PROJECT MILESTONES & PROGRESS

Comprehensive Task Tracking & Implementation Status

Generated: November 24, 2025

EXECUTIVE SUMMARY

Metric	Value
Total Tasks	54
Completed Tasks	45
Partially Complete	3
Not Started	6
Overall Completion	83.3%

TASKS BY CATEGORY

Core Infrastructure (4 tasks)

ID	Task	Priority	Status	Progress
T-001	Recursively parse folders	CRITICAL	COMPLETED (AUTO-VERI	100%
T-002	Detect project language	CRITICAL	COMPLETED (AUTO-VERI	100%
T-003	Build AST	CRITICAL	COMPLETED (AUTO-VERI	100%
T-004	Extract functions/classes	CRITICAL	COMPLETED (AUTO-VERI	100%

Data Flow Analysis (4 tasks)

ID	Task	Priority	Status	Progress
T-008	Track user input	CRITICAL	COMPLETED (AUTO-VERI	100%
T-009	Propagation mapping	CRITICAL	COMPLETED (AUTO-VERI	100%
T-010	Taint analysis	CRITICAL	COMPLETED (AUTO-VERI	100%
T-011	Sanitization check	CRITICAL	COMPLETED (AUTO-VERI	100%

Enhancement (3 tasks)

ID	Task	Priority	Status	Progress
T-046	Unused variables	MEDIUM	COMPLETED (AUTO-VERI	100%
T-047	Dead code	MEDIUM	COMPLETED (AUTO-VERI	100%

T-048	Empty catches	MEDIUM	COMPLETED (AUTO-VERI	100%

Input Security (4 tasks)

ID	Task	Priority	Status	Progress
T-020	Missing validation	HIGH	COMPLETED (AUTO-VERI	100%
T-021	Type checking	HIGH	COMPLETED (AUTO-VERI	100%
T-022	Boundary checks	HIGH	COMPLETED (AUTO-VERI	100%
T-023	Client-side only	HIGH	COMPLETED (AUTO-VERI	100%

Output/Reporting (6 tasks)

ID	Task	Priority	Status	Progress
T-049	Secure code fixes	MEDIUM	PARTIAL	30%
T-050	Sanitization	MEDIUM	PARTIAL	30%
T-051	Prepared statements	MEDIUM	NOT STARTED	0%
T-052	JSON/HTML/PDF/Markdown	MEDIUM	COMPLETED (AUTO-VERI	100%
T-053	CWE/OWASP mapping	MEDIUM	COMPLETED (AUTO-VERI	100%
T-054	Fix recommendations	MEDIUM	COMPLETED (AUTO-VERI	100%

Security Checks (19 tasks)

ID	Task	Priority	Status	Progress
T-016	Weak hashing	MEDIUM	COMPLETED (AUTO-VERI	100%
T-017	Weak encryption	MEDIUM	COMPLETED (AUTO-VERI	100%
T-018	Predictable random	MEDIUM	COMPLETED (AUTO-VERI	100%
T-019	JWT issues	MEDIUM	COMPLETED (AUTO-VERI	100%
T-024	Weak tokens	HIGH	COMPLETED (AUTO-VERI	100%
T-025	Session management	HIGH	COMPLETED (AUTO-VERI	100%
T-026	Cookie security	HIGH	COMPLETED (AUTO-VERI	100%
T-027	Authorization checks	HIGH	NOT STARTED	0%
T-028	Privilege escalation	HIGH	NOT STARTED	0%
T-029	IDOR	HIGH	NOT STARTED	0%

Security Detection (7 tasks)

ID	Task	Priority	Status	Progress
T-005	eval/exec/system detection	CRITICAL	COMPLETED (AUTO-VERI	100%
T-006	OWASP/CWE mapping	CRITICAL	COMPLETED (AUTO-VERI	100%
T-007	Multi-language support	CRITICAL	COMPLETED (AUTO-VERI	100%
T-012	API keys	CRITICAL	COMPLETED (AUTO-VERI	100%
T-013	JWT secrets	CRITICAL	COMPLETED (AUTO-VERI	100%
T-014	Database credentials	CRITICAL	COMPLETED (AUTO-VERI	100%
T-015	Base64 payloads	CRITICAL	COMPLETED (AUTO-VERI	100%

Vulnerability Management (7 tasks)

ID	Task	Priority	Status	Progress
T-033	Parse requirements.txt	HIGH	COMPLETED (AUTO-VERI	100%
T-034	Parse package.json/pom.xml	HIGH	COMPLETED (AUTO-VERI	100%
T-035	Query OSV API	HIGH	COMPLETED (AUTO-VERI	100%
T-036	Query NVD/GitHub APIs	HIGH	COMPLETED (AUTO-VERI	100%
T-037	Version-aware CVE matching	HIGH	COMPLETED (AUTO-VERI	100%
T-038	Severity assessment	HIGH	COMPLETED (AUTO-VERI	100%
T-039	Exploit detection	HIGH	COMPLETED (AUTO-VERI	100%

VULNERABILITY MANAGEMENT REPORT

Metric	Count	Details
Total Dependencies	15	All packages analyzed
Vulnerable Packages	3	Packages with known CVEs
Total Vulnerabilities	5	Unique vulnerability IDs
CRITICAL Severity	0	CVSS 9.0-10.0
HIGH Severity	2	CVSS 7.0-8.9
MEDIUM Severity	2	CVSS 4.0-6.9
LOW Severity	1	CVSS 0.1-3.9

VULNERABLE PACKAGES OVERVIEW

Package	Version	Ecosystem	Vulns	Severity	CVE References
body-parser	1.20.2	npm	2	HIGH	CVE-2024-45590, CVE-2021-3666
axios	0.21.1	npm	2	HIGH	CVE-2023-45857, CVE-2021-3749
lodash	4.17.20	npm	1	LOW	CVE-2020-28500

DETAILED VULNERABILITY BREAKDOWN

body-parser v1.20.2 [npm] - 2 vulnerabilities

ID:	GHSA-qwcr-r2fm-qrc7 (CVE-2024-45590)	Severity:	HIGH (CVSS: 7.5)
Summary:	body-parser vulnerable to denial of service when url encoding is enabled		
Published:	2024-09-10	Exploit:	No
Fixed Version:	1.20.3		
References:	• https://github.com/expressjs/body-parser/security/advisories/GHSA-qwcr-r2fm-qrc7 • https://nvd.nist.gov/vuln/detail/CVE-2024-45590 • https://github.com/expressjs/body-parser/commit/b2695c4450f06ba3b0ccf48d872a229b		

ID:	CVE-2021-3666	Severity:	MEDIUM (CVSS: 5.3)
Summary:	Potential ReDoS vulnerability in body-parser when parsing content type		
Published:	2021-09-13	Exploit:	No
Fixed Version:	1.19.1		
References:	• https://nvd.nist.gov/vuln/detail/CVE-2021-3666 • https://github.com/expressjs/body-parser/issues/404		

axios v0.21.1 [npm] - 2 vulnerabilities

ID:	CVE-2023-45857	Severity:	HIGH (CVSS: 8.1)
Summary:	axios Cross-Site Request Forgery (CSRF) vulnerability allows attacker to forge requests		
Published:	2023-11-08	Exploit:	YES
Fixed Version:	1.6.0		
References:	• https://github.com/axios/axios/security/advisories/GHSA-wf5p-g6vw-rhxx • https://nvd.nist.gov/vuln/detail/CVE-2023-45857 • https://security.snyk.io/vuln/SNYK-JS-AXIOS-6032459		

ID:	CVE-2021-3749	Severity:	MEDIUM (CVSS: 5.9)
Summary:	axios vulnerable to Server-Side Request Forgery (SSRF)		
Published:	2021-08-31	Exploit:	No
Fixed Version:	0.21.2		
References:	• https://nvd.nist.gov/vuln/detail/CVE-2021-3749 • https://github.com/axios/axios/commit/5b457116e31db0e88fede6c428e969e87f290929		

lodash v4.17.20 [npm] - 1 vulnerabilities

ID:	CVE-2020-28500	Severity:	LOW (CVSS: 3.7)

Summary:	lodash vulnerable to Regular Expression Denial of Service (ReDoS) via toNumber, trim and trimEnd functions		
Published:	2021-02-15	Exploit:	No
Fixed Version:	4.17.21		
References:	• https://github.com/lodash/lodash/pull/5065 • https://nvd.nist.gov/vuln/detail/CVE-2020-28500 • https://snyk.io/vuln/SNYK-JS-LODASH-1018905		