ALEJANDRO FLORES COVARRUBIAS

IT SECURITY ENGINEER

alejandrocovrr.com | contact@alejandrocovrr.com | Monterrey, Mexico

I am a dedicated IT security professional with a strong focus on Application Security and Cloud Security. Continuously driven by a passion for learning and innovation, I actively seek out new technologies and best practices. My commitment to sharing knowledge and effectively communicating ideas ensures that I contribute meaningfully to any team. With a particular emphasis on application security, I am keen on enhancing the security posture of modern applications and systems.

EXPERIENCE

SENIOR APPLICATION SECURITY ENGINEER (FULL-TIME)

Dec 2022 - Present | Driscoll's Inc

- Integrated security in DevOps workflows using AWS, Docker, and GitHub, enhancing CI/CD and SDLC.
- Streamlined SCA (Snyk and Sonarqube) and SAST tools in CI/CD pipelines with TeamCity.
- Delivered DevSecOps training, covering topics like Secure Coding, Secure IaC and Container best practices.
- Automated DAST scans in Octopus using StackHawk for early vulnerability detection.
- Established processes for security design reviews, threat modeling, security code reviews, and web pentest.
- Created secure coding practices for Python and JavaScript (React, Vue), leveraging Snyk.
- Performed web application pentesting on internal applications using OWASP ASVS standards and Burpsuite.

Main technologies used: AWS, Burpsuite, Snyk, Github, Sonarqube, StackHawk, Octopus, TeamCity, Jenkins, Python, Javascript (React, Vue), Docker, Jira, New Relic, GCP

EXTERNAL APPLICATION SECURITY TESTER (FREELANCE)

May 2023 - Present | Santander US

- Automated DAST scans for web applications and APIs using HCL AppScan, providing validation with BurpSuite and remediation recommendations in Jira.
- Conducted SAST scans with Fortify Static Code Analyzer, supplemented by manual validation to ensure accuracy, and documented findings in Confluence.
- Performed web application pentesting with BurpSuite, including validating findings and demonstrating exploitation techniques, integrated into DevOps workflows.

Main technologies used: Burpsuite, Fortify Static Code Analyzer, HCL AppScan, Jira, Confluence

EXTERNAL SECURITY TESTER (FREELANCE)

Nov 2023 - May 2023 | Dave

- Automated DevSecOps processes by integrating centralized vulnerability management ingestion using Python and DefectDojo, with workflows managed in GitHub Actions.
- Supported execution and reporting of web application penetration tests using BurpSuite, with results tracked and managed in Jira and Confluence.
- Developed Yara rules for Chronicle SIEM and automated SOAR playbooks, streamlining security operations.
- Improved penetration testing documentation, checklists, and formats in Confluence.

Main technologies used: Burpsuite, Chronicle SIEM and SOAR, Python, Github, Github Actions, DefectDojo, Jira, Confluence

BLOCKCHAIN SECURITY AUDITOR (FREELANCE)

Apr 2022 - Aug 2023 | Least Authority

- Conducted in-depth manual code reviews on blockchain protocols, Web3 applications, and browser extensions, utilizing Foundry, Remix IDE, and VS Code, and working with languages like Solidity, TypeScript, Rust, Golang, Clarity, and Python.
- Collaborated with client teams via GitHub to address remediation efforts, leveraging tools like MythX and Slither to resolve false positives and optimize security measures.
- Performed comprehensive security design reviews of protocol implementation designs, ensuring robust security measures through thorough analysis and tool-assisted audits with Echidna and MythX.
- Investigated and researched emerging attack vectors within the Web3 ecosystem, doing advanced static analysis to stay ahead of new threats.

Main technologies used: Foundry, Remix IDE, Github, MythX, Solidity, Echidna, Typescript, Rust, Golang, Clarity, Python, Slither, VS Code

DEVSECOPS ANALYST (FULL-TIME)

Aug 2021 - Oct 2022 | 3PillarGlobal (Tripwire)

- Monitored and managed cloud alerts and incidents using Alert Logic, integrated with AWS and Kubernetes.
- Developed and implemented remediation plans for cloud vulnerabilities in collaboration with the Operations team, leveraging Terraform and Git for IaC.
- Automated the sorting and filtering of vulnerability reports from Docker images in Artifactory, publishing results to a DynamoDB and integrating with Jenkins for automated scanning.
- Established a vulnerability management program for third-party components, utilizing Artifactory, Jira, and Confluence to track, document, and resolve issues.
- Developed an API and Backstage.io plugin to aggregate and display vulnerability data, improving accessibility and transparency across teams.
- Conducted comprehensive SAST and DAST testing using SonarQube, ZAP, and OWASP's guidelines, integrated with Jenkins for continuous security testing in the CI/CD pipeline.

Main technologies used: AWS, Artifactory, Alert Logic, Terraform, Git, Burpsuite, Sonarqube, Backstage.io Jenkins, Docker, Jira, Python, Typescript (React)

INFORMATION SECURITY CONSULTANT (FULL-TIME)

Aug 2020 - Aug 2021 | Axosnet

- Developed and implemented policies and procedures to ensure alignment with ISO 27001 requirements, utilizing ManageEngine Endpoint Central for policy enforcement and compliance monitoring.
- Designed and deployed an information security awareness program, integrating training courses and evaluations in Moodle, with automated tracking and reporting in Python.
- Participated in daily SecOps activities, monitoring and responding to alerts from CloudWatch, AWS GuardDuty, and Alert Logic, with incident response automation.
- Audited cloud security controls using Prowler and Pacu, ensuring compliance with AWS best practices and the AWS Well-Architected Framework, and addressing gaps through Terraform.
- Conducted web application penetration testing on internal applications using BurpSuite, following OWASP ASVS and OWASP Top 10 guidelines, and integrated findings into the CI/CD pipeline using Jenkins.

Main technologies used: AWS, Burpsuite, Alert Logic, ISO 27001, ManageEngine Endpoint Central, Prowler and Pacu (AWS auditing), Python, Moodle

INFORMATION SECURITY CONSULTANT (FULL-TIME)

Jun 2019 - Aug 2020 | Purple Security

- Conducted internal and external network penetration testing for various clients, utilizing Kali Linux, Metasploit, and Nmap, and adhering to an internal methodology based on OSSTMM and PTES.
- Executed red teaming exercises tailored to client needs, using tools like responder.py and Bloodhound, aligned with the MITRE ATT&CK matrix to identify and address security issues.
- Developed custom exploits and automation tools for penetration testing tasks using Python and Bash scripts.
- Performed web pentesting using BurpSuite and developed an internal methodology based on OWASP ASVS.
- Established a streamlined process for documenting penetration testing activities in GitHub, improving efficiency and accuracy with automated scripts written in Python and Lua.

Main technologies used: Kali Linux, Metasploit, Nmap, Burpsuite, responder.py, Bloodhound, Python, Bash, Acunetix, Lua

INCIDENT RESPONDER (INTERN)

Dec 2017 - May 2019 | FEMSA

- Designed and managed a MySQL database for tracking and managing application vulnerabilities.
- Monitored and responded to security incidents using Palo Alto Firewall, Exabeam SIEM, and Symantec AV, ensuring timely mitigation.
- Developed and implemented threat hunting patterns in Exabeam SIEM to proactively identify and address potential security threats.
- Conducted PoC tests to evaluate EDR solutions' effectiveness against malware and web vulnerabilities.
- Assisted the application security team by validating HP WebInspect vulnerabilities using BurpSuite, and contributing to detailed reporting.

Main technologies used: Palo Alto Firewall, Exabeam SIEM, Linux, HP Web Inspect, Symantec AV, Kali Linux, Burpsuite, SQL

HARD SKILLS

- Bug hunting tools
- Network scanning tools
- Linux, Windows, OSX
- Vuln scanners (Nessus, Nexpose, StackHawk Webinspect, Burpsuite, Nuclei, HCL Appscan)
- Python, Go, Bash, Solidity, Javascript
- CI/CD (Jenkins, Github Actions, Gitlab, TeamCity, Octopus)
- Fortify SCA, Snyk, Sonarqube, JS Linters, Bandit, Semgrep
- Cloud Security (Alert Logic, Wiz, Native Cloud Security Solutions)
- Firewalls (Fortinet, Palo Alto)
- SIEM (Exabeam, Splunk, Chronicle, Insight VM)
- Technical writer
- Artifactory
- Cloud (AWS, GCP)
- Server hardening (CIS)
- Smart contracts
- Terraform, Vault
- Docker, Kubernetes
- Malware analysis
- EDR Solutions (Crowdstrike, Trend Micro)

SOFT SKILLS

- Researcher and desire to learn
- Leadership
- Cooperative
- Risk analysis and management
- Effective communicator
- Proactive attitude
- Good listener
- Results-oriented
- Documentation writer
- Adaptability
- Punctuality
- Self-organized

EDUCATION

2015 - 2019

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

Bachelor of IT Security

CERTIFICATIONS

- CompTIA Security+ ce
- CompTIA PenTest+ ce
- AWS Associate Architect Solutions C03
- Google Cloud Associate Cloud Engineer
- Hashicorp Terraform Associate
- ITIL® Foundation v4
- ISO 27001 Lead Auditor