KILIAN MURPHY

Offensive Security Analyst | Web & API Security

Geneva, Switzerland — Relocating to Amsterdam / Netherlands
EU Citizen (French & Irish) — No Work Permit Required in the Netherlands
kilian.murphy1@gmail.com | +33 6 07 68 00 98 | GitHub: Kiliankm19 | Linkedin: kilianmurphy

PROFESSIONAL SUMMARY

Offensive Security Analyst focused on web and API security testing in production and pre-production environments.

Assessed **10+ applications** and **80+ API endpoints**, delivering **60+ validated** findings with CVSS scoring, exploit validation, and remediation guidance.

Built **12+ offensive security tools** for reconnaissance, credential auditing, attack surface mapping, and web security testing. Conducted smart contract security reviews on Ethereum and Solana, identifying vulnerabilities and validating exploit paths.

TECHNICAL SKILLS

Web & API Security:	Web Application Security Testing · API Security Testing · SQLi · XSS · IDOR · SSRF · JWT Security · CORS Misconfigurations · Broken Access Control
Infrastructure:	Network Enumeration · Attack Surface Mapping · Asset Discovery
Methodology:	OWASP Testing Guide · OWASP API Security Top 10 · MITRE ATT&CK · CVSS
Tools:	Burp Suite · Nmap · Metasploit · Nessus · FFUF · Wireshark · Docker
Systems:	Linux · Windows · TCP/IP

PROFESSIONAL EXPERIENCE

Offensive Security Analyst

Cyber Experts (Internship) — Paris, France | 2026 – Present

Web & API Penetration Testing

- Mapped **80+ API endpoints**, uncovering undocumented routes, exposed Swagger documentation, and broken access control patterns.
- Tested authentication, session management, and authorization on business-critical workflows including payment and account management.
- Identified and validated **40+ vulnerabilities** including access control bypasses, session flaws, and business logic weaknesses.

Exploit Development & Attack Chain Analysis

- Demonstrated end-to-end attack chains reaching account takeover and unauthorized transaction execution in authorized production assessments.
- Analyzed JWT, CORS, and session management mechanisms to confirm end-to-end exploitability.

Critical Findings (Selected)

- CVSS 9.8 — Authentication bypass chain using JWT manipulation and session fixation techniques.
- CVSS 9.6 — Unauthenticated API access enabling full account compromise via exposed admin-level endpoints.
- CVSS 9.1 — Business logic bypass enabling unauthorized high-value transaction execution.

Blockchain Security — Ethereum & Solana

- Performed static security review of Solana (Rust/Anchor) and Ethereum smart contracts and backend infrastructure; delivered full PoC exploitation and remediation-retest cycle.
- Identified **20+ vulnerabilities** including **7 critical** findings rated CVSS 9+ (state validation issues, logic flaws, and insecure authorization patterns).

Security Reporting & Remediation Support

- Delivered 60+ structured findings with CVSS scoring and remediation guidance in collaboration with engineering teams.
- Validated security fixes at commit level to ensure proper remediation of identified vulnerabilities.

SECURITY ENGINEERING PROJECTS

12+ offensive AppSec tools focused real-world web, API, and infrastructure security testing, covering reconnaissance, authentication abuse, secrets discovery and attack path analysis. GitHub: Kiliankm19.

Selected web-based tools (some components private repositories):

- **shellcodes.app —** Shellcodes generation platform for offensive security testing (Linux & Windows).
- **xsspayloads.app —** Context-aware XSS payload generation and analysis platform for web security testing workflows.
- **reverseshell.app —** Multi-languages reverse shell generation tool supporting multiple payload types and execution context.
- **jwttool.com —** JWT offensive workbench to decode, analyze, attack, and forge tokens entirely in the browser.

EDUCATION

Secure Infrastructure Administrator — RNCP Level 6 (Master's Equivalent)
JEDHA — Paris | 2025 – 2026

BTS Management (Higher National Diploma)
Aix-Marseille University — France | 2012 – 2014

CERTIFICATIONS

- INE eJPT — In Progress [Expected: Q3 2026]
- CompTIA Security+ — In Progress [Expected: Q3 2026]

ADDITIONAL PROFESSIONAL EXPERIENCE

Operations & EMEA Logistics Management
Saint Laurent / JYSK / Jo Malone London — Geneva, Switzerland | 2015 – 2025

- Managed multi-site EMEA operations across 3 enterprise environments with 20,000+ product references.
- Led SAP ERP deployment across multiple countries; **reduced** operational reporting **errors by 20%.**

LANGUAGES

English: Full Professional Proficiency | French: Native
EU Citizen (French & Irish Passport) — entitled to work in the Netherlands.s