

Cyber Security Project Report

Bug Hunt 101 – Recon to Report

1. Introduction

The goal of this assignment is to gain knowledge of every detail of the bug bounty process from reconnaissance to finally submitting a formal report of the vulnerability. The basic idea of this assignment is quite simple and straightforward. The primary idea of this assignment is to use knowledge of common vulnerabilities of web applications in a lab environment.

For this purpose, OWASP Juice Shop was selected as the target application on which the tests will be performed. Juice Shop is a vulnerable web application developed specifically for creating a learning environment for web application security tests. Tests in this project are performed in a purely ethical way in the authorized lab.

2. Environment Setup

A local test environment was created using Docker to eliminate problems with dependencies and configuration.

Technologies/Tools Used:

By offering a

OWASP Juice Shop

Docker Desktop (WSL2 backend)

-bash

Web Browser (Chrome)

Windows 11

Deployment Method:

OWASP Juice Shop was deployed using the official Docker image.

docker run -d -p 3000:3000 bkimminich/juice-shop

The application was accessed via:

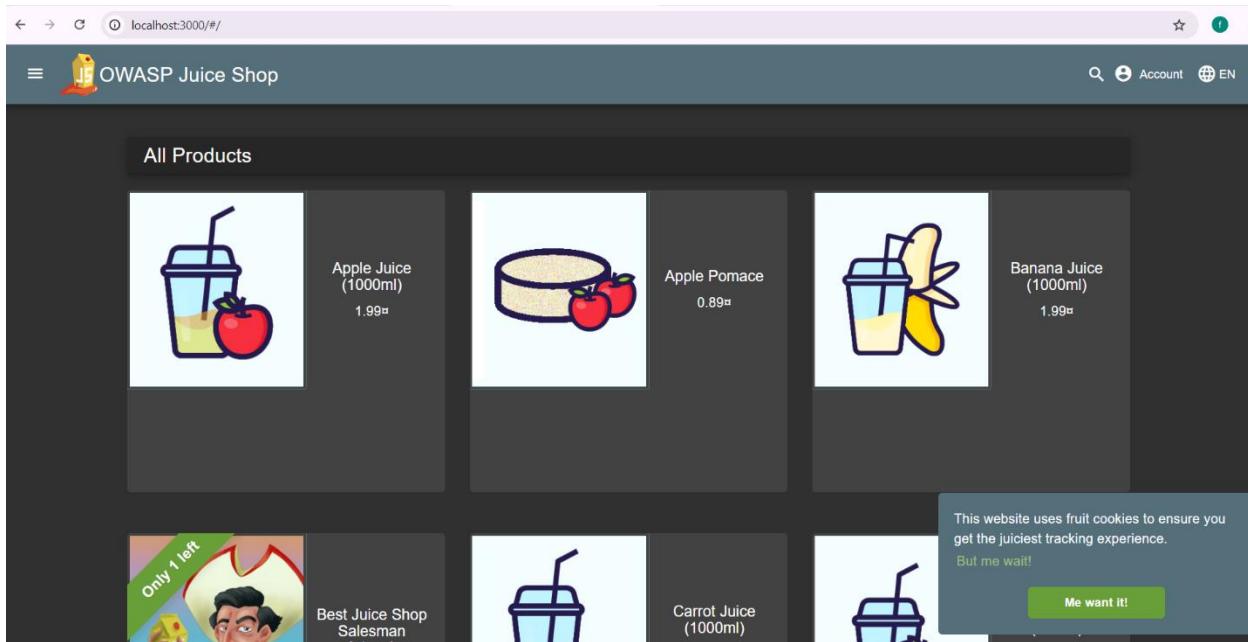
<http://localhost:3000>

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Fawas> docker --version
Docker version 29.1.3, build f52814d
PS C:\Users\Fawas> docker run -d -p 3000:3000 bkimminich/juice-shop
failed to connect to the docker API at npipe:///./pipe/dockerDesktopLinuxEngine; check if the path is correct and if the daemon is running: open //./pipe/dockerDesktopLinuxEngine: The system cannot find the file specified.
PS C:\Users\Fawas> docker run -d -p 3000:3000 bkimminich/juice-shop
Unable to find image 'bkimminich/juice-shop:latest' locally
latest: Pulling from bkimminich/juice-shop
2780920e5dbf: Pull complete
bfb59b82a9b6: Pull complete
62de241dac5f: Pull complete
d8a0d911b13e: Pull complete
dd64bf2dd177: Pull complete
4aa0ea1413d3: Pull complete
3214acf345c0: Pull complete
7c12895b777b: Pull complete
069d1e267530: Pull complete
52630fc75a18: Pull complete
33ce0b1d99fc: Pull complete
7faf0cfa885c: Pull complete
fd4aa3667332: Pull complete
f45e0372ce60: Pull complete
9cd2a1476fcc: Downloading [=====] 23.02MB/51.15MB
9d2a7448ec0d: Download complete
5b14f6c9a813: Pull complete
e7fa9df358f0: Pull complete
ea42d2577342: Downloading [=====] 28.02MB/97.16MB
dcaa5a89b0cc: Pull complete
017886f7e176: Pull complete
29b7e53d0b22: Download complete
docker: short read: expected 97160468 bytes but got 28024192: unexpected EOF

Run 'docker run --help' for more information
PS C:\Users\Fawas> docker run -d -p 3000:3000 bkimminich/juice-shop
Unable to find image 'bkimminich/juice-shop:latest' locally
latest: Pulling from bkimminich/juice-shop
```



3. Reconnaissance

Reconnaissance was done to identify open ports and understand how the application is exposed.

3.1 Target Identification

Target Application: OWASP Juice Shop

Host: localhost

Port: 3000

3.2 Port Scanning Using Nmap

The following Nmap command was used:

```
nmap -p 3000 localhost
```

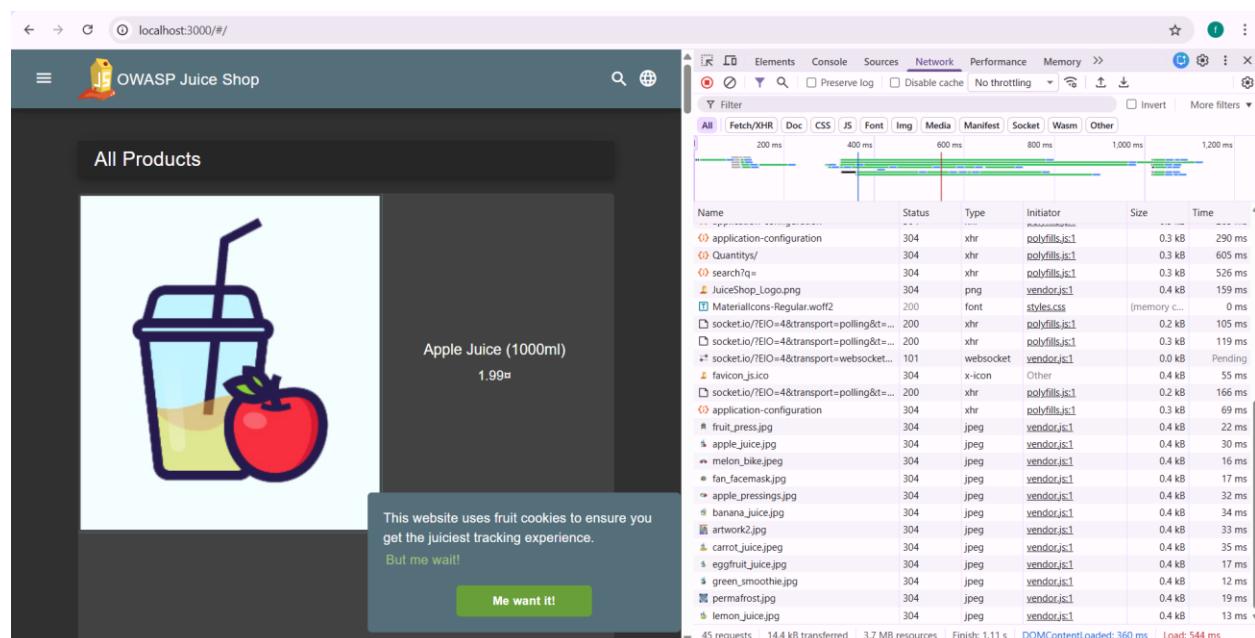
Many of us move to what we will call 'The Field' to get away from this very thing, or at least repress the knowledge of it.

TCP port 3000 was found open, which indicated that the Juice Shop service was running and accessible.

That meant the application had successfully deployed and was ready for further testing.

4. Vulnerability Findings

Testing revealed several vulnerabilities, each with straightforward steps and impact that clearly describe the vulnerability.



4.1 Cross-Site Scripting (XSS)

Description

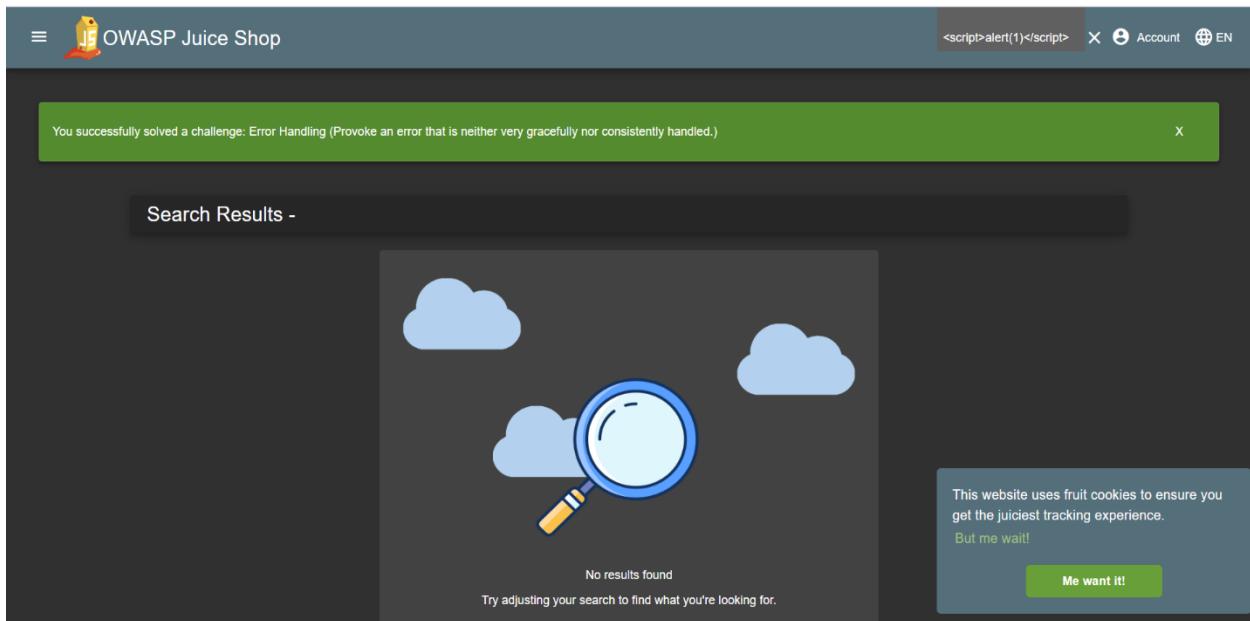
A type of reflected Cross-Site Scripting (XSS) vulnerability was found in the search function in the application. This is because the application does not sanitize the user input before it is rendered on the browser.

Affected Functionality

Search feature

Payload Used

<script>alert(1)</script>



Steps to reproduce:

1. Open OWASP Juice Shop homepage
2. Find the search bar
3. Input XSS payload into the search box
4. Submit the search
5. A JavaScript alert box is executed in the browser

Effect

"An attacker may leverage the identified vulnerability to inject malicious JavaScript in a victim's browser. This may result in session hijacking, stealing cookies, and/or malicious redirection."

Severity

Medium

4.2 Insecure Direct Object Reference (IDOR)

Insecure Direct Object Reference (IDOR) in Product Reviews Endpoint

Affected URL:

GET /rest/reviews?productId=20

Payload:

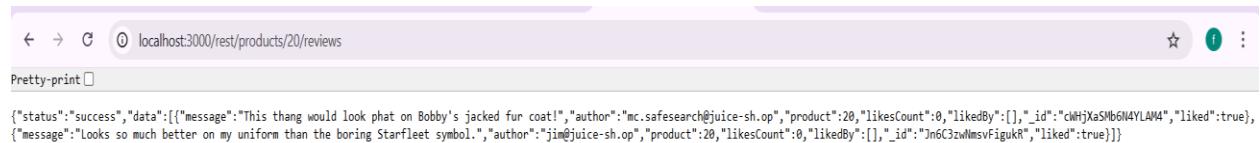
productId=20

Steps to Reproduce:

1. Log in as a normal user.
2. Open the browser developer tools (F12) and navigate to the **Network** tab.
3. Visit any product page and observe the request fetching product reviews.
4. Capture the request:
5. GET /rest/reviews?productId=<original_id>
6. Modify the productId parameter to another valid value (e.g., 20).
7. Send the modified request.
8. Observe that reviews written by other users are returned.

Impact:

The code contains a problem where it enables unauthorized access to reviews posted by the end-users via direct references to internal objects using the identifiers provided by the end-users. The code is prone to the IDOR attack, where the attackers will be able to view information for different end-users.



A screenshot of a browser window showing a Network request. The URL in the address bar is "localhost:3000/rest/products/20/reviews". The response body is displayed in a JSONpretty-printed format:

```
{"status": "success", "data": [{"message": "This thang would look phat on Bobby's jacked fur coat!", "author": "mc.safesearch@juice-sh.op", "product": 20, "likesCount": 0, "likedBy": [], "_id": "cWtjXaSMb6l4YLAM4", "liked": true}, {"message": "Looks so much better on my uniform than the boring Starfleet symbol.", "author": "jim@juice-sh.op", "product": 20, "likesCount": 0, "likedBy": [], "_id": "Jn6C3zWmsvFiguR", "liked": true}]} 
```

localhost:3000/#/

OWASP Juice Shop

All Products

Apple Juice (1000ml)
1.99¤

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

Network tab in developer tools showing request details:

Name	Status	Type	Initiator	Size	Time
application-configuration	304	xhr	polyfills.js:1	0.3 kB	290 ms
Quantums/	304	xhr	polyfills.js:1	0.3 kB	605 ms
search?q=	304	xhr	polyfills.js:1	0.3 kB	526 ms
JuiceShop_Logo.png	304	png	vendorjs:1	0.4 kB	159 ms
MaterialIcons-Regular.woff2	200	font	polyfills.js:1	0.2 kB	0 ms
socket.io/?EIO=4&transport=polling&t=...	200	xhr	polyfills.js:1	0.3 kB	119 ms
socket.io/?EIO=4&transport=websocket	101	websocket	vendorjs:1	0.0 kB	Pending
favicon.ico	304	x-icon	Other	0.4 kB	55 ms
socket.io/?EIO=4&transport=polling&t=...	200	xhr	polyfills.js:1	0.2 kB	166 ms
application-configuration	304	xhr	polyfills.js:1	0.3 kB	69 ms
fruit_press.jpg	304	jpeg	vendorjs:1	0.4 kB	22 ms
apple_juice.jpg	304	jpeg	vendorjs:1	0.4 kB	30 ms
melon_bike.jpeg	304	jpeg	vendorjs:1	0.4 kB	16 ms
fan_facemask.jpg	304	jpeg	vendorjs:1	0.4 kB	17 ms
apple_pressings.jpg	304	jpeg	vendorjs:1	0.4 kB	32 ms
banana_juice.jpg	304	jpeg	vendorjs:1	0.4 kB	34 ms
artwork2.jpg	304	jpeg	vendorjs:1	0.4 kB	33 ms
carrot_juice.jpg	304	jpeg	vendorjs:1	0.4 kB	35 ms
eggfruit_juice.jpg	304	jpeg	vendorjs:1	0.4 kB	17 ms
green_smoothie.jpg	304	jpeg	vendorjs:1	0.4 kB	12 ms
permafrost.jpg	304	jpeg	vendorjs:1	0.4 kB	19 ms
lemon_juice.jpg	304	jpeg	vendorjs:1	0.4 kB	13 ms

45 requests 14.4 kB transferred 3.7 MB resources Finish: 1.11 s DOMContentLoaded: 360 ms Load: 544 ms

localhost:3000/#/search

OWASP Juice Shop

All Products

Apple Juice (1000ml)
0.89¤

Apple Pomace
0.89¤

Banana Juice (1000ml)
1.99¤

Only 1 left

Best Juice Shop Salesman Awkward

Carrot Juice (1000ml)

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

localhost:3000/#/

OWASP Juice Shop

All Products

Apple Juice (1000ml)
1.99¤

(1000ml)
The all-time classic.

Reviews (1)

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

Close

Banana Juice (1000ml)
1.99¤

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

localhost:3000/#/search?q=apple

OWASP Juice Shop

Search Results - apple

	Apple Juice (1000ml) 1.99¤
	Apple Pomace 0.89¤

Items per page: 12

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

localhost:3000/#/about

OWASP Juice Shop

About Us

Corporate History & Policy

Lore ipsum dolor sit amet, consectetur adipisicng elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consectetur adipisicng elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lore ipsum dolor sit amet, consectetur adipisicng elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lore ipsum dolor sit amet, consectetur adipisicng elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lore ipsum dolor sit amet, consectetur adipisicng elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

localhost:3000/#/photo-wall

OWASP Juice Shop

Open side menu

Photo Wall

#zatschi #whoneedstourlegs

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

localhost:3000/#/login

OWASP Juice Shop

Login

Email*
fawas@gmail.com

Password*

Forgot your password?

Log in

Remember me

or

 Log in with Google

Not yet a customer?

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

localhost:3000/profile

User Profile



File Upload Choose File No file chosen
• Maximum file size
150Kb
• All image formats are accepted

[Upload Picture](#)

or

e.g. <https://www.gravatar.com/avatar/> Image URL:

localhost:3000/#/basket

OWASP Juice Shop

Your Basket (mohamadfawas@gmail.com)

	Apple Juice (1000ml)	- 1 +	1.99¤	
	Apple Pomace	- 1 +	0.89¤	

Total Price: 2.88¤

Checkout

You will gain 0 Bonus Points from this order!

This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!

Me want it!

localhost:3000#/order-completion/af2a-3fb7708ea69ec42c

OWASP Juice Shop

Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our [Track Orders](#) page.

Delivery Address

fawas
kandy road , colombo, colombo, 30200
srilanka
Phone Number 758884544

Order Summary

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	1	1.99¤
Apple Pomace	0.89¤	1	0.89¤
		Items	2.88¤
		Delivery	0.99¤
		Promotion	0.00¤
		Total Price	3.87¤

You have gained 0 Bonus Points from this order!

Network Requests (19 requests):

- socketIo... 101 w... vendor 0... 1.00 ms
- Cards/... 201 xhr polyfills 0... 9.00 ms
- Cards 200 xhr polyfills 0... 1.00 ms
- 1 304 xhr polyfills 0... 4.00 ms
- 7 304 xhr polyfills 0... 9.00 ms
- 7 200 xhr polyfills 0... 1.00 ms
- 6 304 xhr polyfills 0... 1.00 ms
- whami 304 xhr polyfills 0... 1.00 ms
- apple_juic... 304 jpg vendor 0... 8.00 ms
- apple_pr... 304 jpg vendor 0... 8.00 ms
- checkout 200 xhr polyfills 0... 3.00 ms
- 6 200 xhr polyfills 0... 2.00 ms
- af2a-3fb7... 200 xhr polyfills 0... 1.00 ms
- application... 304 xhr polyfills 0... 2.00 ms
- 7 304 xhr polyfills 0... 1.00 ms

19 requests | 7.2 kB transferred | 709 kB

localhost:3000#/order-history

OWASP Juice Shop

Order History

Order ID	Total Price	Bonus	Status
#af2a-3fb7708ea69ec42c	3.87¤	0	In Transit

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	1	1.99¤
Apple Pomace	0.89¤	1	0.89¤

Network Requests (37 requests):

- search?q= 304 xhr polyfills 0... 1.00 ms
- apple_juic... 304 jpg vendor 0... 1.00 ms
- apple_pr... 304 jpg vendor 0... 1.00 ms
- banana_jui... 304 jpg vendor 0... 2.00 ms
- artwork2.... 304 jpg vendor 0... 2.00 ms
- carrot_jui... 304 jpg vendor 0... 3.00 ms
- eggfruit_j... 304 jpg vendor 0... 4.00 ms
- fruit_pres... 304 jpg vendor 0... 1.00 ms
- green_sm... 304 jpg vendor 0... 1.00 ms
- permfro... 304 jpg vendor 0... 2.00 ms
- lemon_jui... 304 jpg vendor 0... 2.00 ms
- melon_bla... 304 jpg vendor 0... 2.00 ms
- fan_face... 304 jpg vendor 0... 2.00 ms
- order-his... 200 xhr polyfills 0... 7.00 ms
- no-result... 304 png vendor 0... 7.00 ms

37 requests | 15.0 kB transferred | 1.1 MB

The screenshot shows a user profile page on the left and the Network tab of the developer tools on the right.

User Profile Page:

- Header: localhost:3000/profile?id=102
- Title: User Profile
- Profile Picture: Placeholder image of a person.
- File Upload:
 - Choose File: No file chosen
 - Maximum file size: 150KB
 - All image formats are accepted
- Upload Picture button
- Or input field
- Image URL input field: e.g. https://www.gravatar.com/avatar/02e0d3a0a1c8a3a3a3a3a3a3a3a3a3a3
- Link Image button

Network Tab:

Select a folder to store override files in: Select folder

Name	Status	Type	Initiator	Size	Time
profile?id=102	200	document	Other	2.4 kB	217 ms
icon?family=Material+Icons	200	stylesheet	profile?id=102-1	(memory cache)	0 ms
jquery.min.js	200	script	profile?id=102-1	(memory cache)	0 ms
material.min.css	403	stylesheet	profile?id=102-1	0.1 kB	443 ms
userProfile.css	304	stylesheet	profile?id=102-1	0.4 kB	6 ms
css?family=Roboto:300,400,500,700	307	stylesheet / Redirect	profile?id=102-1	0.0 kB	3 ms
material.min.js	403	script	profile?id=102-1	0.1 kB	448 ms
css?family=Roboto:300,400,500,700	200	stylesheet	profile?id=102-1	(disk cache)	2 ms
JuiceShop_Logo.png	304	png	profile?id=102-1	0.4 kB	15 ms
default.svg	304	svg+xml	profile?id=102-2	0.4 kB	19 ms
f1uhqfzczlQEqJ-Vdg-luaDsNc.wof2	200	font	icon?family=Material+Icons	(memory cache)	0 ms
KFO7CnqEu92Fr1IME7kSn66gLdTyUAMA3yUBA.wof2	200	font	css?family=Roboto:300,400,500,700	(memory cache)	0 ms

A screenshot of a web browser window. The address bar at the top shows the URL "localhost:3000/profile?id=10". To the right of the address bar are several icons: a star, a sync history button, and a three-dot menu. The main content area features a large, bold title "OWASP Juice Shop (Express ^4.21.0)". Below the title, there is an error message: "500 Error: Blocked illegal activity by ::ffff:172.17.0.1" followed by the path "at /juice-shop/build/routes/userProfile.js 60:18".