Container Security Assessment Report

OWASP Juice Shop Vulnerability Analysis

Date: September 8, 2025

Container Security Report

(Juice Shop & DVWA – Docker Security Testing with Trivy)

Project Setup

- **Tools:** Docker, Trivy, Kali Linux
- **Targets:**
    - `bkimminich/juice-shop`
    - `vulnerables/web-dvwa`

Commands Used:

```
 # Juice Shop
sudo docker run --rm -p 3000:3000 bkimminich/juice-shop

sudo trivy image bkimminich/juice-shop -f table -o juice-secrets.txt

sudo trivy image bkimminich/juice-shop -f json -o juice-full.json

# DVWA
sudo docker run --rm -p 8080:80 vulnerables/web-dvwa

sudo trivy image vulnerables/web-dvwa -f table -o dvwa-report.txt
```

```
sudo trivy image vulnerables/web-dvwa -f json -o dvwa-report.json
```

Container Security Report

(Juice Shop & DVWA – Docker Security Testing with Trivy)

Project Setup

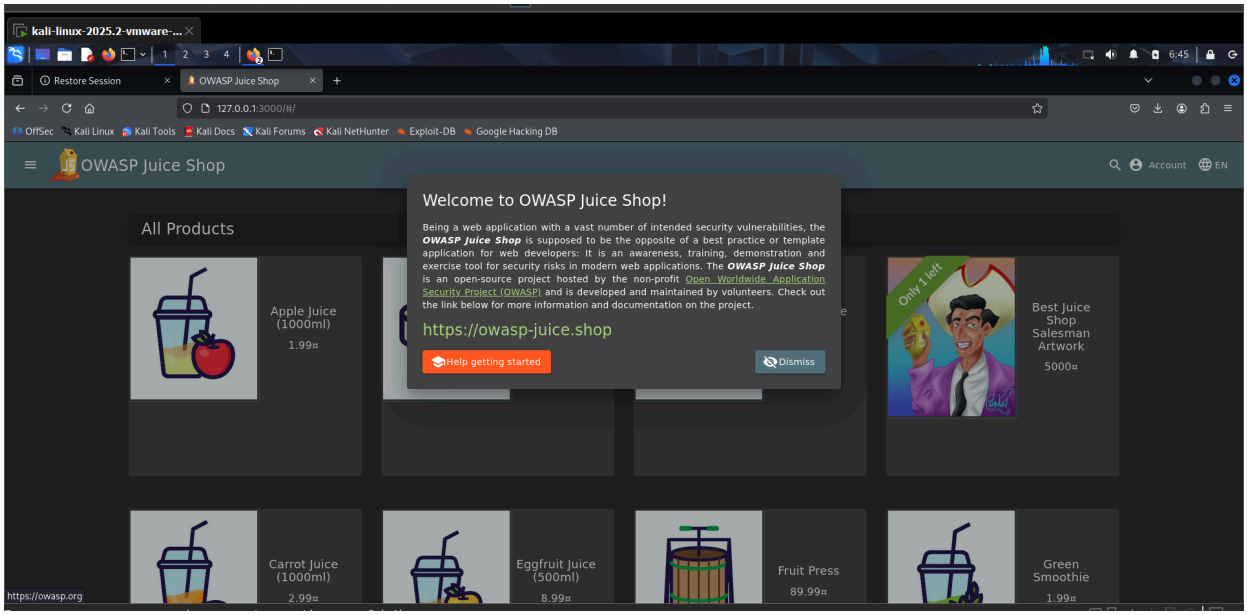
- **Tools:** Docker, Trivy, Kali Linux
- **Targets:**
    - `bkimminich/juice-shop`
    - `vulnerables/web-dvwa`

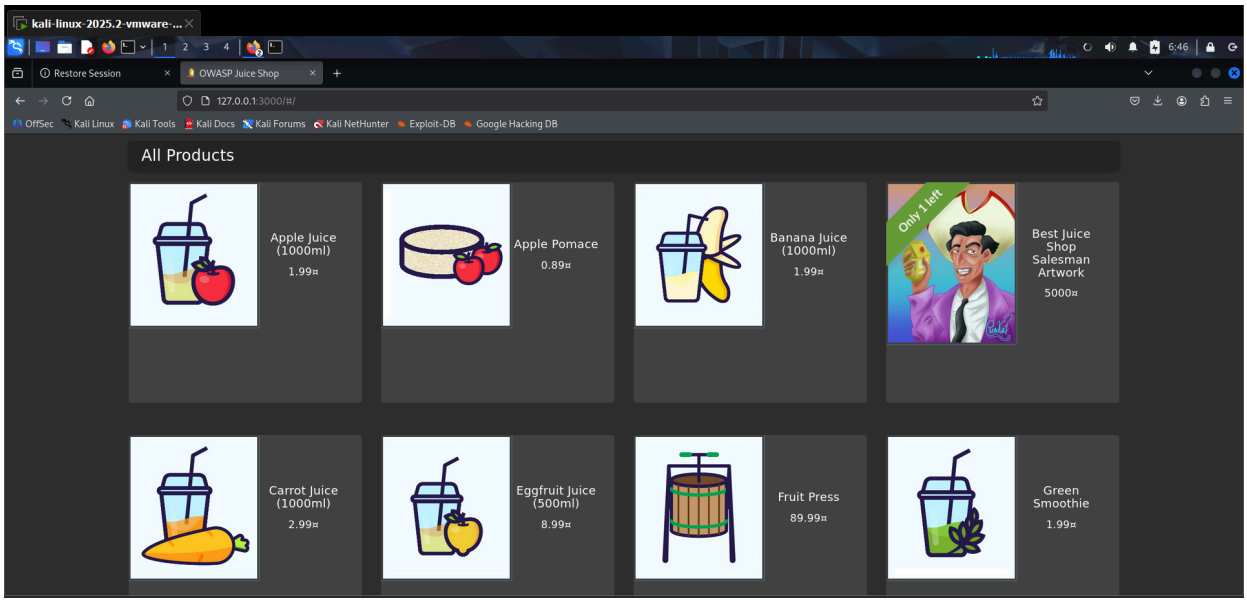
Commands Used:

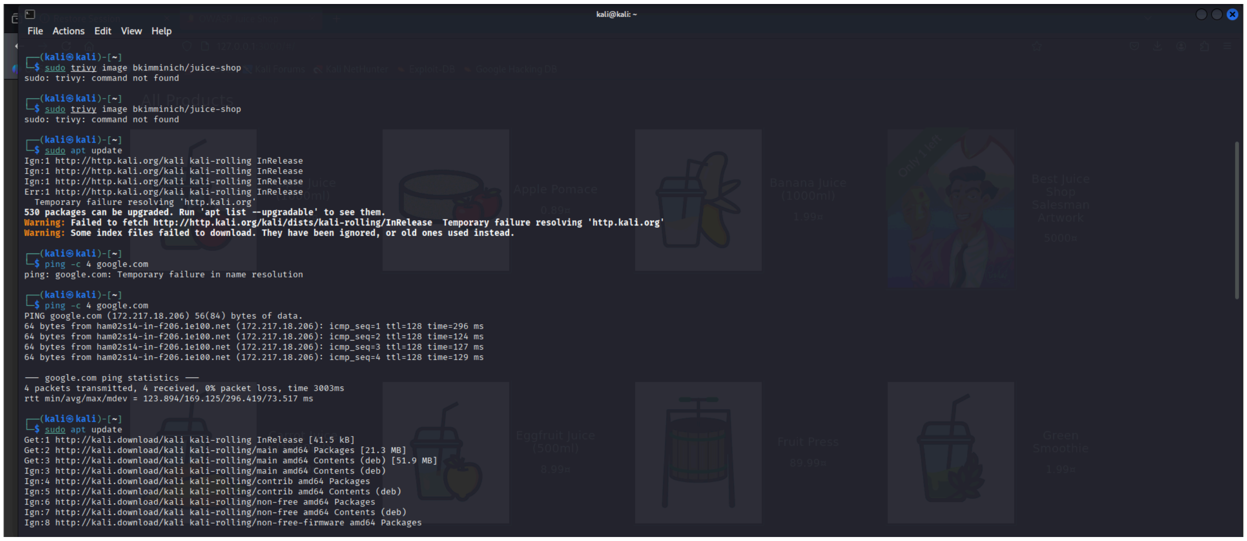
```
 # Juice Shop
Sudo update

Sudo apt install trivy -y

Trivy –version

sudo docker run --rm -p 3000:3000 bkimminich/juice-shop

sudo trivy image bkimminich/juice-shop -f table -o juice-secrets.txt

sudo trivy image bkimminich/juice-shop -f json -o juice-full.json

# DVWA
sudo docker run --rm -p 8080:80 vulnerables/web-dvwa
```

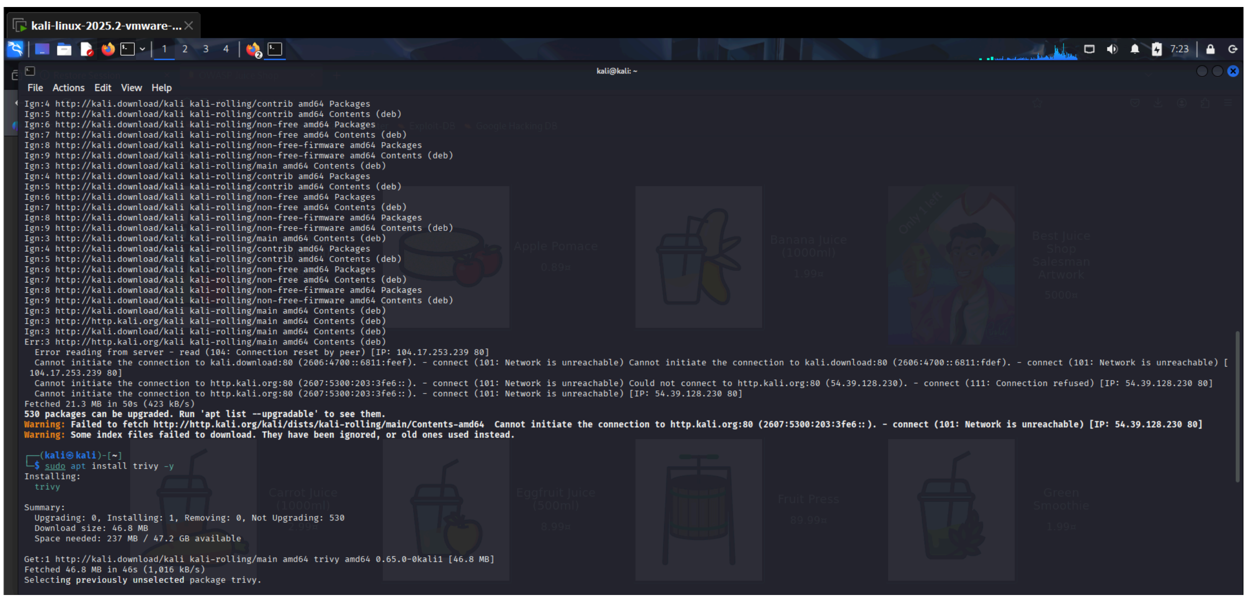
```
sudo trivy image vulnerables/web-dvwa -f table -o dvwa-report.txt
```

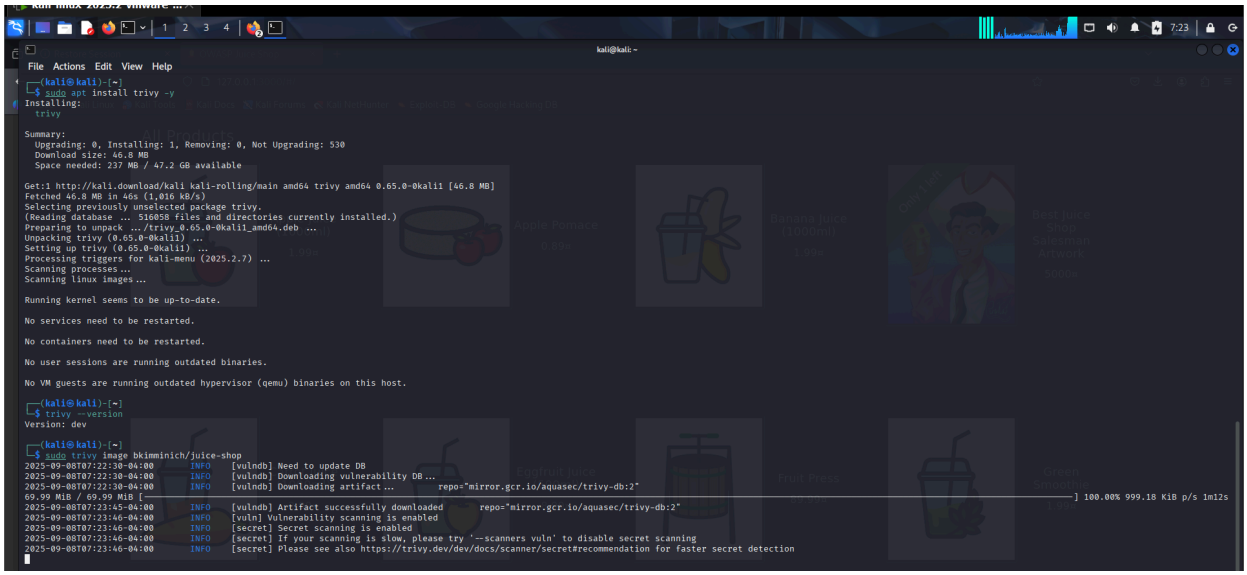
```
sudo trivy image vulnerables/web-dvwa -f json -o dvwa-report.json
```

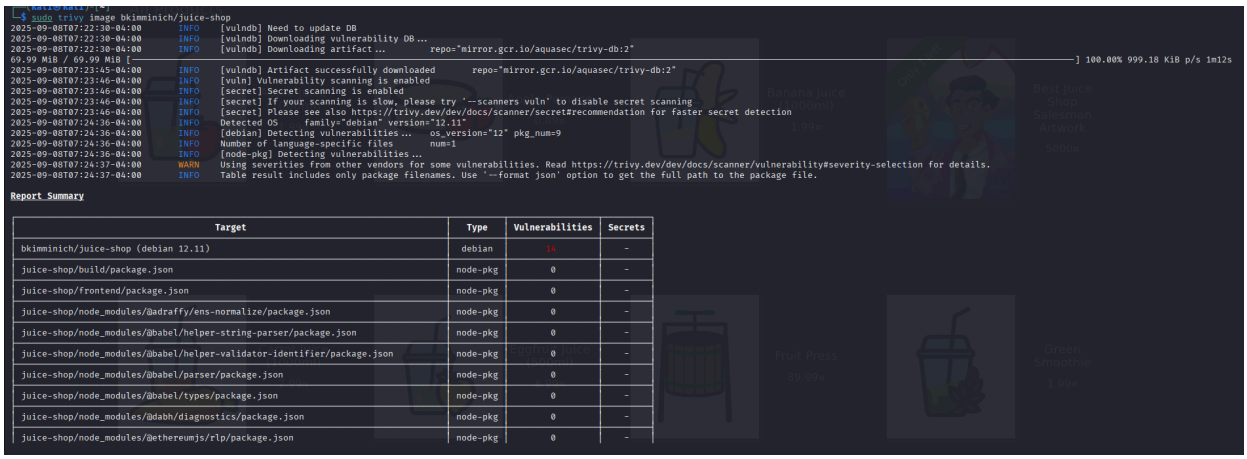





kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo trivy image bkimminich/juice-shop
sudo: trivy: command not found
┌──(kali㉿kali)-[~]
└─$ sudo trivy image bkimminich/juice-shop
sudo: trivy: command not found
┌──(kali㉿kali)-[~]
└─$ sudo apt update
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
Temporary failure resolving 'http.kali.org'
530 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease Temporary failure resolving 'http.kali.org'
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
┌──(kali㉿kali)-[~]
└─$ ping -c 4 google.com
ping: google.com: Temporary failure in name resolution
┌──(kali㉿kali)-[~]
└─$ ping -c 4 google.com
PING google.com (172.217.18.206) 56(84) bytes of data.
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=1 ttl=128 time=296 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=2 ttl=128 time=124 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=3 ttl=128 time=127 ms
64 bytes from ham02s14-in-f206.1e100.net (172.217.18.206): icmp_seq=4 ttl=128 time=129 ms
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 123.894/169.125/296.419/73.517 ms
┌──(kali㉿kali)-[~]
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.9 MB]
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Ign:4 http://kali.download/kali kali-rolling/contrib amd64 Packages
Ign:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb)
Ign:6 http://kali.download/kali kali-rolling/non-free amd64 Packages
Ign:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
Ign:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages

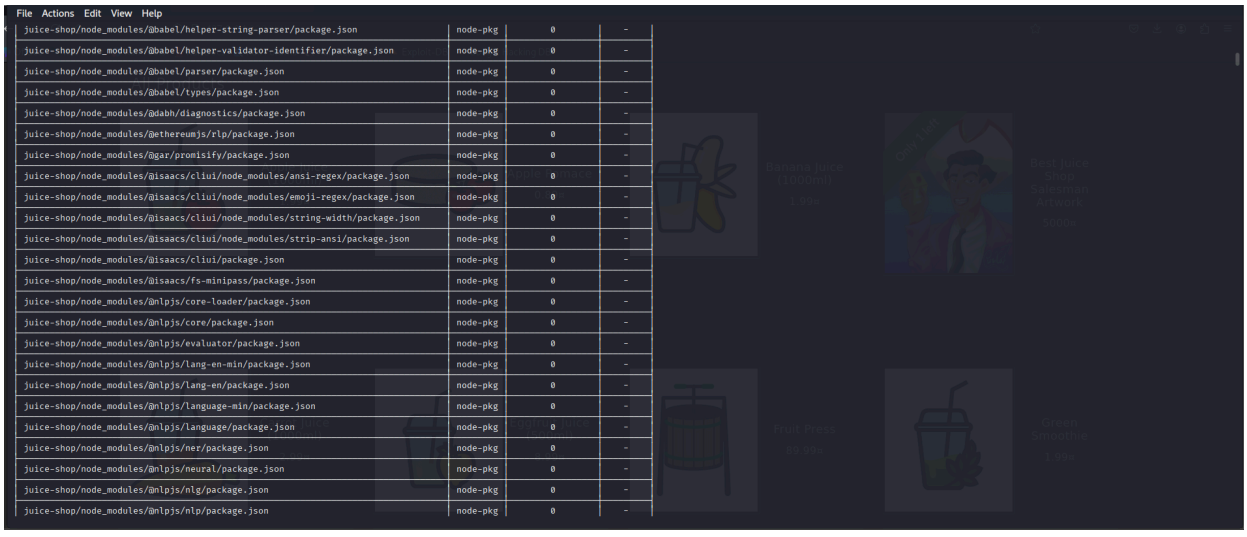

kali-linux-2025.2-vmware-...
kali@kali: ~
File Actions Edit View Help
Ign:4 http://kali.download/kali kali-rolling/contrib amd64 Packages
Ign:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb)
Ign:6 http://kali.download/kali kali-rolling/non-free amd64 Packages
Ign:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
Ign:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
Ign:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb)
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Ign:4 http://kali.download/kali kali-rolling/contrib amd64 Packages
Ign:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb)
Ign:6 http://kali.download/kali kali-rolling/non-free amd64 Packages
Ign:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
Ign:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
Ign:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb)
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Ign:4 http://kali.download/kali kali-rolling/contrib amd64 Packages
Ign:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb)
Ign:6 http://kali.download/kali kali-rolling/non-free amd64 Packages
Ign:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
Ign:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
Ign:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb)
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Ign:3 http://http.kali.org/kali kali-rolling/main amd64 Contents (deb)
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Err:3 http://http.kali.org/kali kali-rolling/main amd64 Contents (deb)
Error reading from server - read (104: Connection reset by peer) [IP: 104.17.253.239 80]
Cannot initiate the connection to kali.download:80 (2606:4700::6811:feef). - connect (101: Network is unreachable) Cannot initiate the connection to kali.download:80 (2606:4700::6811:fdef). - connect (101: Network is unreachable) [
104.17.253.239 80]
Cannot initiate the connection to http.kali.org:80 (2607:5300:203:3fe6::). - connect (101: Network is unreachable) Could not connect to http.kali.org:80 (54.39.128.230). - connect (111: Connection refused) [IP: 54.39.128.230 80]
Cannot initiate the connection to http.kali.org:80 (2607:5300:203:3fe6::). - connect (101: Network is unreachable) [IP: 54.39.128.230 80]
Fetched 21.3 MB in 50s (423 kB/s)
530 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/main/Contents-amd64 Cannot initiate the connection to http.kali.org:80 (2607:5300:203:3fe6::). - connect (101: Network is unreachable) [IP: 54.39.128.230 80]
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
┌──(kali㉿kali)-[~]
└─$ sudo apt install trivy -y
Installing:
trivy
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 530
Download size: 46.8 MB
Space needed: 237 MB / 47.2 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 trivy amd64 0.65.0-0kali1 [46.8 MB]
Fetched 46.8 MB in 46s (1,016 kB/s)
Selecting previously unselected package trivy.





Report Summary

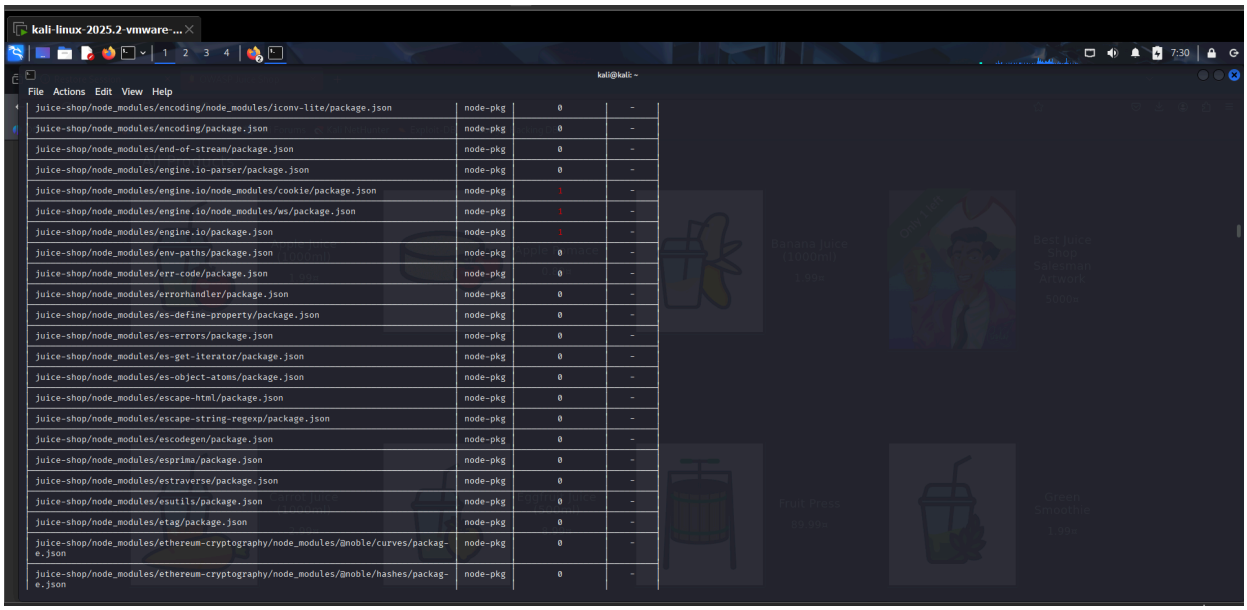
Target	Type	Vulnerabilities	Secrets
bkimminich/juice-shop (debian 12.11)	debian	14	-
juice-shop/build/package.json	node-pkg	0	-
juice-shop/frontend/package.json	node-pkg	0	-
juice-shop/node_modules/@adraffy/ens-normalize/package.json	node-pkg	0	-
juice-shop/node_modules/@babel/helper-string-parser/package.json	node-pkg	0	-
juice-shop/node_modules/@babel/helper-validator-identifier/package.json	node-pkg	0	-
juice-shop/node_modules/@babel/parser/package.json	node-pkg	0	-
juice-shop/node_modules/@babel/types/package.json	node-pkg	0	-
juice-shop/node_modules/@dabh/diagnostics/package.json	node-pkg	0	-
juice-shop/node_modules/@ethereumjs/rlp/package.json	node-pkg	0	-



juice-shop/node_modules/@babel/helper-string-parser/package.json	node-pkg	0	-
juice-shop/node_modules/@babel/helper-validator-identifier/package.json	node-pkg	0	-
juice-shop/node_modules/@babel/parser/package.json	node-pkg	0	-
juice-shop/node_modules/@babel/types/package.json	node-pkg	0	-
juice-shop/node_modules/@dabh/diagnostics/package.json	node-pkg	0	-
juice-shop/node_modules/@ethereumjs/rlp/package.json	node-pkg	0	-
juice-shop/node_modules/@gar/promisify/package.json	node-pkg	0	-
juice-shop/node_modules/@isaacs/cliui/node_modules/ansi-regex/package.json	node-pkg	0	-
juice-shop/node_modules/@isaacs/cliui/node_modules/emoji-regex/package.json	node-pkg	0	-
juice-shop/node_modules/@isaacs/cliui/node_modules/string-width/package.json	node-pkg	0	-
juice-shop/node_modules/@isaacs/cliui/node_modules/strip-ansi/package.json	node-pkg	0	-
juice-shop/node_modules/@isaacs/cliui/package.json	node-pkg	0	-
juice-shop/node_modules/@isaacs/fs-minipass/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/core-loader/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/core/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/evaluator/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/lang-en-min/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/lang-en/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/language-min/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/language/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/ner/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/neural/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/nlg/package.json	node-pkg	0	-
juice-shop/node_modules/@nlpjs/nlp/package.json	node-pkg	0	-


kali@kali: ~
File Actions Edit View Help
juice-shop/node_modules/base64-js/package.json node-pkg 0 -
juice-shop/node_modules/base64id/package.json node-pkg 0 -
juice-shop/node_modules/base64url/package.json node-pkg 2 -
juice-shop/node_modules/batch/package.json node-pkg 0 -
juice-shop/node_modules/big-integer/package.json node-pkg 0 -
juice-shop/node_modules/binary-extensions/package.json node-pkg 0 -
juice-shop/node_modules/binary/package.json node-pkg 0 -
juice-shop/node_modules/bindings/package.json node-pkg 0 -
juice-shop/node_modules/bintrees/package.json node-pkg 0 -
juice-shop/node_modules/bl/package.json node-pkg 0 -
juice-shop/node_modules/bluebird/package.json node-pkg 0 -
juice-shop/node_modules/body-parser/node_modules/debug/package.json node-pkg 0 -
juice-shop/node_modules/body-parser/node_modules/ms/package.json node-pkg 0 -
juice-shop/node_modules/body-parser/package.json node-pkg 0 -
juice-shop/node_modules/bower-config/node_modules/minimist/package.json node-pkg 0 -
juice-shop/node_modules/bower-config/package.json node-pkg 0 -
juice-shop/node_modules/brace-expansion/package.json node-pkg 0 -
juice-shop/node_modules/braces/node_modules/extend-shallow/package.json node-pkg 0 -
juice-shop/node_modules/braces/node_modules/is-extendable/package.json node-pkg 0 -
juice-shop/node_modules/braces/package.json node-pkg 1 -
juice-shop/node_modules/brotli/package.json node-pkg 0 -
juice-shop/node_modules/buffer-alloc-unsafe/package.json node-pkg 0 -
juice-shop/node_modules/buffer-alloc/package.json node-pkg 0 -
juice-shop/node_modules/buffer-crc32/package.json node-pkg 0 -

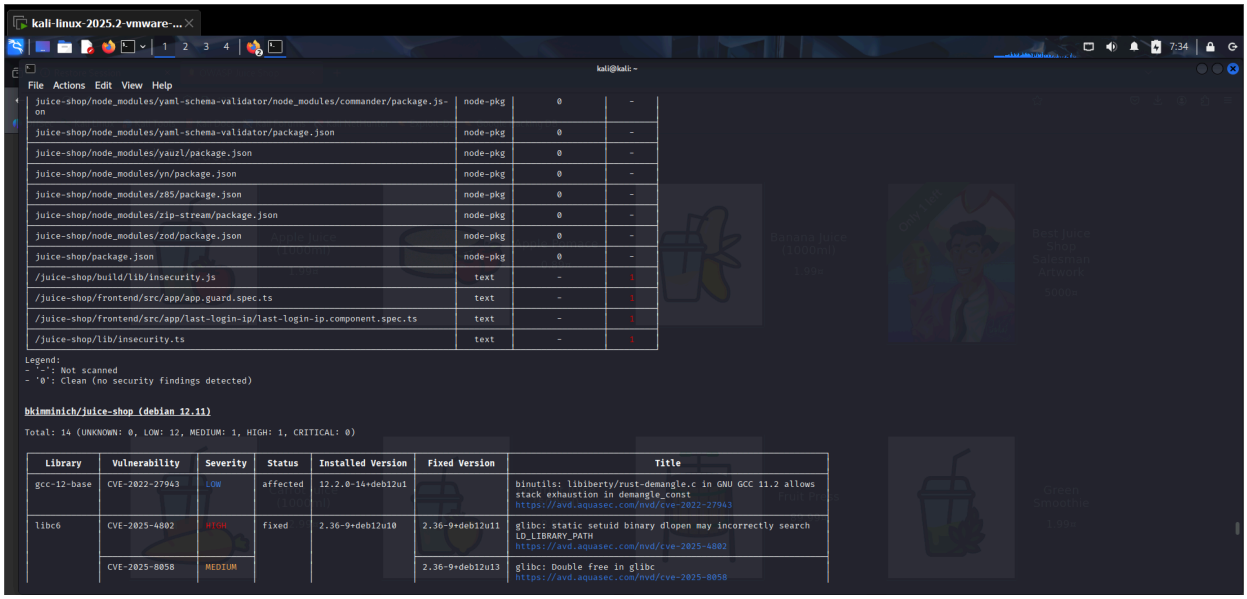

kali-linux-2025.2-vmware-...
1 2 3 4
7:30
kali@kali: ~
File Actions Edit View Help
juice-shop/node_modules/cross-fetch/package.json node-pkg 0 -
juice-shop/node_modules/cross-fetch/polyfill/package.json node-pkg 0 -
juice-shop/node_modules/cross-spawn/package.json node-pkg 0 -
juice-shop/node_modules/crypto-js/package.json node-pkg 1 -
juice-shop/node_modules/dateformat/package.json node-pkg 0 -
juice-shop/node_modules/debug/package.json node-pkg 0 -
juice-shop/node_modules/decamelize/package.json node-pkg 0 -
juice-shop/node_modules/decode-uri-component/package.json node-pkg 0 -
juice-shop/node_modules/decompress-response/package.json node-pkg 0 -
juice-shop/node_modules/decompress-tar/node_modules/file-type/package.json node-pkg 0 -
juice-shop/node_modules/decompress-tar/package.json node-pkg 0 -
juice-shop/node_modules/decompress-tarbz2/node_modules/file-type/package.json node-pkg 0 -
juice-shop/node_modules/decompress-tarbz2/package.json node-pkg 0 -
juice-shop/node_modules/decompress-targz/node_modules/file-type/package.json node-pkg 0 -
juice-shop/node_modules/decompress-targz/package.json node-pkg 0 -
juice-shop/node_modules/decompress-unzip/node_modules/file-type/package.json node-pkg 0 -
juice-shop/node_modules/decompress-unzip/node_modules/get-stream/package.json node-pkg 0 -
juice-shop/node_modules/decompress-unzip/node_modules/pify/package.json node-pkg 0 -
juice-shop/node_modules/decompress-unzip/package.json node-pkg 0 -
juice-shop/node_modules/decompress/node_modules/make-dir/node_modules/pify/package.json node-pkg 0 -
juice-shop/node_modules/decompress/node_modules/make-dir/package.json node-pkg 0 -
juice-shop/node_modules/decompress/node_modules/pify/package.json node-pkg 0 -
juice-shop/node_modules/decompress/package.json node-pkg 0 -


kali-linux-2025.2-vmware-...
kali@kali: ~
File Actions Edit View Help
juice-shop/node_modules/encoding/node_modules/iconv-lite/package.json node-pkg 0 -
juice-shop/node_modules/encoding/package.json node-pkg 0 -
juice-shop/node_modules/end-of-stream/package.json node-pkg 0 -
juice-shop/node_modules/engine.io-parser/package.json node-pkg 0 -
juice-shop/node_modules/engine.io/node_modules/cookie/package.json node-pkg 1 -
juice-shop/node_modules/engine.io/node_modules/ws/package.json node-pkg 1 -
juice-shop/node_modules/engine.io/package.json node-pkg 1 -
juice-shop/node_modules/env-paths/package.json node-pkg 0 -
juice-shop/node_modules/err-code/package.json node-pkg 0 -
juice-shop/node_modules/errorhandler/package.json node-pkg 0 -
juice-shop/node_modules/es-define-property/package.json node-pkg 0 -
juice-shop/node_modules/es-errors/package.json node-pkg 0 -
juice-shop/node_modules/es-get-iterator/package.json node-pkg 0 -
juice-shop/node_modules/es-object-atoms/package.json node-pkg 0 -
juice-shop/node_modules/escape-html/package.json node-pkg 0 -
juice-shop/node_modules/escape-string-regexp/package.json node-pkg 0 -
juice-shop/node_modules/escodegen/package.json node-pkg 0 -
juice-shop/node_modules/esprima/package.json node-pkg 0 -
juice-shop/node_modules/estraverse/package.json node-pkg 0 -
juice-shop/node_modules/esutils/package.json node-pkg 0 -
juice-shop/node_modules/etag/package.json node-pkg 0 -
juice-shop/node_modules/ethereum-cryptography/node_modules/@noble/curves/package.json node-pkg 0 -
juice-shop/node_modules/ethereum-cryptography/node_modules/@noble/hashes/package.json node-pkg 0 -


kali@kali: ~
File Actions Edit View Help
juice-shop/node_modules/express-jwt/node_modules/jsonwebtoken/package.json node-pkg 5 -
juice-shop/node_modules/express-jwt/node_modules/moment/package.json node-pkg 3 -
juice-shop/node_modules/express-jwt/package.json node-pkg 1 -
juice-shop/node_modules/express-rate-limit/package.json node-pkg 0 -
juice-shop/node_modules/express-robots-txt/package.json node-pkg 0 -
juice-shop/node_modules/express-security.txt/package.json node-pkg 0 -
juice-shop/node_modules/express/node_modules/cookie/package.json node-pkg 0 -
juice-shop/node_modules/express/node_modules/debug/package.json node-pkg 0 -
juice-shop/node_modules/express/node_modules/ms/package.json node-pkg 0 -
juice-shop/node_modules/express/package.json node-pkg 0 -
juice-shop/node_modules/ext-list/package.json node-pkg 0 -
juice-shop/node_modules/ext-name/package.json node-pkg 0 -
juice-shop/node_modules/extend-shallow/package.json node-pkg 0 -
juice-shop/node_modules/extend/package.json node-pkg 0 -
juice-shop/node_modules/extglob/node_modules/define-property/package.json node-pkg 0 -
juice-shop/node_modules/extglob/node_modules/extend-shallow/package.json node-pkg 0 -
juice-shop/node_modules/extglob/node_modules/is-extendable/package.json node-pkg 0 -
juice-shop/node_modules/extglob/package.json node-pkg 0 -
juice-shop/node_modules/fast.js/package.json node-pkg 0 -
juice-shop/node_modules/fd-slicer/package.json node-pkg 0 -
juice-shop/node_modules/feature-policy/package.json node-pkg 0 -
juice-shop/node_modules/fecha/package.json node-pkg 0 -
juice-shop/node_modules/file-js/docconfig/template/package.json node-pkg 0 -

File Actions Edit View Help

juice-shop/node_modules/sanitize-html/node_modules/he/package.json	node-pkg	0	-
juice-shop/node_modules/sanitize-html/node_modules/htmlparser2/package.json	node-pkg	0	-
juice-shop/node_modules/sanitize-html/node_modules/isarray/package.json	node-pkg	0	-
juice-shop/node_modules/sanitize-html/node_modules/lodash/package.json	node-pkg	0	-
juice-shop/node_modules/sanitize-html/node_modules/readable-stream/package.json	node-pkg	0	-
juice-shop/node_modules/sanitize-html/node_modules/string_decoder/package.json	node-pkg	0	-
juice-shop/node_modules/sanitize-html/package.json	node-pkg	0	-
juice-shop/node_modules/sax/package.json	node-pkg	0	-
juice-shop/node_modules/seek-bzip/node_modules/commander/package.json	node-pkg	0	-
juice-shop/node_modules/seek-bzip/package.json	node-pkg	0	-
juice-shop/node_modules/semver/package.json	node-pkg	0	-
juice-shop/node_modules/send/node_modules/debug/node_modules/ms/package.json	node-pkg	0	-
juice-shop/node_modules/send/node_modules/debug/package.json	node-pkg	0	-
juice-shop/node_modules/send/node_modules/encodeurl/package.json	node-pkg	0	-
juice-shop/node_modules/send/package.json	node-pkg	0	-
juice-shop/node_modules/sequelize-pool/package.json	node-pkg	0	-
juice-shop/node_modules/sequelize/package.json	node-pkg	0	-
juice-shop/node_modules/serve-index/node_modules/debug/package.json	node-pkg	0	-
juice-shop/node_modules/serve-index/node_modules/depd/package.json	node-pkg	0	-
juice-shop/node_modules/serve-index/node_modules/http-errors/package.json	node-pkg	0	-
juice-shop/node_modules/serve-index/node_modules/inherits/package.json	node-pkg	0	-
juice-shop/node_modules/serve-index/node_modules/ms/package.json	node-pkg	0	-
juice-shop/node_modules/serve-index/node_modules/setprototypeof/package.json	node-pkg	0	-



kali-linux-2025.2-vmware-...

File Actions Edit View Help

kali@kali: ~

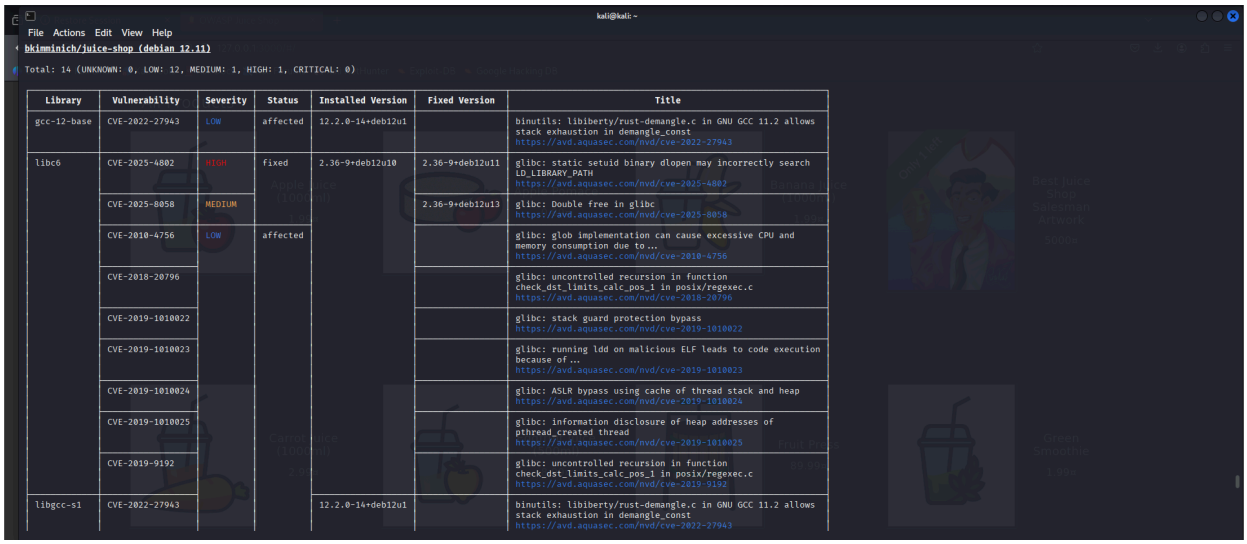
juice-shop/node_modules/yaml-schema-validator/node_modules/commander/package.json	node-pkg	0	-
juice-shop/node_modules/yaml-schema-validator/package.json	node-pkg	0	-
juice-shop/node_modules/yauzl/package.json	node-pkg	0	-
juice-shop/node_modules/yn/package.json	node-pkg	0	-
juice-shop/node_modules/z85/package.json	node-pkg	0	-
juice-shop/node_modules/zip-stream/package.json	node-pkg	0	-
juice-shop/node_modules/zod/package.json	node-pkg	0	-
juice-shop/package.json	node-pkg	0	-
/juice-shop/build/lib/insecurity.js	text	-	1
/juice-shop/frontend/src/app/app.guard.spec.ts	text	-	1
/juice-shop/frontend/src/app/last-login-ip/last-login-ip.component.spec.ts	text	-	1
/juice-shop/lib/insecurity.ts	text	-	1

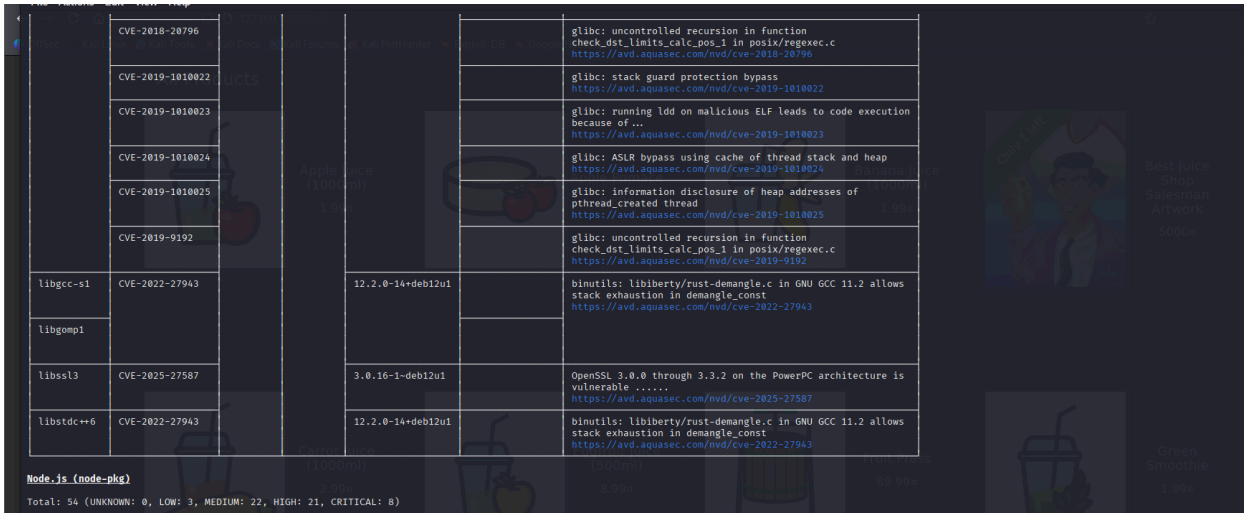
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

bkimminich/juice-shop (debian 12.11)

Total: 14 (UNKNOWN: 0, LOW: 12, MEDIUM: 1, HIGH: 1, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
gcc-12-base	CVE-2022-27943	LOW	affected	12.2.0-14+deb12u1		binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943
libc6	CVE-2025-4802	HIGH	fixed	2.36-9+deb12u10	2.36-9+deb12u11	glibc: static setuid binary dlopen may incorrectly search LD_LIBRARY_PATH https://avd.aquasec.com/nvd/cve-2025-4802
	CVE-2025-8058	MEDIUM			2.36-9+deb12u13	glibc: Double free in glibc https://avd.aquasec.com/nvd/cve-2025-8058


kali@kali: ~
File Actions Edit View Help
bkimminich/juice-shop (debian 12.11)
Total: 14 (UNKNOWN: 0, LOW: 12, MEDIUM: 1, HIGH: 1, CRITICAL: 0)
Library | Vulnerability | Severity | Status | Installed Version | Fixed Version | Title
gcc-12-base | CVE-2022-27943 | LOW | affected | 12.2.0-14+deb12u1 | | binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943
libc6 | CVE-2025-4802 | HIGH | fixed | 2.36-9+deb12u10 | 2.36-9+deb12u11 | glibc: static setuid binary dlopen may incorrectly search LD_LIBRARY_PATH https://avd.aquasec.com/nvd/cve-2025-4802
CVE-2025-8058 | MEDIUM | | 2.36-9+deb12u13 | glibc: Double free in glibc https://avd.aquasec.com/nvd/cve-2025-8058
CVE-2010-4756 | LOW | affected | | glibc: glob implementation can cause excessive CPU and memory consumption due to ... https://avd.aquasec.com/nvd/cve-2010-4756
CVE-2018-20796 | | | | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2018-20796
CVE-2019-1010022 | | | | glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022
CVE-2019-1010023 | | | | glibc: running ldd on malicious ELF leads to code execution because of ... https://avd.aquasec.com/nvd/cve-2019-1010023
CVE-2019-1010024 | | | | glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
CVE-2019-1010025 | | | | glibc: information disclosure of heap addresses of pthread_created thread https://avd.aquasec.com/nvd/cve-2019-1010025
CVE-2019-9192 | | | | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2019-9192
libgcc-s1 | CVE-2022-27943 | | 12.2.0-14+deb12u1 | | binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943


CVE-2018-20796 | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2018-20796
CVE-2019-1010022 | glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022
CVE-2019-1010023 | glibc: running ldd on malicious ELF leads to code execution because of ... https://avd.aquasec.com/nvd/cve-2019-1010023
CVE-2019-1010024 | glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
CVE-2019-1010025 | glibc: information disclosure of heap addresses of pthread_created thread https://avd.aquasec.com/nvd/cve-2019-1010025
CVE-2019-9192 | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2019-9192
libgcc-s1 | CVE-2022-27943 | 12.2.0-14+deb12u1 | binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943
libgomp1
libssl3 | CVE-2025-27587 | 3.0.16-1~deb12u1 | OpenSSL 3.0.0 through 3.3.2 on the PowerPC architecture is vulnerable https://avd.aquasec.com/nvd/cve-2025-27587
libstdc++6 | CVE-2022-27943 | 12.2.0-14+deb12u1 | binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943
Node.js (node-pkg)
Total: 54 (UNKNOWN: 0, LOW: 3, MEDIUM: 22, HIGH: 21, CRITICAL: 8)


kali@kali: ~
File Actions Edit View Help
Library | Vulnerability | Severity | Status | Installed Version | Fixed Version | Title
base64url (package.json) | NSWG-ECO-428 | HIGH | fixed | 0.0.6 | >=3.0.0 | Out-of-bounds Read https://hackerone.com/reports/321687
GHSA-rvg8-pwq2-xj7q | MEDIUM | | | 3.0.0 | Out-of-bounds Read in base64url https://github.com/advisories/GHSA-rvg8-pwq2-xj7q
braces (package.json) | CVE-2024-4068 | HIGH | | 2.3.2 | 3.0.3 | braces: fails to limit the number of characters it can handle https://avd.aquasec.com/nvd/cve-2024-4068
cookie (package.json) | CVE-2024-47764 | LOW | | 0.4.2 | 0.7.0 | cookie: cookie accepts cookie name, path, and domain with out of bounds ... https://avd.aquasec.com/nvd/cve-2024-47764
crypto-js (package.json) | CVE-2023-46233 | CRITICAL | | 3.3.0 | 4.2.0 | crypto-js: PBKDF2 1,000 times weaker than specified in 1993 and 1.3M times ... https://avd.aquasec.com/nvd/cve-2023-46233
engine.io (package.json) | CVE-2022-41940 | MEDIUM | | 4.1.2 | 3.6.1, 6.2.1 | engine.io: Specially crafted HTTP request can trigger an uncaught exception https://avd.aquasec.com/nvd/cve-2022-41940
express-jwt (package.json) | CVE-2020-15084 | HIGH | | 0.1.3 | 6.0.0 | Authorization bypass in express-jwt https://avd.aquasec.com/nvd/cve-2020-15084
got (package.json) | CVE-2022-33987 | MEDIUM | | 8.3.2 | 12.1.0, 11.8.5 | nodejs-got: missing verification of requested URLs allows redirects to UNIX sockets https://avd.aquasec.com/nvd/cve-2022-33987
http-cache-semantics (package.json) | CVE-2022-25881 | HIGH | | 3.8.1 | 4.1.1 | http-cache-semantics: Regular Expression Denial of Service (ReDoS) vulnerability https://avd.aquasec.com/nvd/cve-2022-25881
ip (package.json) | CVE-2024-29415 | | affected | 2.0.1 | | node-ip: Incomplete fix for CVE-2023-42282 https://avd.aquasec.com/nvd/cve-2024-29415
jsonwebtoken (package.json) | CVE-2015-9235 | CRITICAL | fixed | 0.1.0 | 4.2.2 | nodejs-jsonwebtoken: verification step bypass with an altered token https://avd.aquasec.com/nvd/cve-2015-9235
CVE-2022-23539 | HIGH | | | | 9.0.0 | jsonwebtoken: Unrestricted key type could lead to legacy keys usagen https://avd.aquasec.com/nvd/cve-2022-23539
NSWG-ECO-17 | | | | | >=4.2.2 | Verification Bypass

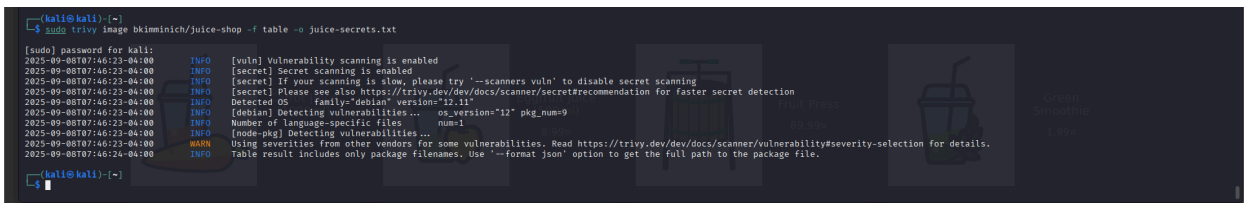
						https://avd.aquasec.com/nvd/cve-2023-46233
engine.io (package.json)	CVE-2022-41940	MEDIUM		4.1.2	3.6.1, 6.2.1	engine.io: Specially crafted HTTP request can trigger an uncaught exception https://avd.aquasec.com/nvd/cve-2022-41940
express-jwt (package.json)	CVE-2020-15084	HIGH		0.1.3	6.0.0	Authorization bypass in express-jwt https://avd.aquasec.com/nvd/cve-2020-15084
got (package.json)	CVE-2022-33987	MEDIUM		8.3.2	12.1.0, 11.8.5	nodejs-got: missing verification of requested URLs allows redirects to UNIX sockets https://avd.aquasec.com/nvd/cve-2022-33987
http-cache-semantics (package.json)	CVE-2022-25881	HIGH		3.8.1	4.1.1	http-cache-semantics: Regular Expression Denial of Service (ReDoS) vulnerability https://avd.aquasec.com/nvd/cve-2022-25881
ip (package.json)	CVE-2024-29415		affected	2.0.1		node-ip: Incomplete fix for CVE-2023-42282 https://avd.aquasec.com/nvd/cve-2024-29415
jsonwebtoken (package.json)	CVE-2015-9235	CRITICAL	fixed	0.1.0	4.2.2	nodejs-jsonwebtoken: verification step bypass with an altered token https://avd.aquasec.com/nvd/cve-2015-9235
	CVE-2022-23539	HIGH			9.0.0	jsonwebtoken: Unrestricted key type could lead to legacy keys usagen https://avd.aquasec.com/nvd/cve-2022-23539
	NSWG-ECO-17				⩾4.2.2	Verification Bypass
	CVE-2022-23540	MEDIUM			9.0.0	jsonwebtoken: Insecure default algorithm in jwt.verify() could lead to signature validation bypass ... https://avd.aquasec.com/nvd/cve-2022-23540
	CVE-2022-23541					jsonwebtoken: Insecure implementation of key retrieval function could lead to Forgeable Public/Private ... https://avd.aquasec.com/nvd/cve-2022-23541
	CVE-2015-9235	CRITICAL		0.4.0	4.2.2	nodejs-jsonwebtoken: verification step bypass with an altered token https://avd.aquasec.com/nvd/cve-2015-9235
	CVE-2022-23539	HIGH			9.0.0	jsonwebtoken: Unrestricted key type could lead to legacy keys usagen https://avd.aquasec.com/nvd/cve-2022-23539
	NSWG-ECO-17				⩾4.2.2	Verification Bypass

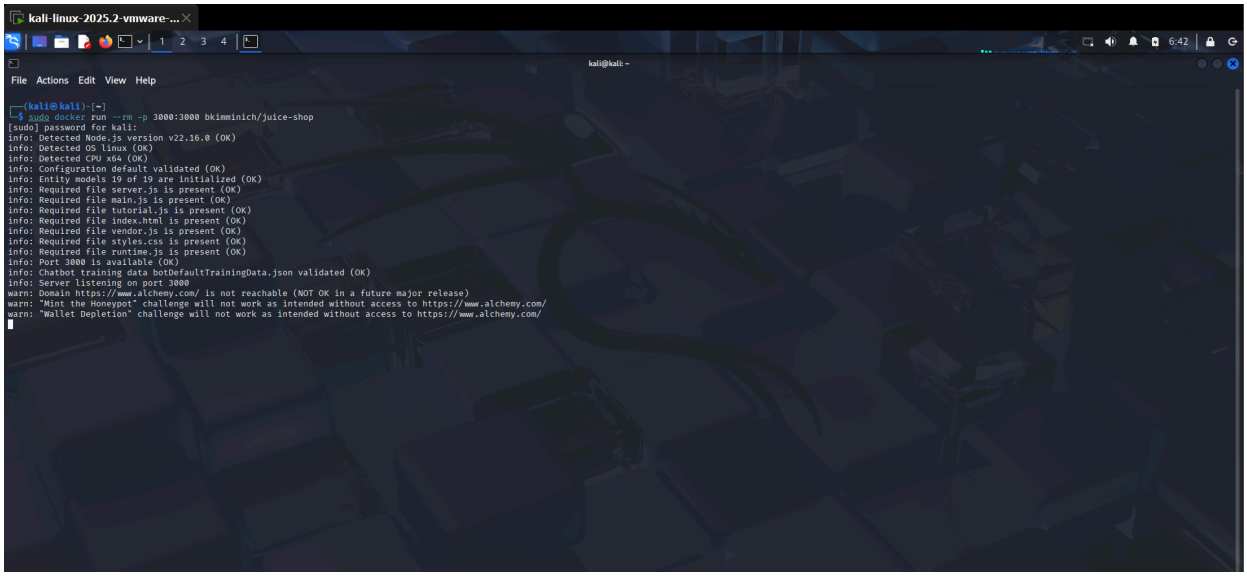
						https://avd.aquasec.com/nvd/cve-2017-16016
	CVE-2021-26539				2.3.1	sanitize-html: improper handling of internationalized domain name (IDN) can lead to bypass ... https://avd.aquasec.com/nvd/cve-2021-26539
	CVE-2021-26540				2.3.2	sanitize-html: improper validation of hostnames set by the "allowedIframeHostnames" option can lead ... https://avd.aquasec.com/nvd/cve-2021-26540
	CVE-2024-21501				2.12.1	sanitize-html: Information Exposure when used on the backend https://avd.aquasec.com/nvd/cve-2024-21501
	NSWG-ECO-154				⩾1.11.4	Cross Site Scripting
socket.io (package.json)	CVE-2024-38355			3.1.2	2.5.1, 4.6.2	socket.io: Unhandled 'error' event https://avd.aquasec.com/nvd/cve-2024-38355
socket.io-parser (package.json)	CVE-2023-32695			4.0.5	4.2.3, 3.4.3, 3.3.4	socket.io parser is a socket.io encoder and decoder written in JavaScr https://avd.aquasec.com/nvd/cve-2023-32695
tar (package.json)	CVE-2024-28863			4.4.19	6.2.1	node-tar: denial of service while parsing a tar file due to lack ... https://avd.aquasec.com/nvd/cve-2024-28863
vm2 (package.json)	CVE-2023-32314	CRITICAL		3.9.17	3.9.18	vm2: Sandbox Escape https://avd.aquasec.com/nvd/cve-2023-32314
	CVE-2023-37466		affected			vm2: Promise handler sanitization can be bypassed allowing attackers to escape the ... https://avd.aquasec.com/nvd/cve-2023-37466
	CVE-2023-37903					vm2: custom inspect function allows attackers to escape the sandbox and run ... https://avd.aquasec.com/nvd/cve-2023-37903
	CVE-2023-32313	MEDIUM	fixed		3.9.18	vm2: Inspect Manipulation https://avd.aquasec.com/nvd/cve-2023-32313
ws (package.json)	CVE-2024-37890	HIGH		7.4.6	5.2.4, 6.2.3, 7.5.10, 8.17.1	nodejs-ws: denial of service when handling a request with many HTTP headers ... https://avd.aquasec.com/nvd/cve-2024-37890

/juice-shop/build/lib/insecurity.js (secrets)


/juice-shop/build/lib/insecurity.js (secrets)
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)
HIGH: AsymmetricPrivateKey (private-key)
Asymmetric Private Key
/juice-shop/build/lib/insecurity.js:47 (added by 'COPY --chown=65532:0 /juice-shop . # bui')
45 const z85 = __importStar(require("z85"));
46 exports.publicKey = node_fs_1.default ? node_fs_1.default.readFileSync('encryptionkeys/jwt.pub', 'ut
47 [-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE
48 const hash = (data) => node_crypto_1.default.createHash('md5').update(data).digest('hex');
/juice-shop/frontend/src/app/app.guard.spec.ts (secrets)
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)
MEDIUM: JWT (jwt-token)
JWT token
/juice-shop/frontend/src/app/app.guard.spec.ts:38 (added by 'COPY --chown=65532:0 /juice-shop . # bui')
36
37 it('returns payload from decoding a valid JWT', inject([LoginGuard], (guard: LoginGuard) => {
38 [localStorage.setItem('token', '
39 expect(guard.tokenDecode()).toEqual({
/juice-shop/frontend/src/app/last-login-ip/last-login-ip.component.spec.ts (secrets)
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)
MEDIUM: JWT (jwt-token)


/juice-shop/frontend/src/app/last-login-ip/last-login-ip.component.spec.ts (secrets)
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)
MEDIUM: JWT (jwt-token)
JWT token
/juice-shop/frontend/src/app/last-login-ip/last-login-ip.component.spec.ts:61 (added by 'COPY --chown=65532:0 /juice-shop . # bui')
59
60 xit('should set Last-Login IP from JWT as trusted HTML', () => { // FIXME Expected state seems to
61 [localStorage.setItem('token', '
62 component.ngOnInit()
/juice-shop/lib/insecurity.ts (secrets)
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)
HIGH: AsymmetricPrivateKey (private-key)
Asymmetric Private Key
/juice-shop/lib/insecurity.ts:23 (added by 'COPY --chown=65532:0 /juice-shop . # bui')
21
22 export const publicKey = fs ? fs.readFileSync('encryptionkeys/jwt.pub', 'utf8') : 'placeholder-publi
23 [-----BEGIN RSA PRIVATE KEY-----
-----END RSA PRIVATE
24
(kali㉿kali)-[~]
$


(kali㉿kali)-[~]
$ sudo trivy image bkimminich/juice-shop -f table -o juice-secrets.txt
[sudo] password for kali:
2025-09-08T07:46:23-04:00 INFO [vuln] Vulnerability scanning is enabled
2025-09-08T07:46:23-04:00 INFO [secret] Secret scanning is enabled
2025-09-08T07:46:23-04:00 INFO [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-09-08T07:46:23-04:00 INFO [secret] Please see also https://trivy.dev/dev/docs/scanner/secret#recommendation for faster secret detection
2025-09-08T07:46:23-04:00 INFO Detected OS family="debian" version="12.11"
2025-09-08T07:46:23-04:00 INFO [debian] Detecting vulnerabilities... os_version="12" pkg_num=9
2025-09-08T07:46:23-04:00 INFO Number of language-specific files num=1
2025-09-08T07:46:23-04:00 INFO [node-pkg] Detecting vulnerabilities...
2025-09-08T07:46:23-04:00 WARN Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/dev/docs/scanner/vulnerability#severity-selection for details.
2025-09-08T07:46:24-04:00 INFO Table result includes only package filenames. Use '--format json' option to get the full path to the package file.
(kali㉿kali)-[~]
$



Summary

A comprehensive security vulnerability assessment was conducted on the OWASP Juice Shop containerized application using Trivy security scanner. The assessment identified multiple security vulnerabilities across different severity levels, including critical findings that require immediate attention.

Key Findings Overview

- **Total Vulnerabilities Detected:** 54+ vulnerabilities
- **Critical Severity:** 8 vulnerabilities
- **High Severity:** 21 vulnerabilities
- **Medium Severity:** 22+ vulnerabilities
- **Low Severity:** 3+ vulnerabilities

- **Secrets Detected:** JWT tokens and asymmetric private keys identified

---

Detailed Vulnerability Analysis

Critical Vulnerabilities (Immediate Action Required)

1. **CVE-2023-32314 (vm2 package)**
    - **Severity:** Critical
    - **Description:** VM2 Sandbox Escape vulnerability
    - **Impact:** Allows attackers to escape the sandbox and execute arbitrary code
    - **Affected Version:** 3.9.17
    - **Fixed Version:** 3.9.18

2. **CVE-2015-9235 (jsonwebtoken package)**
    - **Severity:** Critical
    - **Description:** Verification step bypass with altered token
    - **Impact:** Authentication bypass leading to unauthorized access
    - **Affected Version:** 0.4.0
    - **Fixed Version:** 4.2.2

3. **CVE-2023-46233 (crypto-js package)**
    - **Severity:** Critical
    - **Description:** PBKDF2 cryptographic weakness (1,000x weaker than specified)
    - **Impact:** Cryptographic security compromise
    - **Affected Version:** 3.3.0
    - **Fixed Version:** 4.2.0

High Severity Vulnerabilities

1. **CVE-2020-15084 (express-jwt package)**
    - **Description:** Authorization bypass vulnerability
    - **Affected Version:** 0.1.3
    - **Fixed Version:** 6.0.0

2. **CVE-2022-25881 (http-cache-semantics package)**
    - **Description:** Regular Expression Denial of Service (ReDoS)
    - **Affected Version:** 3.8.1

    - **Fixed Version:** 4.1.1

3. **CVE-2025-4802 (libc6 package)**
    - **Status:** Fixed
    - **Description:** Static setuid binary dlopen vulnerability
    - **Affected Version:** 2.36-9+deb12u10
    - **Fixed Version:** 2.36-9+deb12u11

Secrets Detection Results

The scan identified exposed sensitive information:

- **JWT Tokens:** Found in multiple component specification files
- **Asymmetric Private Keys:** Detected in insecurity.js files
- **Location:** `/juice-shop/lib/insecurity.ts` and build files

Risk Assessment Matrix

Risk Level	Count	Percentage	Priority
Critical	8	14.8%	P0 - Immediate
High	21	38.9%	P1 - Urgent
Medium	22	40.7%	P2 - Important
Low	3	5.6%	P3 - Monitor

Security Recommendations

Immediate Actions (Critical Priority)

1. **Update vm2 package** to version 3.9.18 or later to address sandbox escape
2. **Upgrade jsonwebtoken** to version 4.2.2+ to prevent authentication bypass

3. **Update crypto-js** to version 4.2.0+ to resolve cryptographic weaknesses
4. **Remove or secure exposed JWT tokens** and private keys from source code

High Priority Actions

1. Update all Node.js dependencies to their latest secure versions
2. Implement proper secrets management using environment variables or vault systems
3. Update base Debian image components (libc6, gcc-12-base)
4. Review and update express-jwt and http-cache-semantics packages

Medium Priority Actions

1. Establish regular container image scanning in CI/CD pipeline
2. Implement automated dependency updates with security patches
3. Review and update remaining medium-severity vulnerabilities
4. Enhance container security hardening practices

Long-term Security Improvements

1. **Implement Security Scanning Automation:** Integrate Trivy into CI/CD pipelines
2. **Container Hardening:** Use minimal base images and multi-stage builds
3. **Secrets Management:** Deploy proper secret management solutions
4. **Regular Security Audits:** Schedule periodic comprehensive security assessments
5. **Vulnerability Monitoring:** Set up continuous monitoring for new vulnerabilities

---

Technical Environment Details

- **Operating System:** Debian 12.11
- **Package Manager:** npm (Node.js packages)
- **Container Runtime:** Docker
- **Scan Coverage:** Full container image including OS and application dependencies
- **Scan Duration:** Comprehensive deep scan completed

Compliance and Standards

This assessment aligns with:

- OWASP Container Security Top 10
- NIST Container Security Guidelines
- CIS Docker Benchmark recommendations

- DevSecOps best practices

Next Steps

1. **Immediate Remediation:** Address all critical vulnerabilities within 72 hours
2. **High Priority Fixes:** Complete high-severity updates within 1 week
3. **Process Improvement:** Implement automated security scanning
4. **Documentation:** Update security procedures and incident response plans
5. **Follow-up Scan:** Re-scan after remediation to verify fixes

---

Conclusion

The assessment revealed significant security vulnerabilities that require immediate attention, particularly the critical severity issues that could lead to system compromise. While this is a demonstration environment (OWASP Juice Shop), the findings highlight the importance of regular container security assessments and proactive vulnerability management in production environments.

The identified vulnerabilities provide valuable learning opportunities for understanding container security challenges and implementing appropriate security controls in containerized applications.
