Xavier Fernando Riofrio Machado

Offensive Security Expert | Application Security Testing (Web, API, Mobile, Cloud) | Fintech and Banking Security

PROFESSIONAL PROFILE

Senior offensive security specialist with experience across web, API, mobile, cloud, and infrastructure security, focused on application security testing, vulnerability validation, and remediation-oriented reporting.

I have led offensive assessments in fintech and high-exposure environments, with practical experience in business logic abuse testing, authentication and authorization weaknesses, reverse engineering, and security control validation across end-to-end attack paths.

I work closely with engineering, architecture, and product teams to translate findings into actionable remediation plans and measurable security improvements.

CORE FOCUS

- Application security testing across front-end, back-end, APIs, mobile, cloud, databases, and integrations.
- Business logic abuse testing and authentication/authorization validation.
- Security test case definition, evidence collection, and reproducible validation workflows.
- Vulnerability prioritization and remediation guidance for technical and business stakeholders.
- Security control reviews aligned with secure software development practices.
- Practical support for vulnerability management and follow-up validation.

WHAT I DO

- Execute offensive security tests across web, API, mobile, and cloud attack surfaces.
- Validate exploitability of application vulnerabilities and cross-layer attack paths.
- Document technical findings with evidence, risk context, and remediation actions.
- Contribute to security requirement validation and secure-by-design recommendations.
- Support vulnerability lifecycle follow-up with product and engineering teams.
- Produce clear communication for both technical and executive audiences.

SELECTED IMPACT

- Presented original security research at **DEF CON 34**, **BSides Colombia**, and **PWN OR DIE**.
- Led offensive security assessments across mobile, API, web, and cloud environments in fintech contexts.
- Conducted external exposure analysis and prioritized high-risk issues for focused remediation.
- Executed end-to-end KYC and biometric security assessments, including advanced abuse-case validation in controlled scenarios.
- Produced technical findings and remediation recommendations for architecture, development, and security teams.
- Built reusable testing artifacts, including a KYC mobile pentesting checklist across multiple attack surfaces.

SECURITY TESTING APPROACH

- Threat-informed planning based on high-risk business flows and attacker behavior.
- Test design focused on exploitability, impact, and reproducibility.
- Cross-layer validation across client behavior, APIs, and server-side controls.

- Prioritization of findings using severity and business impact context.
- Clear remediation paths and follow-up validation criteria.

RESEARCH AND PROFESSIONAL EXPERIENCE

Offensive Security Expert - Deuna (Ecuador / LatAm)

December 2023 - Present Mobile Ethical Hacker - API Pentesting - Biometric Security Research - KYC Security

- Led offensive security assessments across mobile, API, web, and cloud attack surfaces.
- Executed end-to-end KYC and biometric assessments, including liveness abuse-case validation and mobile reversing workflows.
- Drove attack-surface analysis and remediation prioritization for critical and high-risk findings.
- Produced remediation-focused recommendations for architecture, development, and security operations teams.

Cyber Security Specialist - Unicomer Group (Remote)

January 2023 - November 2023 Ethical Hacking - Microsoft Defender Security Administrator - Cloud Security - Security Analysis

- Led ethical hacking activities and coordinated security analysis across business systems and applications.
- Supported cloud and defensive operations to strengthen security posture.
- Identified vulnerabilities and documented practical mitigation guidance for internal teams.

Security Engineer (Penetration Testing) - CERN (Geneva, Switzerland)

April 2021 - June 2022 Web Penetration Testing, CI/CD, Vulnerability Analysis, Code Security

- Conducted web penetration testing and vulnerability analysis for critical research infrastructure.
- Reviewed CI/CD and code security exposure, documenting exploitability and remediation paths.
- Partnered with technical teams to improve application security and reduce repeat issues.

Independent Security Consultant & Bug Bounty Researcher - Self-employed

December 2017 - Present Trainer, Penetration Testing Consulting, Bug Bounty Programs

- Delivered security consulting, offensive assessments, and technical reporting across web, mobile, and API environments.
- Supported organizations with remediation strategy, risk communication, and security testing guidance.
- Published practical knowledge from research and bug bounty work to improve testing effectiveness.

Cyber Security Researcher - Universidad de Cuenca (Ecuador)

May 2018 - March 2021 Security Research, White-Black Box Hacking, Zero-day Attacks

- Conducted cybersecurity research focused on white-box and black-box testing approaches.
- Developed research outputs related to attack analysis and vulnerability discovery.

Professor - Universidad Nacional de Loja (Ecuador)

October 2018 - April 2019 Teaching and Research in Cybersecurity

Delivered lectures and conducted research in the cybersecurity field.

Software Developer - Universidad de Cuenca (Ecuador)

August 2014 - August 2016 Frontend (AngularJS), Backend (Java Spring Boot)

EDUCATION

Degree	Institution
MSc Cyber Security with Distinction	University of Birmingham, United Kingdom
BSc in Computer Science and Engineering	Universidad de Cuenca, Ecuador
Administration and Public Management	Universidad Tecnica Particular de Loja, Ecuador

CERTIFICATIONS

Certification	Issuer
Certified Ethical Hacker Master (CEH-T+P)	EC-COUNCIL
eLearnSecurity Junior Penetration Tester (eJPT)	INE
Certified API Penetration Tester (CAPIPEN)	The SecOps Group

PUBLICATIONS

- A Design for a Secure Malware Laboratory
- Technical Selection Guide for Face Liveness Providers: Security Assessment and Robustness Against AI-Based Attacks
- The Zero-day Attack: Deployment and Evolution
- Development of the CMS Detector for the CERN LHC Run 3

Additional publications available upon request.

TALKS

Conference	Location	Year	Talk
DEF CON 34	**Las Vegas, USA**	**2026**	**"Your APP Thinks I'm You: A Complete Kill Chain Against Mobile App Security"**
BSides Colombia	Colombia	2026	"Your Brain > Your Toolkit: Real Bugs, Zero Code, Zero Tools"
PWN OR DIE	Ecuador	2025	"When Your Mind Becomes the Exploit: No Code, No Tools"

COMMUNITY CONTRIBUTIONS

- Published technical content on mobile security, KYC abuse, deepfake risk, and API pentesting.
- Shared conference talks and practical guidance for LatAm security communities.
- Created reusable checklists, notes, and references for hands-on offensive testing.
- Promoted applied security learning through practical write-ups and collaborative sharing.

TECHNICAL SKILLS

Category	Skills
Application Security	Web, API, and mobile security testing, business logic abuse testing, authentication/ authorization validation
Cloud & Infrastructure	

Category	Skills
	AWS security assessments, IAM privilege escalation paths, infrastructure exposure reviews
Mobile Security	Android security testing, APK reversing, static/dynamic analysis, root and anti-tampering bypass validation, RASP validation
Security Research & Methodology	Attack-surface analysis, KYC/biometric abuse testing, threat-informed offensive workflows
Security Controls & Remediation	Compensating control design, secure-by-design recommendations, remediation prioritization
Tools	Burp Suite, Frida, MobSF, JADX, Nuclei, Nmap, Metasploit, SQLmap, Wireshark, AWS CLI, Docker
Programming / Scripting	Python, Java, JavaScript, Bash, AngularJS, Spring Boot
AI-Augmented Security	Purposeful use of AI applied to security testing and research
Mobile App Hardening	RASP, SSL pinning, anti-tampering, root detection, obfuscation, etc.