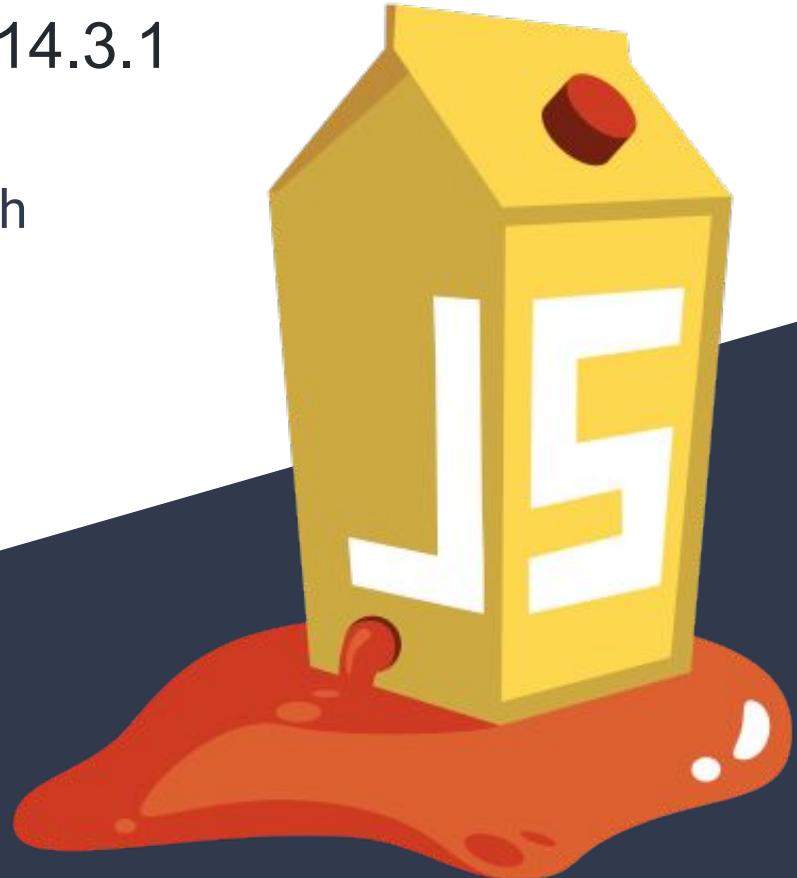


# OWASP Juice Shop v14.3.1

Difficulty Level: 1-star (★) Walkthrough



Abhishek Sharma

<https://www.linkedin.com/in/abhishek27sh/>

# Description

- 1. Insecure web application
- 2. Covers vulnerabilities from entire "Owasp Top 10"
- 3. Version v14.3.1 covers 6 difficulty levels

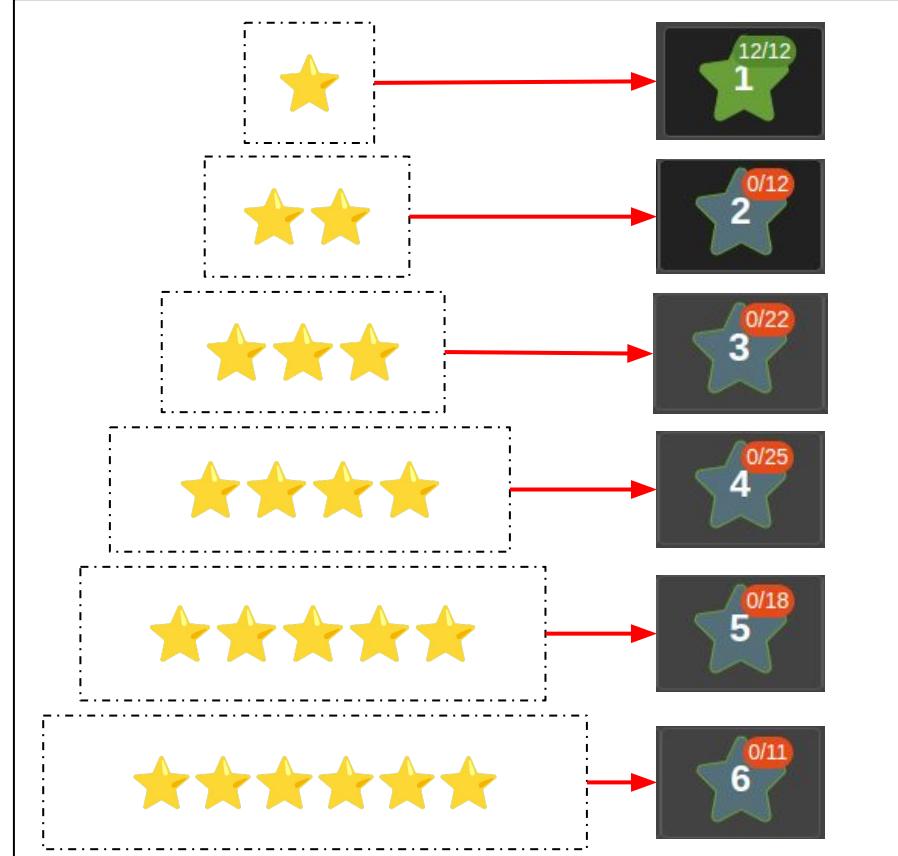


Level of Difficulty: 1-star

## Types of Vulnerabilities Covered:

- 1. XSS
- 2. Sensitive Data Exposure
- 3. Security Misconfiguration
- 4. Improper Input Validation
- 5. Unvalidated Redirects
- 6. Miscellaneous

# 6 Levels - 100 Challenges



*Overall list of vulnerabilities covered in OWASP Juice Shop v14.3.1*

1. Broken Access Control - 10 Challenges

2. Broken Anti-Automation - 4 Challenges

3. Broken Authentication - 9 Challenges

4. Cryptographic Issues - 5 Challenges

5. Improper Input Validation - 9 Challenges

6. Injection - 11 Challenges

7. Insecure Deserialization - 2 Challenges

8. Miscellaneous - 5 Challenges

9. Security Misconfiguration - 4 Challenges

10. Security through Obscurity - 3 Challenges

11. Sensitive Data Exposure - 16 Challenges

12. Unvalidated Redirects - 2 Challenges

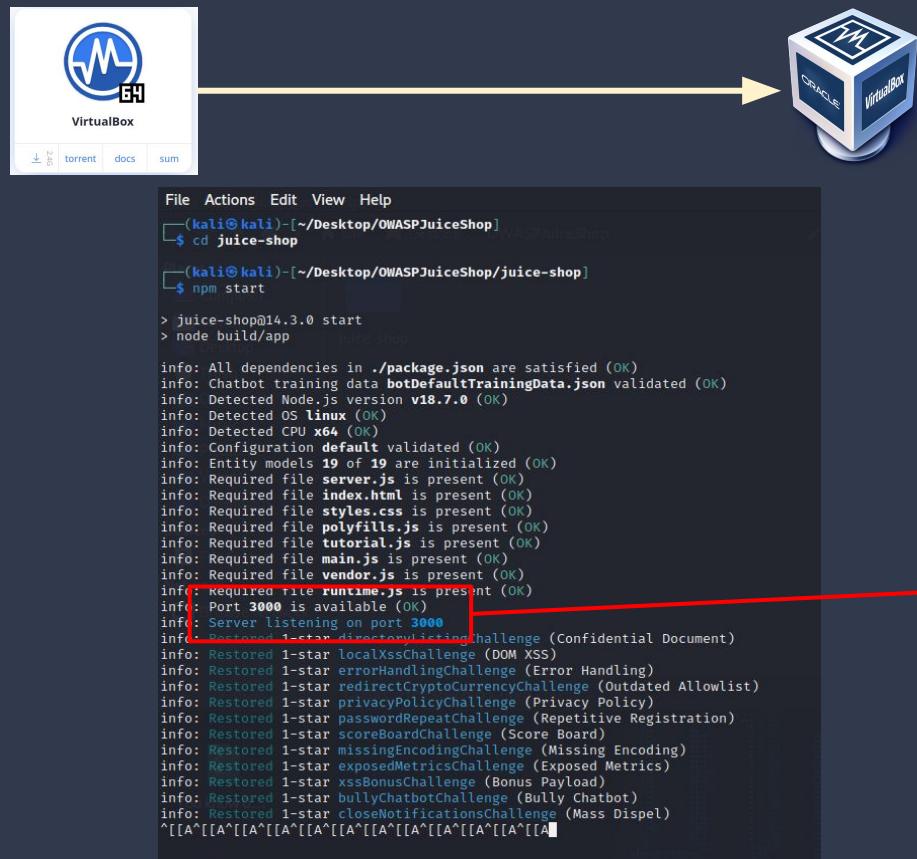
13. Vulnerable Components - 9 Challenges

14. XSS - 9 Challenges

15. XXE - 2 Challenges

XSS(Cross Site Scripting)	Sensitive Data Exposure
<ul style="list-style-type: none"><li>1. DOM XSS</li><li>2. Bonus Payload</li></ul>	<ul style="list-style-type: none"><li>1. Confidential Document</li><li>2. Exposed Metrics</li></ul>
Security Misconfiguration	Improper Input Validation
<ul style="list-style-type: none"><li>1. Error handling</li></ul>	<ul style="list-style-type: none"><li>1. Missing Encoding</li><li>2. Repetitive Registration</li></ul>
Unvalidated Redirects	Miscellaneous
<ul style="list-style-type: none"><li>1. Outdated Allowlist</li></ul>	<ul style="list-style-type: none"><li>1. Bully Chatbot</li><li>2. Mass Dispel</li><li>3. Privacy Policy</li><li>4. Score-board</li></ul>

# Setting up OWASP Juice Shop (v14.5.1) **From Sources**



<https://github.com/juice-shop/juice-shop/tree/v14.3.1#setup>

## Steps for setting up OWASP Juice Shop on Kali Linux VM

1. Install node.js (*sudo apt-get install nodejs npm -y*)
  2. Run “*git clone https://github.com/juice-shop/juice-shop.git --depth 1*” (or clone your own fork of the repository)
  3. Go into the cloned folder with *cd juice-shop*
  4. Run *npm install* (only has to be done before first start or when you change the source code)
  5. Run *npm start*
  6. Browse to *http://localhost:3000*

OWASP Juice Shop × +

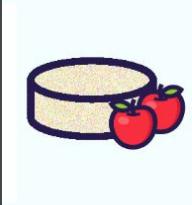
localhost:3000/#/

OWASP Juice Shop

All Products



Apple Juice  
(1000ml)  
1.99¤



Apple Pomace  
0.89¤



Banana Juice  
(1000ml)  
1.99¤



Only 1 left  
Best Juice Shop  
Salesman  
Artwork  
5000¤



Carrot Juice  
(1000ml)  
2.99¤



Eggfruit Juice  
(500ml)  
8.99¤



Fruit Press  
89.99¤



Green Smoothie  
1.99¤

<http://localhost:3000>

OWASP Juice Shop x +

localhost:3000/#/

OWASP Juice Shop

All Products

Debugger → Firefox

Sources Network Performance Memory Application Security Lighthouse DOM Invader

main.js:formatted x

12276 } }, {  
12277 path: "payment/:entity",  
12278 component: Ss  
12279 }, {  
12280 path: "wallet",  
12281 component: yl  
12282 }, {  
12283 path: "login",  
12284 component: On  
12285 }, {  
12286 path: "forgot-password",  
12287 component: en  
12288 }, {  
12289 path: "recycle",  
12290 component: ni  
12291 }, {  
12292 path: "register",  
12293 component: Qo  
12294 }, {  
12295 path: "search",  
12296 component: yt  
12297 }, {  
12298 path: "hacking-instructor",  
12299 component: yt  
12300 }, {  
12301 path: "score-board",  
12302 component: fr  
12303 }, {  
12304 path: "track-result",  
12305 component: Kt  
12306 }, {  
12307 path: "track-result/new",  
12308 component: Kt,  
12309 data: {  
12310 type: "new"  
12311 }  
12312 }, {  
12313 path: "2fa/enter",  
12314 component: vr  
12315 }, {  
12316 path: "privacy-security",  
12317 component: br

path

12287 component: en  
12288 }, {  
12289 path: "recycle",  
12290 component: ni  
12291 }, {  
12292 path: "register",  
12293 component: Qo  
12294 }, {  
12295 path: "search",  
12296 component: yt  
12297 }, {  
12298 path: "hacking-instructor",  
12299 component: yt  
12300 }, {  
12301 path: "score-board",  
12302 component: fr  
12303 }, {  
12304 path: "track-result",  
12305 component: Kt  
12306 }, {  
12307 path: "track-result/new",  
12308 component: Kt,  
12309 data: {  
12310 type: "new"  
12311 }  
12312 }, {  
12313 path: "2fa/enter",  
12314 component: vr  
12315 }, {

\$ Hint : Getting the “score-board”

# XSS(Cross Site Scripting)

1. DOM XSS
2. Bonus Payload

DOM(Document Object Model)  
based XSS

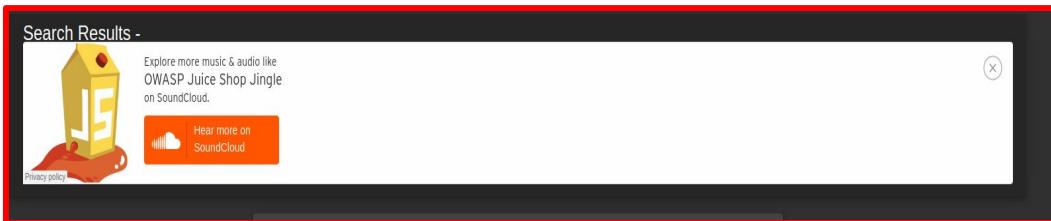
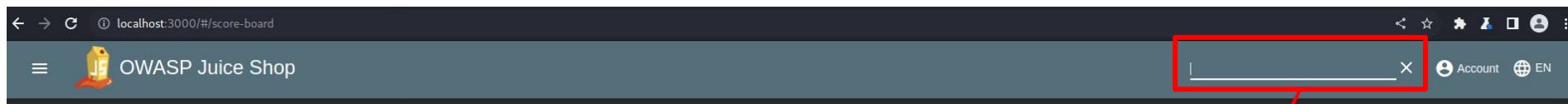
The screenshot shows two browser windows. The top window is the 'Score Board' page at `localhost:3000/#/score-board`. It has a search bar with a red border and a red arrow pointing from the 'Bonus Payload' section above to it. The bottom window is the 'Search' page at `localhost:3000/#/search?q=<iframe%20src%3D'javascript:alert(%60xss%60)'>`. It displays an alert dialog box with the message 'localhost:3000 says xss' and an 'OK' button. A red box highlights the entire search results area, and a red arrow points from the 'DOM XSS' section above to this box. The search results area shows a single row with the text 'No results found'.

XSS: #Challenge: 1. DOM XSS

# XSS(Cross Site Scripting)

1. DOM XSS
2. Bonus Payload

DOM(Document Object Model)  
based XSS



```
<iframe width="100%" height="166"
scrolling="no" frameborder="no"
allow="autoplay"
src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>
```

XSS: #Challenge: 2. Bonus Payload

# Sensitive Data Exposure

1. Confidential Document
2. Exposed Metrics

The screenshot shows a web application interface. On the left is a dark sidebar with navigation links: Contact, Customer Feedback, Company, About Us (which is highlighted with a red box), Photo Wall, Score Board, and GitHub. The main content area has a header "About Us" and a sub-section "Corporate History & Policy". Below this is a large block of placeholder text (Lorem ipsum) containing several instances of the word "Lorem ipsum". A red box highlights the first instance of "Lorem ipsum" in the main text, and another red box highlights the entire paragraph of text. A red arrow points from the top right towards the highlighted text.

localhost:3000/#/about

OWASP Juice Shop

Contact

Customer Feedback

Company

About Us

Photo Wall

Score Board

GitHub

About Us

Corporate History & Policy

Loreum ipsum dolor sit amet, consetetur sadipscing 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, consetetur sadipscing 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, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consetetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. 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, consetetur sadipscing 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, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

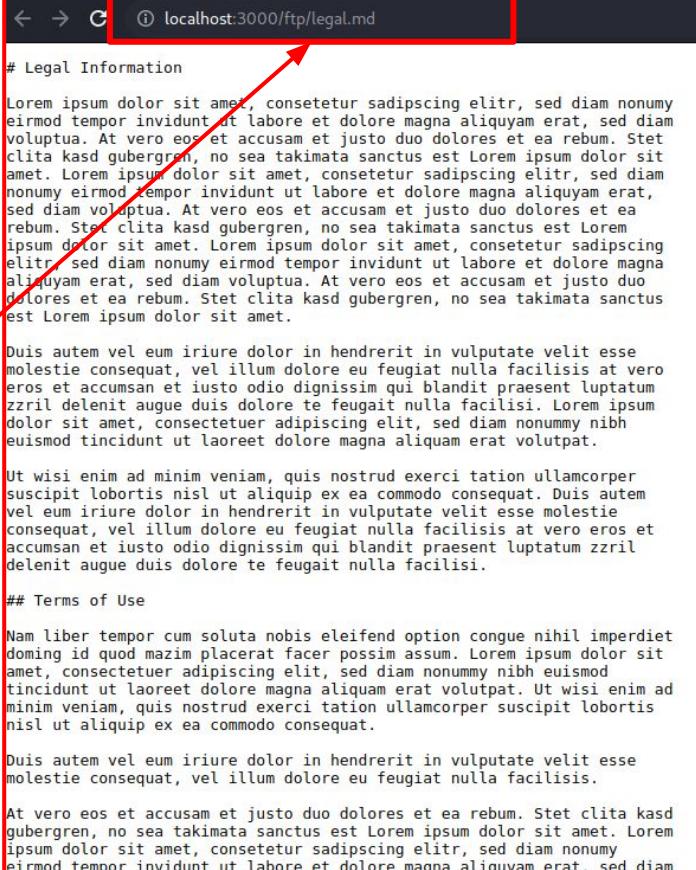
Customer Feedback

Sensitive Data Exposure: #Challenge: 1. Confidential Document

# Sensitive Data Exposure

1. Confidential Document
2. Exposed Metrics

atum zzril delenit augue duis dolore te feugait nulla  
tpat. Check out our boring terms of use if you are  
ipsum dolor sit amet. Lorem ipsum dolor sit amet,



# Legal Information

atum zzril delenit augue duis dolore te feugait nulla  
tpat. Check out our boring terms of use if you are  
ipsum dolor sit amet. Lorem ipsum dolor sit amet,

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse  
molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero  
eros et accumsan et iusto odio dignissim qui blandit praesent luptatum  
zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum  
dolor sit amet, consecetur adipiscing elit, sed diam nonummy nibh  
euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper  
suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem  
vel eum iriure dolor in hendrerit in vulputate velit esse molestie  
consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et  
accumsan et iusto odio dignissim qui blandit praesent luptatum zzril  
delenit augue duis dolore te feugait nulla facilisi.

## Terms of Use

Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet  
doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit  
amet, consecetur adipiscing elit, sed diam nonummy nibh euismod  
tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad  
minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis  
nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse  
molestie consequat, vel illum dolore eu feugiat nulla facilisis.

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, consecetur adipisciing elitr, sed diam nonum  
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam

Sensitive Data Exposure: #Challenge: 1. Confidential Document

OWASP Juice Shop x OWASP Juice Shop x localhost:3000/#/about +

OWASP Juice Shop

About Us

Corporate History & Policy

Customer Feedback

Burp Suite Community Edition v2022.7.1 - Temporary Project

Host Method URL Params Status Length MIME type Extension Title Comment TLS IP Co

433 http://localhost:3000 GET /ftp/legal.md 200 3489 text md 127.0.0.1

434 https://sb-ssl.google.com POST /safebrowsing/clientreport/day... ✓ 400 881 JSON

Send it to the “repeater”

Request Response Inspector

Pretty Raw Hex

Pretty Raw Hex Render

1 GET /ftp/legal.md HTTP/1.1  
2 Host: localhost:3000  
3 Sec-Fetch-Site: same-origin  
4 Sec-Fetch-Mode: navigate  
5 Sec-Fetch-Dest: empty  
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
7 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134  
8 Safari/537.36  
9 Accept-Encoding: gzip, deflate  
10 Accept-Language: en-US;en;q=0.9

Keep up the good work! (anonymous)  
★★★☆☆

legal.md Show all

The screenshot shows a browser window for 'OWASP Juice Shop' with an 'About Us' page. Below it, a 'Burp Suite Community Edition v2022.7.1 - Temporary Project' window is open. In the Burp Suite interface, a red box highlights the URL 'http://localhost:3000 /ftp/legal.md' in the proxy history list. A red arrow points from this highlighted URL to the text 'Send it to the “repeater”' which is enclosed in a red box. The Burp Suite interface includes tabs for Request, Response, and Inspector, with detailed logs and headers visible.

Sensitive Data Exposure: #Challenge: 1. Confidential Document

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x + Send Cancel &lt; &gt; ?

Target: http://localhost:3000

HTTP/1.1

## Request

Pretty Raw Hex

```

1 GET /ftp/ HTTP/1.1
2 Host: localhost:3000
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: navigate
5 Sec-Fetch-Dest: empty
6 Referer: http://localhost:3000/
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=eP6wxKDp0zVa2dx6UZH1TkjiEqhW6Cx7SvEtjjIzjsoVHgROXLjBy08rJ45M
11 Connection: close
12
13

```

```

<li>
  <a href="acquisitions.md" class="icon icon-md icon-text" title="acquisitions.md">
    <span class="name">
      acquisitions.md
    </span>
    <span class="size">
      909
    </span>
  </a>
</li>

```

## Response

Pretty Raw Hex Render

```

353 <input id="search" type="text" placeholder="Search" autocomplete="off" />
354 <div id="wrapper">
355   <h1>
356     <a href="">
357       ~
358     </a>
359     / <a href="">
360       ftp
361     </a>
362   </h1>
363   <ul id="files" class="view-tiles">
364     <li>
365       <a href="quarantine" class="icon icon-md icon-text" title="quarantine">
366         <span class="name">
367           quarantine
368         </span>
369         <span class="size">
370           10</span>
371         <span class="date">
372           10/22/2022 12:29:57 AM
373         </span>
374       </a>
375     </li>
376     <li>
377       <a href="acquisitions.md" class="icon icon-md icon-text" title="acquisitions.md">
378         <span class="name">
379           acquisitions.md
380         </span>
381         <span class="size">
382           909
383         </span>
384         <span class="date">
385           10/22/2022 12:29:57 AM
386         </span>
387       </a>
388     </li>
389     <li>
390       <a href="announcement_encrypted.md" class="icon icon-md icon-text" title="announcement_encrypted.md">
391         <span class="name">
392           announcement_encrypted.md
393         </span>
394         <span class="size">
395           369237
396         </span>
397         <span class="date">
398           10/22/2022 12:29:57 AM
399         </span>
400       </a>
401     </li>
402   </ul>
403

```

## Inspector

Request Attributes	2
Request Query Parameters	0
Request Body Parameters	0
Request Cookies	4
Request Headers	10
Response Headers	10

0 matches

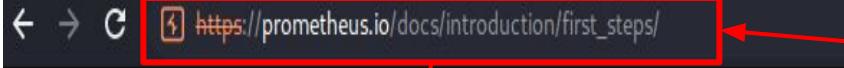
0 matches

12 matches

# Sensitive Data Exposure: #Challenge: 1. Confidential Document

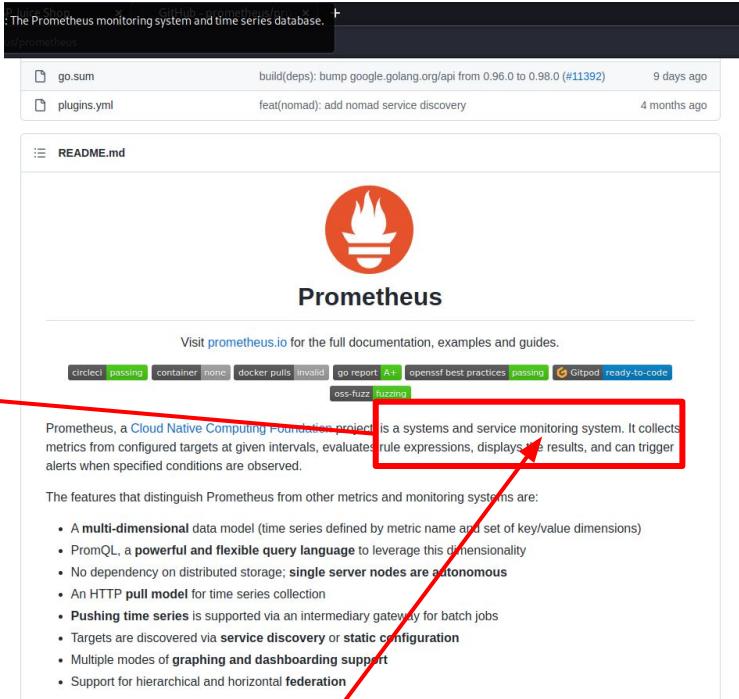
# Sensitive Data Exposure

1. Confidential Document
2. Exposed Metrics



The last block, `scrape_configs`, controls what resources Prometheus monitors. Since Prometheus also exposes data about itself as an HTTP endpoint it can scrape and monitor its own health. In the default configuration there is a single job, called `prometheus`, which scrapes the time series data exposed by the Prometheus server. The job contains a single statically configured target, the `localhost` on port `9090`. Prometheus expects metrics to be available on targets on a path of `/metrics`. So this default job is scraping via the URL:

<http://localhost:9090/metrics>.



The screenshot shows the Prometheus GitHub repository. A commit from 4 months ago adds Nomad service discovery. The README.md page is displayed, featuring the Prometheus logo and a brief description: "Prometheus, a Cloud Native Computing Foundation project, is a systems and service monitoring system. It collects metrics from configured targets at given intervals, evaluates rule expressions, displays the results, and can trigger alerts when specified conditions are observed." A red box highlights the sentence "It collects metrics from configured targets at given intervals, evaluates rule expressions, displays the results, and can trigger alerts when specified conditions are observed." Another red box highlights the URL [https://prometheus.io/docs/introduction/first\\_steps/](https://prometheus.io/docs/introduction/first_steps/) in the browser address bar.

Exposed Metrics



Find the endpoint that serves usage data to be scraped by a popular monitoring system.

Sensitive Data Exposure

Mass Dispel



Close multiple "Challenge solved"-notifications in one go.

Miscellaneous

Sensitive Data Exposure: #Challenge: 2. Exposed Metrics

```
localhost:3000/metrics  + 
localhost:3000/metrics

# HELP file_uploads_count Total number of successful file uploads grouped by file type.
# TYPE file_uploads_count counter

# HELP file_upload_errors Total number of failed file uploads grouped by file type.
# TYPE file_upload_errors counter

# HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup_duration_seconds gauge
juiceshop_startup_duration_seconds{task="cleanupFTPFolder",app="juiceshop"} 0.20913017
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.177678887
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.393360411
juiceshop_startup_duration_seconds{task="restoreOverwrittenFilesWithOriginals",app="juiceshop"} 0.27060769
juiceshop_startup_duration_seconds{task="datacreator",app="juiceshop"} 6.290739465
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"} 0.030332703
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"} 0.008647561
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"} 10.957

# HELP process_cpu_user_seconds_total Total user CPU time spent in seconds.
# TYPE process_cpu_user_seconds_total counter
process_cpu_user_seconds_total{app="juiceshop"} 243.279598

# HELP process_cpu_system_seconds_total Total system CPU time spent in seconds.
# TYPE process_cpu_system_seconds_total counter
process_cpu_system_seconds_total{app="juiceshop"} 46.682185

# HELP process_cpu_seconds_total Total user and system CPU time spent in seconds.
# TYPE process_cpu_seconds_total counter
process_cpu_seconds_total{app="juiceshop"} 289.961783

# HELP process_start_time_seconds Start time of the process since unix epoch in seconds.
# TYPE process_start_time_seconds gauge
process_start_time_seconds{app="juiceshop"} 1666419129

# HELP process_resident_memory_bytes Resident memory size in bytes.
# TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes{app="juiceshop"} 216621056

# HELP process_virtual_memory_bytes Virtual memory size in bytes.
# TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes{app="juiceshop"} 11818082304

# HELP process_heap_bytes Process heap size in bytes.
# TYPE process_heap_bytes gauge
process_heap_bytes{app="juiceshop"} 236707840

# HELP process_open_fds Number of open file descriptors.
# TYPE process_open_fds gauge
process_open_fds{app="juiceshop"} 26

# HELP process_max_fds Maximum number of open file descriptors.
# TYPE process_max_fds gauge
process_max_fds{app="juiceshop"} 1048576

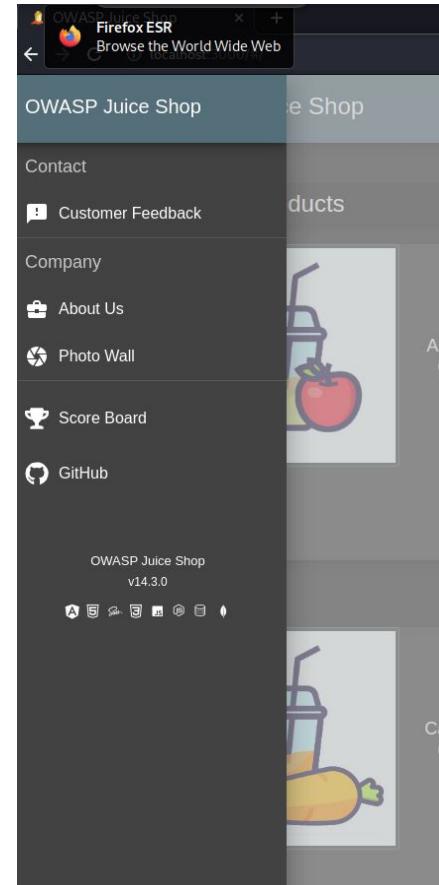
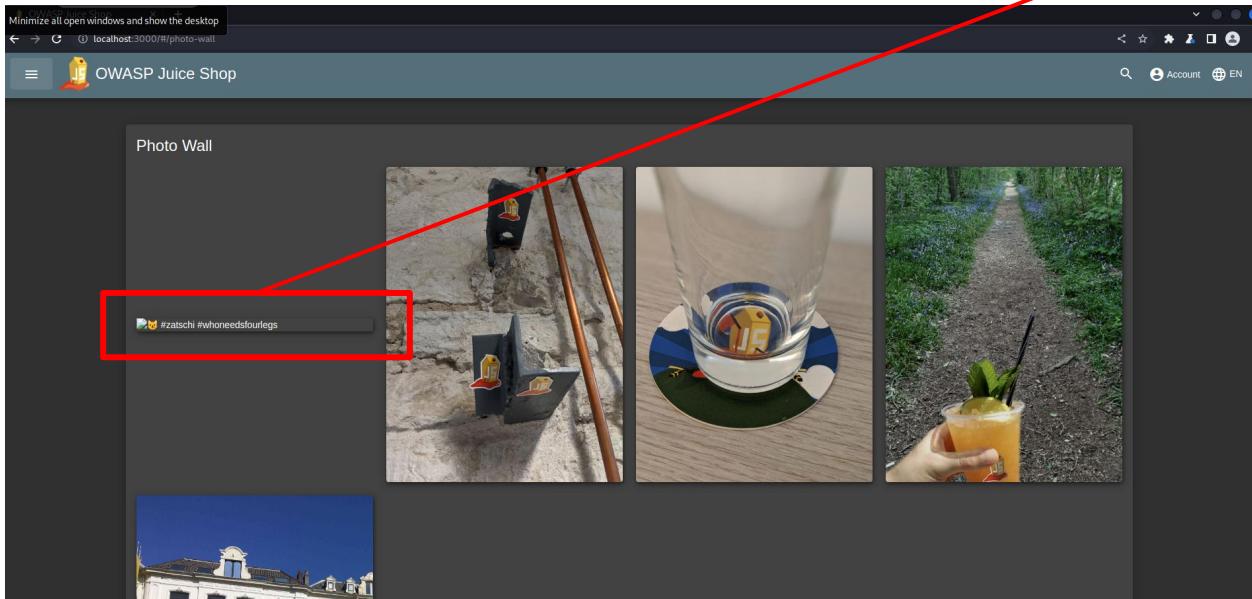
# HELP nodejs_eventloop_lag_seconds Lag of event loop in seconds.
# TYPE nodejs_eventloop_lag_seconds gauge
```

## Sensitive Data Exposure: #Challenge: 2. Exposed Metrics

# Improper Input Validation

1. Missing Encoding
2. Repetitive Registration

*"Inspect Element"*



Improper Input Validation: #Challenge 1: *Missing Encoding*

OWASP Juice Shop x +

localhost:3000/#/photo-wall

OWASP Juice Shop

Photo Wall

#zatschi #whoneedsfourlegs

Elements Console Sources Network Performance Memory Application Security Lighthouse DOM Invader

```
<app>Welcome _ngcontent-gjv-c266 _nghost-gjv-c257>_</app>Welcome>
<router-outlet _ngcontent-gjv-c266></router-outlet>
<app-photo-wall _nghost-gjv-c241 class="ng-star-inserted">
  <mat-card _ngcontent-gjv-c241 class="mat-card mat-focus-indicator heading mat-elevation-z6 mat-own-card" style="margin-bottom: 10px;">
    <h1 _ngcontent-gjv-c241>Photo Wall</h1>
    <div _ngcontent-gjv-c241>
      <div _ngcontent-gjv-c241 class="grid ng-star-inserted">
        <span _ngcontent-gjv-c241 class="container mat-elevation-z6 ng-star-inserted">
          
        <div _ngcontent-gjv-c241 class="overlays">_</div>
      </span>
      <span _ngcontent-gjv-c241 class="container mat-elevation-z6 ng-star-inserted">_</span>
      <span _ngcontent-gjv-c241 class="container mat-elevation-z6 ng-star-inserted">_</span>
      <span _ngcontent-gjv-c241 class="container mat-elevation-z6 no-star-inserted">_</span>
    </div>
  </mat-card>
</app-photo-wall>
```

Styles Computed Layout Event Listeners >

Filter :hov .cls +

element.style { }

.bluegrey-lightgreen-theme .mat-app-background, .bluegrey-lightgreen-theme.mat-app-background { background-color: #303030; color: #ffff; }

.bluegrey-lightgreen-theme.mat-app-background { background-color: #303030; color: #ffff; }

body { display: block; }

A red box highlights the image element containing the image source. A red arrow points from this box to a red-bordered box containing the text "#".

## Improper Input Validation: #Challenge 1: Missing Encoding

Burp Suite Community Edition v2022.7.1 - Temporary Project

Decoder

# %23

Text Hex

Decode as ...

Encode as ...

Plain URL HTML

Base64 ASCII hex Hex Octal Binary Gzip Smart decode

Photo Wall

its Console Sources Network Performance Memory Application Security Lighthouse DOM Invader

```
welcome_ngcontent-giv-c266_nghost-giv-c257></app>Welcome  
er-outlet_ngcontent-giv-c266</router-outlet>  
photo-wall_nghost-giv-c241 class="ng-star-inserted">  
t-card_ngcontent-giv-c241 class="mat-card mat-focus-indicator heading mat-elevation-26 mat-own-card" style="margin-bottom: 10px;">  
i1_ngcontent-giv-c241>Photo Wall<h1>  
div_ngcontent-giv-c241>  
<div_ngcontent-giv-c241 class="grid ng-star-inserted"> grid  
  <span_ngcontent-giv-c241 class="container mat-elevation-26 ng-star-inserted">  
    <img_ngcontent-giv-c241 class="image" src="assets/public/images/uploads/%23zatschi%23whoneedsfourlegs_1572600969477.jpg" alt="%" #zatschi #whoneedsfourlegs" style="width: 100%; height: 100%; object-fit: cover;"/>  
    <div_ngcontent-giv-c241 class="overlay"></div>  
  </span>  
  <span_ngcontent-giv-c241 class="container mat-elevation-26 ng-star-inserted"></span>  
  <span_ngcontent-giv-c241 class="container mat-elevation-26 ng-star-inserted"></span>  
  <span_ngcontent-giv-c241 class="container mat-elevation-26 ng-star-inserted"></span>  
  <span_ngcontent-giv-c241 class="container mat-elevation-26 no-star-inserted"></span>  
mat-drawer-content.mat-sidenav-content.ng-star-inserted app-photo-wall.ng-star-inserted mat-card.mat-card.mat-focus-indicator.heading.mat-elevation-26.mat-own-card div div.grid.ng-star-inserted span.com
```

## Improper Input Validation: #Challenge 1: Missing Encoding

# Improper Input Validation

- 1. Missing Encoding
- 2. Repetitive Registration

The screenshot shows the OWASP Juice Shop User Registration page at [localhost:3000/#/register](http://localhost:3000/#/register). The page has a dark theme with a light gray header bar. The main form is titled "User Registration". It contains fields for "Email \*", "Password \*", "Repeat Password \*", "Security Question \*", and "Answer \*". A "Register" button is at the bottom.

- 1. A blue arrow points from the "Repeat Password" field to a red box labeled "Repeat Password".
- 2. A green arrow points from the "Repeat Password" field to the "Repeat Password \*" label below it.
- 3. A red arrow points from the "Repeat Password" field to the "Please repeat your password" placeholder text.
- 4. A pink arrow points from the "Repeat Password" field to the "4-update" text above the "Repeat Password" input field.

The "Repeat Password" field contains the value "4-update". Error messages are visible: "Password must be 5-40 characters long" next to the "Password" field, and "Please repeat your password" next to the "Repeat Password" field. A "Show password advice" checkbox is present below the "Repeat Password" field.

Improper Input Validation: #Challenge 2: Repetitive Registration

# Security Misconfiguration

## 1. Error handling

The screenshot shows the OWASP Juice Shop application running on localhost:3000. The main page displays a list of products, including "Carrot Juice (1000ml)" at 2.99€ and "Fruit Press" at 89.99€. A red box highlights the URL for viewing reviews: /rest/products/reviews. Below the list, a detailed view of a juice is shown with an illustration of a juice glass and a carrot.

Request:

```
GET /rest/products/1/reviews HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="103", ".Not/A/Brand";v="99"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=eP6wxK0p02Va2d6UZH1Tkj1EqHWGcT75VEjjIzjsovH0XLjBy0Rj45M
If-None-Match: W/"ac-sFHLjArGotQJNMM9KvvNzKd3v"
Connection: close
```

Response:

```
HTTP/1.1 500 Internal Server Error
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
Vary: Accept-Encoding
Date: Sat, 22 Oct 2022 16:28:29 GMT
Connection: close
Content-Length: 2586
```

Detailed Response Headers:

```
14: {
  "error": {
    "message": "Unexpected path: /rest/products/someprod",
    "stack": "Error: Unexpected path: /rest/products/someprod\n  at /home/kali/Desktop/OWASPJuiceShop/juice-shop/build/routes/angular.js:15:18\n  at Layer.handle [as handle_request] (/home/kali/Desktop/OWASPJuiceShop/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n  at trim_prefix (/home/kali/Desktop/OWASPJuiceShop/juice-shop/node_modules/express/lib/router/index.js:328:13)\n  at /home/kali/Desktop/OWASPJuiceShop/juice-shop/node_modules/express/lib/router/index.js:286:9\n  at Function
```

The screenshot shows Burp Suite's Repeater tab. A red box highlights the request URL: /rest/products/someprod. The response shows a 500 Internal Server Error with the message "Unexpected path: /rest/products/someprod". Another red box highlights the detailed response headers.

Request:

```
GET /rest/products/someprod HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="103", ".Not/A/Brand";v="99"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=eP6wxK0p02Va2d6UZH1Tkj1EqHWGcT75VEjjIzjsovH0XLjBy0Rj45M
If-None-Match: W/"ac-sFHLjArGotQJNMM9KvvNzKd3v"
Connection: close
```

Response:

```
HTTP/1.1 500 Internal Server Error
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
Vary: Accept-Encoding
Date: Sat, 22 Oct 2022 16:29:57 GMT
Connection: close
Content-Length: 2586
```

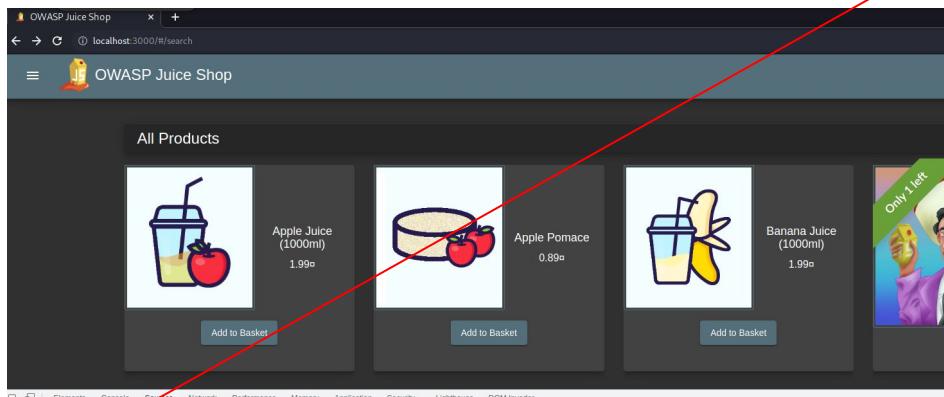
Detailed Response Headers:

```
14: {
  "error": {
    "message": "Unexpected path: /rest/products/someprod",
    "stack": "Error: Unexpected path: /rest/products/someprod\n  at /home/kali/Desktop/OWASPJuiceShop/juice-shop/build/routes/angular.js:15:18\n  at Layer.handle [as handle_request] (/home/kali/Desktop/OWASPJuiceShop/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n  at trim_prefix (/home/kali/Desktop/OWASPJuiceShop/juice-shop/node_modules/express/lib/router/index.js:328:13)\n  at /home/kali/Desktop/OWASPJuiceShop/juice-shop/node_modules/express/lib/router/index.js:286:9\n  at Function
```

Security Misconfiguration: #Challenge - Error Handling

# Unvalidated Redirects

## 1. Outdated Allowlist



```
Page Filesystem > main.js main.js.formatted x
Filesystem
top
localhost:3000
assets/public/images
(index)
main.js
polylift.js
polyfills.js
runtime.js
vendor.js
styles.css
MaterialIcons-Regular.woff2
font-mitz.css
font-mitz.woff
cdnjs.cloudflare.com redirect
```

This code block shows the main.js file from the assets/public/images directory. It contains logic to handle a redirect. A red box highlights the section where a URL is being constructed.

```
this.ngZone.run((b, k, z){function*() {
    return yield e.router.navigate(["/order-summary"])
}}
);
noop();
showBitcoinOrCode();
this.dialog.open(Mt, {
    data: {
        address: "bitcoinc:1AbKfgvw9ps041NbL18kufD0TezwG8DRZm",
        url: "./redirect?url=https://blockchain.info/address/1AbKfgvw9ps041NbL18kufD0TezwG8DRZm",
        address: "1AbKfgvw9ps041NbL18kufD0TezwG8DRZm",
        title: "TITLE BITCOIN ADDRESS"
}}
```

```
Page Filesystem > main.js
Filesystem
top
localhost:3000
assets/public/images
(index)
main.js
polylift.js
polyfills.js
runtime.js
vendor.js
styles.css
MaterialIcons-Regular.woff2
font-mitz.css
font-mitz.woff
cdnjs.cloudflare.com redirect
```

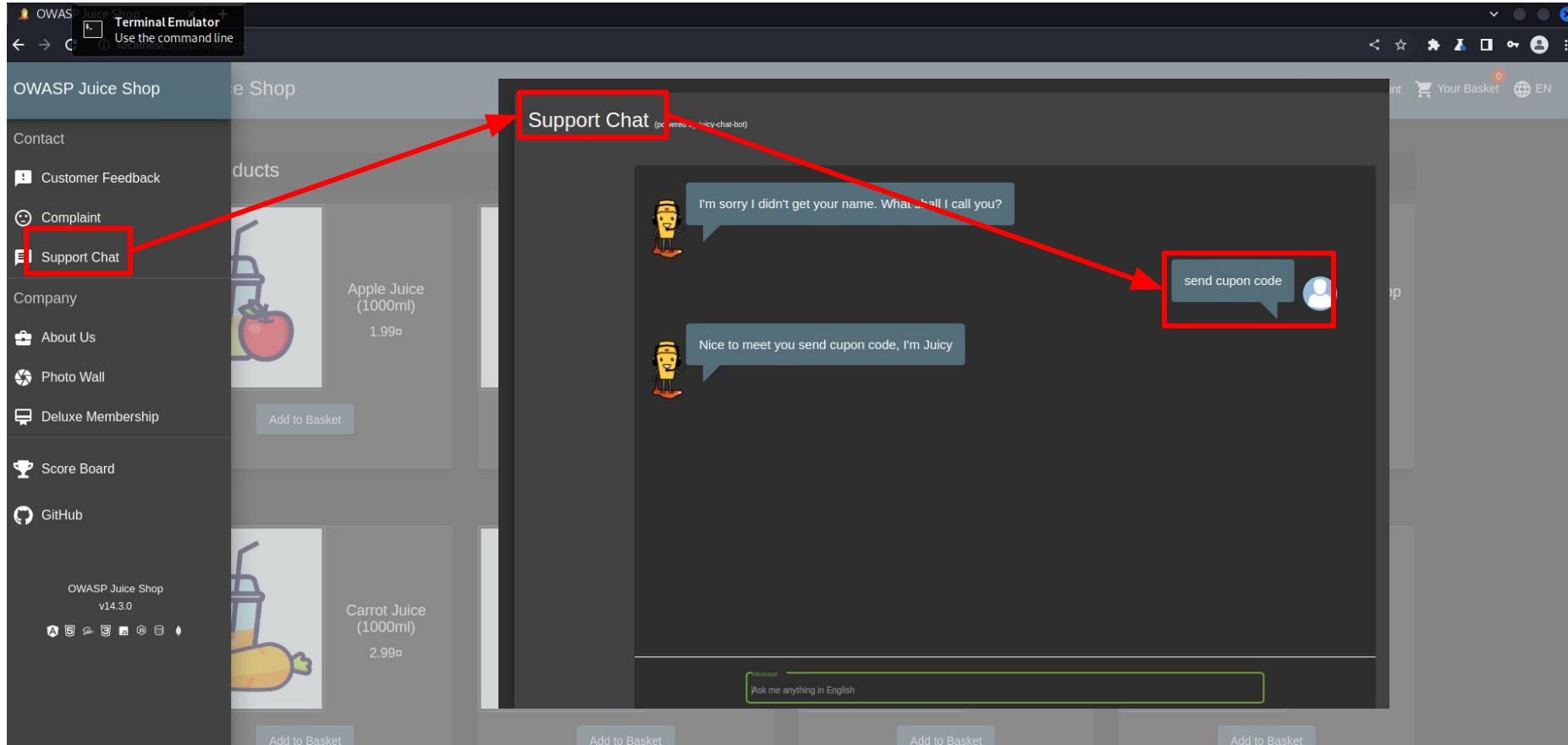
This screenshot shows the browser's developer tools Sources tab. A red box highlights the main.js file under the localhost:3000 assets/public/images directory. Another red box highlights the 'redirect' entry in the cdnjs.cloudflare.com list.

```
Page Filesystem > main.js main.js.formatted x
Filesystem
top
localhost:3000
assets/public/images
(index)
main.js
polylift.js
polyfills.js
runtime.js
vendor.js
styles.css
MaterialIcons-Regular.woff2
font-mitz.css
font-mitz.woff
cdnjs.cloudflare.com redirect
```

This screenshot shows the browser's developer tools Sources tab with the main.js file open. A red box highlights the 'redirect' entry in the cdnjs.cloudflare.com list. Another red box highlights the specific redirect code within the main.js file.

```
this.ngZone.run((b, k, z){function*() {
    return yield e.router.navigate(["/order-summary"])
}}
);
noop();
showBitcoinOrCode();
this.dialog.open(Mt, {
    data: {
        address: "bitcoinc:1AbKfgvw9ps041NbL18kufD0TezwG8DRZm",
        url: "./redirect?url=https://blockchain.info/address/1AbKfgvw9ps041NbL18kufD0TezwG8DRZm",
        address: "1AbKfgvw9ps041NbL18kufD0TezwG8DRZm",
        title: "TITLE BITCOIN ADDRESS"
}}
```

Unvalidated Redirects: #Challenge - 1. Outdated Whitelist



Miscellaneous: #Challenge - 1. *Bully Chatbot*

OWASP Juice Shop × +

localhost:3000/#/score-board

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Juice Shop

The server has been restarted: Your previous hacking progress has been restored automatically.  Delete cookie to clear hacking progress

**Shift + [x] icon**

You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

You successfully solved a challenge: Confidential Document (Access a confidential document.)

You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.)

You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

You successfully solved a challenge: Outdated Allowlist (Let us redirect you to one of our crypto currency addresses which are not promoted any longer.)

You successfully solved a challenge: Privacy Policy (Read our privacy policy.)

x

x

x

x

x

x

x

x

x

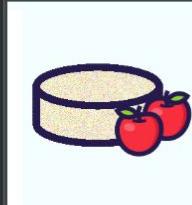
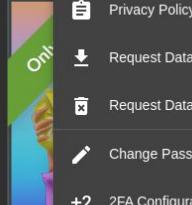
## Miscellaneous: #Challenge - 2. Mass Dispel

OWASP Juice Shop x +

localhost:3000/#/search

OWASP Juice Shop

All Products

 Apple Juice (1000ml) 1.99¤ <a href="#">Add to Basket</a>	 Apple Pomace 0.89¤ <a href="#">Add to Basket</a>	 Banana Juice (1000ml) 1.99¤ <a href="#">Add to Basket</a>	 Carrot Juice (1000ml) 2.99¤ <a href="#">Add to Basket</a>
 Eggfruit Juice (500ml) 8.99¤ <a href="#">Add to Basket</a>	 Fruit Press 89.99¤ <a href="#">Add to Basket</a>	 Green Smoothie 1.99¤ <a href="#">Add to Basket</a>	

Search Account Your Basket 0 EN

b@randomsomeone.com

Orders & Payment

Privacy & Security

Logout

Request Data Export

Request Data Erasure

Change Password

2FA Configuration

Last Login IP

Only 1 item left!

Juice Shop Salesman artwork 5000¤

Add to Basket

Miscellaneous: #Challenge - 3. Privacy Policy

# OWASP Juice Shop v14.3.1

*Coding Challenge*

Difficulty Level: 1-star

*“6 Coding Challenges”*

*Two phases of coding challenge:*

**I. “Find it”** - Select the vulnerable line(s) of code

**II. “Fix it”** - Select the correct solution for the vulnerable code that you have selected.

Coding Challenge: Outdated Allowlist

Find It      Fix It

Correct Fix  
Fix 4

Only Show Lines with Differences (3)

Side by Side Line by Line

1 const redirectAllowlist = new Set([	1 const redirectAllowlist = new Set([
2 'https://github.com/bkimminich/juice-shop',	2 'https://github.com/bkimminich/juice-shop',
3 - 'https://blockchain.info/address/1AbKfgvw9psQ41Nk'	
4 - 'https://explorer.dash.org/address/Xr556RzuwX6hg5'	
5 - 'https://etherscan.io/address/0x0f933ab9fc当地782d'	
6 'http://shop.spreadshirt.com/juiceshop',	3 'http://shop.spreadshirt.com/juiceshop',
7 'http://shop.spreadshirt.de/juiceshop',	4 'http://shop.spreadshirt.de/juiceshop',
8 'https://www.stickeryou.com/products/owasp-juice-s	5 'https://www.stickeryou.com/products/owasp-juice-s
9 'http://leanpub.com/juice-shop'	6 'http://leanpub.com/juice-shop'
10 ])	7 ])
11 exports.redirectAllowlist = redirectAllowlist	8 exports.redirectAllowlist = redirectAllowlist
12	9

localhost:3000/#/score-board

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Broken Access Control Broken Anti Automation Broken Authentication Cryptographic Issues Improper Input Validation Injection Insecure Deserialization Miscellaneous Security Misconfiguration Security through Obscurity

Sensitive Data Exposure Unvalidated Redirects Vulnerable Components XSS XXE Hide all

## Coding Challenge: Bonus Payload

Name Difficulty

Bonus Payload ★

Bully Chatbot ★

Confidential Document ★

DOM XSS ★

Error Handling ★

Exposed Metrics ★

Mass Dispel ★

Missing Encoding ★

Outdated Allowlist ★

Find It

Fix It

Correct Fix  
Fix 2

Only Show Lines with Differences (1)

Side by Side Line by Line

```
filterTable () {  
  let queryParam: string = this.route.snapshot.queryParams.q  
  if (queryParam) {  
    queryParam = queryParam.trim()  
    this.dataSource.filter = queryParam.toLowerCase()  
  }  
  - this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParam)  
  + this.searchValue = queryParam  
  this.gridDataSource.subscribe((result: any) => {  
    if (result.length === 0) {  
      this.emptyState = true  
    } else {  
      this.emptyState = false  
    }  
  })  
}
```

Close multiple "Challenge solved"-notifications in one go.

MISCELLANEOUS

Retrieval photo of Bjoern's cat in "melee combat-mode".

Improper Input Validation Shenanigans

Let us redirect you to one of our crypto currency addresses which are not promoted any longer.

Unvalidated Redirects Code Analysis

Status Feedback

solved 1/2

unsolved

unsolved

unsolved

unsolved

unsolved

unsolved

unsolved

unsolved

# Coding Challenge #1: *Bonus Payload*

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Bully Chatbot ★ Receive a coupon code from the support chatbot.

Confidential Document ★ Access a confidential document.

DOM XSS ★

Error Handling ★

Exposed Metrics ★

Mass Dispel ★

Missing Encoding ★

Outdated Allowlist ★

Privacy Policy ★

Repetitive Registration ★

Score Board ★

Miscellaneous

Shenanigans Good for Demos

Sensitive Data Exposure Good for Demos

Unsolved

Coding Challenge: Score Board

Find It

Fix It

Correct Fix

Fix 3

Only Show Lines with Differences (1)

Side by Side Line by Line

```
const routes: Routes = [
  {
    path: 'administration',
    component: AdministrationComponent,
    canActivate: [AdminGuard]
  },
  {
    path: 'accounting',
    component: AccountingComponent,
    canActivate: [AccountingGuard]
  },
]
```

Got an idea for a new challenge? Found a vulnerability that is not tracked here? Let us know via Gitter.im community chat or by opening a GitHub issue!

## Coding Challenge #2: Score Board

localhost:3000/#/score-board queryparam javascript - Google Search

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Name	Difficulty	Description	Category	Tags	Status	Feedback			
Bonus Payload	★	Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/77198407&color=%23ff5500&quot;	XSS	Shenanigans	<input checked="" type="checkbox"/> solved				
Bully Chatbot	★								
Confidential Document	★				<input checked="" type="checkbox"/> solved				
DOM XSS	★								
Error Handling	★								
Exposed Metrics	★								
Mass Dispel	★								
Missing Encoding	★								
Outdated Allowlist	★								
Privacy Policy	★								
Repetitive Registration	★	Follow the DRY principle while registering a user.	Improper Input Validation						
Score Board	★	Find the carefully hidden 'Score Board' page.	Miscellaneous	Code Analysis	<input checked="" type="checkbox"/> solved				

### Coding Challenge: Confidential Document

Find It

Fix It

Correct Fix

Fix 1

Only Show Lines with Differences (3)

Side by Side Line by Line

1 - /* /ftp directory browsing and file download */	1 + /* /ftp directory browsing */
2 app.use('/ftp', serveIndexMiddleware, serveIndex('ft	2 app.use('/ftp', serveIndexMiddleware, serveIndex('
3 - app.use('/ftp(?:/quarantine)/:file', fileServer())	
4 - app.use('/ftp/quarantine/:file', quarantineServer())	
5	3
6 /* /encryptionkeys directory browsing */	4 /* /encryptionkeys directory browsing */
7 app.use('/encryptionkeys', serveIndexMiddleware,	5 app.use('/encryptionkeys', serveIndexMiddleware,
8 app.use('/encryptionkeys/:file', keyServer())	6 app.use('/encryptionkeys/:file', keyServer())
9	7
10 /* /logs directory browsing */	8 /* /logs directory browsing */
11 app.use('/support/logs', serveIndexMiddleware, serv	9 app.use('/support/logs', serveIndexMiddleware, serv
12 app.use('/support/logs/:file', logFileServer())	10 app.use('/support/logs/:file', logFileServer())

Tutorial

## Coding Challenge #3: Confidential Document

localhost:3000/#/score-board JAX-RS @QueryParam example - Mkyong.com

show\_user=true&show\_reposts=false&show\_teaser=true"></iframe> in the DOM XSS challenge.

Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force	unsolved
Confidential Document	★			solved	<>
DOM XSS	★			solved	<>
Error Handling	★			unsolved	<>
Exposed Metrics	★			unsolved	<>
Mass Dispel	★			unsolved	<>
Missing Encoding	★			unsolved	<>
Outdated Allowlist	★			unsolved	<>
Privacy Policy	★			unsolved	graduation cap icon
Repetitive Registration	★			unsolved	
Score Board	★			solved	<>

Coding Challenge: DOM XSS

Find It Fix It 🔒

Correct Fix Fix 3

Only Show Lines with Differences (1) Side by Side Line by Line

```
filterTable () {  
    let queryParam: string = this.route.snapshot.queryParams.get('query');  
    if (queryParam) {  
        queryParam = queryParam.trim();  
        this.dataSource.filter = queryParam.toLowerCase();  
    }  
    this.searchValue = this.sanitizer.bypassSecurityTrustString(queryParam);  
}  
  
filterTable () {  
    let queryParam: string = this.route.snapshot.queryParams.get('query');  
    if (queryParam) {  
        queryParam = queryParam.trim();  
        this.dataSource.filter = queryParam.toLowerCase();  
    }  
    this.searchValue = queryParam;  
}
```

Got an idea for a new challenge? Found a vulnerability that is not tracked here? Let us know via [Gitter.im](#) community chat or by opening a [GitHub issue!](#)

## Coding Challenge #4: DOM XSS (Similar to “Bonus Payload Challenge”)

localhost:3000/#/score-board JAX-RS @QueryParam example - Mkyong.com

show\_user=true&show\_reposts=false&show\_teaser=true"></iframe> in the DOM XSS challenge.

Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force	Shenanigans	unsolved
Confidential Document	★					solved
DOM XSS	★					solved
Error Handling	★					unsolved
Exposed Metrics	★					solved
Mass Dispel	★					unsolved
Missing Encoding	★					solved
Outdated Allowlist	★					unsolved
Privacy Policy	★					unsolved
Repetitive Registration	★					unsolved
Score Board	★					solved

Coding Challenge: Exposed Metrics

Find It Fix It 🔒

Correct Fix Fix 2

Only Show Lines with Differences (1) Side by Side Line by Line

```
/* Serve metrics */  
let metricsUpdateLoop  
const Metrics = metrics.observeMetrics()  
- app.get('/metrics', metrics.serveMetrics())  
+ app.get('/metrics', security.denyAll(), metrics.serveMetrics)  
errorhandler.title = `${config.get('application.name')}`  
const registerWebSocketEvents = require('./lib/startup/events').register  
const customizeApplication = require('./lib/startup/customize').customize  
export async function start (readyCallback: Function)  
const datacreatorEnd = startupGauge.startTimer({  
    await sequelize.sync({ force: true })  
})
```

Got an idea for a new challenge? Found a vulnerability that is not tracked here? Let us know via [Gitter.im](#) community chat or by opening a [GitHub](#) issue!

## Coding Challenge #5: Exposed Metrics

← → ⌛ 🔍 localhost:3000/#/score-board

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Your Battery is discharging (100%) Estimated time left is 4 hours 18 minutes

Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Shenanigans	unsolved
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	Good for Demos	solved
DOM XSS	★			Good for Demos	solved
Error Handling	★				solved
Exposed Metrics	★				solved
Mass Dispel	★				solved
Missing Encoding	★				solved
Outdated Allowlist	★				solved
Privacy Policy	★				solved
Repetitive Registration	★				solved
Score Board	★				solved

### Coding Challenge: Outdated Allowlist

Find It Fix It

Correct Fix  
Fix 4

Only Show Lines with Differences (3)

	Side by Side	Line by Line	
1	const redirectAllowlist = new Set([	1	const redirectAllowlist = new Set([
2	'https://github.com/bkimminich/juice-shop',	2	'https://github.com/bkimminich/juice-shop',
3	- 'https://blockchain.info/address/1AbKfgvw9psQ41Nt'	3	
4	- 'https://explorer.dash.org/address/Xr556RzuwX6hg5'	4	
5	- 'https://etherscan.io/address/0x0f933ab9fc当地782d'	5	
6	'http://shop.spreadshirt.com/juiceshop',	6	'http://shop.spreadshirt.com/juiceshop',
7	'http://shop.spreadshirt.de/juiceshop',	7	'http://shop.spreadshirt.de/juiceshop',
8	'https://www.stickeryou.com/products/owasp-juice-s	8	'https://www.stickeryou.com/products/owasp-juice-s
9	'http://leanpub.com/juice-shop'	9	'http://leanpub.com/juice-shop'
10	])	10	])
11	exports.redirectAllowlist = redirectAllowlist	11	exports.redirectAllowlist = redirectAllowlist

Got an idea for a new challenge? Found a vulnerability that is not tracked here? Let us know via [!](#)

## Coding Challenge #6: Outdated Allowlist