Worrachatr Phoonbamphen

App Developer & Independent Penetration Tester — mobile/web product engineering and security testing, per engagement

Chiang Mai, Thailand (UTC+7) · remote worldwide · willworachat@gmail.com · linkedin.com/in/worrachatrp · Portfolio & published reports: worrachatrph.web.app

PROFILE

Offensive-security specialist who tests web applications, APIs, smart contracts, blockchain infrastructure and AI/LLM features as a real adversary would: manual, hypothesis-driven, and proven with a working proof-of-concept. I have run 96 authorised bug-bounty and audit-competition engagements across 18 platforms (HackerOne, Bugcrowd, Immunefi, Cantina, Sherlock, HackenProof, CertIK, Google VRP, Meta and others), demonstrating Critical account-takeover and authentication-bypass chains against exchanges, payment providers and custody platforms, and clearing whole protocols with documented coverage. I also design and ship production mobile and web software end to end, so my findings come with remediation an engineering team can actually apply. Before software I spent eighteen years in high-consequence industries — seven years of engineering in precision electronics manufacturing, then eleven as a flight dispatcher in commercial aviation. I work job by job on fixed scope, not as an employee.

96
authorised programs engaged across 18 platforms

18
bounty / audit platforms

19
published research summaries (portfolio site)

1,000 USDC
paid bounty, Redbelly Network (2 valid findings)

SERVICES OFFERED

Web application & API penetration testing

- Auth, session, SSO (SAML / OAuth 2.1 / OIDC)
- IDOR & multi-tenant boundaries, privilege escalation
- Business-logic and approval-workflow abuse
- REST, GraphQL, WebSocket, gRPC

Smart-contract & blockchain audit

- Solidity / EVM: lending, vaults, AMMs, bridges, staking
- Solana (Anchor / Rust), CosmWasm, Cadence, FunC
- L1/L2 clients, precompiles, RPC, bridge verifiers, ZK circuits
- Economic invariants, rounding, reentrancy, replay, upgradeability

AI / LLM application security

- Direct & indirect prompt injection, data exfiltration
- Agent tool-authorisation scope and side-effects
- MCP servers, grounding-channel leaks
- Reporting: CVSS / platform severity, CWE, PoC, retest letter

SELECTED ENGAGEMENTS (2026) — FULL SUMMARIES AT WORRACHATRPH.WEB.APP

TARGET · PLATFORM	SCOPE	RESULT
Redbelly Network · Hashlock	L1 consensus, custom RPC namespace, identity/KYC dApp (Averer)	Paid 1,000 USDC 3 findings confirmed valid by vendor: authentication weakness, exposed backend service key, phishing-dependent PII exposure
Blockchain.com · Bugcrowd	WebSocket real-time API, pairing key exchange, KYC tiers	Critical end-to-end account takeover demonstrated (unauthenticated channel subscription chained into wallet-credential decryption); confirmed accurate, duplicate
Memento DFM · YesWeHack	DeFi web app, 85 API endpoints across 5 testnets	Critical JWT signature-verification bypass + High broken access control; duplicate / RTFS
Rapyd · Bugcrowd	SAML SSO, merchant dashboard, 203 payment-API endpoints	SAML NameID-injection cross-account login with live PoC; cross-merchant data exposure; duplicates
LaunchDarkly · Bugcrowd	Feature-flag REST API, 242 endpoints, SOC 2 approval workflow	High approval-workflow bypass via 3 write paths; known issue
BitGo · Cantina	eth-multisig v2/v4 wallet contracts	Critical cross-chain signature replay (missing chain-id); duplicate
Morpho Midnight · Cantina competition	Fixed-rate P2P lending, ~1,900 lines core + bundler	4 Medium DoS at price-tick boundaries; invariant analysis found no Critical
Circle · HackerOne	Malachite BFT consensus, Stellar CCTP, Arc Remote Signer	7 reports: consensus overflow, nonce-replay window, stateless-signing gap; 6 duplicate, 1 informative
Crypto.com · HackerOne	Exchange REST/WS, merchant & NFT GraphQL, KYC API	Medium unauthenticated mutation; two-account IDOR sweep clean everywhere
Google NotebookLM · Google VRP	LLM search-grounding channel	Autonomous exfiltration of private document identifiers with zero user interaction; known issue
Stripe · HackerOne	Payments API, MCP OAuth 2.1, Connect, Smokescreen source	Coverage report: 316 hosts, 16 redirect-URI bypass techniques, 12 leads closed; clean

Quantus Network · Immunefi comp.	Post-quantum Substrate L1, ML-DSA, Plonky2 zk-wormhole circuits	Coverage report: 10 surfaces incl. leaf + aggregator circuit soundness; clean
Telcoin PSV / Zynk · HackenProof	Solana Anchor programs, Token-2022, timelock governance	Coverage reports: 100% line-by-line, executable Anchor PoC built to test the one Critical hypothesis; clean
15 further engagements	L2 rollups & bridges, CosmWasm CDP/AMM, MPC custody, DePIN bridge, perpetuals DEX, AI commerce agent	Critical / High / Major findings reported, still under vendor review; details available under NDA

PROFESSIONAL EXPERIENCE

Independent Security Researcher & Penetration Tester · Phoenix5981 Security (own research label) May 2025 – present · remote

- Ran 96 authorised engagements on 18 platforms, from black-box web/API testing of exchanges and payment providers to source-level audits of Solidity, Rust/Anchor, CosmWasm, Go and Substrate codebases.
- Built a repeatable methodology: threat-model and prior-audit baseline first, systematic recon (150–300 endpoints per target), two-tenant authorisation testing, invariant-first contract review, fork-tested PoCs, then a report with dollar/data impact and specific remediation.
- Publish a coverage summary for every target, including clean results, so clients know exactly what was tested and cleared.

Full-Stack Engineer (product engineering) · Phenovative Studio (own software-development studio), Chiang Mai May 2025 – present

- Sole engineer on **FixIt** (fixitth.com): a home-repair marketplace shipped to iOS, Android and web (React Native / Expo, TypeScript, Firebase Auth, Firestore, Cloud Functions, Hosting), with an admin dashboard, partner onboarding and verification, an SMS engagement pipeline and App Store / Play submissions.
- Own security and infrastructure end to end: Firestore rules, auth and device-trust design, secrets handling, CI/CD and release signing.

Earlier career · electronics manufacturing engineering, then commercial aviation 2004 – 2022

- **Flight Dispatcher — Thai Airways International** (2011 – October 2022): route and fuel planning, weather and NOTAM analysis, payload and regulatory limits, and in-flight monitoring — time-critical operational decisions inside a safety-critical regulatory framework.
- **Engineering — precision electronics manufacturing** (2004 – 2011): R&D engineer at **Fujitsu** (hard-disk drives, 2004–2005), process engineer at **Delta Electronics** (PCB assembly, 2005–2006) and **Nidec** (electric motors, 2006–2007), maintenance engineer at **Rohm Integrated** (semiconductors, 2007–2009), quality engineer at **Sony** (DSLR cameras, 2009–2011).

TOOLING & TECHNICAL SKILLS

Testing & analysis

- Burp Suite, custom Python tooling, Playwright / headless-browser instrumentation, JS-bundle and API-surface mining
- Foundry, Anchor, Solana CLI, Substrate toolchain, Sourcify bytecode-vs-source verification, fork-based exploit simulation
- Frameworks: OWASP Top 10, OWASP Smart Contract Top 10, CWE Top 25, CVSS v3.1/v4

Languages & platforms

- Read/audit: Solidity, Rust, Go, TypeScript/JavaScript, Python, CosmWasm, Cadence, FunC
- Build: TypeScript, React / React Native, Node.js, Python, Firebase / GCP
- Languages: Thai (native), English (professional working)

EDUCATION

Software engineering — self-directed study · from Java, then JavaScript/TypeScript, React, Node.js, cloud architecture 2022 – present

- **IBM full-stack & DevOps certificate track** (Coursera, 2022) — 9 courses: Getting Started with Git & GitHub · Linux Commands & Shell Scripting · Python for Data Science, AI & Development · Developing AI Applications with Python and Flask · Containers with Docker, Kubernetes & OpenShift · Application Development using Microservices and Serverless · Continuous Integration and Continuous Delivery (CI/CD) · Introduction to Agile Development and Scrum · Test and Behavior Driven Development.
- **freeCodeCamp** — JavaScript Algorithms and Data Structures (2023).

Bachelor of Engineering (BEng), Electrical Engineering · King Mongkut's University of Technology North Bangkok 1999 – 2003

ENGAGEMENT TERMS

Per-project, fixed-scope, fixed-price contracts (typical: 5–10 days for a web/API pentest, 1–3 weeks for a smart-contract audit); retainers for continuous release review. Testing only against systems the client owns or is authorised to have tested, under a signed statement of work and NDA. Deliverables: executive summary, technical findings with PoCs, coverage statement, one free retest round and a retest letter. Response within one business day.

References and full technical reports for every published engagement: worrachatrph.web.app · Confidential engagement details available under NDA · Last updated September 2026