Malik M.

Offensive Security Engineer

mwlik.github.io — malik.email@proton.me — Morocco (Open to relocation)

Offensive security engineer focused on web and browser exploitation. Passionate about uncovering, reproducing, and tinkering with intricate bugs in high-impact, widely used software.

Work Experience

Axis — Morocco — 2024–Present
Core Pentester — Full-time

* Performed penetration testing on tens of web applications spanning diverse tech stacks and AI-powered solutions for high-profile Moroccan clients, including the "Marhaba operation", OCP Group (Fortune 500 Arabia), and other big Moroccan companies.
* Findings from engagements led to multiple CVEs in widely-used open-source projects (see Security Advisories), as well as community-recognized security research: "Revisiting ReDoS Attacks" and "Reading your files is two flags away".

Security Advisories

Security vulnerabilities discovered and responsibly disclosed in widely-used open-source projects:

* **CVE-2026-112653:** [WebKit, Safari 27.2, mandatory engine of every iOS/iPadOS browser, >2.5B active Apple devices] — Use-after-free granting read/write access to the process's heap, enabling further exploitation.
* **CVE-2026-115575:** [tus-node-server, @tus/server ≈ 0.9M monthly downloads, and @tus/file-store] — Path traversal allowing arbitrary file deletion and modification outside the upload directory.
* **CVE-2026-118779:** [node-forge, native TLS in JavaScript, ≈ 158M monthly downloads] — ReDoS in pem.decode() allowing unauthenticated denial of service via crafted PEM input.
* **CVE-2026-24486:** [python-multipart, used by FastAPI ≈ tens of millions of downloads] — Arbitrary file write via a non-default configuration.
* **CVE-2026-22256:** [Salvo web framework] — Reflected XSS allowing arbitrary JavaScript execution in victims' browsers.
* **CVE-2026-22257:** [Salvo web framework] — Stored XSS via malicious file uploads, enabling persistent code execution.
* **CVE-2025-58362:** [Hono web framework ≈ 27M monthly downloads] — Path confusion flaw allowing bypass of proxy-level access controls (e.g. Nginx).
* **CVE-2025-59139:** [Hono web framework ≈ 27M monthly downloads] — HTTP header parsing violation allowing bypass of body size limits.
* **CVE-2025-53535:** [Better-Auth library ≈ 2.8M monthly downloads] — Open redirect affecting authentication flows across multiple routes.
* **GHSA-hq75-xg7r-rx6c:** [Better-Call framework ≈ 2.7M monthly downloads] — Routing flaw leading to cache deception attacks.

Bug Bounty — Reported 4 critical bugs

* Account takeover via XSS in a multi-million-user platform, reported through a private program ($4,500 bounty).
* Web2/XSS in `require_payment` function in `x402.fastapi.middleware` Python package can lead to ATO or funds stealing in Coinbase's x402 protocol ($2,000 bounty).
* Web2/XSS in the basic HTML paywall in `@x402/express`, `@x402/hono`, `@x402/next` packages can lead to ATO or funds stealing in Coinbase's x402 protocol ($200).
* NULL pointer dereference in a blockchain library allowing full denial of service ($400).

Browser Exploitation Research

* **CVE-2026-112653:** Discovered and exploited a use-after-free in JavaScriptCore's DFG store barrier insertion phase, turning an elided barrier into heap read/write primitives in the WebKit WebContent process (published in RewriteLab).
* **CVE-2026-3910:** Reproduced and chained Issue 491410818 with Issue 483092905 and Issue 485784597 to exploit V8 and compromise the Chromium renderer process (published in RewriteLab).
* **CVE-2025-10891:** Reproduced and exploited Issue 443765373, an integer truncation in Ignition -V8's interpreter- that leads to arbitrary bytecode execution ultimately leading to sandbox renderer process RCE.
* **CVE-2023-6702:** Reproduced Issue 40941600, a Type confusion vulnerability in V8 leading to memory corruption and RCE eventually.

CTF Experience

* **Cyber Odyssey 2024:** Secured first place in Cyber Odyssey 2024, the biggest CTF competition in Morocco, winning a total of 80,000 DH with my team FC2MK, focused on Web challenges.
* **MCSC National CTF 2024:** Secured second place with my team FC2MK, winning a total of 10,000 DH, focused on Web challenges.
* **NULL Hat Morocco 2025:** Secured second place with my team FC2MK focusing on Web challenges.
* **The International Days of Ethical Hacking (IDEH) v7 CTF:** Secured the third place with my team FC2MK, winning a total of 3,000 DH, focusing on Web challenges.

Education

1337 Coding School - University Mohammed VI Polytechnic — Khouribga, Morocco — 2023–2025
Software Engineering — Completed 42's project-based curriculum focused on systems, algorithms, and practical engineering fundamentals.

Languages

Arabic (Native), English (Professional), French (Working Proficiency).