

ABDELRHMAN ISLAM 2305152

MOSTAFA FATHI 2305190

Web Penetration Testing Report

Executive Summary

Purpose of the Test

The objective of this penetration test is to evaluate the security posture of the OWASP Juice Shop by identifying and exploiting vulnerabilities. This exercise aims to simulate real-world attack scenarios, demonstrating the impact of vulnerabilities and providing actionable recommendations for remediation.

Key Findings

- **Critical Vulnerabilities:** Admin brute force, XSS in product search.
- **High-Level Impact:** Unauthorized admin access, malicious script execution affecting user sessions.

Summary of Recommendations

- Implement strong password policies and account lockout mechanisms.
- Sanitize user inputs to prevent XSS and other injection attacks.

Scope and Methodology

Scope

- **Websites:** OWASP Juice Shop application.
- **APIs:** None specified for this test.

Methodology

- **Approach:** Black-box testing.
- **Tools Used:** Kali Linux, Burp Suite, Gobuster, client url(curl).
- **All links:**

Vid link: <https://drive.google.com/drive/folders/1jtLCj-cZVxf1dLGCp25iQ4A1wvfb8Ecy?usp=sharing>

Repo link: <https://github.com/AbdelrhmanIslam/cys-final-project.git>

word list used : <https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/best1050.txt>

Vulnerability Findings

1. Enumeration to Find Admin Path

- Description: By browsing and analyzing the URL structure of the application, hidden admin paths were discovered.
- Risk: Medium.
- Impact: Access to admin functionalities that could lead to further exploitation.
- Evidence:

All discover paths belong to admin:

/myadmin (Status: 503) [Size: 506]

/navSiteAdmin (Status: 503) [Size: 506]

/navsiteadmin (Status: 503) [Size: 506]

/newsadmin (Status: 503) [Size: 506]

/newadmin (Status: 503) [Size: 506]

```
(root@kali) ~#
# gobuster dir -u http://demo.owasp-juice.shop/ -w SecLists/Discovery/Web-Content/common.txt -t 30 --exclude-length 3748

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://demo.owasp-juice.shop/
[+] Method: GET
[+] Threads: 30
[+] Wordlist: SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] Exclude Length: 3748
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./htpasswd (Status: 403) [Size: 199]
./htaccess (Status: 403) [Size: 199]
./hta (Status: 403) [Size: 199]
./well-known/core (Status: 403) [Size: 199]
./well-known/security.txt (Status: 200) [Size: 475]
/api (Status: 500) [Size: 2863]
/api/experiments (Status: 500) [Size: 2887]
/api/experiments/configurations (Status: 500) [Size: 2917]
/apis (Status: 500) [Size: 2865]
/assets (Status: 301) [Size: 156] [→ /assets/]
./core (Status: 403) [Size: 199]

Progress: 4735 / 4736 (99.98%)
./logs (Status: 503) [Size: 506]
Finished

(root@kali) ~#
# curl -i http://demo.owasp-juice.shop/myadmin

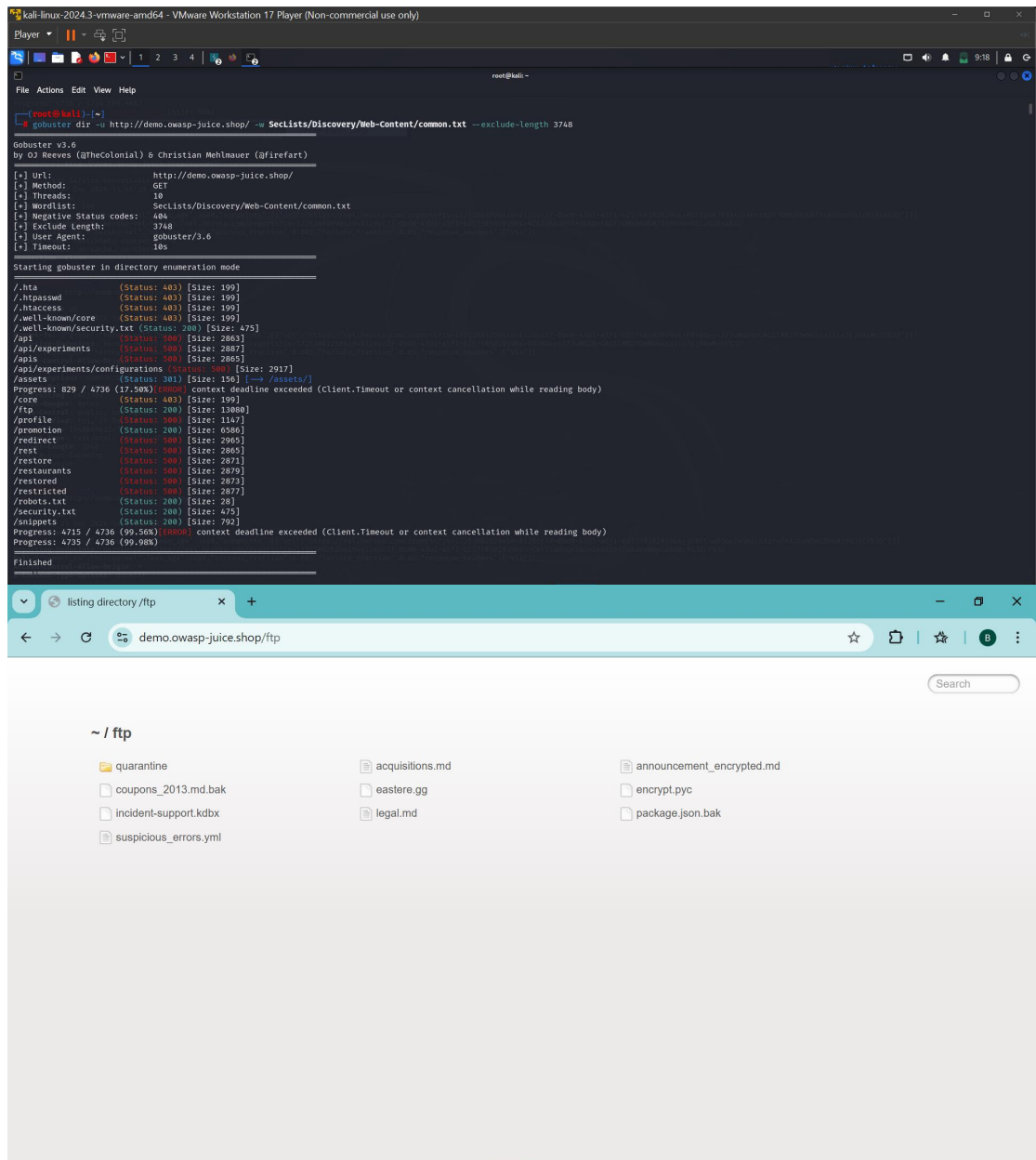
HTTP/1.1 503 Service Unavailable
Date: Fri, 27 Dec 2024 13:41:39 GMT
Server: Cowboy
Content-Length: 506
Report-To: [{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1735386899&id=812dc77-8b08-43b1-a5f1-b257583829598s-MZK1pSKj993+3hXDVtSz2F7OMABRUGM/1490VouVB1yX28sAK3D"}]}]
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1735386899&id=812dc77-8b08-43b1-a5f1-b257583829598s-MZK1pSKj993+3hXDVtSz2F7OMABRUGM/1490VouVB1yX28sAK3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache, no-store
Connection: close

(root@kali) ~#
# curl -i http://demo.owasp-juice.shop/newadmin

HTTP/1.1 200 OK
Date: Fri, 27 Dec 2024 14:02:05 GMT
Server: Cowboy
Report-To: [{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1735388125&id=812dc77-8b08-43b1-a5f1-b257583829598s-PAY8days377uN2BrQAQ1lM2FomNkhea31iq3sJHxWcSEK3D"}]}]
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1735388125&id=812dc77-8b08-43b1-a5f1-b257583829598s-PAY8days377uN2BrQAQ1lM2FomNkhea31iq3sJHxWcSEK3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /e/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 27 Dec 2024 13:59:04 GMT
etag: W/"aa-1ha869c2c"
Content-Type: text/html; charset=UTF-8
Content-Length: 3748
Vary: Accept-Encoding
Via: 1.1 vegur

(root@kali) ~#
# curl -i http://demo.owasp-juice.shop/navsiteadmin

HTTP/1.1 200 OK
Date: Fri, 27 Dec 2024 14:04:42 GMT
Server: Cowboy
Report-To: [{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1735388282&id=812dc77-8b08-43b1-a5f1-b257583829598s-JCYliw8Qqe2w5nZcGtzzrInkx5yWn186o8z9UJ1cYK3D"}]}]
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1735388282&id=812dc77-8b08-43b1-a5f1-b257583829598s-JCYliw8Qqe2w5nZcGtzzrInkx5yWn186o8z9UJ1cYK3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
```



demo.owasp-juice.shop/well-k

OWASP Juice Shop

demo.owasp-juice.shop/snippe


+

demo.owasp-juice.shop/promotion

Back

OWASP Juice Shop

Promotion Video



1:13 / 1:30

https://demo.owasp-juice.shop/#/

demo.owasp-juice.shop/well-k

OWASP Juice Shop

demo.owasp-juice.shop/snippe

+

https://demo.owasp-juice.shop/well-known/security.txt

Google Lens

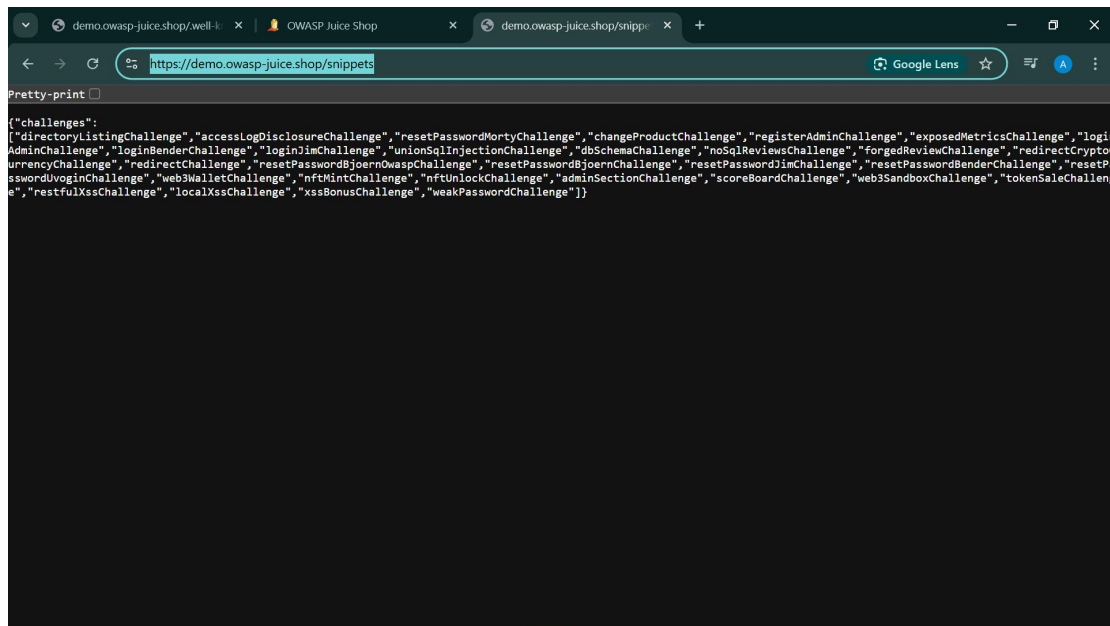
☆

⌵

A

⋮

Contact: <mailto:donotreply@owasp-juice.shop>
Encryption: https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcd
Acknowledgements: [/#/score-board](#)
Preferred-languages: en, ar, az, bg, bn, ca, cs, da, de, ga, el, es, et, fi, fr, ka, he, hi, hu, id, it, ja, ko, lv, my, nl, no, pl, pt, ro, ru, si, sv, th, tr, uk, zh
Hiring: [/#/jobs](#)
Csaf: <http://localhost:3000/.well-known/csaf/provider-metadata.json>
Expires: Sat, 27 Dec 2025 13:59:02 GMT



- Remediation: Use obfuscated URLs and restrict access to sensitive paths with proper authentication.

2. Admin Brute Force

- **Description:** Lack of rate-limiting on admin login allows brute-force attacks.
- **Risk:** High.
- **Impact:** Full application control.
- **Evidence:**

kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player

Burp Suite Community Edition v2024.9.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn

HTTP History

Match and replace

Proxy settings

Request to http://demo.owasp-juice.shop:80 [81.168.145.156]

Open browser

Time	Type	Direction	Method	URL	Status code	Length
17:09:35.26 Dec 2024	HTTP	Request	POST	http://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&PGSTW&sid=CMp_7hB86Q_zrl_AkAr		
17:09:35.26 Dec 2024	HTTP	Request	GET	http://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&PGSTW&sid=CMp_7hB86Q_zrl_AkAr		
17:09:47.92 Dec 2024	HTTP	Request	POST	http://demo.owasp-juice.shop/rest/user/login		
17:09:47.92 Dec 2024	HTTP	Request	GET	http://demo.owasp-juice.shop/rest/user/home		
17:09:47.92 Dec 2024	HTTP	Request	GET	http://demo.owasp-juice.shop/rest/user/home		
17:09:49.92 Dec 2024	HTTP	Request	GET	http://demo.owasp-juice.shop/rest/user/home		
17:09:49.92 Dec 2024	HTTP	Request	POST	http://demo.owasp-juice.shop/rest/user/login		
17:09:49.92 Dec 2024	HTTP	Request	GET	http://demo.owasp-juice.shop/rest/user/home		
17:10:05.26 Dec 2024	HTTP	Request	POST	http://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&PGSTW&sid=CMp_7hB86Q_zrl_AkAr		
17:10:05.26 Dec 2024	HTTP	Request	GET	http://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&PGSTW		

Request

Raw

1 POST /rest/user/login HTTP/1.1

2 Host: demo.owasp-juice.shop

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

4 Accept: application/json, text/plain, */*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/json

8 Content-Length: 46

9 Origin: http://demo.owasp-juice.shop

10 Connection: keep-alive

11 Referer: http://demo.owasp-juice.shop/

12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=3eVh618WREPVLx52jalokwH4YfVrkubgZ2y0Xte4b87yRp0V52vKQwud

13 Pragma: no-cache

14 { "email": "admin@juice-sh.op", "password": "123\$"

Inspector

Selection

46 (JSON)

Selected text

{ "email": "admin@juice-sh.op", "password": "123\$"

Decoded from: Select

{ "email": "admin@juice-sh.op", "password": "123\$"

Cancel Apply changes

Request attributes

Request query parameters

Request cookies

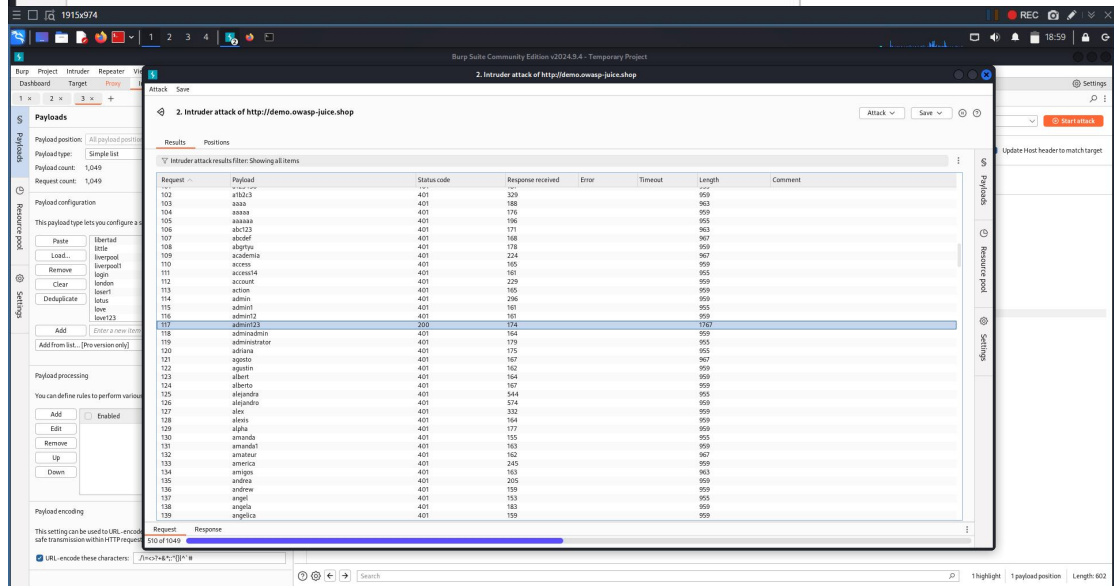
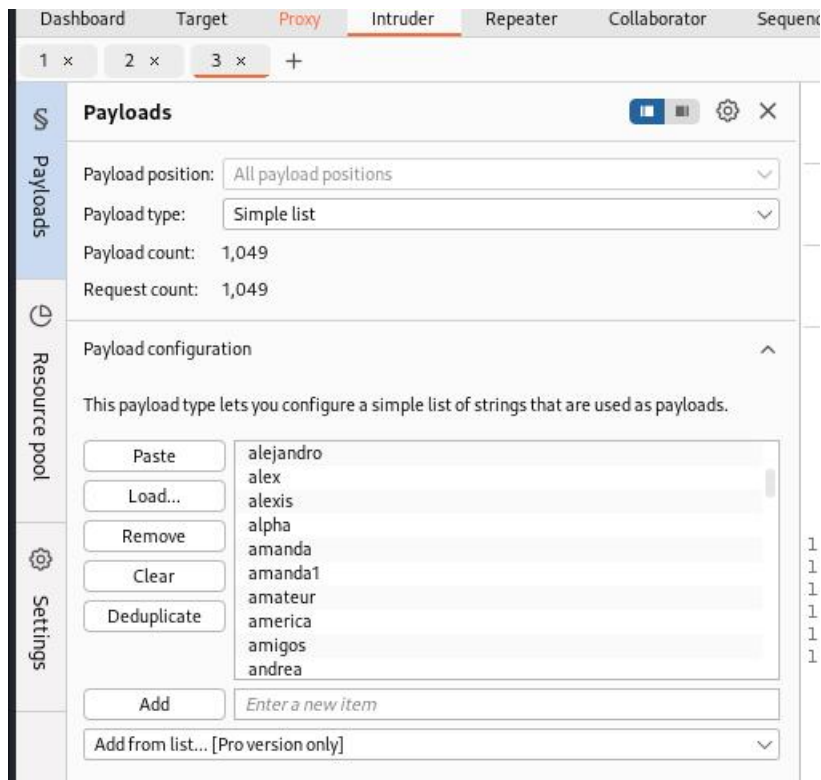
0 highlights

Event log (25) All issues

Memory: 148 MB

```
POST /rest/user/login HTTP/1.1
Host: demo.owasp-juice.shop
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 46
Origin: http://demo.owasp-juice.shop
Connection: keep-alive
Referer: http://demo.owasp-juice.shop/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=3eVh618WREPVLx52jalokwH4YfVrkubgZ2y0Xte4b87yRp0V52vKQwud
Pragma: no-cache
{ "email": "admin@juice-sh.op", "password": "123$"
```

```
{ "email": "admin@juice-sh.op", "password": "123$"
```



- **Remediation:** Implement rate-limiting and account lockout policies.

3. XSS in Product Search

- **Description:** User input in the product search bar is not sanitized.
- **Risk:** Medium.
- **Impact:** Arbitrary JavaScript execution, session hijacking.
- **Evidence:**



- **Remediation:** Properly sanitize and validate user input or use regular expressions.

Exploitation and Attack Simulation

Tools and Techniques

Burp Suite: Used for brute-forcing admin credentials

Outcomes

- **Admin Brute Force:** Successfully obtained admin access.
- **XSS:** Executed arbitrary JavaScript to demonstrate session hijacking.

Conclusion

The penetration test revealed critical vulnerabilities in the OWASP Juice Shop. The absence of basic security measures like input validation and account protection mechanisms poses a significant risk. Addressing these issues will improve the overall security posture and reduce the attack surface.

Overall Risk Level

High.

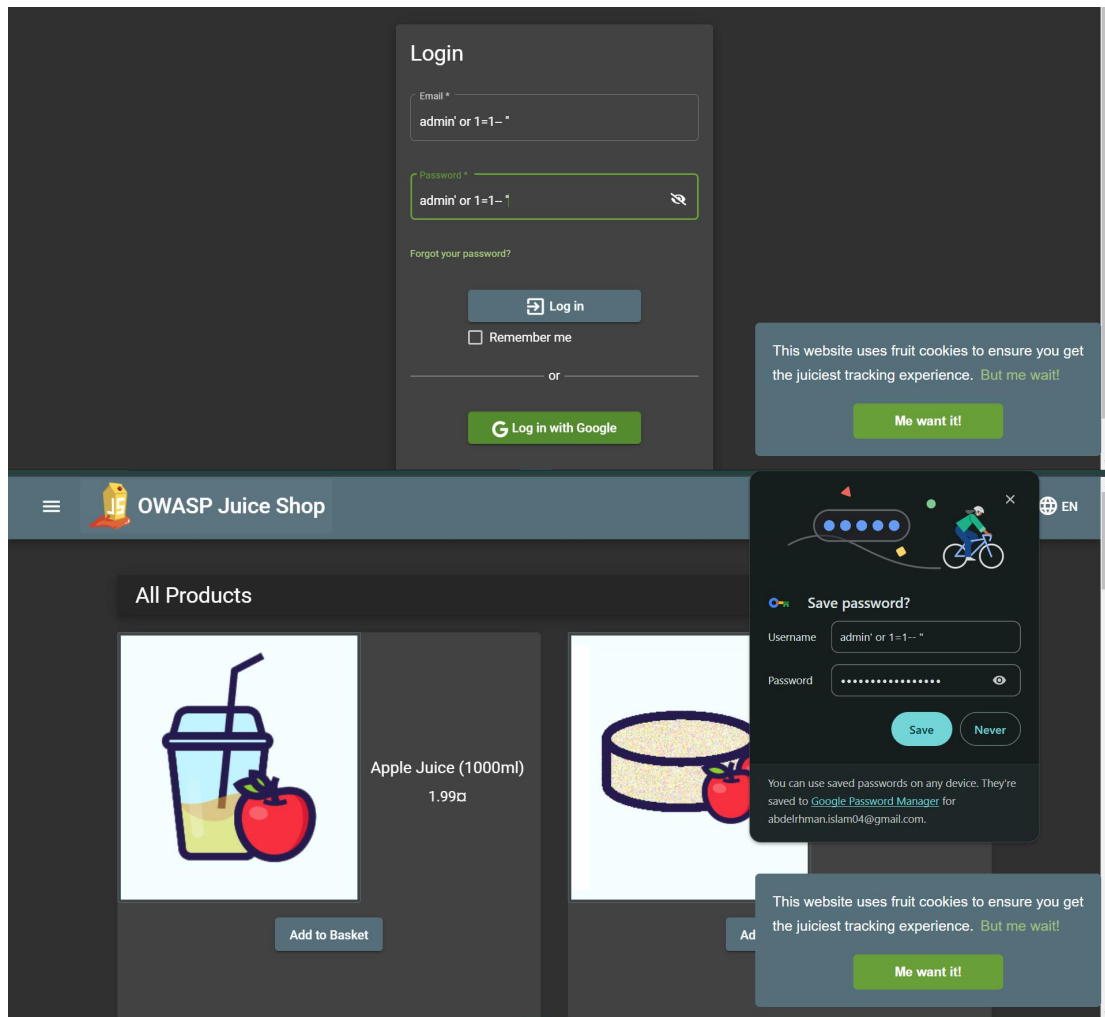
Recommendations

- Prioritize fixing authentication and input validation vulnerabilities.
 - Conduct regular security assessments.
-

Bonus: Additional Vulnerabilities

1. SQL Injection

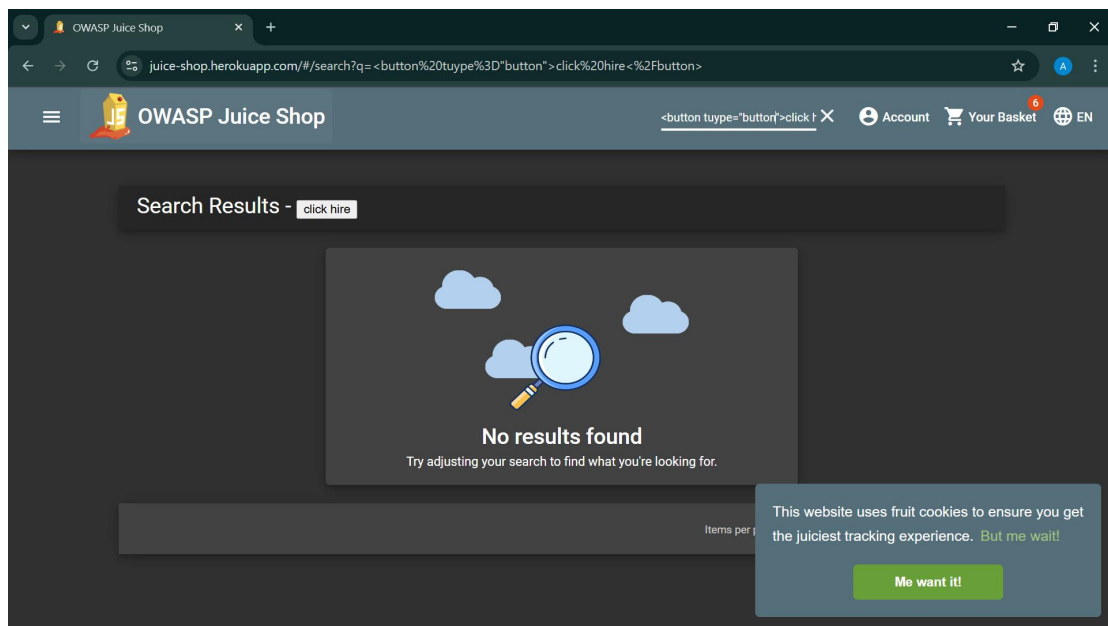
- **Description:** Exploiting unsanitized SQL queries to manipulate the database.
- **Impact:** Data exfiltration or database compromise.
- **Evidence:**



- **Remediation:** Use parameterized queries and prepared statements.

2. HTML Injection

- **Description:** Injecting malicious HTML to manipulate the web page content.
- **Impact:** User interface manipulation, phishing.
-
- **Evidence:**



- **Remediation:** Encode user inputs and enforce strict content security policies.

All commends and codes are used:

gobuster dir -u http://demo.owasp-juice.shop/ -w SecLists/Discovery/Web-Content/common.txt -t 30 --exclude-length 3748

```
gobuster dir -u http://demo.owasp-juice.shop/ -w  
SecLists/Discovery/Web-Content/common.txt --exclude-length  
3748
```

```
curl -I http://demo.owasp-juice.shop/myadmin  
curl -I http://demo.owasp-juice.shop/navSiteAdmin  
curl -I http://demo.owasp-juice.shop/newadmin
```

<iframe src = javascript:alert(22);>

```
<iframe src = javascript:alert(document.cookie);>
```

admin' or 1=1-- "

<button type="button">click hire</button>

**<iframe
src="https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D8%B5
%D9%81%D8%AD%D8%A9_%D8%A7%D9%84%D8%B1%D8%
A6%D9%8A%D8%B3%D8%A9"></iframe>**