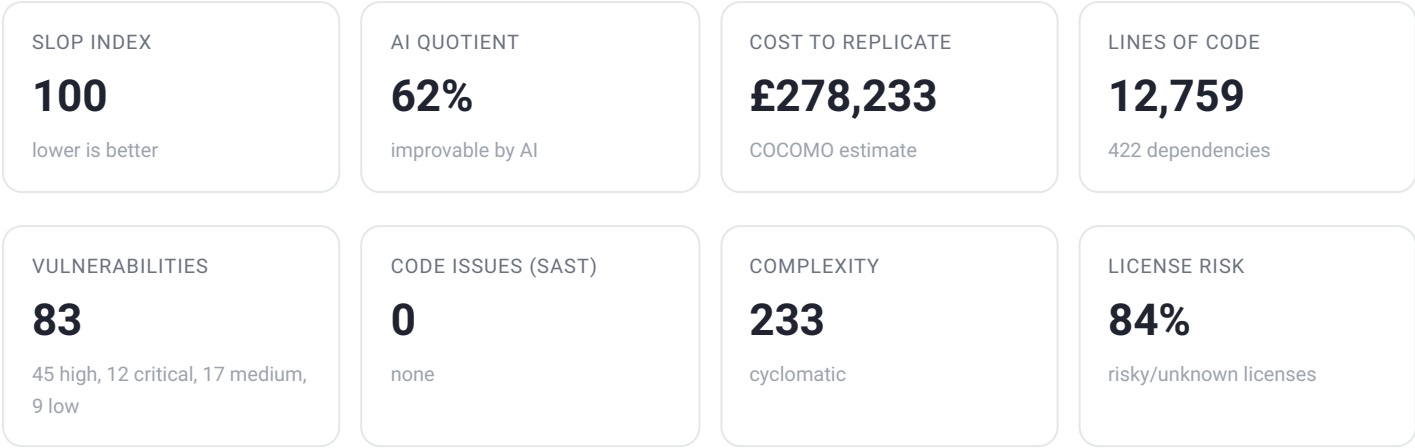


OWASP/NodeGoat

branch master · 2026-06-22



Executive Summary

Executive Summary: OWASP NodeGoat

What This Software Does

NodeGoat is an intentionally vulnerable web application created by OWASP (a respected web security organisation) as a training tool. It is designed to teach developers how to identify and fix the top 10 most common web security risks in Node.js applications. It is not a production business application — its purpose is education and security training.

Overall Health

Because this is a deliberately insecure teaching tool, its health metrics must be understood in that context. That said, the codebase is relatively small (~13,000 lines), and many of the vulnerabilities present are *intentional* features of the training environment. The dependency list is significantly outdated, with 422 packages, many of which are old and unmaintained. The "Slop Index" score of 100/100 (worst possible) indicates the code is not following modern best practices, which again aligns with its educational purpose.

Most Important Risks

The most serious concern is that this application should **never be deployed on a public-facing server or used in a production environment**. It contains 12 critical and 45 high-severity security vulnerabilities across its third-party components — including weaknesses in core libraries that handle file processing, data parsing, and user input. If accidentally deployed in a real environment, it would be trivially easy for an attacker to compromise. The outdated dependencies (some dating back to 2015–2018) compound this risk considerably.

Top Recommended Actions

1. **Enforce strict deployment controls** — Ensure this application is only ever run in isolated, local, or sandboxed training environments, never on shared infrastructure or the public internet.
2. **Update the dependency inventory** — Even for a training tool, refreshing the 422 dependencies would reduce noise and ensure the *intentional* vulnerabilities remain the focus, rather than accidental ones introduced by outdated packages.
3. **Add clear governance labels** — Attach prominent documentation to the repository and any internal deployments explicitly stating this is a training tool, so it cannot be mistakenly treated as a deployable product.

Languages

CSS	6,324
JavaScript	2,873
HTML	2,546
SVG	414
Markdown	179

License	155
JSON	137
YAML	111

Security & Code Findings (83)

high vulnerability

GHSA-c4w7-xm78-47vh in **y18n@3.2.1**

Upgrade y18n to 3.2.2

high vulnerability

GHSA-w573-4hg7-7wgq in **decode-uri-component@0.2.0**

Upgrade decode-uri-component to 0.2.1

high vulnerability

GHSA-3jfq-g458-7qm9 in **tar@4.4.8**

Upgrade tar to 4.4.14

high vulnerability

GHSA-hrpp-h998-j3pp in **qs@6.5.2**

Upgrade qs to 6.5.3

high vulnerability

GHSA-r628-mhmq-qjhw in **tar@4.4.8**

Upgrade tar to 4.4.15

critical vulnerability

GHSA-xvch-5gv4-984h in **minimist@0.0.10**

Upgrade minimist to 0.2.4

critical vulnerability

GHSA-xvch-5gv4-984h in **minimist@0.0.8**

Upgrade minimist to 0.2.4

critical vulnerability

GHSA-xvch-5gv4-984h in **minimist@0.0.8**

Upgrade minimist to 0.2.4

critical vulnerability

GHSA-xvch-5gv4-984h in **minimist@1.2.0**

Upgrade minimist to 1.2.6

critical vulnerability

GHSA-xvch-5gv4-984h in **minimist@1.2.5**

Upgrade minimist to 1.2.6

critical vulnerability

GHSA-cf4h-3jhx-xvhq in **underscore@1.9.1**

Upgrade underscore to 1.12.1

critical vulnerability

GHSA-fhjf-83wg-r2j9 in **mixin-deep@1.3.1**

Upgrade mixin-deep to 1.3.2

high vulnerability
GHSA-qqgx-2p2h-9c37 in **ini@1.3.5**
[Upgrade ini to 1.3.6](#)

high vulnerability
GHSA-qqgx-2p2h-9c37 in **ini@1.3.5**
[Upgrade ini to 1.3.6](#)

high vulnerability
GHSA-9r2w-394v-53qc in **tar@4.4.8**
[Upgrade tar to 4.4.16](#)

critical vulnerability
GHSA-4g88-fppr-53pp in **set-value@0.4.3**
[Upgrade set-value to 2.0.1](#)

critical vulnerability
GHSA-4g88-fppr-53pp in **set-value@2.0.0**
[Upgrade set-value to 2.0.1](#)

high vulnerability
GHSA-rrrm-qjm4-v8hf in **marked@0.3.5**
[Upgrade marked to 4.0.10](#)

high vulnerability
GHSA-5v2h-r2cx-5xgj in **marked@0.3.5**
[Upgrade marked to 4.0.10](#)

critical vulnerability
GHSA-v8w9-2789-6hhr in **bson@1.0.9**
[Upgrade bson to 1.1.4](#)

high vulnerability
GHSA-c2qf-rxjj-qqgw in **semver@5.6.0**
[Upgrade semver to 5.7.2](#)

high vulnerability
GHSA-c2qf-rxjj-qqgw in **semver@5.7.0**
[Upgrade semver to 5.7.2](#)

high vulnerability
GHSA-c9f4-xj24-8jqx in **uglify-js@2.4.24**
[Upgrade uglify-js to 2.6.0](#)

high vulnerability
GHSA-6c8f-qphg-qjgp in **kind-of@6.0.2**
[Upgrade kind-of to 6.0.3](#)

high vulnerability
GHSA-4jqc-8m5r-9rpr in **set-value@0.4.3**
[Upgrade set-value to 2.0.1](#)

COMPONENT	VERSION	ECOSYSTEM	LICENSE
abbrev	1.1.1	npm	ISC
accepts	1.3.5	npm	unknown
actions/cache	v2	github	unknown
actions/checkout	v2	github	unknown
actions/checkout	v2	github	unknown
actions/setup-node	v1	github	unknown
actions/setup-node	v1	github	unknown
actions/upload-artifact	v2	github	unknown
amdefine	1.0.1	npm	unknown
ansi-regex	2.1.1	npm	MIT
ansi-regex	2.1.1	npm	unknown
anymatch	2.0.0	npm	unknown
aproba	1.2.0	npm	ISC
are-we-there-yet	1.1.5	npm	ISC
arr-diff	4.0.0	npm	unknown
arr-flatten	1.1.0	npm	unknown
arr-union	3.1.0	npm	unknown
array-filter	1.0.0	npm	unknown
array-flatten	1.1.1	npm	unknown
array-unique	0.3.2	npm	unknown
assign-symbols	1.0.0	npm	unknown
async	0.2.10	npm	unknown
async	0.2.9	npm	unknown
async	0.9.2	npm	unknown
async	1.5.2	npm	unknown
async-each	1.0.3	npm	unknown
atob	2.1.2	npm	unknown
available-typed-arrays	1.0.2	npm	unknown
balanced-match	1.0.0	npm	MIT
balanced-match	1.0.0	npm	unknown
base	0.11.2	npm	unknown
bcrypt-nodejs	0.0.3	npm	unknown
binary-extensions	1.13.1	npm	unknown
bluebird	3.5.3	npm	unknown
body-parser	1.18.3	npm	unknown
brace-expansion	1.1.11	npm	MIT
brace-expansion	1.1.11	npm	unknown
braces	2.3.2	npm	unknown
broadway	0.3.6	npm	unknown

COMPONENT	VERSION	ECOSYSTEM	LICENSE
bson	1.0.9	npm	unknown

Contributors

AUTHOR	COMMITTS	+LINES	-LINES	SCORE
ckarande	112	652910	3624	3394.7
Jesús Pérez	13	620	626793	3150.1
Liran Tal	38	16888	1268	128.8
Josep	6	5641	6159	65
Kim Carter	35	1078	607	43.4
Ulises Gascon	23	2282	699	37.9
Rob Cowsill	23	1240	938	33.9
fabre-pierre-jean	2	2744	2066	26.1
Ulises Gascon	17	426	401	21.1
Liran Tal	11	46	22	11.3
lucas jin	9	88	90	9.9
Ulises Gascón	6	158	95	7.3