Input Validation & Cross-Site Scripting

Lab Setup

1. Target Lab Used

- OWASP Juice Shop
- Deployed using Docker

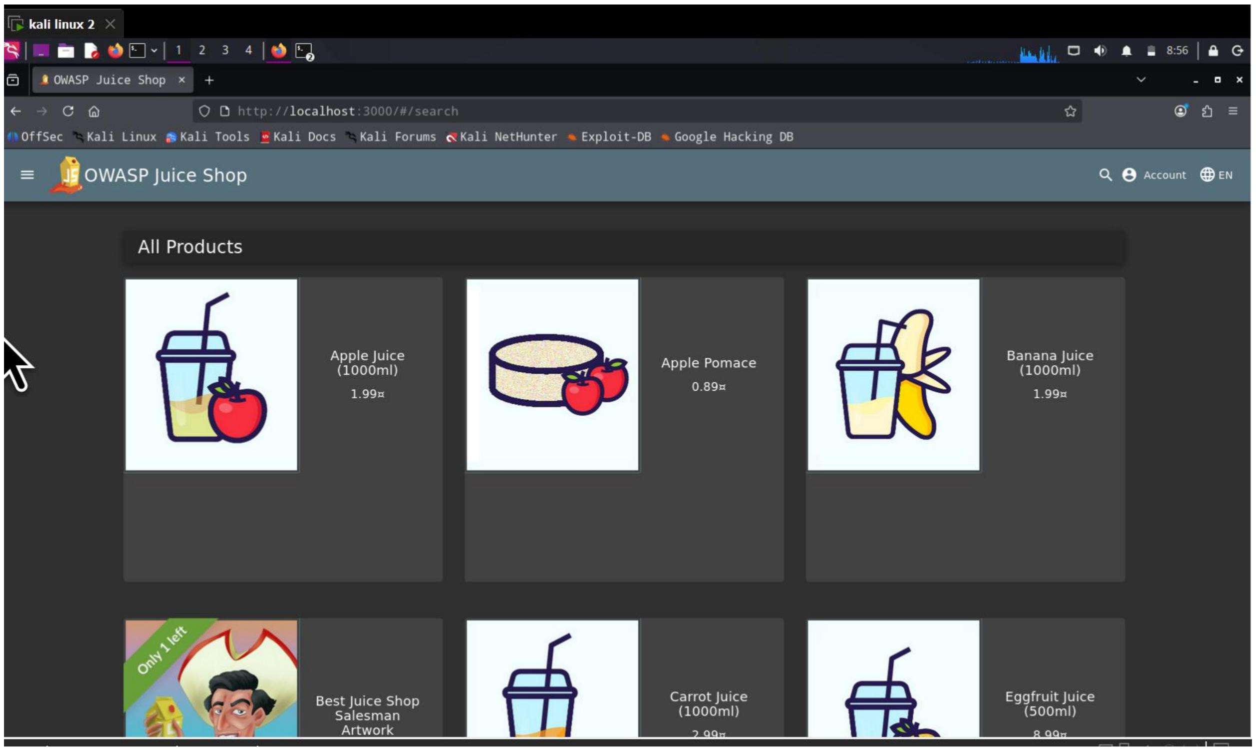


Figure 1 Juice Shop homepage visible

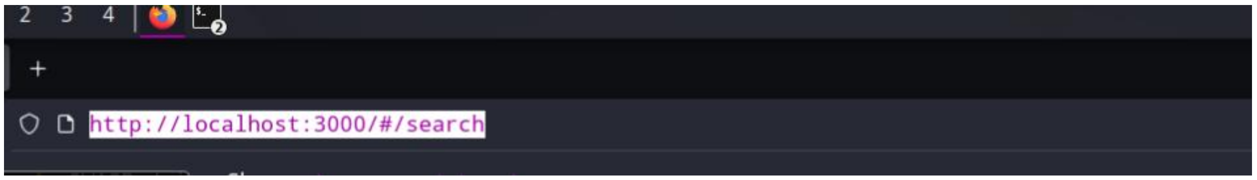


Figure 2 localhost:3000

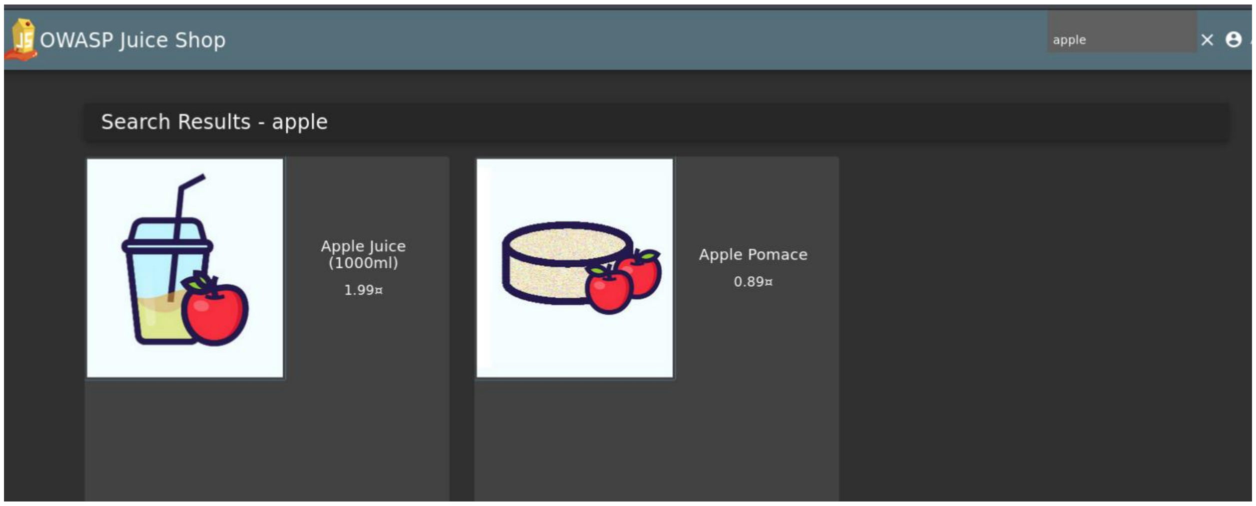
2. Types of XSS Demonstrated

- Reflected XSS
- Stored XSS
- DOM-Based XSS

Input & Output Flow

Input goes from browser → JS → rendered on page

- Input is user-controlled
- Reflected back without encoding
- Unsafe rendering causes XSS



---

3. Reflected XSS

Location: Search Bar
Payload:

```
<script>alert('Reflected XSS')</script>
```

Result: Script executed immediately in response.

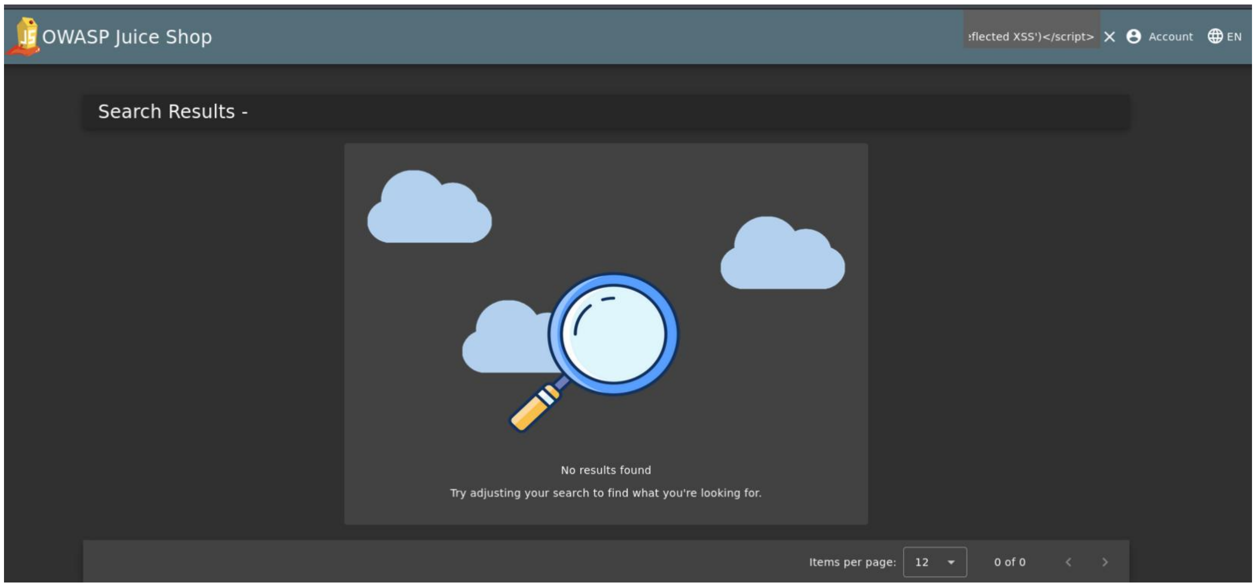
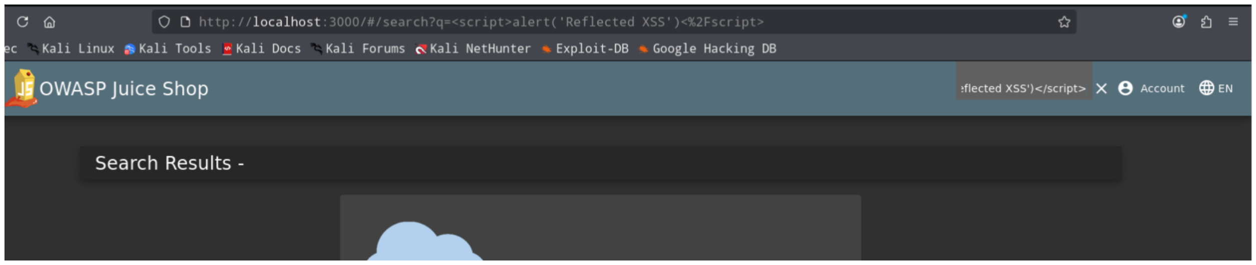


Figure 3 Alert popup showing Reflected XSS



```
http://localhost:3000/#/search?q=<script>alert('Reflected XSS')<%2Fscript>
```

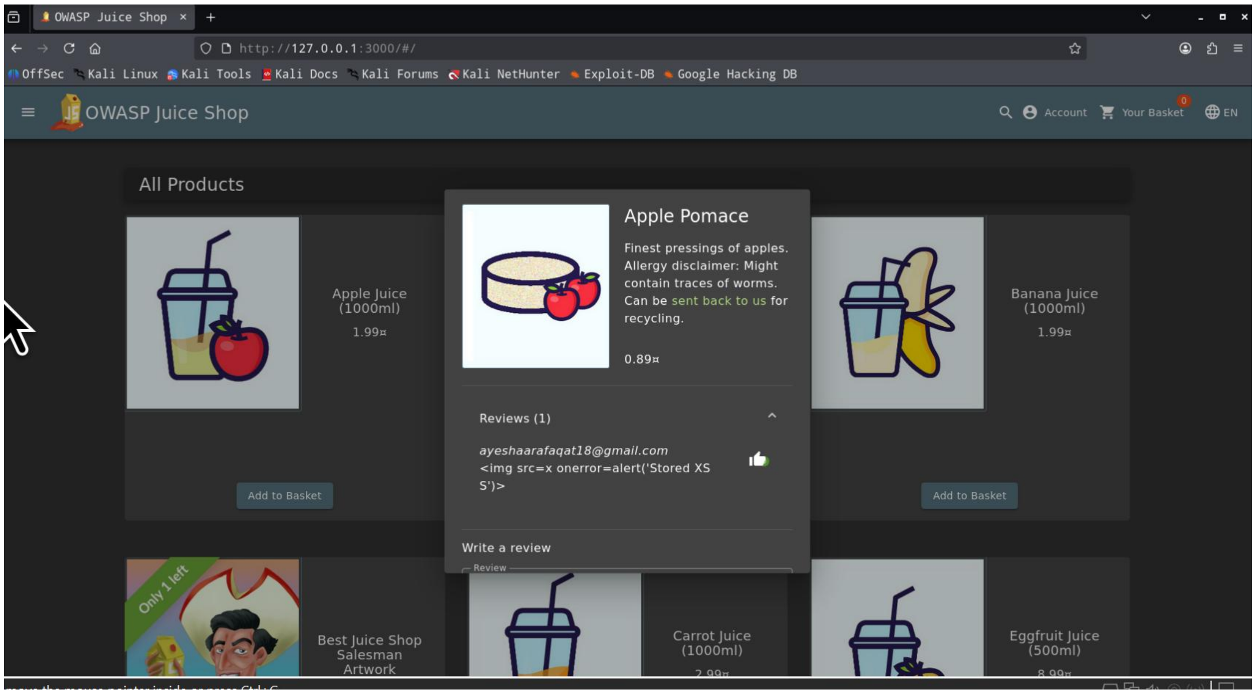
Figure 4 URL visible in background

4. Stored XSS

Location: Product Review
Payload:

```
<img src=x onerror=alert('Stored XSS')>
```

Result: Payload stored and executed on every page load.



Apple Pomace

Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.

0.89¤

Reviews (1)

ayeshaarafaqat18@gmail.com
<img src=x onerror=alert('Stored XSS')>

Write a review

Review

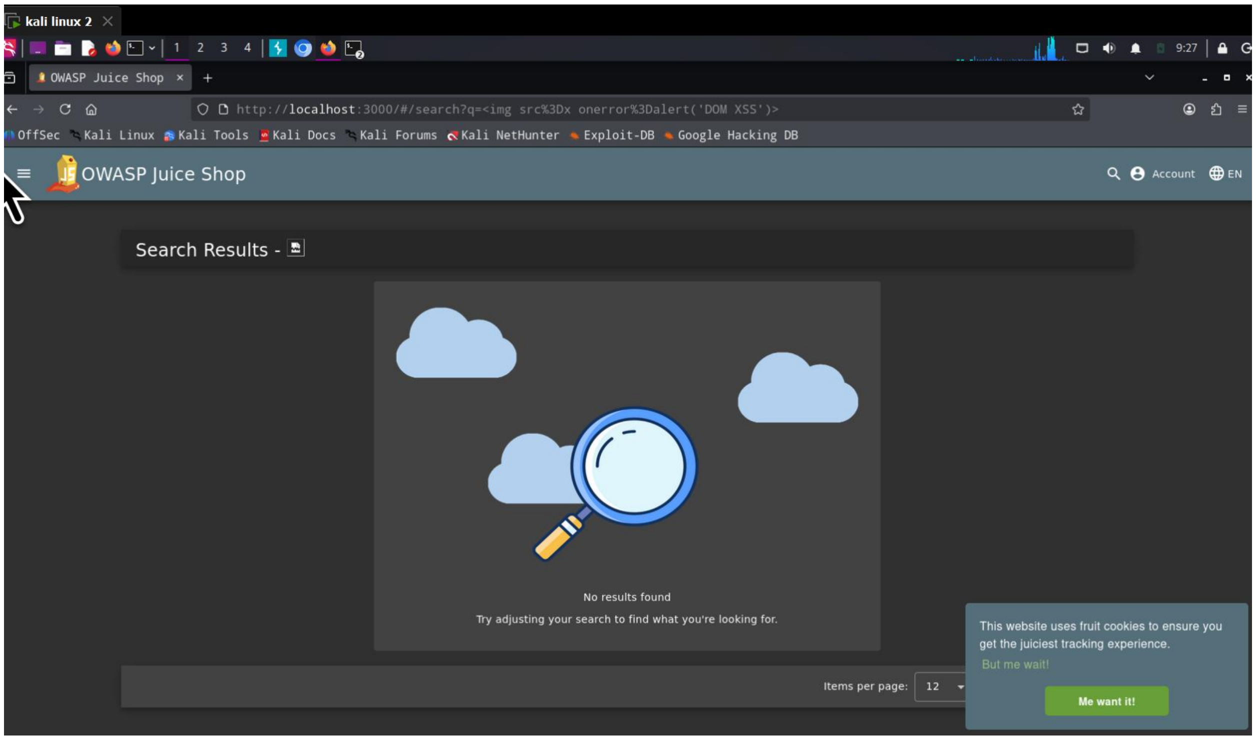
Figure 5 Review text containing payload

5. DOM-Based XSS

Source: `location.hash`
Sink: `innerHTML`
Payload:

```
#/search?q=<img src=x onerror=alert('DOM XSS')>
```

Result: Client-side execution without server interaction.



```
http://localhost:3000/#/search?q=<img src%3Dx onerror%3Dalert('DOM XSS')>
```

Search Results -

No results found

Try adjusting your search to find what you're looking for.

This website uses fruit cookies to ensure you get the juiciest tracking experience.

---

6. Insecure Coding Anti-Patterns

- Use of `innerHTML`
- Unsafe DOM manipulation
- Lack of output encoding
- Absence of CSP

---

7. Remediation Summary

- Validate input using allowlists
- Encode output based on context
- Use `textContent` instead of `innerHTML`
- Implement Content Security Policy
- Use secure frameworks

---

8. Ethical Statement

All testing was performed on authorized vulnerable labs for educational purposes only.