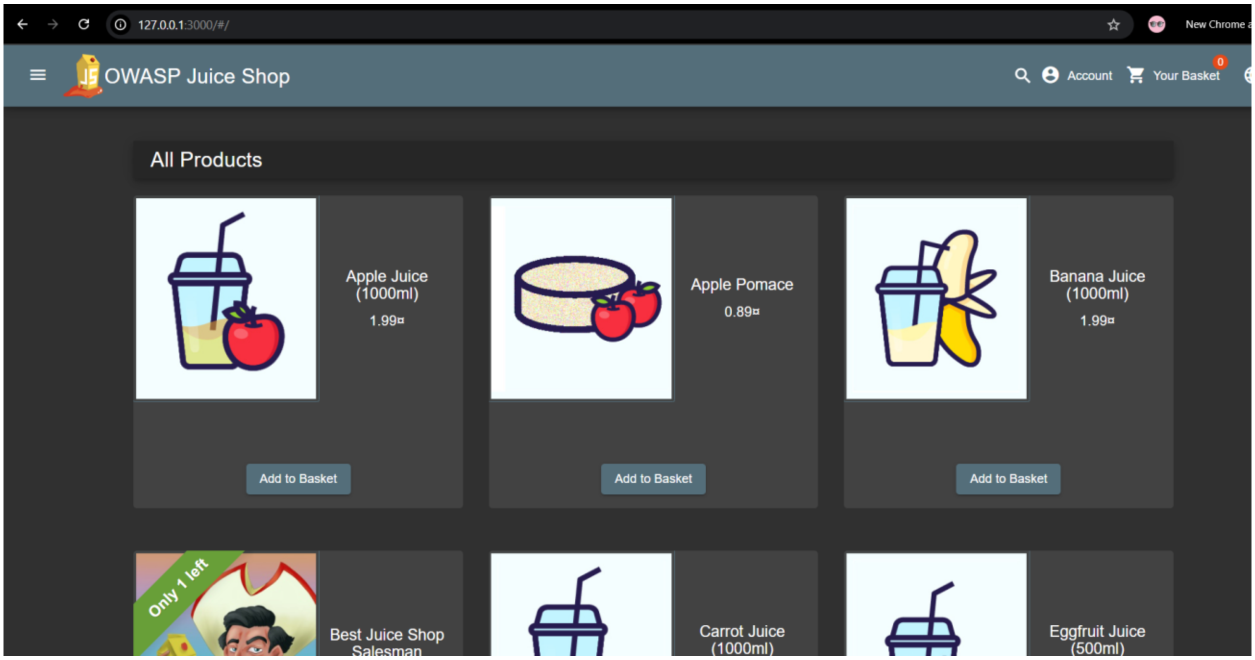
OWASP Juice Shop:



Mitigation Report:

Lab 01: Missing Encoding

Before showing user input, modify it using proper output encoding (for example, < to &lt; > to &gt; # to %23).

For the browser to display user input as text and not run it, always treat it as data rather than code.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

---

Lab 02: Outdated Allowlist [Redirection]

Block redirects to the unfamiliar/unrecognized links and only authorize redirects to reputable domains [trusted sites].

The website ought to stop the redirect if the URL/link is not on the authorized/allow list.

References:

https://techdocs.f5.com/en-us/bigip-16-1-0/big-ip-asm-implementations/mitigating-open-redirects.html

---

Lab 03: Confidential Document Exposure

When a website improperly controls access, anyone may see private information, resulting to the disclosure of private documents. Attackers can view or steal important data, which makes this risky.

References:

https://owasp.org/Top10/2025/A01_2025-Broken_Access_Control/

https://www.activestate.com/blog/the-risks-of-broken-access-control-explained-vulnerabilities-examples-best-practices/