Security Testing Report Task-1

Intern name : Mithileshwaran

Internship domain : Cyber Security

Task tittle : Web Application Security Testing

Website tested : https://demo.owasp-juice.shop

Date : August 2025

Tool used : Burpsuite(community edition),web browser(manual testing)

1)Objective

To perform basic web application security testing and identify common vulnerabilities like:

- **SQL Injection**
- **Cross-Site Scripting (XSS)**
- **Insecure Direct Object Reference (IDOR)**
- **Information Disclosure**
- **Broken Access Control**

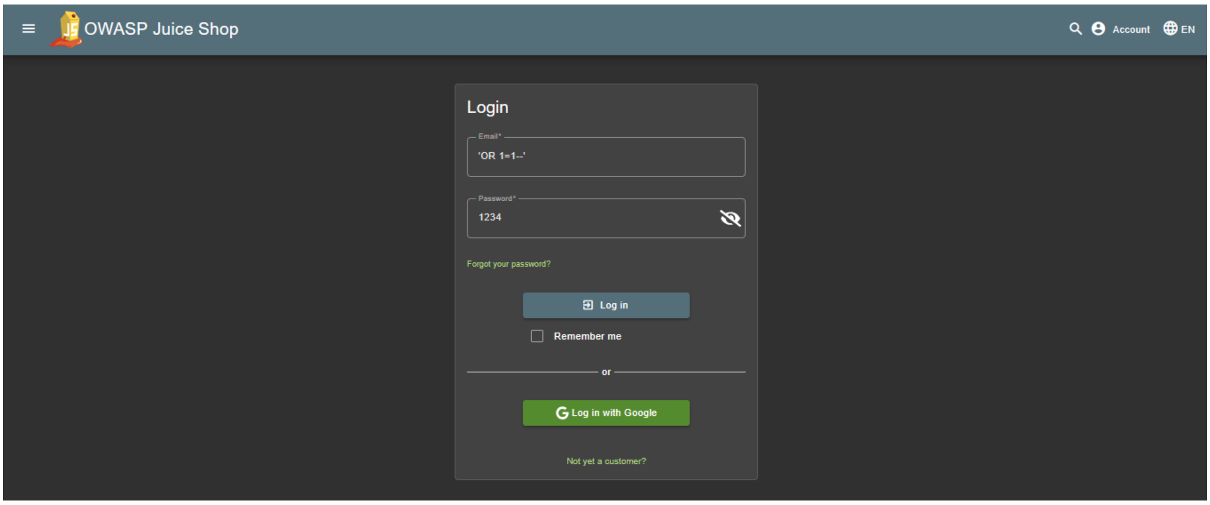
2)Summary of Findings

#	Vulnerability	Risk Rating	Status
1	SQL Injection	High	Confirmed
2	Cross-Site Scripting (XSS)	Medium	Medium confirmed
3	IDOR	High	Confirmed
4	Information Disclosure	Medium	Medium Confirmed
5	Broken Access Control	No Risk	403 - Unauthorized Access Blocked

3)Detailed Vulnerablity Report

1. SQL Injection Test

- **Description**: Bypassed login using ' OR 1=1--
- **Payload Used:** ' OR 1=1--
- **Outcome:** Logged in without valid credentials
- **Screenshots:**
- **1)Payload entered in login**

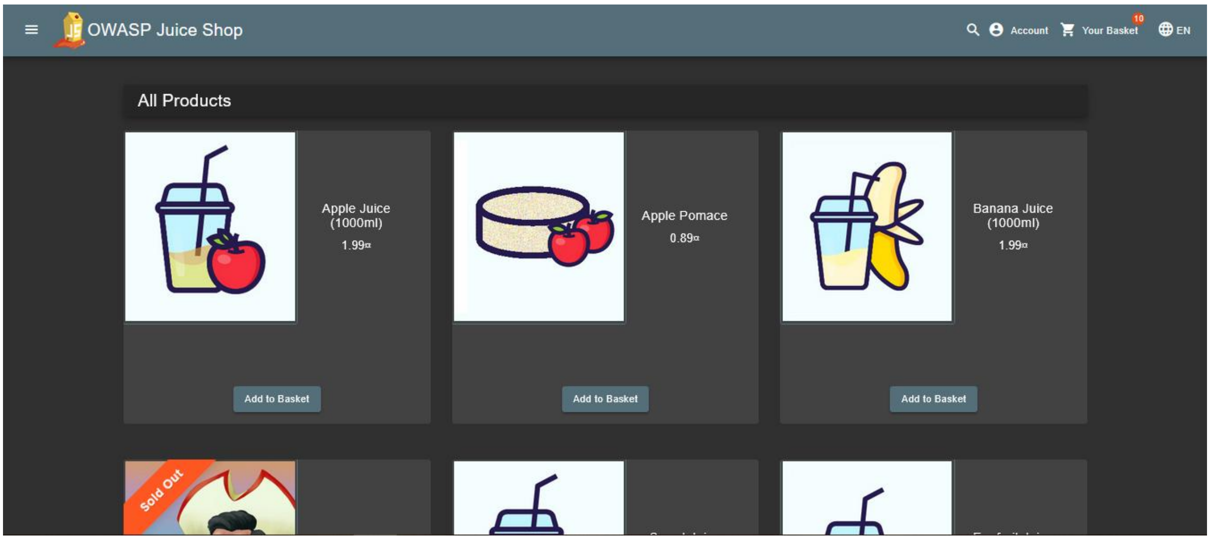


Login

Email*
'OR 1=1--'

Password*
1234

- **2) Successfully logged in**



All Products

Apple Juice (1000ml)
1.99¤

Apple Pomace
0.89¤

Banana Juice (1000ml)
1.99¤

- **Vulnerability Type:** Authentication Bypass via SQLi

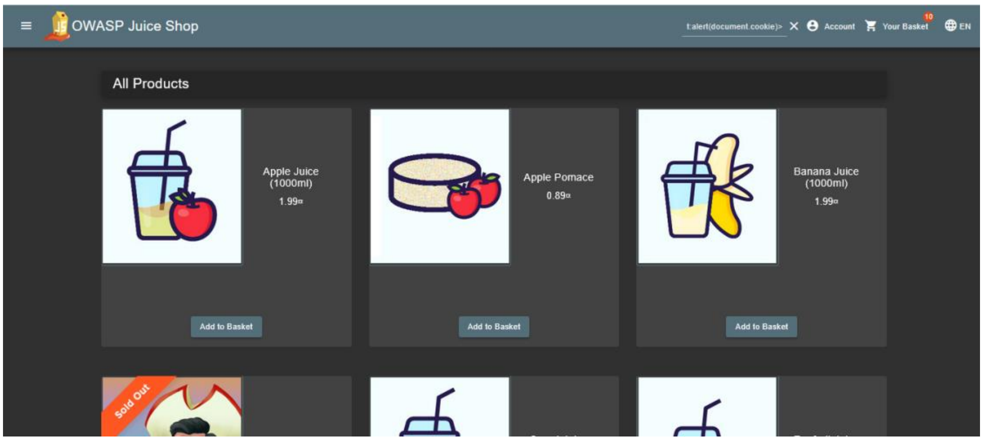
- **Risk Rating:** High
- **Mitigation Suggestion:**

  1)Use parameterized queries

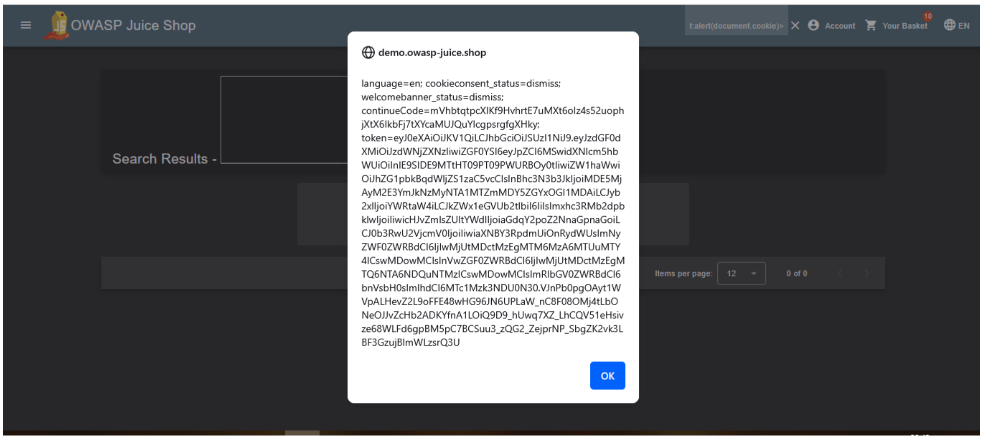
  2)Validate and sanitize user inputs

2. Cross-Site Scripting (XSS)

- **Description:** Reflected XSS in search/comment field
- **Payload Used:** <iframe src=javascript:alert(document.cookie)>
- **Outcome:** Alert popup triggered
- **Screenshots**
- **1) Payload entered**



- **2) Cookies exposed in alert box**



demo.owasp-juice.shop

```
language=en; cookieconsent_status=dismiss;
welcomebanner_status=dismiss;
continueCode=mVhbtqtpcXIKf9HvhrtE7uMXt6olz4s52uoph
jXtX6lkbFj7tXYcaMUJQuYlcgpsrgfgXHky;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0d
XMiOiJzdWNjZXNzliwiZGF0YSI6eyJpZCI6MSwidXNlcm5hb
WUiOiInIE9SIDE9MTtHT09PT09PWURBOy0tliwiZW1haWwi
OiJhZG1pbkBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMDE5Mj
AyM2E3YmJkNzMyNTA1MTZmMDY5ZGYxOGI1MDAiLCJyb
2xlIjoiYWRtaW4iLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpb
klwIjoiliwicHJvZmlsZUltYWdlIjoiaGdqY2poZ2NnaGpnaGoiL
CJ0b3RwU2VjcmV0IjoiliwiaXNBY3RpdmUiOnRydWUsImNy
ZWF0ZWRBdCI6IjIwMjUtMDctMzEgMTM6MzA6MTUuMTY
4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDctMzEgM
TQ6NTA6NDQuNTMzICswMDowMCIsImRlbGV0ZWRBdCI6
bnVsbH0sImlhdCI6MTc1Mzk3NDU0N30.VJnPb0pgOAyt1W
VpALHevZ2L9oFFE48wHG96JN6UPLaW_nC8F08OMj4tLbO
NeOJJvZcHb2ADKYfnA1LOiQ9D9_hUwq7XZ_LhCQV51eHsiv
ze68WLFd6gpBM5pC7BCSuu3_zQG2_ZejprNP_SbgZK2vk3L
BF3GzujBlmWLzsrQ3U
```

OK

- **Vulnerability Type:** Reflected XSS
- **Risk Rating:** Medium
- **Mitigation Suggestion:**

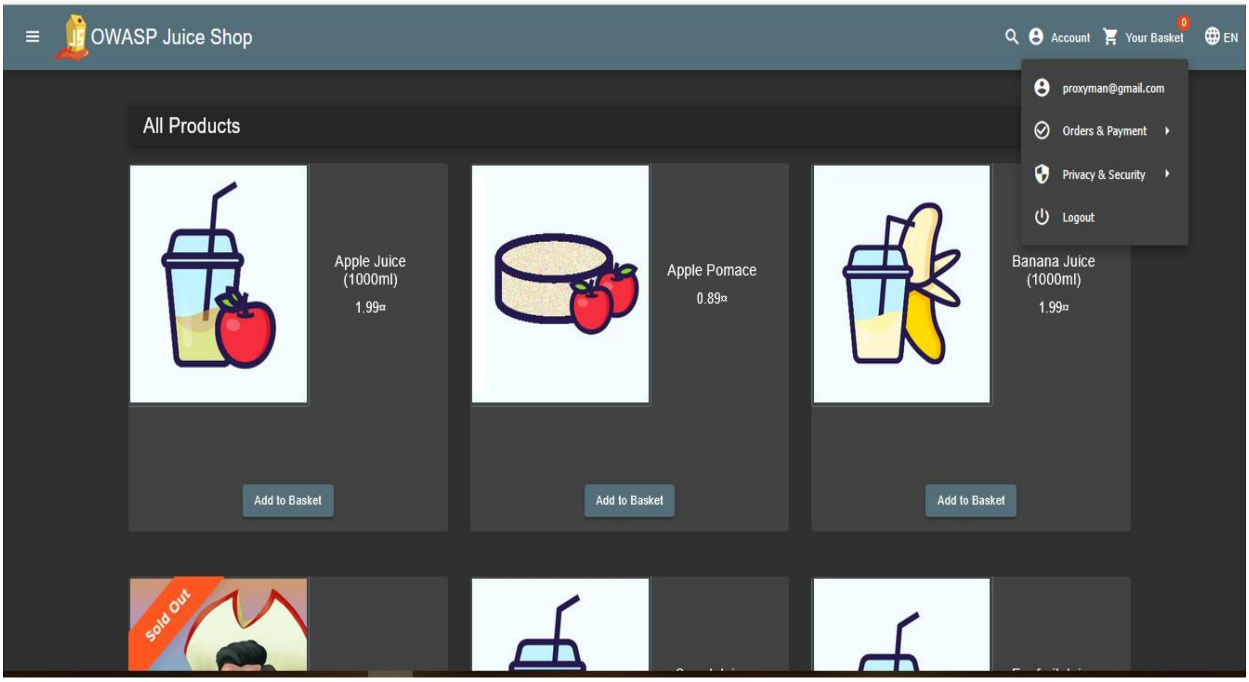
  1)Encode output in HTML

  2)Use Content Security Policy (CSP)

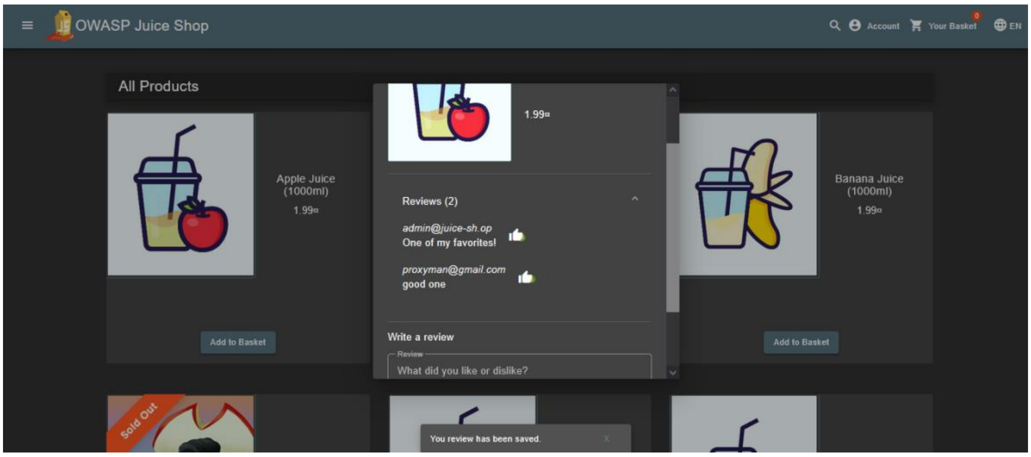
  3)Sanitize user inputs

3. Insecure Direct Object Reference (IDOR)

- **Description:** Modified comment username via request
- **Payload Used:** Changed user: proxyman@gmail.com to admin@juice-sh.op
- **Outcome:** Comment posted as admin
- **Screenshots**
- **1)Normal review by proxyman**



- **2) Burp Suite intercept (original)**

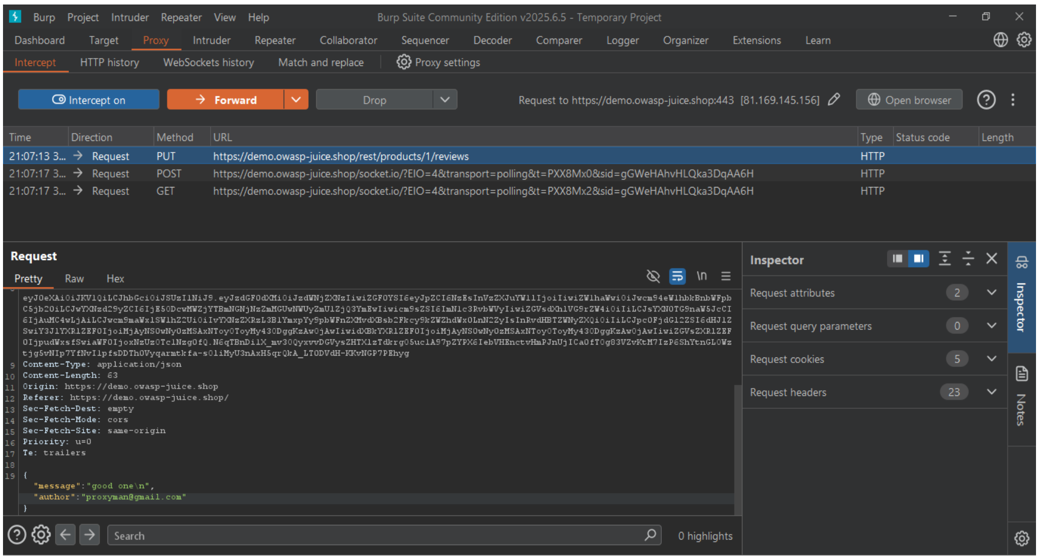


admin@juice-sh.op
One of my favorites!

proxyman@gmail.com
good one

You review has been saved

- **3) Payload modified with admin email**


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.6.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Request
Pretty Raw Hex
\n
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request cookies 5
Request headers 23
Inspector
Notes

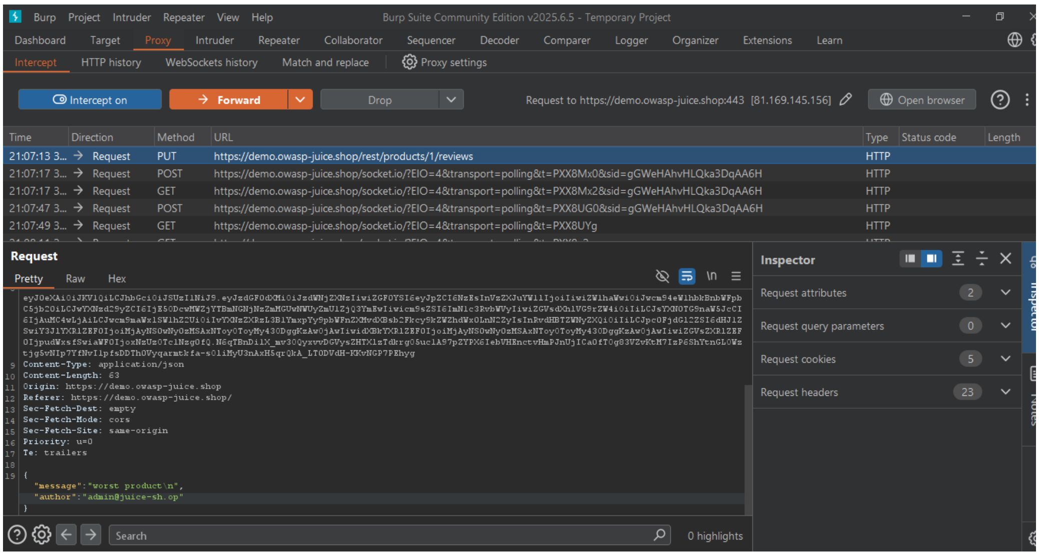
Request to https://demo.owasp-juice.shop:443 [81.169.145.156]

```
Time          Direction   Method  URL                                                                                      Type  Status code  Length
21:07:13 3... → Request   PUT     https://demo.owasp-juice.shop/rest/products/1/reviews                                    HTTP
21:07:17 3... → Request   POST    https://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&t=PXX8Mx0&sid=gGWeHAhvHLQka3DqAA6H   HTTP
21:07:17 3... → Request   GET     https://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&t=PXX8Mx2&sid=gGWeHAhvHLQka3DqAA6H   HTTP
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6NzEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJwcm94eW1hbkBnbWFpb
C5jb20iLCJwYXNzd29yZCI6IjE5ODcwMWZjYTBmNGNjNzZmMGUwNWUyZmU1ZjQ3YmEwIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI
6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1Z
SwiY3JlYXRlZEF0IjoiMjAyNS0wNy0zMSAxNToyOToyMy430DggKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0wNy0zMSAxNToyOToyMy430DggKzAwOjAwIiwiZGVsZXRlZEF
0IjpudWxsfSwiaWF0IjoxNzUzOTc1Nzg0fQ.N6qTBnDi1X_mv30QyxvvDGVysZHTXlzTdkrg05uclA97pZYPX6IebVHEnctvHmPJnUjICa0fT0g83VZvKtM7IzP6ShYtnGL0Wz
tjg5vNIp7YfNvIlpfsDDTh0Vyqarmtkfa-s0liMyU3nAxH5qrQkA_LT0DVdH-KKvNGP7PEhyg
Content-Type: application/json
Content-Length: 63
Origin: https://demo.owasp-juice.shop
Referer: https://demo.owasp-juice.shop/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "message":"good one\n",
  "author":"proxyman@gmail.com"
}
```

- **4) Forwarded & accepted by server**


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.6.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Request
Pretty Raw Hex
\n
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request cookies 5
Request headers 23

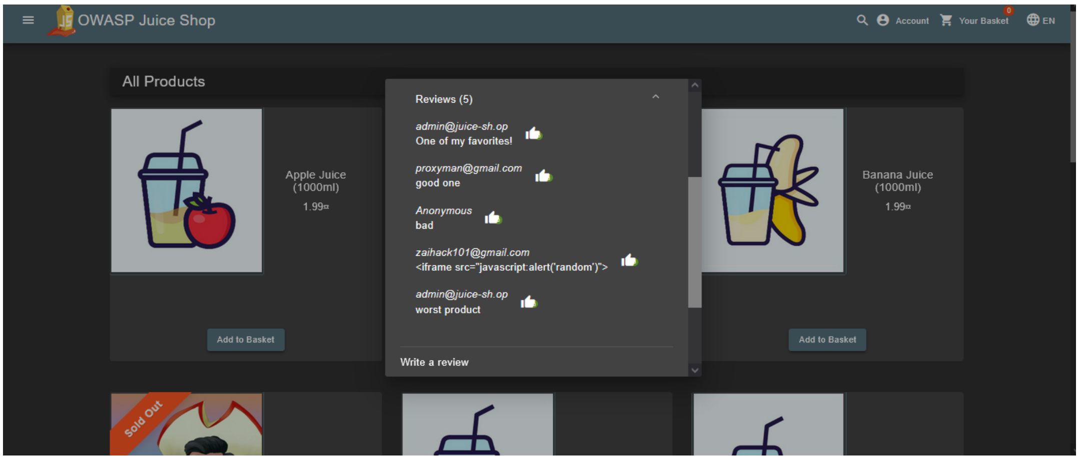
Request to https://demo.owasp-juice.shop:443 [81.169.145.156]

```
Time          Direction   Method  URL                                                                                      Type  Status code  Length
21:07:13 3... → Request   PUT     https://demo.owasp-juice.shop/rest/products/1/reviews                                    HTTP
21:07:17 3... → Request   POST    https://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&t=PXX8Mx0&sid=gGWeHAhvHLQka3DqAA6H   HTTP
21:07:17 3... → Request   GET     https://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&t=PXX8Mx2&sid=gGWeHAhvHLQka3DqAA6H   HTTP
21:07:47 3... → Request   POST    https://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&t=PXX8UG0&sid=gGWeHAhvHLQka3DqAA6H   HTTP
21:07:49 3... → Request   GET     https://demo.owasp-juice.shop/socket.io/?EIO=4&transport=polling&t=PXX8UYg                      HTTP
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6NzEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJwcm94eW1hbkBnbWFpb
C5jb20iLCJwYXNzd29yZCI6IjE5ODcwMWZjYTBmNGNjNzZmMGUwNWUyZmU1ZjQ3YmEwIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI
6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1Z
SwiY3JlYXRlZEF0IjoiMjAyNS0wNy0zMSAxNToyOToyMy430DggKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0wNy0zMSAxNToyOToyMy430DggKzAwOjAwIiwiZGVsZXRlZEF
0IjpudWxsfSwiaWF0IjoxNzUzOTc1Nzg0fQ.N6qTBnDi1X_mv30QyxvvDGVysZHTXlzTdkrg05uclA97pZYPX6IebVHEnctvHmPJnUjICa0fT0g83VZvKtM7IzP6ShYtnGL0Wz
tjg5vNIp7YfNvIlpfsDDTh0Vyqarmtkfa-s0liMyU3nAxH5qrQkA_LT0DVdH-KKvNGP7PEhyg
Content-Type: application/json
Content-Length: 63
Origin: https://demo.owasp-juice.shop
Referer: https://demo.owasp-juice.shop/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

{
  "message":"worst product\n",
  "author":"admin@juice-sh.op"
}
```

- **5)UI shows review under admin’s name**



Reviews (5)

admin@juice-sh.op
One of my favorites!

proxyman@gmail.com
good one

Anonymous
bad

zaihack101@gmail.com
<iframe src="javascript:alert('random')">

admin@juice-sh.op
worst product

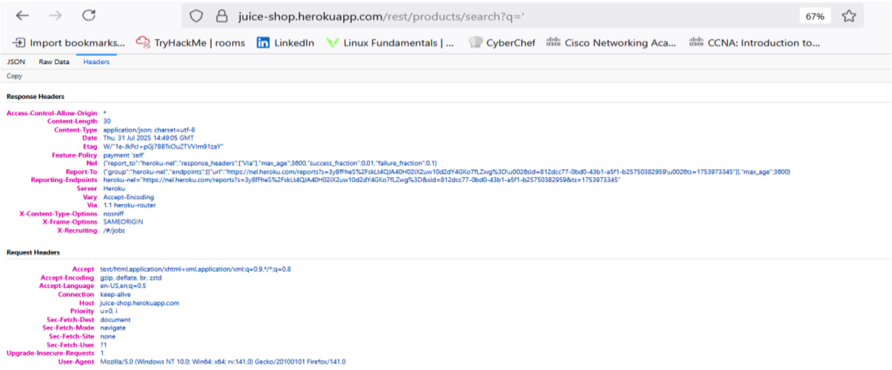
- **Vulnerability Type:** IDOR
- **Risk Rating:** High
- **Mitigation Suggestion:**

1)Implement proper access control

2)Avoid trusting client-side parameters

4. Information Disclosure

- **Description:** Sensitive header info in response
- **Outcome:** X-Powered-By, Server info exposed
- **Screenshot**
- **Info disclosure header**



```
Response Headers

 Access-Control-Allow-Origin  *
              Content-Length  30
                Content-Type  application/json; charset=utf-8
                        Date  Thu, 31 Jul 2025 14:49:05 GMT
                        Etag  W/"1e-JkPcl+pGj7BBTxOuZTVVlm91zaY"
              Feature-Policy  payment 'self'
                         Nel  {"report_to":"heroku-nel","response_headers":["Via"],"max_age":3600,"success_fraction":0.01,"failure_fraction":0.1}
                   Report-To  {"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku.com/reports?s=3y8fFheS%2FskLt4QJA40H02iX2uw10d2dY4GKo7fLZwg%3D\u0026sid=812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=1753973345"}],"max_age":3600}
         Reporting-Endpoints  heroku-nel="https://nel.heroku.com/reports?s=3y8fFheS%2FskLt4QJA40H02iX2uw10d2dY4GKo7fLZwg%3D&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&ts=1753973345"
                      Server  Heroku
                        Vary  Accept-Encoding
                         Via  1.1 heroku-router
      X-Content-Type-Options  nosniff
             X-Frame-Options  SAMEORIGIN
                X-Recruiting  /#/jobs

Request Headers

                      Accept  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
             Accept-Encoding  gzip, deflate, br, zstd
             Accept-Language  en-US,en;q=0.5
                  Connection  keep-alive
                        Host  juice-shop.herokuapp.com
                    Priority  u=0, i
              Sec-Fetch-Dest  document
              Sec-Fetch-Mode  navigate
              Sec-Fetch-Site  none
              Sec-Fetch-User  ?1
   Upgrade-Insecure-Requests  1
                  User-Agent  Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
```

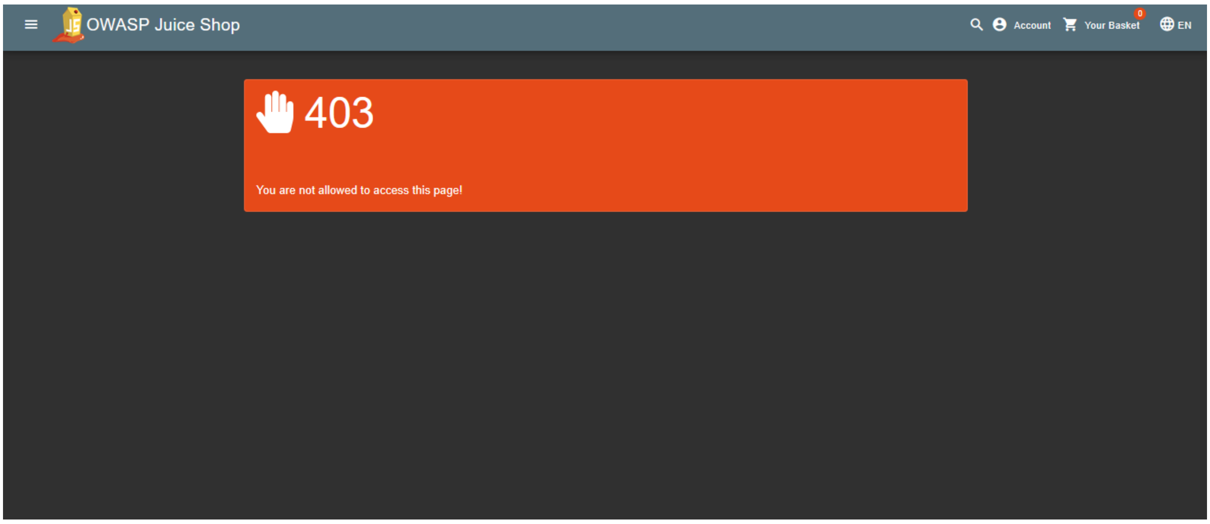
- **Vulnerability Type:** Info Disclosure
- **Risk Rating:** Medium
- **Mitigation** Suggestion:

1)Remove unnecessary response headers

2)Use security headers like Strict-Transport-Security, X-Content-Type-Options

5. Broken Access Control

- **Description:** Attempted unauthorized admin pages
- **Payload Used:** Direct URL access /#/administration
- **Outcome:** 403 display you are not allowed to this page
- **Screenshot**
- **Unauthorized Access Blocked**



403

You are not allowed to access this page!

- **Vulnerability Type:** Attemted Broken Access Control
- **Mitigation Suggestion:**

1)unauthorized user are blocked

2) Use role-based access (RBAC)

5. OWASP Top 10 Mapping Checklist

OWASP Category	Found	Evidence
A1: Broken Access Control	NO	/#/administration access
A2: Cryptographic Failures	NO	-
A3: Injection (SQL)	YES	SQL login bypass,Xss
A4: Insecure Design	NO	-
A5: Security Misconfiguration	YES	Headers disclosure
A6: Vulnerable Components	NO	-
A7: Identification & Auth	YES	Login bypass
A8: Software/Data Integrity	NO	-
A9: Security Logging/Monitoring	NO	-
A10: SSRF	NO	-

6)Conclusion

If this was a real website, the bugs we found like SQL Injection and IDOR could let hackers steal data or act like other users. This can cause serious problems for the company and its users. Fixing these issues quickly is important to keep the site safe and trusted.