Raul Garcia Lagunas

Security Engineer | Open to relocation | Mexico

Cellphone: +52 722 246 3437 **Email:** rulopssec@gmail.com

Websites, Portfolios & Profiles

- **Portfolio:** **resume.rulops.net**
- **HTB profile:** **app.hackthebox.com/profile/774057**
- **LinkedIn:** **linkedin.com/in/rgl00/**

Professional Summary

Results-oriented and **proactive** Security Engineer with a robust software engineering and cybersecurity foundation. Skilled in embedding security throughout the SDLC, conducting security assessments, threat modeling, secure code review, and implementing security controls. Adept at working cross-functionally with multiple teams to drive risk reduction and foster security by design. Passionate about purple teaming, automating security, educating teams, and building security programs.

Core competencies & Technical skills

Cloud & Infrastructure Security

- AWS Security Hub, IAM, S3, KMS, VPC, Route 53, Cloud9, Lambda
- Terraform
- Kubernetes orchestration & container security
- CI/CD pipeline security (GitHub Actions)
- Docker, Kubernetes, container scanning

Application & Product Security:

- Secure SDLC integration (DAST, SAST, SCA, IAST)
- Code review & secure coding guidance (Python, Bash)
- Vulnerability triage & mitigation strategies
- Threat modeling & security architecture assessments
- Web, API, and Mobile pentesting (OWASP Top 10, SSRF, SQLi, XSS, fuzzing, etc.)
- Exploit development (Python), red teaming, phishing simulations
- Tools: Burp Suite, Wireshark, Nmap, Nessus, Qualys, Accunetix, etc.
- Standards: MITRE ATT&CK, OSSTMM, NIST, ISO 27001, GDPR

General

- Communication: Executive & technical reporting, clear communication
- Collaboration: Cross-team collaboration, reliability, proactivity
- Leadership: Coaching & mentorship, conflict resolution
- Problem solving: Critical thinking, curiosity, analytical

Experience - *References can be provided upon request*

Application Security Engineer | *Deloitte* — Nov 2023 - Present

- Performed **white box testing**, analyzing code in-depth, and successfully triaging **100%** of security issues.
- Conducted **DAST, SAST & IAST** scans, identifying and mitigating critical vulnerabilities, and helping **harden** stakeholders' systems by **80%**.
- Diagnosed and optimized security tools, improving scanning efficiency and **resolving 100%** of reported incidents.
- Prioritized vulnerabilities by re-scoring issue severity, **accelerating remediation** of **90%** of security risks.
- Conducted in-depth security testing of **web applications** within **complex network** environments, uncovering **critical vulnerabilities**.
- Developed and delivered tailored **mitigation plans** to developers, effectively **educating** them on **secure coding practices** and **reducing** recurring vulnerabilities.
- Validated and documented security tools, ensuring **comprehensive test coverage** and future reference.
- Defined and implemented **DevSecOps** strategies to embed security throughout the **SDLC**, partnering closely with engineering teams.
- Utilized **Kubernetes orchestration tools** to efficiently deploy, manage, and scale Docker containerized applications, ensuring **high availability** and streamlined workflows.
- Advised clients on **IAM strategy**, **Zero Trust** principles, and **secrets management** within cloud environments (*AWS, Azure, GCP*).
- Collaborated directly with **cross-functional teams**, sharing **security findings** consistently and discussing them in detail.

Cybersecurity Penetration Tester | *IQSEC* — Apr 2023 - Nov 2023

- Designed and led end-to-end product security assessments, including **architecture reviews**, **threat modeling**, and p**enetration testing**.
- Conducted comprehensive security assessments utilizing frameworks and methodologies such as **MITRE ATT&CK**, **OSSTMM**, and **OWASP**, ensuring thorough vulnerability identification.
- Conducted **black box** & **gray box** penetration tests, identifying and exploiting **60%** of **critical** vulnerabilities.
- Led **web, infrastructure,** and **mobile** security assessments, testing **d**iverse environments.
- Automated vulnerability assessments using **Qualys, Nessus & Accunetix,** delivering actionable **mitigation plans**.
- Designed and executed **phishing campaigns**, improving **security awareness** by **100%**.
- Led **adversarial simulations** using **Threat Simulator**, collaborating closely with the **SOC** to emulate real-world attack scenarios, and successfully remained undetected **70%** of the time.
- Developed **custom exploits** & **payloads**, **bypassing 70% of t**arget security controls.

- **Created** detailed, replicable Proof of Concepts (PoCs) for security assessments, enabling efficient **issue validation** and r**eplication**.
- Assessed **cloud** and complex **network environments**, uncovering **high-value** security findings.
- Authored **detailed technical** and **executive reports**, clearly communicating findings and remediation strategies to **technical** and **non-technical** stakeholders.

SOC Monitor | *Smartekh Group* Dec 2022 - Apr 2023

- Implemented a range of **proactive security measures** to safeguard systems, effectively **preventing** potential hacker attacks
- Monitored **IDS, IPS, SIEM, XSOAR, and Firewalls**, **detecting threats i**n real-time, reducing **MTTD by 20%**.
- Collaborated closely with the team to identify **critical vulnerabilities** and implement **effective solutions**, reducing the **MTTR by 30%** and enhancing overall incident response efficiency.
- Participated in incident response rotations, **collaborating** with internal teams to improve **post-incident** processes and **documentation**.
- Responded to incidents following **NIST & MITRE ATT&CK frameworks**, ensuring **100%** resolution efficiency.
- Analyzed network traffic to **identify** suspicious behavior from **IP addresses**, promptly taking action to **block** malicious activity and **mitigate** potential security threats.
- **Deobfuscated** and analyzed **malicious code**, successfully identifying a **C2** server and **uncovering** attack infrastructure.
- Performed **Firewall, SIEM, EDR, & XSOAR troubleshooting**, resolving **complex misconfigurations**.
- Ensured stakeholder **data security** by strictly adhering to **ISO 27001** and **GDPR standards**, implementing **robust controls** to protect sensitive information, and maintaining compliance.
- Managed **ticketing systems**, streamlining **incident tracking,** and **clearing** customer **communication**.
- Participated in study groups to **share** cybersecurity **knowledge**, collaborate with peers, and continuously **enhance** skills through **mutual learning**.

Cloud Office Technician | *Rackspace* Jan 2022 - July 2022

- Delivered **technical support** and **troubleshooting**, resolving **100%** of customer issues **satisfactorily**.
- Managed **ticketing systems** and performed **L1 - L2 troubleshooting** across various **cloud platforms**.
- Configured **DNS** servers**, DMARC, and SPF policies**, ensuring **secure email communications**.
- Deployed AWS, GCP & Azure **cloud environments**, **optimizing** customer **infrastructure**.
- Applied **Terraform** to **automate** and manage cloud infrastructure **deployment**, ensuring scalable, repeatable, and secure provisioning of resources.
- **Identified** and **blacklisted** suspicious IP addresses, **preventing potential threat**s, and successfully **securing** the network.

Education

Hybridge University | Mexico **2024 - 2026**

BS in ***Software Engineering***

Certifications

CBBH | *Certified Bug Bounty Hunter* | **HTB** **Expected Q3 2025**

CPTS | *Certified Penetration Tester Specialist* | **HTB** **Expected Q4 2025**

Languages

- Spanish - **Native speaker**
- English - **C2 Fluent**
- French - **A1 Beginner**