WARD PROTOCOL

Deterministic default resolution for on-chain lending

ALL SYSTEMS GREEN — READY FOR MAINNET PILOTS

559	22	53	92%	0	4
Automated Tests	Rust Tests	TypeScript Tests	Critical Path Coverage	Open CVEs	Invariant Layers

1. CORE INVARIANT — ward_signed = False — always

Static Analysis: Ruff + mypy enforce signing boundary at lint time — CI fails on violation
Property Testing: Hypothesis fuzz tests confirm ward_signed never set True across 10,000+ inputs
Formal Spec (TLA+): TLA+ model checked — signing state machine proven unreachable
Runtime Guard: Production paths assert ward_signed == False before every settlement call

2. TEST SUITE — 559 PYTHON · 22 RUST · 53 TYPESCRIPT

Python — Main Suite (3.10 / 3.11 / 3.12 matrix)	449	PASS
Python — SDK Integration Tests	101	PASS
Python — Additional SDK Tests	9	PASS
Rust — Core Ward Library	22	PASS
TypeScript — Site & Demo	53	PASS
TOTAL	**634**	PASS

3. CI PIPELINE — 8/8 JOBS GREEN (commit eba46bf)

- Signing Boundary Check (INV-003) ✓
- TLA+ Model Check (INV-007/016) ✓
- Lint & Type Check (ruff, mypy, security scan) ✓
- Test — Python 3.10 ✓
- Test — Python 3.11 ✓
- Test — Python 3.12 ✓
- Test — TypeScript ✓
- Test — Rust + Clippy ✓

Will Flores · Founder, Ward Protocol · June 11, 2026

wardprotocol.org · api.wardprotocol.org · wardprotocol.org/assurance · github: wflores9/ward-protocol

4. SAST / SCA FINDINGS — AIKIDO CONTINUOUS SCANNING (18 findings)

CRITICAL	**Next.js 14 EOL (multiple CVEs)** Upgraded to Next.js 15.5.19	Fixed
CRITICAL	**starlette <1.0.1 — input validation + HTTP smuggling** Pinned >=1.0.1 in all requirement files	Fixed
HIGH	**monitor.rs .post(rpc_url) — SSRF** validate_rpc_url() at construction + call site	Fixed
HIGH	**axios <1.17.0 — cleartext + prototype pollution** npm overrides force 1.17.0	Fixed
HIGH	**index.html document.write — XSS** Replaced with safe DOM insertion	Fixed
HIGH	**11 unpinned GitHub Actions — supply chain** SHA-pinned in test.yml + publish.yml	Fixed
HIGH	**bcprov-jdk18on 1.78.1 — timing channel (CVE)** Pinned to 1.84 in pom.xml	Fixed
HIGH	**jackson-core 2.14.3 — buffer overflow + DOS** Pinned to 2.15.0 in pom.xml	Fixed
MEDIUM	**Rust transitive deps (h2, rustls, openssl)** cargo update	Fixed
MEDIUM	**uuid 8.3.2 — buffer overwrite (CVE-2026-41907)** Bumped to 14.0.0 in package.json + SDK TS	Fixed
MEDIUM	**logback-core 1.3.15 — arbitrary code exec** Pinned to 1.3.16 in pom.xml	Fixed
MEDIUM	**flows.py SSRF via WARD_API_BASE** _validate_api_base() rejects non-https	Fixed
MEDIUM	**13 assert statements — stripped by python -O** Replaced with explicit RuntimeError/ValueError	Fixed
MEDIUM	**Git history — pycryptodome .venv test vectors** git filter-repo: 2,241 blobs, 399 commits rewritten	Scrubbed
LOW	**01-vault-registration.ts SSRF** Hardcoded https:// constant — AI: hard to exploit	False +
LOW	**webhooks.py urllib SSRF** Validated by _validate_api_base(); Aikido AI downgraded	False +
LOW	**postcss XSS (moderate)** Inside Next.js internals; no fix without major downgrade	Accepted
LOW	**ws memory disclosure (moderate)** Inside ethers internals; no upstream fix available	Accepted

5. MAINNET READINESS — B1 NETWORK CONFIG GUARD (CLOSED)

New file: ward/_network.py

Six production constructors (ClaimValidator, Resolver, EscrowSettlement, PoolHealthMonitor, VaultMonitor, WardClient) require explicit WARD_XRPL_URL and WARD_XRPL_WS environment variables. Missing vars raise ConfigurationError with copy-paste export commands for both mainnet and testnet. WARD_NETWORK mismatch is a hard failure even when the URL is passed explicitly. 13 new TestNetworkConfig tests cover all failure and success paths.

6. AUDIT DELIVERABLES — COMMITTED TO MAIN

AUDIT_REPORT.md
Full findings across all 5 categories — deps, mainnet readiness, bug hunt, multi-chain, hygiene. Includes git history scrub record.

MAINNET_READINESS.md
4 numbered blockers, go-live checklist, remediation paths. B1 (network config) closed. B2–B4 scoped with effort estimates.

MULTICHAIN_GAPS.md
42 adapter stubs inventoried, XRPL leakage map, 9-step refactor list. Stellar recommended as second mainnet chain (~1 day level-1 adapter).

7. GIT HISTORY SCRUB — COMPLETED June 11, 2026

Tool: git filter-repo · Blobs removed: 2,241 · Commits rewritten: 399

All findings originated in sdk/python/.venv — pycryptodome library self-test vectors (ECDH, HPKE, ECC, RSA, PGP, KDF). Briefly committed, deleted in b878053. Not production secrets. Not reachable at Ward runtime. tests/conftest.py inspected: pure test fixtures, no real secrets.

8. DEPENDENCY STATE — POST-AUDIT

Ecosystem	Package	Was	Now	
Python	starlette	0.36.3	**>=1.0.1**	✓
Python	fastapi	transitive	**>=0.136.0 (CI pin)**	✓
Node	Next.js	14.x (EOL)	**^15.3.4**	✓
Node	axios	1.0–1.15.2	**1.17.0 (override)**	✓
Node	uuid	8.3.2	**^14.0.0**	✓
Rust	h2 / rustls / openssl	various	**cargo update**	✓
Java	jackson-core	2.14.3	**2.15.0**	✓
Java	bcprov-jdk18on	1.78.1	**1.84**	✓
Java	logback-core	1.3.15	**1.3.16**	✓

9. PRODUCTION HEALTH CHECK — Verified June 11, 2026 02:51 UTC

Endpoint: https://api.wardprotocol.org/health
Status: HTTP 200 — healthy
Version: 0.2.6
ward_signed: false
Invariant: ward_signed = False — always
Demo Page: wardprotocol.org/demo — HTTP 200