Vulnerability: Error Handling

Juice Shop Challenge: None

Date Found: 2025-04-15

Severity/Difficulty (Juice Shop Rating): ⭐ ⭐ ☆☆☆

Location/URL:
/#/product

Parameter/Input Field: None

Description:
Server fails to return proper error messages on invalid or malformed requests.

Steps to Reproduce (STR):
1. Press on a product to view it
2. Intercept the request in Burp Suite
3. Resend the request with modifications
4. Observe error 500 without a clear error message.

Proof of Concept (PoC):
Payload Used:
Modified GET request to invalid product ID

Impact:
Server exposes internal error messages without clear user guidance.

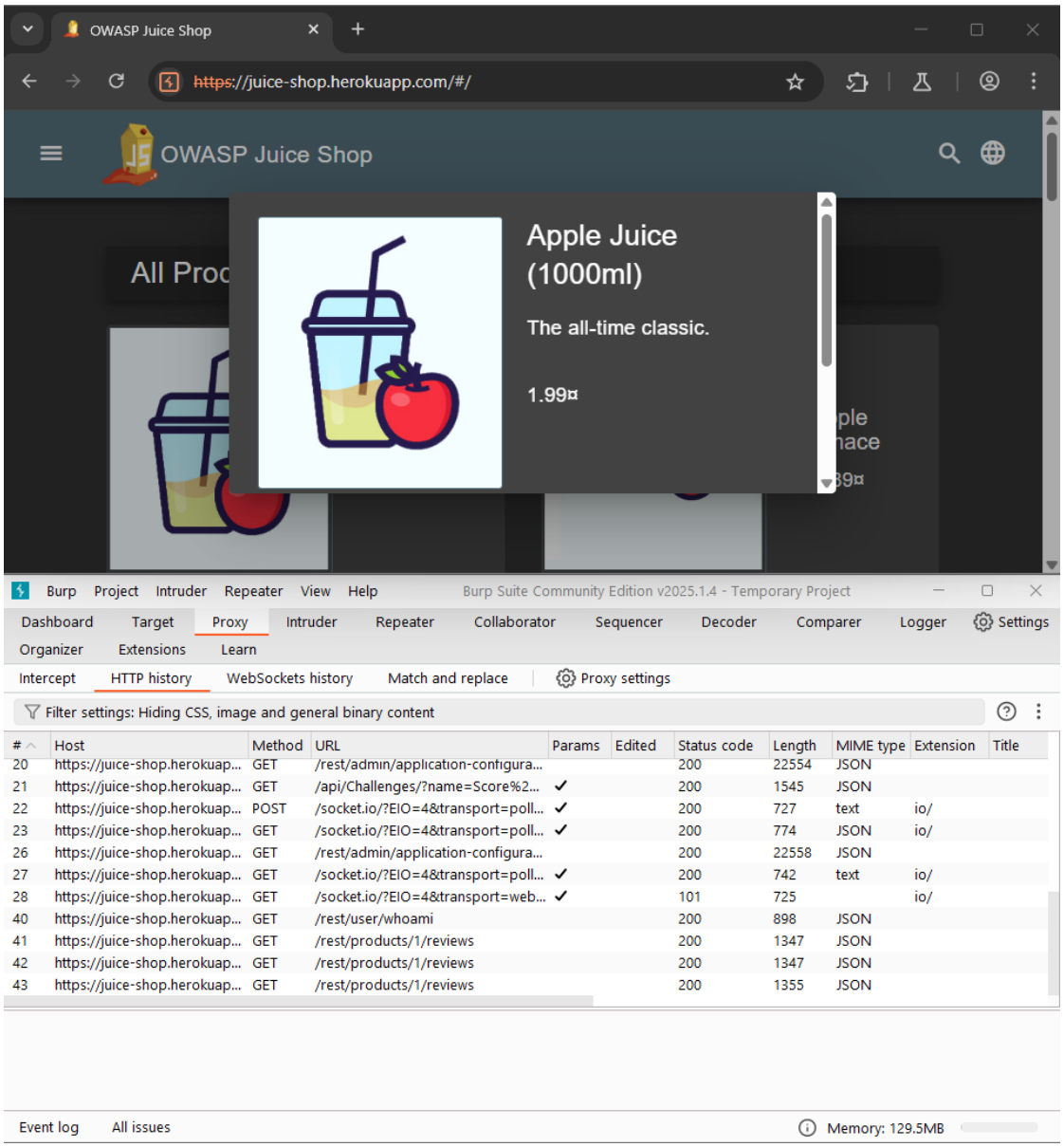
Root Cause (Conceptual):
Lack of error-handling structure in backend code.

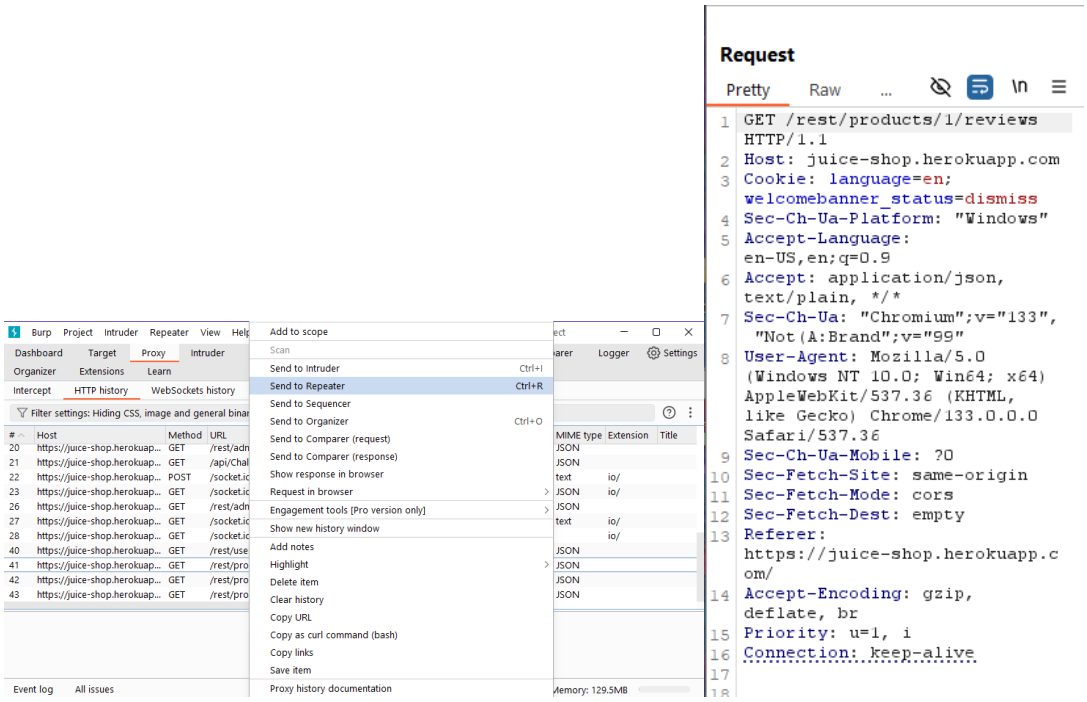
Remediation / How to Fix:
Implement user-friendly error messages with proper HTTP codes.

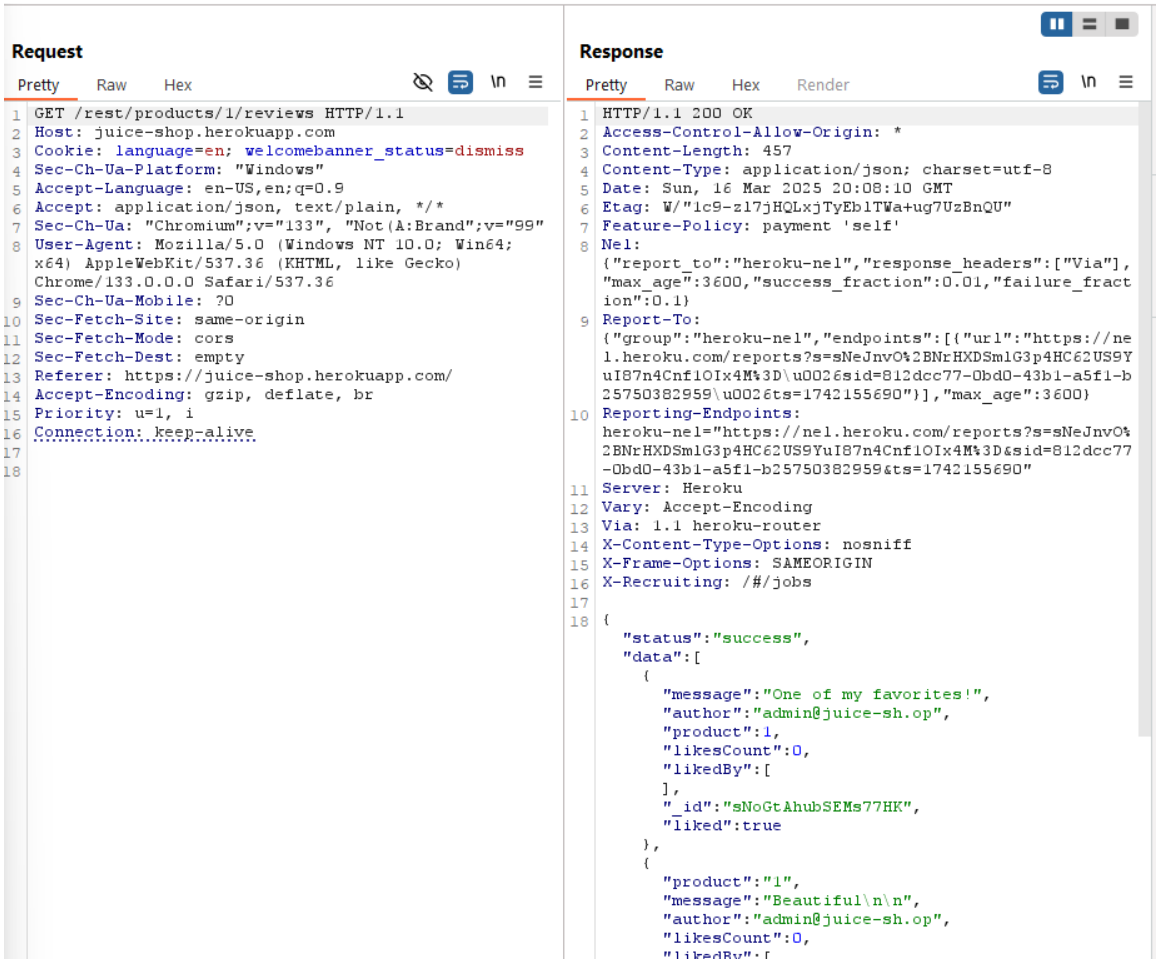
Relevant OWASP Resource: OWASP Error Handling Cheat Sheet

Tools Used:
Burp Suite

Personal Notes/Learnings:
Learned how lack of proper error handling can leak backend issues.


OWASP Juice Shop
https://juice-shop.herokuapp.com/#/
OWASP Juice Shop
All Proc
Apple Juice (1000ml)
The all-time classic.
1.99¤
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.1.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Extension Title
20 https://juice-shop.herokuap... GET /rest/admin/application-configura... 200 22554 JSON
21 https://juice-shop.herokuap... GET /api/Challenges/?name=Score%2... ✓ 200 1545 JSON
22 https://juice-shop.herokuap... POST /socket.io/?EIO=4&transport=poll... ✓ 200 727 text io/
23 https://juice-shop.herokuap... GET /socket.io/?EIO=4&transport=poll... ✓ 200 774 JSON io/
26 https://juice-shop.herokuap... GET /rest/admin/application-configura... 200 22558 JSON
27 https://juice-shop.herokuap... GET /socket.io/?EIO=4&transport=poll... ✓ 200 742 text io/
28 https://juice-shop.herokuap... GET /socket.io/?EIO=4&transport=web... ✓ 101 725 io/
40 https://juice-shop.herokuap... GET /rest/user/whoami 200 898 JSON
41 https://juice-shop.herokuap... GET /rest/products/1/reviews 200 1347 JSON
42 https://juice-shop.herokuap... GET /rest/products/1/reviews 200 1347 JSON
43 https://juice-shop.herokuap... GET /rest/products/1/reviews 200 1355 JSON
Event log All issues
Memory: 129.5MB


Request
Pretty
Raw
GET /rest/products/1/reviews HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
Burp
Project
Intruder
Repeater
View
Dashboard
Target
Proxy
Intruder
Organizer
Extensions
Learn
Intercept
HTTP history
WebSockets history
Logger
Settings
Add to scope
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Organizer Ctrl+O
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools [Pro version only]
Show new history window
Add notes
Highlight
Delete item
Clear history
Copy URL
Copy as curl command (bash)
Copy links
Save item
Proxy history documentation
Event log
All issues



Request

Pretty Raw Hex

```
GET /rest/products/1/reviews HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Length: 457
Content-Type: application/json; charset=utf-8
Date: Sun, 16 Mar 2025 20:08:10 GMT
Etag: W/"1c9-zl7jHQLxjTyEblTWa+ug7UzBnQU"
Feature-Policy: payment 'self'
Nel:
{"report_to":"heroku-nel","response_headers":["Via"],
"max_age":3600,"success_fraction":0.01,"failure_fract
ion":0.1}
Report-To:
{"group":"heroku-nel","endpoints":[{"url":"https://ne
l.heroku.com/reports?s=sNeJnvO%2BNrHXDSmlG3p4HC62US9Y
uI87n4Cnf1OIx4M%3D\u0026sid=812dcc77-0bd0-43b1-a5f1-b
25750382959\u0026ts=1742155690"}],"max_age":3600}
Reporting-Endpoints:
heroku-nel="https://nel.heroku.com/reports?s=sNeJnvO%
2BNrHXDSmlG3p4HC62US9YuI87n4Cnf1OIx4M%3D&sid=812dcc77
-0bd0-43b1-a5f1-b25750382959&ts=1742155690"
Server: Heroku
Vary: Accept-Encoding
Via: 1.1 heroku-router
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs

{
  "status":"success",
  "data":[
    {
      "message":"One of my favorites!",
      "author":"admin@juice-sh.op",
      "product":1,
      "likesCount":0,
      "likedBy":[
      ],
      "_id":"sNoGtAhubSEMs77HK",
      "liked":true
    },
    {
      "product":"1",
      "message":"Beautiful\n\n",
      "author":"admin@juice-sh.op",
      "likesCount":0,
      "likedBy":[
```

Request

Pretty Raw Hex

```
GET /rest/products/1/reviews HTTP/1.1
```

Request

Pretty Raw Hex

```
GET /rest/AZIZ/1/reviews HTTP/1.1
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 500 Internal Server Error
```

```
{
  "error": {
    "message": "Unexpected path: /rest/AZIZ/1/reviews",
    "stack":
"Error: Unexpected path: /rest/AZIZ/1/reviews\n    at /app
/build/routes/angular.js:38:18\n    at Layer.handle [as ha
ndle_request] (/app/node_modules/express/lib/router/layer.
js:95:5)\n    at trim_prefix (/app/node_modules/express/li
b/router/index.js:328:13)\n    at /app/node_modules/expres
s/lib/router/index.js:286:9\n    at Function.process_param
s (/app/node_modules/express/lib/router/index.js:346:12)\n
    at next (/app/node_modules/express/lib/router/index.js
:280:10)\n    at /app/build/routes/verify.js:171:5\n    at
 Layer.handle [as handle_request] (/app/node_modules/expre
ss/lib/router/layer.js:95:5)\n    at trim_prefix (/app/nod
e_modules/express/lib/router/index.js:328:13)\n    at /app
/node_modules/express/lib/router/index.js:286:9\n    at Fu
nction.process_params (/app/node_modules/express/lib/route
r/index.js:346:12)\n    at next (/app/node_modules/express
/lib/router/index.js:280:10)\n    at /app/build/routes/ver
ify.js:105:5\n    at Layer.handle [as handle_request] (/ap
```