Alejandro Hernandez Padron

Canary Islands, Spain | alehdezp8@gmail.com | 611 45 14 43 | dinospacedive.com | alehdezp | alejandro-hernandez-padron

Summary

Cybersecurity Analyst with 4.5+ years of experience in vulnerability triage and risk evaluation for enterprise bug-bounty programs. Conducted security validation across Salesforce's ecosystem and for leading global organizations via HackerOne. OSCP-certified with deep technical curiosity about vulnerability mechanics - from surface-level symptoms down to underlying root causes and exploitation techniques.

Experience

Salesforce *(via Hexod)*, Security Triager / Cybersecurity Analyst — Remote, ESP
May 2021 – present

- Performed end-to-end vulnerability triage across Salesforce's full ecosystem (MuleSoft, Slack, Heroku, Tableau).
- Validated 1,400+ reports by confirming reproduction steps, assessing exploitability and determining business impact, before escalating them to the relevant internal teams.
- Served as a trusted liaison to the security research community—providing technical feedback and reliable communication that improved report quality and reinforced researcher trust.
- Contributed to team decision-making on process improvements, edge-case handling, and workflow optimization.
- Created automation tools (Python/Bash scripts, Chrome extensions, Burp plugins) that reduced manual workload and improved triage speed and consistency.

HackerOne *(via Hexod)*, Security Triager / Cybersecurity Analyst — Remote, ESP
Oct 2021 – Oct 2024

- Provided ~1.3 years of on-demand vulnerability triage for HackerOne's enterprise programs over a 3-year period, supporting Fortune 500 clients including Amazon, PayPal, Spotify, Tiktok and Sony while maintaining key Salesforce responsibilities.
- Served as a communication bridge between security researchers and program security teams, requesting clarifications, validating reproduction steps, and delivering technical summaries.

Certifications

OSCP (Offensive Security Certified Professional) — Mar 2021

OSCP-accredited, demonstrating hands-on penetration testing and exploitation capabilities.

- Mastered reconnaissance, vulnerability identification, exploitation, lateral movement, and privilege escalation across diverse operating systems.
- Developed proficiency with industry-standard security tools (Metasploit, Burp Suite, Nmap, Wireshark) and custom exploit development using Python and Bash scripting.

OSWE (Offensive Security Web Expert) – In Progress — Expected - Q1 2026

Enrolled in WEB-300 course covering advanced web application penetration testing, white-box code review, and manual exploit development.

API Penetration Testing — Aug 2023

APIsec University. Completed hands-on training in API penetration testing, covering advanced techniques for discovering and exploiting API vulnerabilities such as authentication flaws, JWT issues, injections, mass assignment, and SSRF.

Skills

Security Specializations: Triage, Bug Bounty, Web App Hacking, Secure Code Review

Vulnerability Analysis: CVSS scoring & risk assessment, Exploit Validation, OWASP Top 10, CWE/CVE classification

Programming Languages: Rust, Java, Python, JavaScript, C/C++, .NET, Bash

Toolbox: Chrome Extension Development, Burp Extensions development, Python security automation

Education

Universidad de La Laguna (ULL), Bachelor's Degree in Computer Science and Engineering — La Laguna, ESP

Sept 2014 – July 2019

- Focus on algorithms, data structures, OOP, and database systems.
- Valuable knowledge in Java applications using OOP principles and design patterns MVC/MVVM.
- Proficiency in C/C++ through other low-level programming and memory management projects.

Projects

DinoSpaceDive Personal Website

Personal portfolio and blog used to share cybersecurity notes and upcoming research projects.