Teycir Ben Soltane



Security Researcher & Tooling Engineer | CVE author | 15+ Years Enterprise Engineering

Availability: remote B2B contractor/consultant from Tunisia (direct or via Deel/Remote), international invoicing, no visa sponsorship needed; open to relocation.

Email: teycir@pxdmail.net **Website:** teycirbensoltane.tn **GitHub:** github.com/Teycir
Dev.to: dev.to/teycir **Medium:** medium.com/@teycir_44045 **LinkedIn:** linkedin.com/in/teycir-ben-soltane-4118a1240

PROFESSIONAL EXPERIENCE

Founder & Tech Lead — Teycitek

2023 - Present | Independent security research & open-source security tooling

Independent vulnerability research and open-source security tool building. Research is published through a vendor-first coordinated-disclosure process with dual-CNA submission (VulnCheck + Vulners), public proof-of-concept artifacts and SHA256-verified evidence archives — 4 CVEs published.

- Independent vulnerability research across MCP protocols, autonomous agent tool calling, and cryptographic access schemes — 4 CVEs published
- Design and ship open-source, developer-first AppSec tooling in TypeScript, Rust, Python, and C#
- Built automated pre-production security gates to catch broken authorization, injection, and logic flaws before merge
- Run a professional coordinated-disclosure pipeline end to end: vendor-first contact, dual-CNA submission (VulnCheck + Vulners), public evidence repos
- Build and ship open-source security tooling used by practitioners (BurpAPISecuritySuite 384★, MCPwn, AgentSec, SkillsGuard)

Technologies: Rust, TypeScript, Python, C#, Burp Suite Pro, Cryptography, WebRTC, ZKP, Cloudflare Workers/KV/D1

Tech Lead — Essilor

Créteil, France | 2019 - 2023

Led a 4-year enterprise migration of mission-critical institutional contact-lens billing software from ASP to ASP.NET, embedding shift-left application security and automated code quality gates into the development lifecycle.

- Replaced vulnerable legacy string-parsing with a custom Roslyn-based rule interpreter for billing logic, eliminating code injection risks and ensuring deterministic execution
- Led and mentored a 4-person senior developer team in Manila: owned pull request security reviews, threat modeling, architecture validation, and coding standards
- Established TFS branch protection policies, mandatory gated PR builds, and automated unit testing to prevent regressions and insecure code deployments
- Optimized and hardened production SQL Server & Oracle databases (T-SQL indexing, stored procedures, parameterized queries) preventing SQL injection risks
- Authored comprehensive English-language security and technical guides; provided Level 3 production support

Technologies: C#, WCF, ASP.NET MVC, Roslyn AST Interpreter, SQL Server 2016, Oracle 11g, TFS, Entity Framework, BizTalk

Tech Lead / AppSec — Conduent (Ex-Xerox)

Valence, France | 2018 - 2019

Led architectural evolution and security hardening of customer ticketing and billing systems, delivering sensitive transaction and smart-card workflows end-to-end.

- Designed and implemented end-to-end encryption for sensitive customer and payment data flows across WCF web services and Oracle databases
- Supervised and coached 2 junior developers in secure coding standards, defensive programming, and threat modeling
- Served as Level 3 security escalation point for critical production anomalies, patching vulnerabilities before release
- Designed and delivered core invoicing functionality from PL/SQL data layer through C# secure service integration

Technologies: C#, WCF, SOAPui, Cryptography/Encryption, Oracle 11g, Git, TFS, Jira, Visual Studio 2015, Entity Framework

C# Software Engineer / Security — Docapost (Ex-Monéo Applicam)

Tunis, Tunisia | 2016 - 2017

Developed gas station fleet management platform for Total Morocco service stations, enforcing strict transaction authorization, audit logging, and anti-tamper controls.

Technologies: C#, VB, WCF, Silverlight 5, Oracle 11g, Git, Jira, Visual Studio 2015, Entity Framework

C# Software Engineer — Deltametrics

Tunis, Tunisia | 2016

Built high-throughput web crawler tracking insider trades for fund managers, with anomaly detection algorithms and real-time alert mechanisms for block trade patterns.

Technologies: C#, WinForms, Windows 7, Visual Studio 2012, .NET 4.5, MySQL, SVN, HTMLAgilityPack

C# Software Engineer — Carmignac Gestion

Paris, France | 2014 - 2016

Developed Pyramid1: financial reporting engine for hedge fund managers. Hardened data access layers, implemented role-based controls, and automated batch deployment safeguards.

Technologies: C#, ASP.NET, Windows 7, Visual Studio 2010, .NET 4, SQL Server 2012, TFS, DevExpress 13

Early Career — C# Software Engineer

Paris Region, France | 2008 - 2013

Five years of enterprise software engineering across cyber security, investment banking, and media:

- **Kernel Networks** (2011-2013) - Cyber security solutions, identity and access management (IAM), and enterprise directory integration
- **Eurosport** (2010-2011) - Scalable web services and media delivery APIs
- **CACIB / Ex-Calyon** (2009-2010) - Investment banking financial applications and compliance reporting
- **AXA Risk Management** (2008) - Actuarial and insurance risk management platforms

Technologies: C# 2.0-4.0, ASP.NET MVC, WinForms, T-SQL, LINQ to SQL, SQL Server 2005/2008, jQuery, Visual Studio, SVN

POSITIONING

Security researcher and tooling engineer — a rare combination. Most vulnerability researchers cannot ship production-grade tools; most tool builders do not run coordinated disclosure. I do both: 15+ years building and leading C#/.NET and TypeScript systems for CAC40 clients, plus applied security research and coordinated vulnerability disclosure with published CVEs. Open to Security Researcher, Security Tooling Engineer, or Application Security Engineer roles: remote B2B/contractor, or hybrid/on-site with relocation.

SUMMARY

Security researcher and tooling engineer with 15+ years architecting and securing enterprise software for CAC40-listed clients in France. Deep C#/.NET and TypeScript engineering applied to security: agent and MCP security review, API/AppSec pentesting, and shift-left AppSec (AST/Roslyn rules, automated threat modeling, PR security gating). Author of widely adopted offensive security tools (BurpAPISecuritySuite 384★, Timeseal 65★) and AI-agent security tooling (MCPwn, AgentSec, SkillsGuard), with 4 published CVEs — now focused on independent vulnerability research and open-source security tooling.

SKILLS

AppSec & DevSecOps

Shift-Left Security | Threat Modeling | PR Security Gating | Static Analysis (SAST) | Roslyn AST Analyzers | OWASP Top 10 | OWASP API Top 10 | Secure Code Review | Burp Suite Pro | API Pentesting | MCP Security

Cryptography & Privacy

End-to-End Encryption | Split-Key Vaults | Zero-Knowledge Proofs | Time-Locked Encryption | WebRTC P2P | Plausible Deniability

Programming Languages

C# | TypeScript | Python | Rust | SQL | JavaScript | Solidity | Java | C | HTML | CSS

C# / .NET Ecosystem

ASP.NET Core/MVC | WCF | WinForms | Entity Framework | Roslyn Parser | LINQ | BizTalk

TypeScript & Frontend

React | Next.js | Node.js | Cloudflare Workers/KV | Tailwind CSS | REST | GraphQL

Databases & Systems

SQL Server | Oracle 11g | PostgreSQL | MySQL | Docker | Git | TFS | Jira

Leadership & Practices

Technical Architecture | Team Mentoring | PR Security Validation | Workload Estimation | Secure SDLC | AI Pair Programming

OPEN SOURCE PORTFOLIO

BurpAPISecuritySuite (384★) - github.com/Teycir/BurpAPISecuritySuite - Burp Suite Pro extension for automated REST/GraphQL/SOAP API security testing: 15 attack vectors, 108+ payloads, OWASP API Top 10
Timeseal (65★) - github.com/teycir/timeseal - Time-locked cryptographic vault with Dead Man's Switch, split-key architecture, zero-knowledge proofs
MCPwn (31★) - github.com/Teycir/Mcpwn - Security scanner for Model Context Protocol servers detecting RCE, SSRF, prompt injection, tool poisoning, authz bypass
Sanctum (50★) - github.com/teycir/sanctum - Zero-trust encrypted vault with cryptographic plausible deniability
Assumptions (20★) - github.com/Teycir/Assumptions - SKILL turning a code diff into an evidence-backed ledger of assumptions and falsification tests
SkillsGuard (15★) - github.com/Teycir/SkillsGuard - Static security scanner for AI agent skill packages detecting malicious SKILL.md files
AgentSec (5★) - github.com/Teycir/AgentSec - Local-first Rust CLI scanning LLM wrappers, RAG databases, and AI agents for OWASP Top 10 flaws
Plus ApiHunter, GhostChat, and more - full portfolio at github.com/Teycir

CTF

ARKX AI Agent Security CTF: 3,300 points, rank MASTER. 8 Advanced/Expert levels solved by hand and published as write-ups (root cause, CWE and OWASP LLM mapping, CVSS, remediation). Exploit chains on AI agent tool calling and broken authorization.
Tool capability: eval() injection behind a calculator tool (CWE-95, **High 7.7**); blind OS command injection with out-of-band exfiltration through the platform's own request log (CWE-78); unsafe YAML deserialization to command execution (CWE-502).
Validation and authorization: path traversal via validate-before-decode (CWE-22/180); forged badge with no signature check, clearance read from attacker-controlled claims (CWE-347, **High 8.1**); authorization keyed on a caller-supplied session id, chained through an error-message key leak and cache poisoning (CWE-639).
MCP and business logic: protected value exposed as a readable MCP resource (CWE-284/200); caller-supplied price with no execution-time balance check (CWE-472/840).
Takeaway: six of the eight map to OWASP LLM06 Excessive Agency, and none was solved by getting an instruction past the model: the weakness was in the tool, MCP and API contract around the LLM, not the LLM itself.
Method: one hypothesis per test, proven with side effects (DNS canaries, server-side logs) rather than chat output; impact split into demonstrated / available but not exercised / not tested; no CVSS where the inputs were not established.
CTF write-ups on GitHub

VULNERABILITY DISCLOSURES

CVE-2026-137091 (VulnCheck): EverOS cross-origin local file disclosure via permissive CORS + file:// ingestion — **High 8.2**.
CVE-2026-132121 (VulnCheck): Supergateway Cross-Site WebSocket Hijacking via missing Origin validation (stdio → WS) — **High 8.1**.
CVE-2026-131857 (VulnCheck): Supergateway unauthenticated DoS via prototype-inherited sessionId (stdio → SSE) — **High 7.5**.
CVE-2026-132122 (VulnCheck): agentic-radar malicious .env hijacks OPENAI_BASE_URL, steals OpenAI API key — **Medium 4.7**.
All responsible disclosures on GitHub
Exploit development scope: application-layer and logic exploits (injection, authz bypass, sandbox-escape via trusted execution tiers, agent/tooling abuse). Memory-corruption exploit development (browser/kernel/pwn) is adjacent territory actively being built — not claimed here.

EDUCATION

Master of Science in Data Science
Openclassrooms & Centrale Supélec | April 2022
Master of Science in Computer Science (Valedictorian)
University Marne-La Vallée | July 2008
Master of Science in Political Science
Panthéon-Sorbonne Paris 1 | 2005

CERTIFICATIONS

Claude Academy: Claude Code in Action
Anthropic | September 2026 - ID: 29735452894d8394a3b1d7d8cee443e6
Claude Academy: Claude Code 101
Anthropic | September 2026 - ID: 89a0d62909b07adcce5aa8f936904187
Claude Academy: AI Fluency: Framework & Foundations
Anthropic | September 2026 - ID: d60f0675da56176cd5a9cc0f8fec16e6
Microsoft AI Security Controls
Microsoft Learn | 2026
Microsoft Fundamentals of AI Security
Microsoft Learn | 2026
Microsoft MCPD .NET 4 Desktop & Web
Microsoft | 2009 - 2014 - ID: 6865160
Cyfrin Updraft: Smart Contract Security & ZKP
Cyfrin | August 2025 - March 2026

LANGUAGES

Arabic: Native | **French:** Native | **English:** Fluent
Italian: Spoken | **Spanish:** Basic | **German:** Basic

Last updated: November 2026