

Elieser Hernandez

Offensive Penetration Tester | Web, APIs & Infrastructure
astoreal031@gmail.com | +53 59805123 | linkedin | Remote

EXPERIENCE

INTRUST SECURITY PENETRATION TESTER (MID-LEVEL)

Aug 2025 -- Mar 2026 | Remote

- Performed offensive security assessments following OWASP and PTES methodologies across web applications, APIs, and mobile platforms.
- Executed **27+ security assessments**, identifying an average of **8+ vulnerabilities per engagement**, including high and critical severity findings.
- Actively exploited vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Server-Side Request Forgery (SSRF), Remote Code Execution (RCE), and business logic flaws.
- Automated reconnaissance and exploitation workflows using Python and Bash scripting.
- Produced detailed technical reports and executive summaries focused on risk exposure and business impact.

FREELANCER / BUG BOUNTY INDEPENDENT SECURITY RESEARCHER

Dec 2023 -- Aug 2025 | Remote

- Actively participated in multiple Bug Bounty programs targeting web applications and infrastructure.
- Achieved a **75% report acceptance rate** (6 out of 8 submissions validated).
- Combined in-depth manual testing with automated tooling to uncover complex vulnerabilities.
- Identified issues related to access control weaknesses, insufficient validation, and insecure configurations.

XETID DEVELOPMENT COMPANY SYSTEMS MONITORING & SECURITY SPECIALIST

May 2023 -- Dec 2023 | Havana, Cuba

- Monitored system availability, integrity, and security using the Elastic Stack (Elasticsearch and Kibana).
- Conducted controlled Denial of Service (DoS) simulations to evaluate infrastructure resilience.
- Generated **40+ security incident reports**, including post-incident analysis and documentation.

EDUCATION

UNIVERSITY OF INFORMATICS SCIENCES (UCI) BACHELOR OF SCIENCE IN COMPUTER SCIENCE

2022 -- 2026 | Havana, Cuba

PROFILE

Offensive penetration tester specializing in web applications, APIs, and infrastructure security testing. Hands-on experience in security assessments, bug bounty programs, and test automation. Methodical, impact-driven approach with a strong focus on identifying high-risk vulnerabilities and delivering clear technical and executive-level reporting.

CERTIFICATIONS

EF SET Certificate

B1 Intermediate (41/100)

EF Standard English Test

Issued: Feb 2026

Verify: cert.efset.org/YfMbVQ

ICIP Certificate

(Institution: ICIP)

[View Certificate](#)

TECHNICAL SKILLS

METHODOLOGIES

OWASP Top 10, PTES, MITRE ATT&CK, Bug Bounty, Threat Modeling

TOOLS

Burp Suite, Nmap, Metasploit, SQLMap, Nuclei, FFUF, Amass, Hashcat, John the Ripper

LANGUAGES

Python, Bash, JavaScript, SQL

SPECIALIZATIONS

Web Pentesting, API Security, Mobile Security, Reconnaissance, Exploitation

LANGUAGES

- Spanish — Native
- English — B1 (Technical reading & reporting)