

Daniel Miranda Barcelona

Offensive Security · Vulnerability Research · Pentester | eJPTv2 · eWPT · ICCA · OSCP (in progress)

daniel.mirandabarcelona@gmail.com · +34 697 38 23 93 · danielmb.es · github.com/ex-calibur · linkedin.com/in/daniel-miranda-barcelona · Zaragoza, Spain

[NASA VDP] 3× official recognition · [ESA] CVE-2026-54086 · 4 published CVEs — 2026

Three confirmed and patched vulnerabilities in NASA's Core Flight System: P2 stack buffer overflow in SBN-Client, P1 path traversal in AIT-Core (BSC Logger) and P2 heap buffer overflow in ION-DTN. CVE in ESA ground-station software (SLE API Java). Four published CVEs: CVE-2026-44595/44596/42568 (YAMCS) and CVE-2026-54086 (ESA SLE API Java).

PROFESSIONAL PROFILE

Offensive security researcher who has found and reported vulnerabilities in software that flies on real satellites: 3 official NASA recognitions (VDP), a CVE in ESA ground-station software, 4 published CVEs and 4 PoCs on Exploit-DB. Experience in real-world audits (internal and external) under the PTES methodology with CVSS v3 reporting, static code analysis and reproducible PoC development with coordinated responsible disclosure. Solid development background (PL/SQL, Python, Bash) that accelerates recon and exploitation scripting. OSCP in progress. Looking to join an offensive security team in Zaragoza (on-site/hybrid) or remote in Spain.

KEY ACHIEVEMENTS & RECOGNITION

- **3× NASA VDP Recognition (2026)** — Official recognitions for vulnerabilities in the Core Flight System: P2 stack buffer overflow in SBN-Client, P1 path traversal in AIT-Core (BSC Logger) and P2 heap buffer overflow in ION-DTN. All confirmed, patched and closed.
- **ESA CVE — CVE-2026-54086** — Vulnerability in SLE API Java (sleapi-j), ESA/ESOC ground-station software: unauthenticated users trigger unhandled exceptions and resource leakage via a malformed ISP1 PDU. Confirmed, patched and disclosed in coordination with ESA.
- **3× CVEs assigned in YAMCS** — CVE-2026-44595, CVE-2026-44596 and CVE-2026-42568 (yamcs-core), with technical writeups published on The Dumpster and Arintel.
- **4× PoCs published on Exploit-DB** — EDB-52325 (CVE-2025-24071), EDB-52603, EDB-52604 and EDB-52605.
- **Confirmed and rewarded bug bounty** — CreatorIQ (XSS + CSRF token exfiltration, P2). Active research on YesWeHack and Bugcrowd programs.
- **Vulnerabilities in Basilisk** (AVSLab, University of Colorado) — PR #1362, credited as BSK-2026-001/002/003. Disclosure completed.
- **SPARQL injection** reported to CCMAD (Madrid) under coordinated disclosure; XXE vectors researched in AutoFirma.
- **Official Hak5 contributor** (payloads accepted into the USB Rubber Ducky repository) · TryHackMe Top 6% Global · Hack The Box — Hacker rank.

EXPERIENCE

Pentester & Offensive Security Researcher

Jun 2025 – Present

The Dumpster / Freelance — Spain

- Research, exploitation and documentation of vulnerabilities in real-world software (space, web and infrastructure) with reproducible PoCs and impact reports.
- Full attack chain on Active Directory: LLMNR/NBT-NS poisoning, Pass-the-Hash, Kerberoast, AS-REP roasting, NTDS dump and Golden Ticket — 49-page technical report.
- NASA VDP recognitions, ESA CVE, YAMCS CVEs and Exploit-DB PoCs (see Achievements). Responsible disclosure coordinated with INCIBE-CERT on a Spanish public-sector platform.
- Development of in-house AI pipelines for code analysis and vulnerability monitoring.

Software Engineer — Oracle / PL/SQL

Nov 2022 – Present

Ayesa / Minsait (Indra) — Zaragoza

- Development and maintenance of business-critical platforms in Oracle Forms and PL/SQL; participated in the 10g to 12c migration.
- Reduced production errors and incident resolution time through systematic debugging and automation.
- Technical training of three junior profiles. Development background applied to application pentesting — understanding how a system is built is part of knowing how to break it.

Cybersecurity Technical Writer

Oct 2025 – Present

Araintel — Zaragoza (Remote)

- Technical articles on pentesting, vulnerability exploitation and Red Team / Blue Team analysis in corporate environments (Araintel and The Dumpster).

Security Content Tester

Sep 2024 – Apr 2025

HackJourney — Remote

- Validation of CTF environments and labs (Linux, Windows, AD) in alpha/beta phases, ensuring technical consistency and offensive realism.

PROJECTS

- **OrbiDump Atlas** — Real-time satellite tracking platform (SGP4, TLE data from Celestrak/SpaceTrack/SatNOGS). Stack: FastAPI · PostgreSQL · Redis · React + Three.js, deployed on a VPS.
- **VulnWatch** — Automated GitHub repository monitoring pipeline with LLM-based verification and Telegram notifications.
- **The Dumpster** — Offensive security blog: writeups, scripts and original research.

TECHNICAL STACK

Pentesting	Burp Suite, Nmap, Nessus, Sqlmap, FFUF, Gobuster, Nuclei, Dirsearch
Post-exploit. / AD	Impacket, BloodHound, Mimikatz, CrackMapExec, Evil-WinRM, Responder, SharpHound
Web	OWASP ZAP, JWT Inspector, XSSStrike
Dev / Scripting	Python, Bash, PowerShell, JavaScript, PL/SQL, MySQL, Git, Docker
Systems	Kali, Debian, Parrot, Windows Server, Active Directory, Wireshark, VMware
Management	JIRA, Redmine

CERTIFICATIONS

- **OSCP** — Offensive Security Certified Professional · In progress
- **eJPTv2** — eLearnSecurity / INE · Apr 2024–2027
- **eWPT** — Web Application Penetration Tester, INE · Oct 2024–2027
- **ICCA** — INE Certified Cloud Associate · Jul 2024–2027
- **Google Cybersecurity** Professional Certificate · Sep 2024

LANGUAGES

- **Spanish** — Native
- **English** — B2 (EF-SET 65/100, C1 equivalent)

EDUCATION

BSc in Telecommunication Technologies and Services Engineering

2026 – In progress

Universitat Oberta de Catalunya (UOC)

Master's in Cybersecurity

May – Dec 2025

TSSciberseguridad

Security audits, ethical hacking, vulnerability management. Includes 2 real-world audits (internal + external) on client environments, PTES methodology with technical and executive CVSS v3 reporting.

Advanced Vocational Degree — Web Application Development (DAW)

2020 – 2022

CPIFP Los Enlacs

Intermediate Vocational Degree — Microcomputer Systems & Networks (SMR)

2017 – 2020

CPIFP Los Enlacs