WEB APPLICATION SECURITY ASSESSMENT REPORT

OWASP Juice Shop

Prepared For: Future Interns

Prepared By: Doddy Shivani

Email: d.shiv1922@gmail.com

Phone: +91-9703561119

Date: 22 October 2025

Version: 1.0

CONFIDENTIAL – This report contains sensitive information intended solely for authorized recipients. Unauthorized distribution is prohibited.

Vulnerability Assessment Report – OWASP Juice Shop

Executive Summary

A comprehensive **Vulnerability Assessment** was conducted on the **OWASP Juice Shop** web application, simulating real-world attack scenarios to uncover potential weaknesses.

During the assessment, **multiple Critical and High-severity vulnerabilities** were identified — the most severe being a **SQL Injection flaw** that allows **administrator authentication bypass**, granting **full control** over the application.

The current **security posture is rated as Critical**, and **immediate remediation** is strongly recommended to prevent **data breaches, privilege escalation, and system compromise**.

Scope & Methodology

Scope

Defines what was tested and what remained outside the assessment boundary.

- **In-Scope Target:** http://localhost:3000
- **Out-of-Scope:** All other company systems, networks, and infrastructure

Methodology

The testing process adhered to industry standards and followed a **risk-based approach** guided by the **OWASP Top 10 (2021)** framework.

- Employed both **manual penetration testing** and **automated vulnerability scanning** to ensure coverage of both business logic flaws and technical vulnerabilities.
- Every finding was validated, documented, and mapped to its **relevant OWASP category** for clarity and prioritization.

Tools Utilized

- **OWASP ZAP (v2.1x.x)** – Automated vulnerability scanning
- **Docker** – Application containerization and testing environment
- **Kali Linux** – Manual exploitation and testing toolkit
- **Mozilla Firefox** – Web interface testing and PoC verification

---

Detailed Findings

Finding 1: SQL Injection – Administrator Authentication Bypass

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

Description:
The login page’s email input field fails to sanitize user input, allowing **SQL commands to be injected** into backend queries. Attackers can manipulate the logic to **bypass authentication** and gain **administrator privileges**.

Proof of Concept (PoC):

1. Navigate to: http://localhost:3000/#/login
2. Enter payload in **Email field:** ' OR 1=1 --
3. Enter any password (e.g., password)
4. Click **“Log in”** → You are logged in as **admin@juice-sh.op**

Evidence:
📸 Screenshot showing successful login as admin using the injected payload.

Impact:

- Complete administrative takeover
- Exposure of all user data
- Ability to modify or delete products and records
- Full database compromise

Recommended Mitigation:
Implement **parameterized queries (prepared statements)** to strictly separate user input from SQL logic, preventing injection attacks.

Finding 2: Reflected Cross-Site Scripting (XSS)

- **Risk Level:** High
- **OWASP Mapping:** A03:2021 – Injection

Description:
The **search bar** fails to properly encode user-supplied input, allowing the injection of JavaScript code into the page.

PoC:
Enter the following payload in the search field:

```
<script>alert('XSS')</script>
```

Evidence:

Screenshot showing the alert popup executing in the browser.

Mitigation:
Apply **context-aware output encoding** before displaying any user data in HTML to prevent script execution.

Finding 3: Broken Access Control – Sensitive File Exposure

- **Risk Level:** Medium
- **OWASP Mapping:** A01:2021 – Broken Access Control

Description:
Unauthenticated users can access sensitive internal files by directly navigating to restricted directories.

PoC:
Visit: http://localhost:3000/ftp

Evidence:
Screenshot displaying directory listing with accessible files.

Mitigation:
Disable directory listing and enforce strict **authentication & authorization** checks on sensitive endpoints.

Finding 4: Missing Content Security Policy (CSP) Header

- **Risk Level:** Medium
- **OWASP Mapping:** A05:2021 – Security Misconfiguration

Description:
The application lacks a **CSP header**, allowing the browser to execute potentially malicious inline scripts or load untrusted resources.

PoC:
OWASP ZAP scan results indicating “CSP Header Not Set.”

Evidence:
Screenshot from OWASP ZAP “Alerts” panel highlighting the finding.

Mitigation:
Add a **Content Security Policy (CSP)** header to restrict allowed sources for scripts, images, and styles, reducing XSS attack risk.

OWASP Top 10 Vulnerability Mapping

OWASP Top 10 Category	Status	Associated 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	Missing CSP Header

Final Conclusion

The **security evaluation of the OWASP Juice Shop** application revealed multiple high-risk vulnerabilities capable of leading to **complete application compromise**.

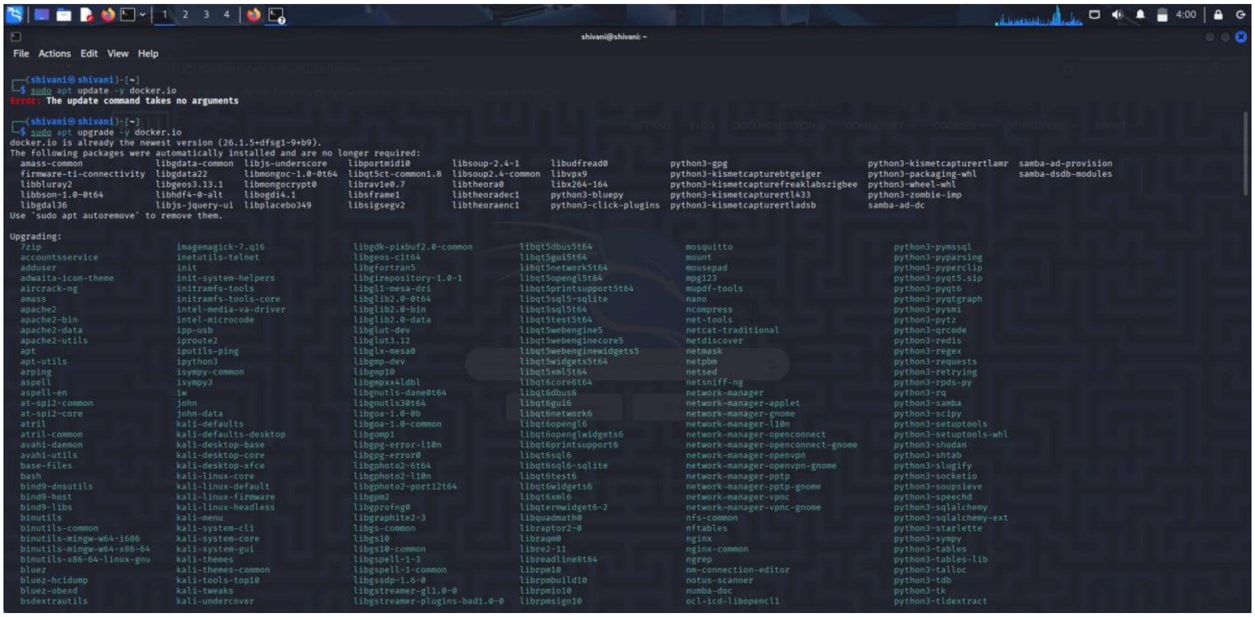
Particularly, the **SQL Injection** issue poses a **critical threat**, enabling attackers to gain unrestricted administrative access.

To enhance the application’s security posture, it is **imperative** to:

1. Immediately patch the **Critical** and **High** severity issues.
2. Conduct **secure code reviews** and **developer training** on OWASP best practices.

3. Reassess the application after remediation to verify fixes and prevent regression.

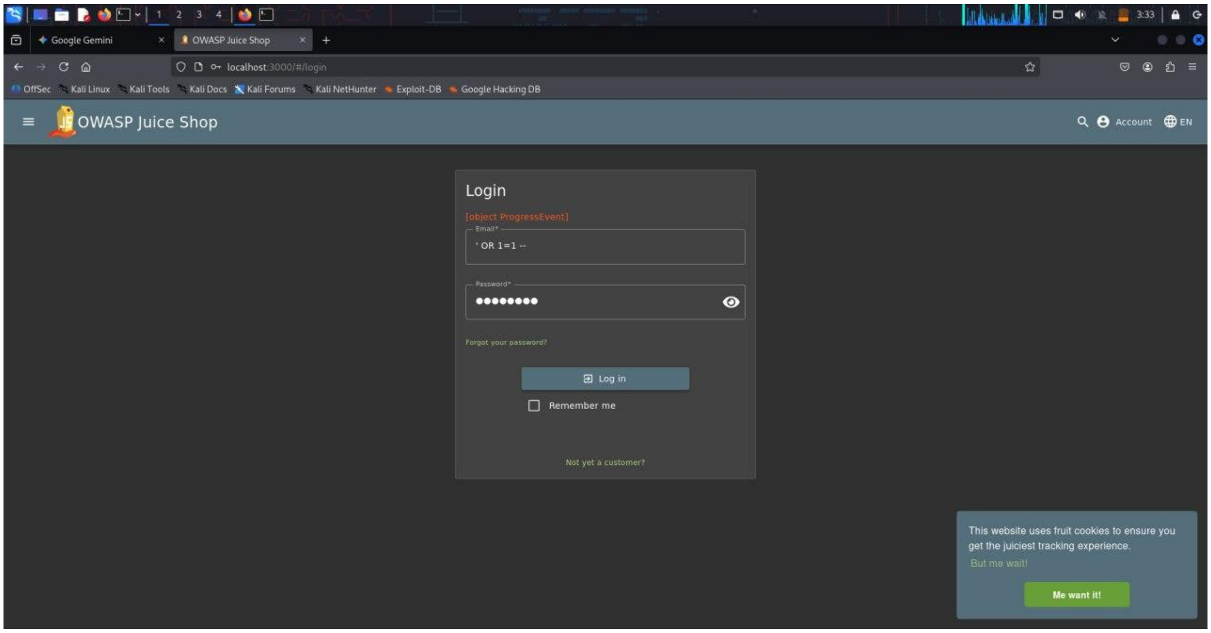
By implementing the recommended mitigations, the organization can significantly **reduce its attack surface** and **strengthen its resilience** against web-based threats.



```
┌──(shivani㉿shivani)-[~]
└─$ sudo apt update -y docker.io
Error: The update command takes no arguments

┌──(shivani㉿shivani)-[~]
└─$ sudo apt upgrade -y docker.io
docker.io is already the newest version (26.1.5+dfsg1-9+b9).
The following packages were automatically installed and are no longer required:
  amass-common              libgdata-common  libjs-underscore    libportmidi0        libsoup-2.4-1      libudfread0            python3-gpg                           python3-kismetcapturertlamr  samba-ad-provision
  firmware-ti-connectivity  libgdata22       libmongoc-1.0-0t64  libqt5ct-common1.8  libsoup2.4-common  libvpx9                python3-kismetcapturebtgeiger         python3-packaging-whl        samba-dsdb-modules
  libbluray2                libgeos3.13.1    libmongocrypt0      librav1e0.7         libtheora0         libx264-164            python3-kismetcapturefreaklabszigbee  python3-wheel-whl
  libbson-1.0-0t64          libhdf4-0-alt    libogdi4.1          libsframe1          libtheoradec1      python3-bluepy         python3-kismetcapturertl433           python3-zombie-imp
  libgdal36                 libjs-jquery-ui  libplacebo349       libsigsegv2         libtheoraenc1      python3-click-plugins  python3-kismetcapturertladsb          samba-ad-dc
Use 'sudo apt autoremove' to remove them.

Upgrading:
  7zip                          imagemagick-7.q16                 libgdk-pixbuf2.0-common         libqt5dbus5t64                  mosquitto                               python3-pymssql
  accountsservice               inetutils-telnet                  libgeos-c1t64                   libqt5gui5t64                   mount                                   python3-pyparsing
  adduser                       init                              libgfortran5                    libqt5network5t64               mousepad                                python3-pyperclip
  adwaita-icon-theme            init-system-helpers               libgirepository-1.0-1           libqt5opengl5t64                mpg123                                  python3-pyqt5.sip
  aircrack-ng                   initramfs-tools                   libgl1-mesa-dri                 libqt5printsupport5t64          mupdf-tools                             python3-pyqt6
  amass                         initramfs-tools-core              libglib2.0-0t64                 libqt5sql5-sqlite               nano                                    python3-pyqtgraph
  apache2                       intel-media-va-driver             libglib2.0-bin                  libqt5sql5t64                   ncompress                               python3-pysmi
  apache2-bin                   intel-microcode                   libglib2.0-data                 libqt5test5t64                  net-tools                               python3-pytz
  apache2-data                  ipp-usb                           libglut-dev                     libqt5webengine5                netcat-traditional                      python3-qrcode
  apache2-utils                 iproute2                          libglut3.12                     libqt5webenginecore5            netdiscover                             python3-redis
  apt                           iputils-ping                      libglx-mesa0                    libqt5webenginewidgets5         netmask                                 python3-regex
  apt-utils                     ipython3                          libgmp-dev                      libqt5widgets5t64               netpbm                                  python3-requests
  arping                        isympy-common                     libgmp10                        libqt5xml5t64                   netsed                                  python3-retrying
  aspell                        isympy3                           libgmpxx4ldbl                   libqt6core6t64                  netsniff-ng                             python3-rpds-py
  aspell-en                     iw                                libgnutls-dane0t64              libqt6dbus6                     network-manager                         python3-rq
  at-spi2-common                john                              libgnutls30t64                  libqt6gui6                      network-manager-applet                  python3-samba
  at-spi2-core                  john-data                         libgoa-1.0-0b                   libqt6network6                  network-manager-gnome                   python3-scipy
  atril                         kali-defaults                     libgoa-1.0-common               libqt6opengl6                   network-manager-l10n                    python3-setuptools
  atril-common                  kali-defaults-desktop             libgomp1                        libqt6openglwidgets6            network-manager-openconnect             python3-setuptools-whl
  avahi-daemon                  kali-desktop-base                 libgpg-error-l10n               libqt6printsupport6             network-manager-openconnect-gnome       python3-shodan
  avahi-utils                   kali-desktop-core                 libgpg-error0                   libqt6sql6                      network-manager-openvpn                 python3-shtab
  base-files                    kali-desktop-xfce                 libgphoto2-6t64                 libqt6sql6-sqlite               network-manager-openvpn-gnome           python3-slugify
  bash                          kali-linux-core                   libgphoto2-l10n                 libqt6test6                     network-manager-pptp                    python3-socketio
  bind9-dnsutils                kali-linux-default                libgphoto2-port12t64            libqt6widgets6                  network-manager-pptp-gnome              python3-soupsieve
  bind9-host                    kali-linux-firmware               libgpm2                         libqt6xml6                      network-manager-vpnc                    python3-speechd
  bind9-libs                    kali-linux-headless               libgprofng0                     libqtermwidget6-2               network-manager-vpnc-gnome              python3-sqlalchemy
  binutils                      kali-menu                         libgraphite2-3                  libquadmath0                    nfs-common                              python3-sqlalchemy-ext
  binutils-common               kali-system-cli                   libgs-common                    libraptor2-0                    nftables                                python3-starlette
  binutils-mingw-w64-i686       kali-system-core                  libgs10                         libraqm0                        nginx                                   python3-sympy
  binutils-mingw-w64-x86-64     kali-system-gui                   libgs10-common                  libre2-11                       nginx-common                            python3-tables
  binutils-x86-64-linux-gnu     kali-themes                       libgspell-1-3                   libreadline8t64                 ngrep                                   python3-tables-lib
  bluez                         kali-themes-common                libgspell-1-common              librpm10                        nm-connection-editor                    python3-talloc
  bluez-hcidump                 kali-tools-top10                  libgssdp-1.6-0                  librpmbuild10                   notus-scanner                           python3-tdb
  bluez-obexd                   kali-tweaks                       libgstreamer-gl1.0-0            librpmio10                      numba-doc                               python3-tk
  bsdextrautils                 kali-undercover                   libgstreamer-plugins-bad1.0-0   librpmsign10                    ocl-icd-libopencl1                      python3-tldextract
```



Login

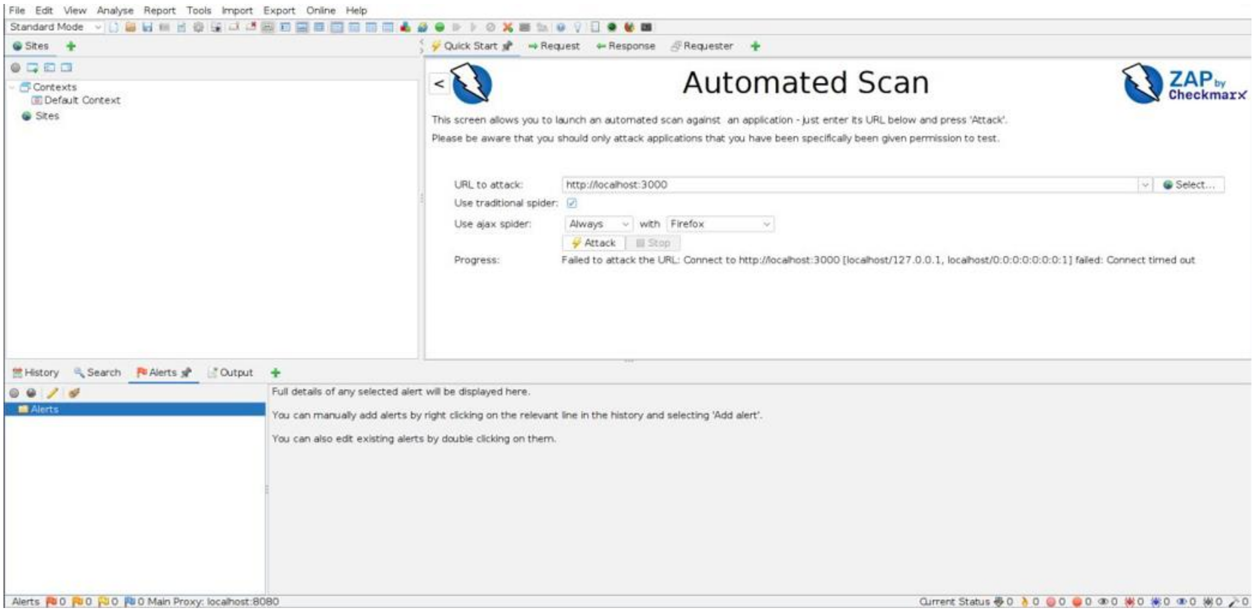
[object ProgressEvent]

Email*: ' OR 1=1 --

Password*: ••••••••

□ Remember me

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



Automated Scan

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

Use traditional spider: ☑

Use ajax spider: Always with Firefox

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

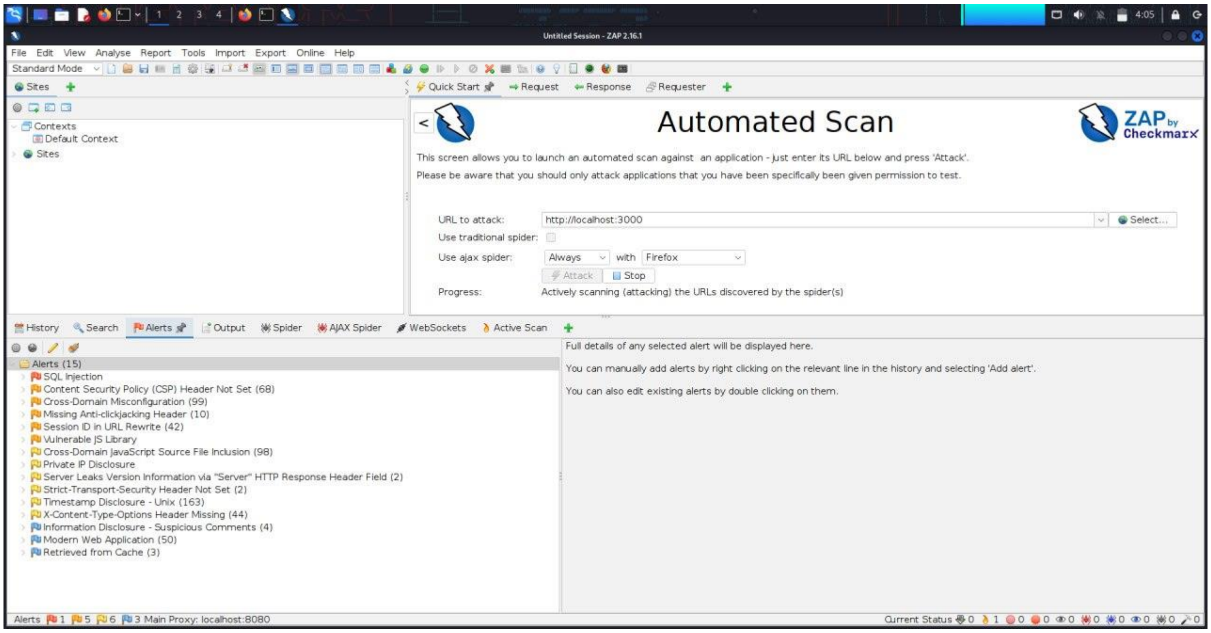
Full details of any selected alert will be displayed here.

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 0 0 0 0 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 0 0



Automated Scan

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

Use traditional spider: □

Use ajax spider: Always with Firefox

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

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)

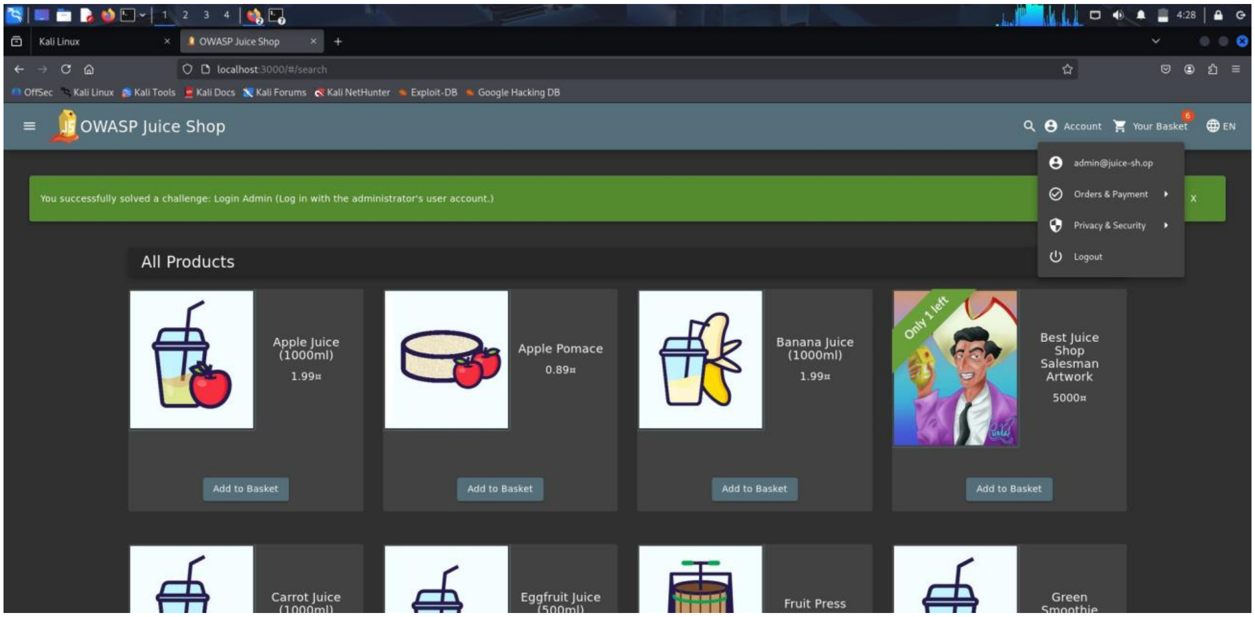
Full details of any selected alert will be displayed here.

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 1 5 6 3 Main Proxy: localhost:8080

Current Status 0 1 0 0 0 0 0 0 0 0



You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)