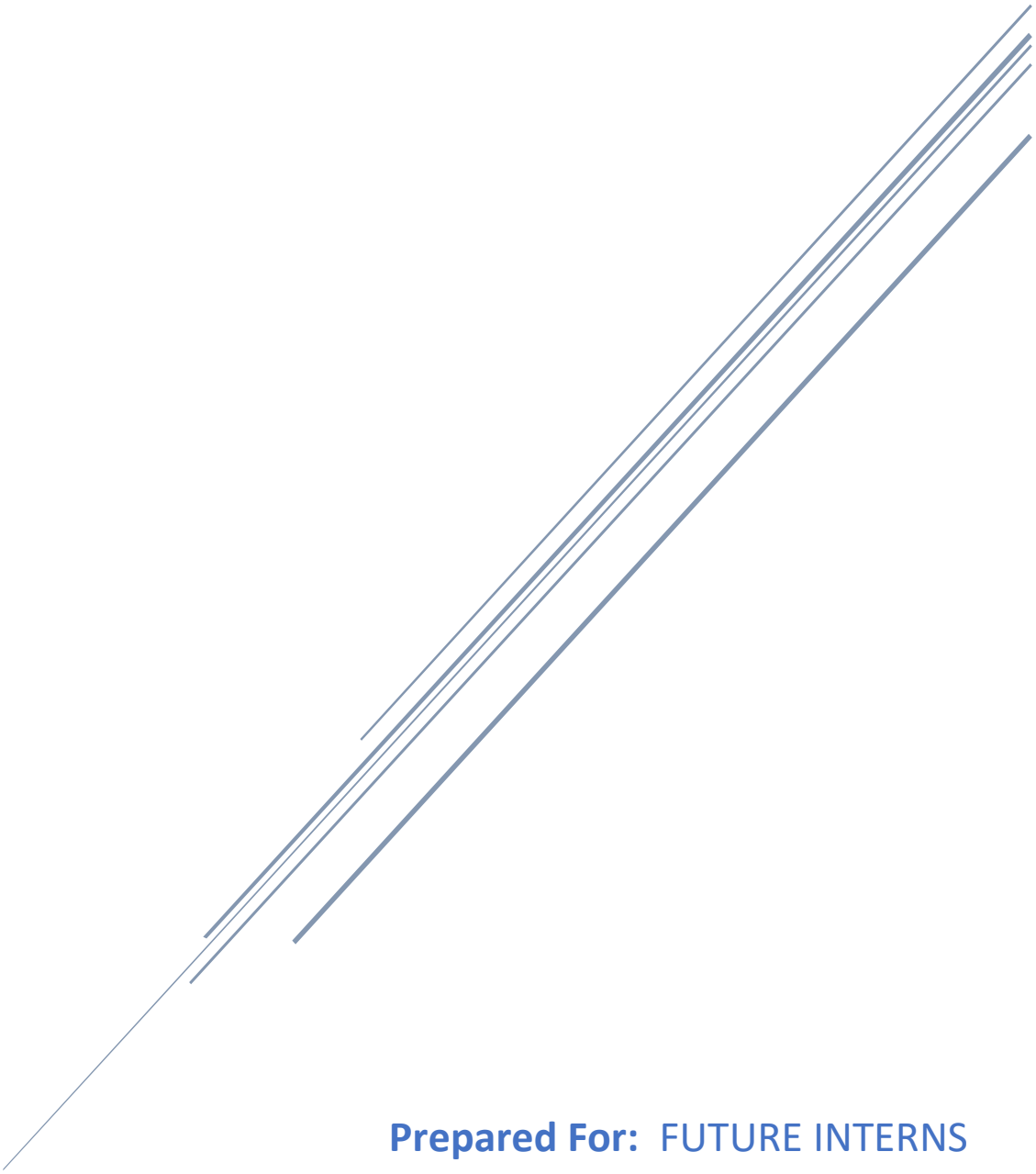
FUTURE INTERNS

Web Application Security Assessment Report

OWASP JUICE SHOP



Prepared For: FUTURE INTERNS
Prepared By: S Mansoor

A vulnerability assessment was conducted on the OWASP Juice Shop web application...

The assessment discovered several **Critical** and **High** severity vulnerabilities.

Notably, a critical **SQL Injection** vulnerability was found that allows an attacker to bypass the login page and gain full administrator access to the application.

The application's current security posture is considered **Critical**. Immediate remediation is required to protect against data theft and system compromise.

Define the Scope & Methodology

This section tells the client exactly what you tested and how you tested it.

- **Scope:** Be specific.
    - **In-Scope Target:** The application at http://localhost:3000.
    - **Out-of-Scope:** "All other company assets or infrastructure were out of scope."
- **Methodology:** Explain your process.
    - "The assessment was based on the **OWASP Top 10** framework."
    - "Testing involved both **manual penetration testing** techniques and **automated vulnerability scanning**."
- **Tools Used:** List the tools from your project.
    - OWASP ZAP (v2.1x.x)
    - Docker
    - Kali Linux
    - Mozilla Firefox

Document Each Finding (The Core Section)

Each Vulnerability:

Finding 1: SQL Injection Allows Administrator Authentication Bypass

- **Risk Level: Critical**
- **OWASP Mapping:** A03:2021 - Injection

Description:

The login form's email field is vulnerable to a classic SQL Injection (SQLi) attack. The application fails to properly sanitize user-supplied input, allowing an attacker to manipulate the backend database query. By injecting a specific payload, an attacker can bypass the password check and log in as any user.

Proof of Concept (PoC):

This section is your step-by-step guide showing how to replicate the flaw.

1. Navigate to the login page: http://localhost:3000/#/login
2. In the **Email** field, enter the payload: ' OR 1=1 --
3. In the **Password** field, enter any value (e.g., "password").
4. Click the "Log in" button.

Evidence:

[Insert your screenshot here. Show the login page with the payload typed in, or the screen after you've successfully logged in as 'admin@juice-sh.op'.]

Impact:

A successful exploit of this vulnerability gives an attacker full administrator privileges. This allows them to view all user data, delete or modify products, deface the website, and compromise the entire application and its database.

Recommended Mitigation:

Do not build SQL queries by concatenating strings. The application must be updated to use parameterized queries (also known as prepared statements). This approach separates the query logic from the data, ensuring that user input is always treated as text and never as executable SQL code.

Finding 2: Reflected Cross-Site Scripting (XSS) in Search Bar

- **Risk:** High
- **OWASP:** A03:2021 - Injection
- **PoC:** Describe entering <script>alert('XSS')</script> in the search bar.

- **Evidence:** Screenshot of the alert box popping up.
- **Mitigation:** Implement **context-aware output encoding**. All user-supplied data must be encoded *before* being rendered back to the HTML page.

Finding 3: Broken Access Control Exposes Sensitive Files

- **Risk:** Medium
- **OWASP:** A01:2021 - Broken Access Control
- **PoC:** Describe navigating directly to the http://localhost:3000/ftp directory.
- **Evidence:** Screenshot of the file directory listing in your browser.
- **Mitigation:** Disable directory listing on the web server. All sensitive files and directories should have strict access controls applied, allowing access only to authenticated and authorized users.

Finding 4: (From ZAP) Content Security Policy (CSP) Header Not Set

- **Risk:** Medium
- **OWASP:** A05:2021 - Security Misconfiguration
- **PoC:** Show the output from your OWASP ZAP scan.
- **Evidence:** Screenshot of the ZAP "Alerts" tab highlighting this finding.
- **Mitigation:** Implement a strong Content Security Policy (CSP) header to control which resources (scripts, styles, images) are allowed to be loaded by the browser, mitigating the risk of XSS attacks.

Create the OWASP Top 10 Checklist

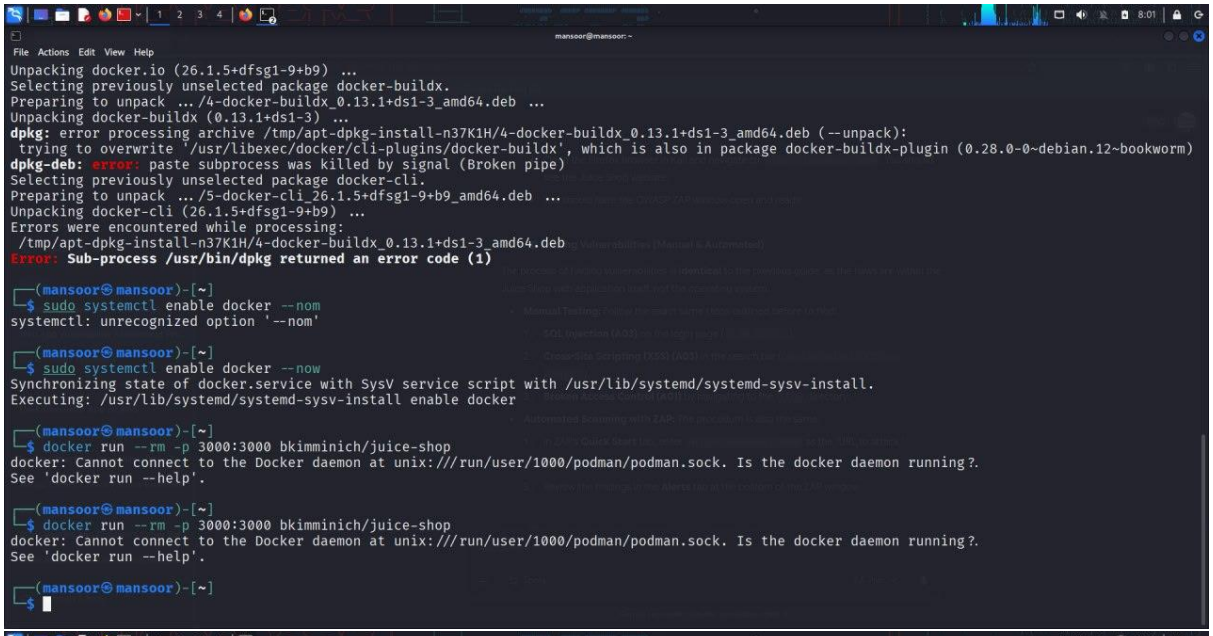
As required by the project, create a simple table that maps your findings.

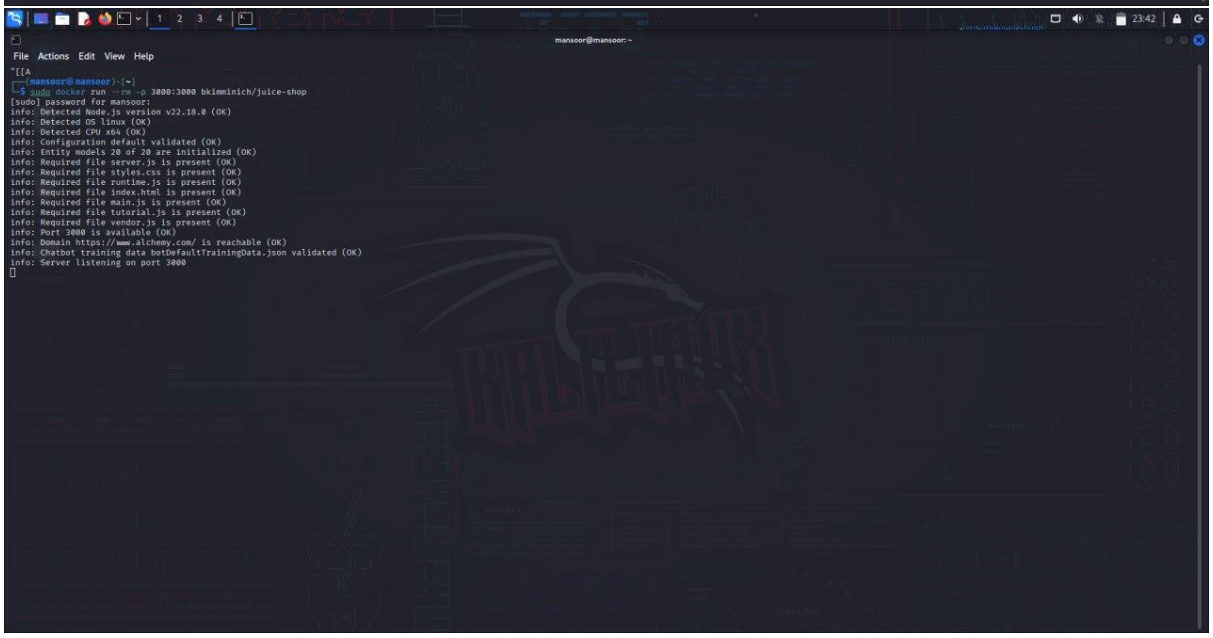
OWASP Top 10 Category	Status	Corresponding Finding(s)
A01: Broken Access Control	**Vulnerable**	Sensitive File Exposure (/ftp)
A02: Cryptographic Failures	Not Tested	-
A03: Injection	**Vulnerable**	SQL Injection, Reflected XSS
A04: Insecure Design	Not Tested	-
A05: Security Misconfiguration	**Vulnerable**	CSP Header Not Set

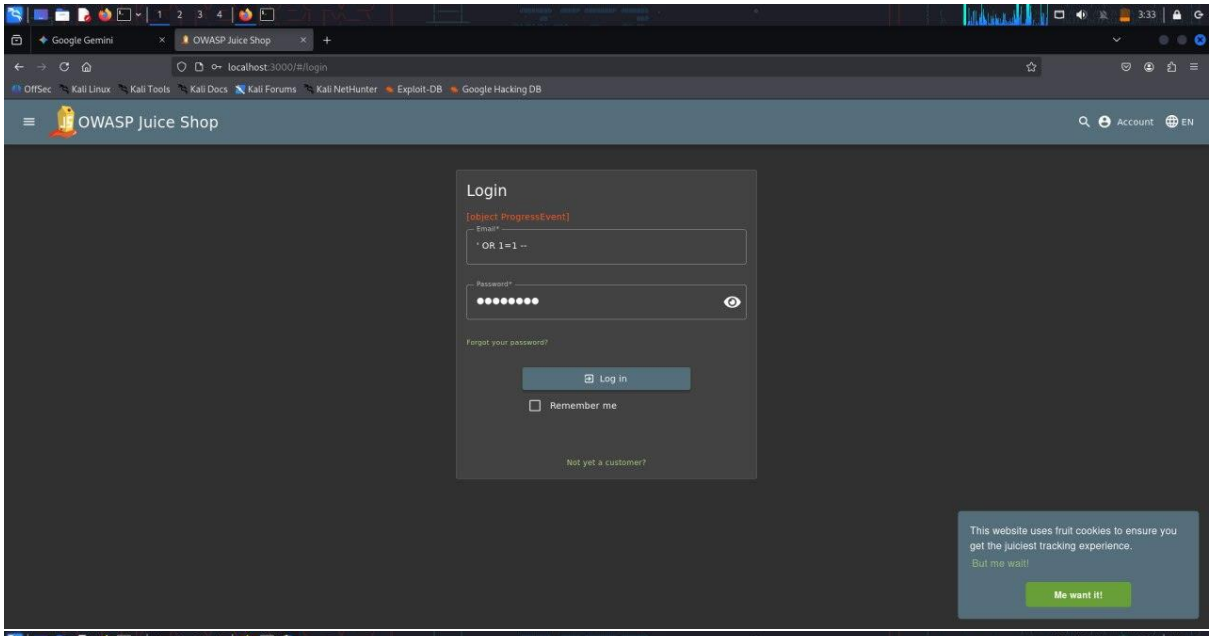
---

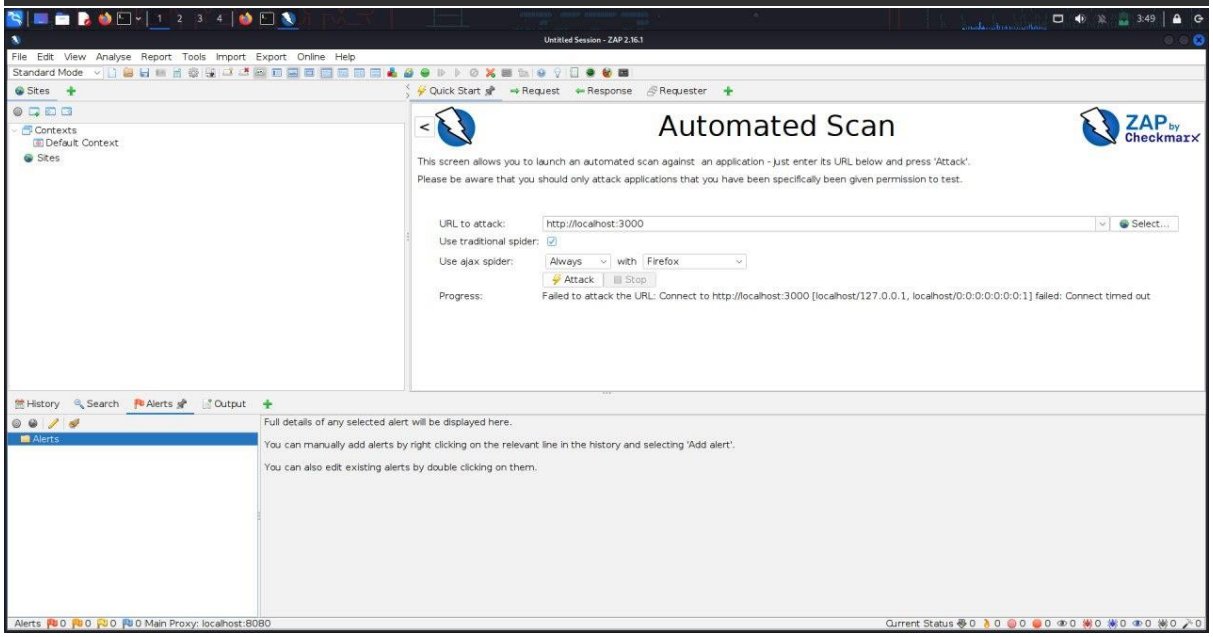
The Final Conclusion

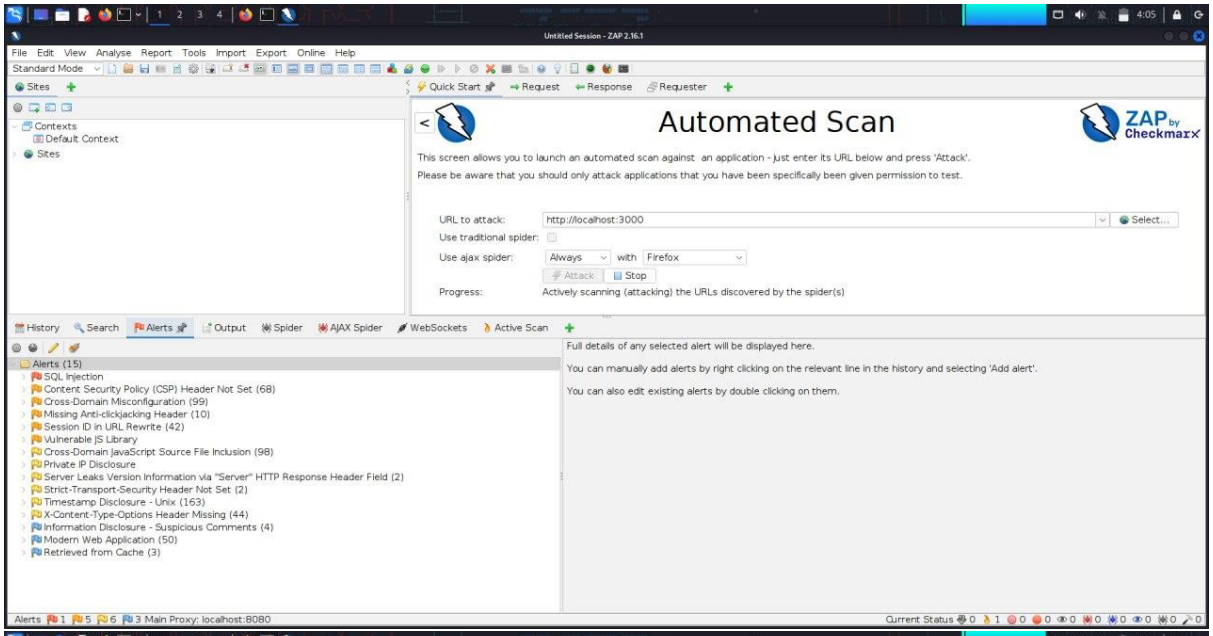
The security assessment of the OWASP Juice Shop confirmed it contains several high-impact vulnerabilities, most notably an SQL Injection flaw. The findings in this report indicate a high risk of system compromise. We recommend that the development team prioritize the **Mitigation** steps outlined for each finding, starting with the **Critical** and **High** severity items, to improve the application's overall security posture.

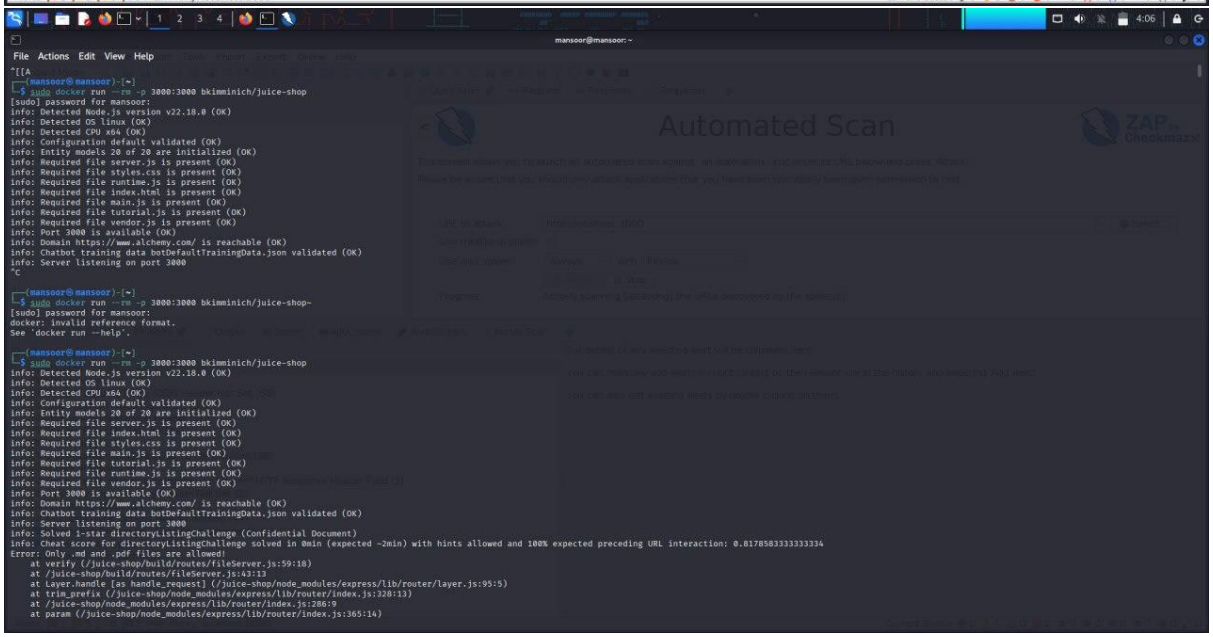

mansoor@mansoor: ~
File Actions Edit View Help
Unpacking docker.io (26.1.5+dfsg1-9+b9) ...
Selecting previously unselected package docker-buildx.
Preparing to unpack .../4-docker-buildx_0.13.1+ds1-3_amd64.deb ...
Unpacking docker-buildx (0.13.1+ds1-3) ...
dpkg: error processing archive /tmp/apt-dpkg-install-n37K1H/4-docker-buildx_0.13.1+ds1-3_amd64.deb (--unpack):
trying to overwrite '/usr/libexec/docker/cli-plugins/docker-buildx', which is also in package docker-buildx-plugin (0.28.0-0~debian.12~bookworm)
dpkg-deb: error: paste subprocess was killed by signal (Broken pipe)
Selecting previously unselected package docker-cli.
Preparing to unpack .../5-docker-cli_26.1.5+dfsg1-9+b9_amd64.deb ...
Unpacking docker-cli (26.1.5+dfsg1-9+b9) ...
Errors were encountered while processing:
/tmp/apt-dpkg-install-n37K1H/4-docker-buildx_0.13.1+ds1-3_amd64.deb
Error: Sub-process /usr/bin/dpkg returned an error code (1)
┌──(mansoor㉿mansoor)-[~]
└─$ sudo systemctl enable docker --nom
systemctl: unrecognized option '--nom'
┌──(mansoor㉿mansoor)-[~]
└─$ sudo systemctl enable docker --now
Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker
┌──(mansoor㉿mansoor)-[~]
└─$ docker run --rm -p 3000:3000 bkimminich/juice-shop
docker: Cannot connect to the Docker daemon at unix:///run/user/1000/podman/podman.sock. Is the docker daemon running?.
See 'docker run --help'.
┌──(mansoor㉿mansoor)-[~]
└─$ docker run --rm -p 3000:3000 bkimminich/juice-shop
docker: Cannot connect to the Docker daemon at unix:///run/user/1000/podman/podman.sock. Is the docker daemon running?.
See 'docker run --help'.
┌──(mansoor㉿mansoor)-[~]
└─$

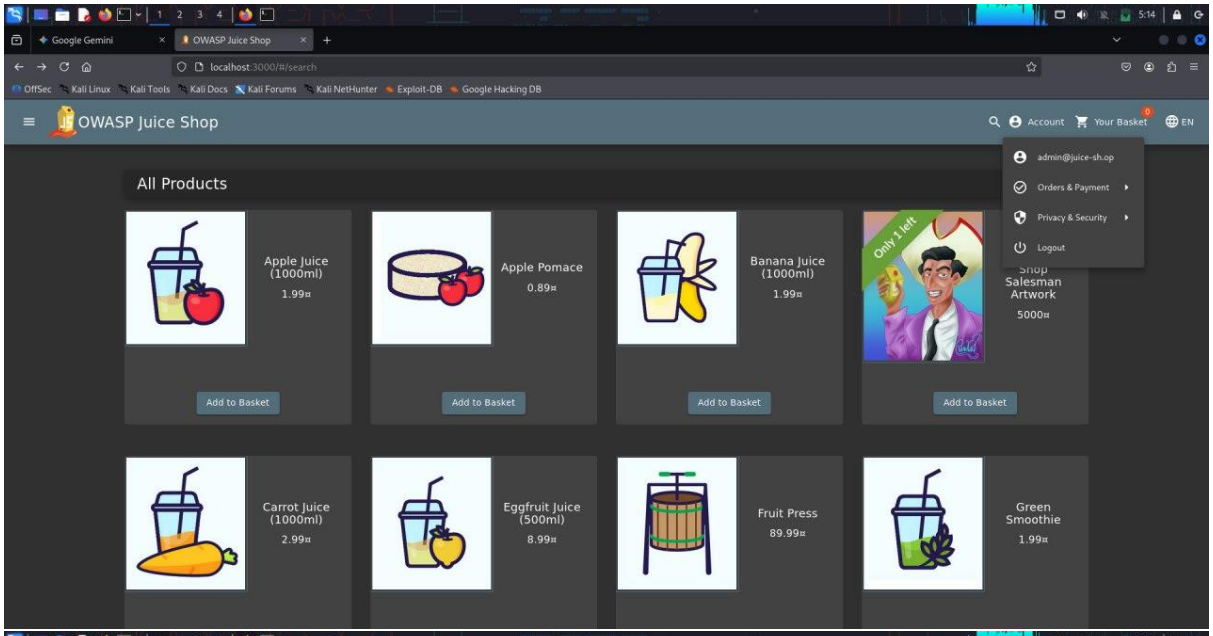

mansoor@mansoor: ~
File Actions Edit View Help
^[[A
┌──(mansoor㉿mansoor)-[~]
└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
[sudo] password for mansoor:
info: Detected Node.js version v22.18.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 20 of 20 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file runtime.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000

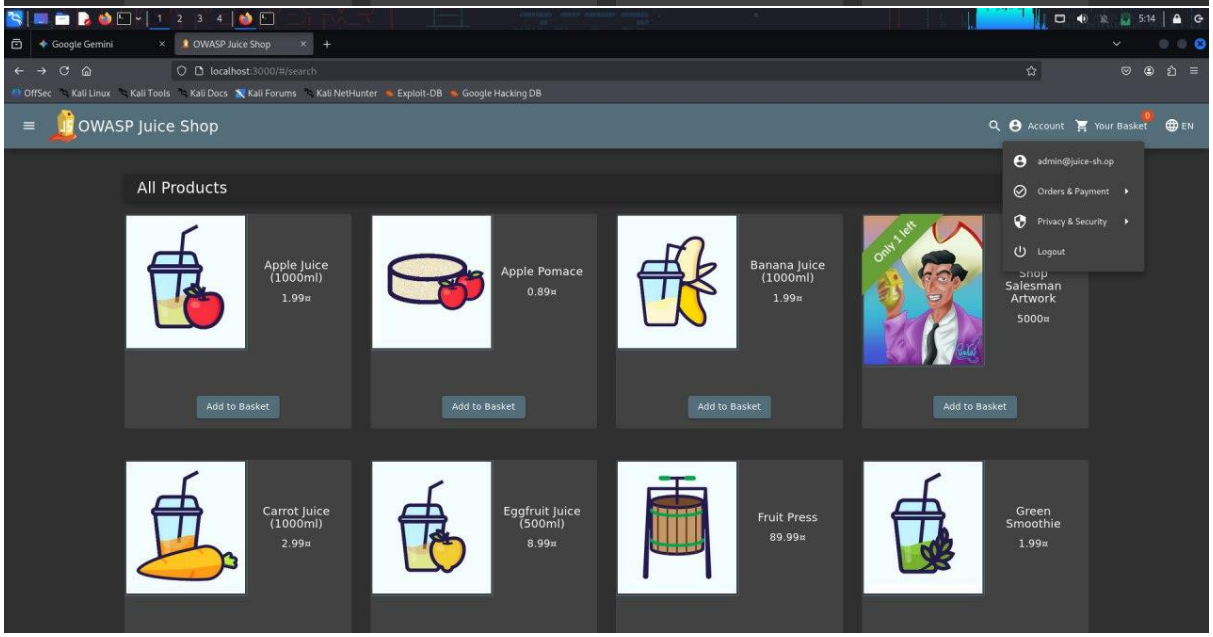

Google Gemini
OWASP Juice Shop
localhost:3000/#/login
OWASP Juice Shop
Account
EN
Login
[object ProgressEvent]
Email*
' OR 1=1 --
Password*
Forgot your password?
Log in
Remember me
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://localhost:3000
Select...
Use traditional spider:
Use ajax spider:
Always
with
Firefox
Attack
Stop
Progress:
Failed to attack the URL: Connect to http://localhost:3000 [localhost/127.0.0.1, localhost/0:0:0:0:0:0:0:1] failed: Connect timed out
History
Search
Alerts
Output
Alerts
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts
Main Proxy: localhost:8080
Current Status


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://localhost:3000
Select...
Use traditional spider:
Use ajax spider:
Always
with
Firefox
Attack
Stop
Progress:
Actively scanning (attacking) the URLs discovered by the spider(s)
History
Search
Alerts
Output
Spider
AJAX Spider
WebSockets
Active Scan
Alerts (15)
SQL Injection
Content Security Policy (CSP) Header Not Set (68)
Cross-Domain Misconfiguration (99)
Missing Anti-clickjacking Header (10)
Session ID in URL Rewrite (42)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (98)
Private IP Disclosure
Server Leaks Version Information via "Server" HTTP Response Header Field (2)
Strict-Transport-Security Header Not Set (2)
Timestamp Disclosure - Unix (163)
X-Content-Type-Options Header Missing (44)
Information Disclosure - Suspicious Comments (4)
Modern Web Application (50)
Retrieved from Cache (3)
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts
Main Proxy: localhost:8080
Current Status


mansoor@mansoor: ~
File Actions Edit View Help
^[[A
┌──(mansoor㉿mansoor)-[~]
└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
[sudo] password for mansoor:
info: Detected Node.js version v22.18.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 20 of 20 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file runtime.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
^C
┌──(mansoor㉿mansoor)-[~]
└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop-
[sudo] password for mansoor:
docker: invalid reference format.
See 'docker run --help'.
┌──(mansoor㉿mansoor)-[~]
└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
info: Detected Node.js version v22.18.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 20 of 20 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
info: Solved 1-star directoryListingChallenge (Confidential Document)
info: Cheat score for directoryListingChallenge solved in 0min (expected ~2min) with hints allowed and 100% expected preceding URL interaction: 0.8178583333333334
Error: Only .md and .pdf files are allowed!
at verify (/juice-shop/build/routes/fileServer.js:59:18)
at /juice-shop/build/routes/fileServer.js:43:13
at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)


OWASP Juice Shop
Account
Your Basket
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
Only 1 left
Salesman Artwork
5000¤
Add to Basket
Carrot Juice (1000ml)
2.99¤
Eggfruit Juice (500ml)
8.99¤
Fruit Press
89.99¤
Green Smoothie
1.99¤


OWASP Juice Shop
Account
Your Basket
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
Only 1 left
Salesman Artwork
5000¤
Add to Basket
Carrot Juice (1000ml)
2.99¤
Eggfruit Juice (500ml)
8.99¤
Fruit Press
89.99¤
Green Smoothie
1.99¤