

+33 761893808  
Paris, France  
yassine@damiri.fr

# Yassine Damiri

Cybersecurity Consultant / Security Engineer

Portfolio: [Damiri.fr](https://damiri.fr)  
[github.com/Yasha-Ops](https://github.com/Yasha-Ops)  
[linkedin.com/in/yassine-damiri](https://linkedin.com/in/yassine-damiri)

Experienced Software Security Engineer and Cybersecurity Consultant with expertise in offensive security, vulnerability and patch management, and secure software lifecycle. I have conducted 100+ penetration tests and 20+ code, architecture, and configuration audits for CAC40 enterprises and government organizations. Recognized in multiple Hall of Fame programs, author of several CVEs, and speaker at international conferences. Open to new opportunities in software security, SRE, vulnerability management, or cybersecurity consulting.

## COMMON VULNERABILITIES AND EXPOSURES (CVEs)

<b>CVE-2025-29660</b>	Arbitrary remote code execution on Yi IOT XY-3820
<b>CVE-2025-29659</b>	Remote Command Execution (RCE) via a Hidden Backdoor on Yi IOT XY-3820
<b>CVE-2025-25680</b>	Arbitrary Code Execution via a specially crafted QR code
<b>CVE-2025-65287</b>	Unauthenticated directory traversal vulnerability on SNMP Web Pro 1.1
<b>CVE-2025-65289</b>	Remote Unauthenticated Cross site scripting (XSS) vulnerability on the Mercury MR816v2 Router
<b>CVE-2025-65288</b>	Buffer Overflow leading to DoS and potential Code Execution on the Mercury MR816v2 Router
<b>CVE-2026-22809</b>	Regular Expression Denial of Service (ReDoS) vulnerability on Tartaucitron.js opensource library

## HALL OF FAMES

<b>Indonesian Government</b>	Honored in the Hall of Fame of the Indonesian government following the discovery of a major web vulnerability.
<b>Asus</b>	Recognized in Asus' Hall of Fame after identifying multiple critical vulnerabilities (CVEs) in their routers
<b>Ohio Secretary of State</b>	Entered the Hall of Fame of a U.S. institution after uncovering a widespread web vulnerability with critical impact.
<b>Mercedes</b>	Listed in Mercedes-Benz's Hall of Fame following the identification of a vulnerability that granted privileged initial access to the company's information system.
<b>Vim</b>	Listed in Vim's Hall of Fame after discovering a flaw leading to full account compromise (account takeover).
<b>Linksys Cisco</b>	Discovered a CVE affecting hundreds of thousands of Linksys routers exposed on the Internet.

## PROFESSIONAL EXPERIENCE

### Cybersecurity Consultant / Pentester & Red Teamer

February 2024 — Present

*Ernst & Young (EY)*

*Paris, France*

- Conducted over 100 penetration tests and Red Team operations for CAC40 enterprises across energy, nuclear, banking, insurance, and industrial sectors.
- Led web, internal network, mobile, and hardware security assessments, providing actionable recommendations to strengthen defenses.
- Performed architecture and configuration audits, aligned with ISO 27001/27002, PSSI, SWIFT CSCF, and best practices.
- Developed R&D initiatives for physical Red Team implants and implemented tooling for source code analysis supporting audit teams.
- Presented technical findings to stakeholders and contributed to strategic cybersecurity decisions.

### Bug Bounty Hunter / Pentester

December 2022 — Present

*[Bentley, Cisco Linksys, Ohio Secretary of State, Vim, Mercedes, Asus]*

*Paris, France*

- Identified and responsibly disclosed vulnerabilities across numerous public and private organizations, many recognizing contributions in their Hall of Fame programs.
- Actively participated in HackerOne and Bugcrowd programs, collaborating with security teams to remediate risks.
- Conducted detailed security research and contributed to community knowledge through public advisories and CVE reports.

### IT Manager / Volunteer Cybersecurity Lead

January 2021 — Present

*CRI - Conception Réalisation Ingénierie*

*Casablanca, Morocco*

- Built the entire cybersecurity structure from scratch on a volunteer basis, including network overhaul and Active Directory deployment.
- Hardened configurations according to CIS, ANSSI, and DGSSI recommendations, and implemented patch management across 50+ systems.
- Designed and deployed a Wazuh-based SOC with automated AI-assisted XDR incident response and custom detection rules.
- Developed PSSI policies, managed hypervisors, and ensured operational cybersecurity across organizational systems.
- Took ownership of strategic cybersecurity responsibilities, mentoring teams and guiding the organization's security posture.

## Security and Network Engineer / IT Infrastructure Consultant

Bolton Group

January 2024 — December 2024

Agadir, Morocco

- Designed and deployed a resilient internal network with redundancies suitable for industrial operations.
- Implemented patch management processes and built a fully operational SOC with alerting, monitoring, and incident response workflows.
- Conducted security hardening and compliance audits for Active Directory and critical systems.
- Collaborated with internal teams to optimize IT processes and ensure operational continuity.

## Fullstack Developer / Blockchain Explorer & Smart Contracts

Massa Labs

January 2023 — February 2024

Paris, France

- Designed and implemented a hybrid architecture combining centralized and decentralized components for the Massa blockchain explorer.
- Optimized system design to handle peak traffic of over 2 million daily users, ensuring performance, scalability, and reliability.
- Developed fullstack components using React, Node.js, gRPC, Rust, and integrated DevSecOps pipelines for secure deployments.
- Ensured transparent and accessible visualization of blockchain transactions through UI/UX design and API optimizations.

## Fullstack Developer & DevSecOps

Domany's

September 2022 — January 2024

Paris, France

- Overhauled business applications and software architecture for public housing platform used by hundreds of users daily.
- Refactored critical codebases to handle scale-up requirements and integrated CI/CD pipelines with security checks for deployment and data leak prevention.
- Implemented DevSecOps practices, automated security testing, and ensured operational resilience for production systems.

## EDUCATION

Computer Science Engineer, Systems, Networks, and Security Engineer at EPITA

2019-2024

Licence of Computer Science, Healthcare (parallel program) at UPEC

2019-2022

## SKILLS

Computer Languages	Golang, Next.js, TypeScript, C/C++, CUDA, Rust, Blockchain, Python, Git, $\text{\LaTeX}$ , Bash, PowerShell,
Tools	Wireshark, Nmap, Metasploit, Burp Suite, Ghidra, IDA Pro
Offensive Security	Web and network pentesting, Mobile and Hardware pentesting, Red Team operations, Exploit Development, Vulnerability Research, CVE Analysis
Defensive Security / SOC	SOC, SIEM, Wazuh, CrowdSec, MISP, ELK Stack, Active Directory, GPO Hardening, Privilege Management
Software Security / Development	Secure Software Lifecycle, Code Review, Static Analysis, Dynamic Analysis, Vulnerability Remediation, Patch Management
Human Languages	French (native), English (fluent), Arabic (native), Russian (professional)

## CONFERENCES

InCyber Forum	From IoT to compromise: analysis of a connected camera	2025
Clusir Bretagne	Cybersecurity challenges applied to connected objects	2025
EPITA TechWeek	In search of a CVE	2025

## ACTIVITIES

Teaching Assistant, EPITA (SUP / ING1)	Delivered lectures, tutorials, and practical sessions to first-year preparatory (SUP) and engineering (ING1) students, covering programming languages including C, OCaml, C, C++, Java, and JavaScript. Supported course design, graded assignments, mentored students, and provided guidance on coding best practices, problem-solving, and software development fundamentals.
iGEM MIT Hackathon	
Gotta Go Hack - LSB 2023	Developed an AI-powered onboarding platform in under 24 hours, reducing onboarding time and improving employee experience for new hires.
Gotta Go Hack - Massa 2022	Created "Gummu", a blockchain-based fair music platform with transparent funding and passive income for artists, delivering a fully functional solution in 3 days.
Gotta Go Hack - Societe Generale 2021	Led a 42-hour project developing an IoT traffic light optimization system with real-time traffic analysis and a public app, improving urban traffic flow and demonstrating AI-driven solutions.
Defnet 2023	Participated in Defnet 2023, executing advanced cybersecurity challenges and demonstrating expertise in network defense and penetration testing.
Wavegame	Completed the Wavegame cybersecurity challenge, applying offensive and defensive security techniques to identify vulnerabilities and secure systems.