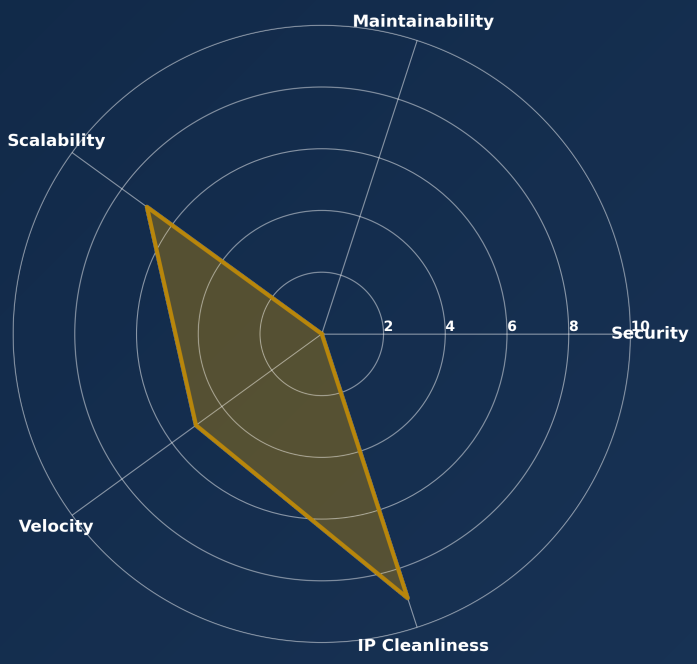
VIGILCAP

Technical Due Diligence Report

juice-shop-master

WALK AWAY

TDR of 100.0% or 12 critical leaks is unacceptable.



100.0%	$409,230	$324,591
TECHNICAL DEBT RATIO	REMEDIATION CAPEX	REPLACEMENT COST

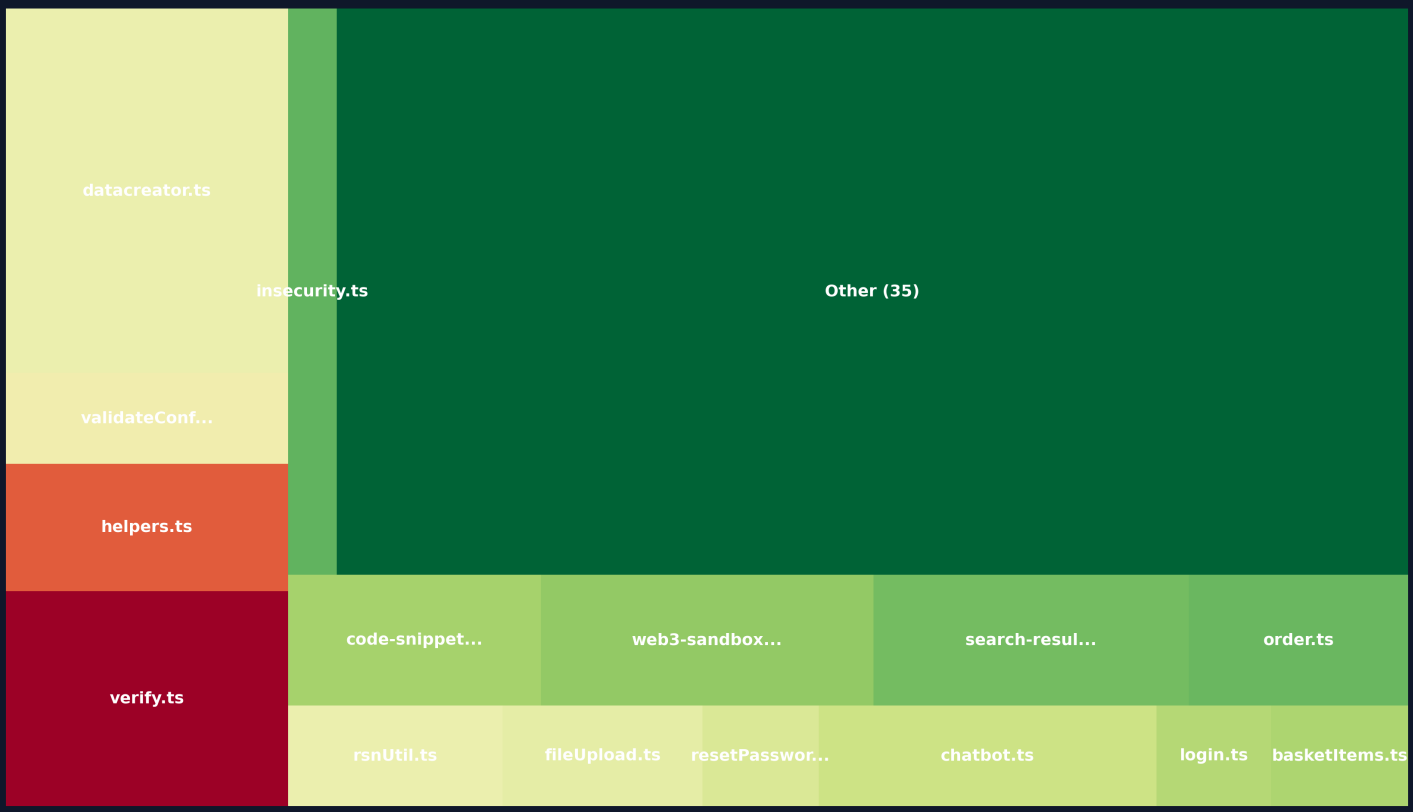
Executive Summary

This codebase is structurally and security-wise unfit for any production use: it contains explicit “insecurity/vuln” modules and 50 known vulnerabilities, indicating vulnerabilities are likely a product feature rather than a defect. The backend is a route-heavy Express monolith with high cyclomatic complexity concentrated in authentication, verification, file upload, and data-generation paths, making fixes risky and regression-prone. Even if this is “training software,” the dependency set includes multiple obsolete security libraries that materially increase breach/supply-chain risk and undermine any enterprise/compliance narrative.

50	50	2/10
FILES ANALYZED	SECURITY ISSUES	BUS FACTOR

Codebase Hotspot Map

Each rectangle represents a file, sized by lines of code. Colors show **relative complexity** within this codebase: Red = Most Complex, Green = Least Complex. High-complexity files are harder to maintain and more prone to bugs.



Strategic Risk Analysis

Severity	Risk	Impact	Est. Capex
CRITICAL	Product appears intentionally vulnerable (unmarketable for production / enterprise)	If customers or internal stakeholders believe this is a real commerce/SaaS platform, it is effectively unsellable into regulated/enterprise environments (SOC2/ISO27001, vendor security reviews) and creates immediate reputational and legal exposure if deployed with real data. If it is training software, the business moat is weak because it resembles a commodity OWASP Juice Shop derivative rather than proprietary IP.	$240,000
CRITICAL	Authentication/authorization and account flows are concentrated, complex, and high-risk	High-complexity auth-adjacent routes (e.g., routes/verify.ts, routes/login.ts, routes/resetPassword.ts, routes/2fa.ts) increase the likelihood of auth bypass, token/session flaws, and data exposure. Any modernization (JWT libs, session handling, password reset, 2FA) will be a breaking change requiring careful migration and extensive testing.	$120,000
HIGH	Dependency obsolescence and security toolchain debt will block remediation velocity	Multiple security-critical libraries are extremely outdated (notably JWT stack and sanitization). Upgrading will trigger API breaks across the codebase and tests, slowing feature work and increasing incident probability. Native modules (e.g., libxmljs2, sqlite3 toolchain, node-pre-gyp) also increase build fragility and supply-chain risk.	$75,000
HIGH	Route-level business logic monolith with weak separation of concerns	Business logic, validation, persistence, and security controls appear embedded directly in route handlers (routes/*.ts), creating duplicated logic, inconsistent authorization, and high regression risk. This architecture will not scale with team size and materially increases the cost of adding controls (audit logging, RBAC, rate limits, abuse prevention).	$60,000
HIGH	Operational/compliance exposure (data erasure, metrics, file handling) without mature governance	Presence of routes/dataErasure.ts and routes/metrics.ts suggests privacy and telemetry concerns, but the codebase maturity (complexity, vulnerabilities, outdated security deps) indicates likely non-compliance with retention, auditability, and secure SDLC expectations—directly impacting deal value if enterprise growth is part of the thesis.	$45,000

Security Deep Dive

#	Severity	Rule	File	Line
1	MEDIUM	jwt	frontend/src/app/app.guard.spec.ts	38
2	MEDIUM	generic-api-key	frontend/src/app/faucet/faucet.component.ts	34
3	MEDIUM	generic-api-key	data/static/users.yml	88
4	MEDIUM	generic-api-key	data/static/users.yml	150
5	MEDIUM	generic-api-key	frontend/src/app/last-login-ip/last-login-ip.component.spec.ts	67
6	MEDIUM	jwt	frontend/src/app/last-login-ip/last-login-ip.component.spec.ts	61
7	MEDIUM	generic-api-key	frontend/src/app/oauth/oauth.component.spec.ts	84
8	MEDIUM	generic-api-key	frontend/src/app/oauth/oauth.component.spec.ts	84
9	MEDIUM	generic-api-key	frontend/src/app/oauth/oauth.component.spec.ts	91
10	CRITICAL	private-key	lib/insecurity.ts	23
11	MEDIUM	generic-api-key	test/api/basketApiSpec.ts	101
12	MEDIUM	generic-api-key	test/api/erasureRequestApiSpec.ts	37
13	MEDIUM	generic-api-key	test/api/erasureRequestApiSpec.ts	64
14	MEDIUM	generic-api-key	test/api/erasureRequestApiSpec.ts	80
15	MEDIUM	generic-api-key	test/api/erasureRequestApiSpec.ts	99
16	MEDIUM	generic-api-key	test/api/erasureRequestApiSpec.ts	119
17	MEDIUM	generic-api-key	test/api/erasureRequestApiSpec.ts	140
18	MEDIUM	generic-api-key	test/api/feedbackApiSpec.ts	120
19	MEDIUM	generic-api-key	test/api/feedbackApiSpec.ts	153
20	MEDIUM	generic-api-key	test/api/loginApiSpec.ts	142
21	MEDIUM	generic-api-key	test/api/loginApiSpec.ts	245
22	MEDIUM	generic-api-key	test/api/loginApiSpec.ts	266
23	MEDIUM	generic-api-key	test/api/2faSpec.ts	175
24	MEDIUM	generic-api-key	test/api/2faSpec.ts	370
25	MEDIUM	generic-api-key	test/api/productReviewApiSpec.ts	112
26	MEDIUM	generic-api-key	test/api/productReviewApiSpec.ts	132
27	MEDIUM	generic-api-key	test/api/chatBotSpec.ts	108
28	MEDIUM	generic-api-key	test/api/chatBotSpec.ts	140
29	MEDIUM	generic-api-key	test/api/chatBotSpec.ts	174
30	MEDIUM	generic-api-key	test/api/chatBotSpec.ts	250
31	MEDIUM	generic-api-key	test/cypress/e2e/login.spec.ts	126
32	MEDIUM	generic-api-key	routes/login.ts	65
33	MEDIUM	generic-api-key	test/api/dataExportApiSpec.ts	21
34	MEDIUM	generic-api-key	test/api/dataExportApiSpec.ts	48
35	MEDIUM	generic-api-key	test/api/dataExportApiSpec.ts	77
36	MEDIUM	generic-api-key	test/api/userApiSpec.ts	256

#	Severity	Rule	File	Line
37	MEDIUM	jwt	test/api/userApiSpec.ts	302
38	MEDIUM	generic-api-key	test/api/userApiSpec.ts	302
39	MEDIUM	generic-api-key	test/api/web3Spec.ts	36
40	MEDIUM	generic-api-key	test/api/web3Spec.ts	48
41	MEDIUM	generic-api-key	test/api/web3Spec.ts	60
42	MEDIUM	jwt	test/cypress/e2e/forgedJwt.spec.ts	7
43	MEDIUM	jwt	test/cypress/e2e/forgedJwt.spec.ts	22
44	MEDIUM	generic-api-key	test/cypress/e2e/totpSetup.spec.ts	7
45	MEDIUM	jwt	test/server/currentUserSpec.ts	33
46	MEDIUM	jwt	test/server/currentUserSpec.ts	36
47	MEDIUM	jwt	test/server/verifySpec.ts	263
48	MEDIUM	jwt	test/server/verifySpec.ts	275
49	MEDIUM	jwt	test/server/verifySpec.ts	297
50	MEDIUM	jwt	test/server/verifySpec.ts	309

Open Source Liability (High Risk)

Showing top high-risk dependencies. See Appendix A for full manifest.

Package	Version	Status	Risk	Action
express-jwt	0.1.3	EOL	High	Remove/replace with maintained JWT middleware (e.g., express-jwt v8+ or alternative) and rework auth pipeline; add regression tests for all auth flows.
jsonwebtoken	0.4.0	EOL	High	Upgrade to current jsonwebtoken and rotate signing keys; audit token claims, algorithms, expiration, and error handling; validate against downgrade/confusion issues.
sanitize-html	1.4.2	EOL	High	Upgrade to latest sanitize-html (major-version breaking changes likely) and add comprehensive XSS test coverage; standardize output encoding strategy.
js-yaml	3.14.0	OUTDATED	High	Upgrade to v4+ and audit any schema/loading usage; lock down unsafe load patterns; run SCA and regression tests.
helmet	4.6.0	OUTDATED	Medium	Upgrade to current helmet and re-validate CSP, HSTS, and header behavior; ensure compatibility with frontend and any embedded content.
socket.io	3.1.2	OUTDATED	Medium	Upgrade to v4+ and rework client/server handshake/auth; re-audit real-time endpoints for authorization and rate limiting.
multer	1.4.5-lts.1	OUTDATED	High	Upgrade and harden file upload pipeline: strict allowlist, size limits, AV scanning, storage isolation, and remove any path traversal/overwrite vectors.
feature-policy	0.5.0	EOL	Medium	Remove/replace with Permissions-Policy header; validate across browsers and update security header configuration.
pdfkit	0.11.0	OUTDATED	Medium	Upgrade to current pdfkit and fuzz/test any user-influenced PDF generation inputs to prevent injection/DoS vectors.
node-pre-gyp	0.15.0	OUTDATED	Medium	Minimize native dependency toolchain; migrate to supported prebuild tooling or eliminate native modules where feasible; pin and verify build provenance.
libxmljs2	0.37.0	OUTDATED	High	Reassess XML parsing needs; migrate to safer, maintained parsers; if retained, harden against XXE and ensure native library patching process exists.

Appendix A: Full Dependency Manifest (208 items)

Package	Version	Type	Origin File
body-parser	1.20.2	npm	
check-dependencies	1.1.1	npm	
check-internet-connected	2.0.6	npm	
clarinet	0.12.6	npm	
colors	1.4.0	npm	
compression	1.7.4	npm	
config	3.3.12	npm	
cookie-parser	1.4.6	npm	
cors	2.8.5	npm	
dottie	2.0.6	npm	
download	8.0.0	npm	
errorhandler	1.5.1	npm	
ethers	6.13.2	npm	
express	4.21.0	npm	
express-ipfilter	1.3.2	npm	
express-jwt	0.1.3	npm	
express-rate-limit	7.5.0	npm	
express-robots-txt	0.4.1	npm	
express-security.txt	2.0.0	npm	
feature-policy	0.5.0	npm	
file-stream-rotator	1.0.0	npm	
file-type	16.5.4	npm	
filesniffer	1.0.3	npm	
finale-rest	1.2.2	npm	
fs-extra	9.1.0	npm	
fuzzball	1.4.0	npm	
glob	10.4.5	npm	
graceful-fs	4.2.11	npm	
grunt	1.6.1	npm	
grunt-contrib-compress	1.6.0	npm	
grunt-replace-json	0.1.0	npm	
hashids	2.3.0	npm	
hbs	4.2.0	npm	
helmet	4.6.0	npm	
html-entities	1.4.0	npm	
i18n	0.11.1	npm	

Package	Version	Type	Origin File
js-yaml	3.14.0	npm	
jsonwebtoken	0.4.0	npm	
jssha	3.3.1	npm	
juicy-chat-bot	0.9.0	npm	
libxmljs2	0.37.0	npm	
marsdb	0.6.11	npm	
median	0.0.2	npm	
morgan	1.10.0	npm	
multer	1.4.5-lts.1	npm	
node-pre-gyp	0.15.0	npm	
notevil	1.3.3	npm	
on-finished	2.3.0	npm	
otplib	12.0.1	npm	
pdfkit	0.11.0	npm	
portscanner	2.2.0	npm	
prom-client	14.2.0	npm	
pug	3.0.3	npm	
replace	1.2.2	npm	
sanitize-filename	1.6.3	npm	
sanitize-html	1.4.2	npm	
semver	7.6.3	npm	
sequelize	6.37.3	npm	
serve-index	1.9.1	npm	
socket.io	3.1.2	npm	
sqlite3	5.1.7	npm	
svg-captcha	1.4.0	npm	
swagger-ui-express	5.0.1	npm	
ts-node-dev	1.1.8	npm	
unzipper	0.9.15	npm	
web3	4.13.0	npm	
winston	3.16.0	npm	
yaml-schema-validator	1.2.3	npm	
z85	0.0.2	npm	
@cyclonedx/cyclonedx-npm	2.0.0||^3.0.0	npm	
@istanbuljs/nyc-config-typescript	1.0.2	npm	
@types/chai	4.3.20	npm	
@types/clarinet	0.12.3	npm	
@types/compression	1.7.5	npm	
@types/config	3.3.5	npm	
@types/cookie-parser	1.4.7	npm	

Package	Version	Type	Origin File
@types/cors	2.8.17	npm	
@types/cross-spawn	6.0.6	npm	
@types/cypress	1.1.6	npm	
@types/diff	7.0.1	npm	
@types/download	8.0.5	npm	
@types/errorhandler	1.5.3	npm	
@types/exif	0.6.5	npm	
@types/express	4.17.21	npm	
@types/express-jwt	6.0.4	npm	
@types/frisby	2.0.17	npm	
@types/fs-extra	9.0.13	npm	
@types/glob	7.2.0	npm	
@types/graceful-fs	4.1.9	npm	
@types/i18n	0.12.0	npm	
@types/jasmine	3.9.1	npm	
@types/jest	26.0.24	npm	
@types/js-yaml	3.12.10	npm	
@types/jsonwebtoken	8.5.9	npm	
@types/jws	3.2.10	npm	
@types/lodash	4.17.14	npm	
@types/mocha	8.2.3	npm	
@types/morgan	1.9.9	npm	
@types/multer	1.4.12	npm	
@types/node	20.17.25	npm	
@types/on-finished	2.3.4	npm	
@types/pdfkit	0.10.6	npm	
@types/portscanner	2.1.4	npm	
@types/pug	2.0.10	npm	
@types/request	2.48.12	npm	
@types/sanitize-html	1.27.2	npm	
@types/semver	7.5.8	npm	
@types/sequelize	4.28.20	npm	
@types/serve-index	1.9.4	npm	
@types/sinon	10.0.20	npm	
@types/sinon-chai	3.2.12	npm	
@types/socket.io	2.1.13	npm	
@types/socket.io-client	1.4.36	npm	
@types/swagger-ui-express	4.1.6	npm	
@types/unzipper	0.10.10	npm	
@types/validator	13.12.2	npm	

Package	Version	Type	Origin File
@typescript-eslint/eslint-plugin	6.18.1	npm	
@typescript-eslint/parser	6.18.1	npm	
chai	4.5.0	npm	
concurrently	5.3.0	npm	
cross-spawn	7.0.3	npm	
cypress	13.17.0	npm	
eslint	8.57.1	npm	
eslint-config-standard-with-typescript	43.0.1	npm	
eslint-plugin-import	2.31.0	npm	
eslint-plugin-node	11.1.0	npm	
eslint-plugin-promise	6.6.0	npm	
exif	0.6.0	npm	
frisby	github:bkimminich/frisby	npm	
grunt-cli	1.5.0	npm	
http-server	0.12.3	npm	
jasmine	3.99.0	npm	
jasmine-core	3.9.0	npm	
jasmine-reporters	2.5.2	npm	
jest	29.7.0	npm	
mocha	8.4.0	npm	
nyc	15.1.0	npm	
shelljs	0.8.5	npm	
sinon	11.1.2	npm	
sinon-chai	3.7.0	npm	
socket.io-client	3.1.3	npm	
source-map-support	0.5.21	npm	
ts-jest	29.2.5	npm	
ts-node	10.9.2	npm	
typescript	5.3.3	npm	
@angular-builders/custom-webpack	20.0.0	npm	
@angular-devkit/build-angular	20.1.0	npm	
@angular/animations	20.1.0	npm	
@angular/cdk	20.1.0	npm	
@angular/cli	20.1.6	npm	
@angular/common	20.1.0	npm	
@angular/compiler	20.1.0	npm	
@angular/compiler-cli	20.1.0	npm	
@angular/core	20.1.0	npm	
@angular/forms	20.1.0	npm	
@angular/material	20.1.0	npm	

Package	Version	Type	Origin File
@angular/platform-browser	20.1.0	npm	
@angular/platform-browser-dynamic	20.1.0	npm	
@angular/router	20.1.0	npm	
@ctrl/ngx-codemirror	6.1.0	npm	
@cyclonedx/webpack-plugin	5.0.0	npm	
@fortawesome/fontawesome-svg-core	1.2.30	npm	
@fortawesome/free-brands-svg-icons	5.14.0	npm	
@fortawesome/free-regular-svg-icons	5.14.0	npm	
@fortawesome/free-solid-svg-icons	5.14.0	npm	
@ngx-translate/core	15.0.0	npm	
@ngx-translate/http-loader	8.0.0	npm	
@wagmi/core	0.5.8	npm	
@winarg/ngx-text-diff	19.0.1	npm	
canvas-confetti	1.9.3	npm	
codemirror	5.65.14	npm	
codemirror-solidity	0.2.5	npm	
file-saver	2.0.2	npm	
flag-icons	6.9.2	npm	
font-mfizz	2.4.1	npm	
jwt-decode	2.2.0	npm	
lodash-es	4.17.21	npm	
material-icons	0.3.1	npm	
ng-gallery	12.0.0	npm	
ng-qrcode	20.0.0	npm	
ng2-file-upload	9.0.0	npm	
ngx-clipboard	15.1.0	npm	
ngx-highlightjs	6.1.2	npm	
ngx-window-token	6.0.0	npm	
ngy-cookie	6.0.0	npm	
rxjs	7.8.2	npm	
sass	1.86.3	npm	
snarkdown	1.2.2	npm	
solidity-browser-compiler	1.1.0	npm	
tslib	2.5.0	npm	
zone.js	0.15.0	npm	
@angular/language-service	20.1.0	npm	
@types/express-serve-static-core	4.17.9	npm	
@types/file-saver	2.0.1	npm	
@types/jasminewd2	2.0.10	npm	
@types/jwt-decode	2.2.1	npm	

Package	Version	Type	Origin File
@eslint/js	9.33.0	npm	
angular-eslint	20.1.0	npm	
jasmine-spec-reporter	7.0.0	npm	
karma	6.4.0	npm	
karma-chrome-launcher	3.2.0	npm	
karma-coverage	2.2.0	npm	
karma-jasmine	5.1.0	npm	
karma-jasmine-html-reporter	2.1.0	npm	
stylelint	13.8.0	npm	
stylelint-config-sass-guidelines	7.1.0	npm	
stylelint-scss	3.18.0	npm	
typescript-eslint	8.42.0	npm	

Appendix B: Codebase Complexity Ledger (Top 200)

#	File	Complexity	Lines	Language
1	routes/verify.ts	77	440	TypeScript
2	frontend/src/hacking-instructor/helpers/helpers.ts	66	261	TypeScript
3	lib/startup/validateConfig.ts	48	186	TypeScript
4	data/datacreator.ts	46	746	TypeScript
5	rsn/rsnUtil.ts	46	157	TypeScript
6	routes/fileUpload.ts	45	146	TypeScript
7	routes/resetPassword.ts	43	85	TypeScript
8	routes/chatbot.ts	41	247	TypeScript
9	routes/login.ts	38	84	TypeScript
10	routes/basketItems.ts	37	100	TypeScript
11	frontend/src/app/code-snippet/code-snippet.component.ts	36	240	TypeScript
12	frontend/src/app/web3-sandbox/web3-sandbox.component.ts	34	315	TypeScript
13	frontend/src/app/search-result/search-result.component.ts	31	299	TypeScript
14	routes/order.ts	30	208	TypeScript
15	lib/insecurity.ts	29	201	TypeScript
16	frontend/src/app/navbar/navbar.component.ts	29	303	TypeScript
17	routes/2fa.ts	27	176	TypeScript
18	frontend/src/app/score-board/helpers/challenge-filtering.ts	26	108	TypeScript
19	frontend/src/app/payment/payment.component.ts	25	298	TypeScript
20	routes/deluxe.ts	24	70	TypeScript
21	lib/antiCheat.ts	23	166	TypeScript
22	routes/vulnCodeSnippet.ts	23	116	TypeScript
23	lib/codingChallenges.ts	21	112	TypeScript
24	lib/challengeUtils.ts	20	120	TypeScript
25	routes/restoreProgress.ts	18	80	TypeScript
26	routes/changePassword.ts	17	61	TypeScript
27	routes/fileServer.ts	17	55	TypeScript
28	routes/languages.ts	17	74	TypeScript
29	routes/search.ts	17	74	TypeScript
30	frontend/src/app/challenge-solved-notification/challenge-solved-notification.component.ts	17	146	TypeScript
31	frontend/src/app/score-board/score-board.component.ts	17	204	TypeScript
32	lib/startup/validatePreconditions.ts	16	129	TypeScript
33	routes/vulnCodeFixes.ts	16	99	TypeScript
34	frontend/src/app/faucet/faucet.component.ts	16	316	TypeScript
35	frontend/src/hacking-instructor/index.ts	16	218	TypeScript
36	lib/startup/validateChatBot.ts	15	42	TypeScript

#	File	Complexity	Lines	Language
37	routes/dataErasure.ts	15	96	TypeScript
38	routes/metrics.ts	15	233	TypeScript
39	routes/basket.ts	14	36	TypeScript
40	frontend/src/app/app.guard.ts	13	88	TypeScript
41	frontend/src/app/score-board/filter-settings/query-params-converters.ts	13	41	TypeScript
42	frontend/src/app/sidenav/sidenav.component.ts	13	167	TypeScript
43	routes/userProfile.ts	12	103	TypeScript
44	data/static/codefixes/restfulXssChallenge_2.ts	12	64	TypeScript
45	data/static/codefixes/restfulXssChallenge_4.ts	12	64	TypeScript
46	frontend/src/app/login/login.component.ts	12	136	TypeScript
47	frontend/src/app/photo-wall/mime-type.validator.ts	12	52	TypeScript
48	frontend/src/app/score-board/components/filter-settings/pipes/difficulty-selection-summary.pipe.ts	12	54	TypeScript
49	routes/saveLoginIp.ts	11	43	TypeScript
50	test/cypress/e2e/contact.spec.ts	11	261	TypeScript