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

- Initiated and led the application security program, integrating best security practices into the existing SDLC.
- Implemented SCA and SAST tools in CI/CD pipelines.
- Developed and delivered application security training programs.
- Introduced initial implementation of DAST scans in the CI/CD pipeline.
- Established processes for security design reviews, threat modeling, security code reviews, and web pentest.
- Created best practices and secure defaults for code and IaC, focusing on JS, Python and Terraform.
- Performed web application security testing on internal applications using OWASP ASVS standards.

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

- Conduct DAST scans for web applications and APIs, providing validation and remediation recommendations.
- Perform SAST scans, supplemented with manual validation for accuracy.
- Engage in web app pentesting, including validation of findings and demonstration of exploitation techniques.

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

EXTERNAL SECURITY TESTER (FREELANCE)

Nov 2023 - May 2023 | Dave

- Developed automation for DevSecOps processes, such as centralized vulnerabilities management ingestion.
- Assisted in the execution and reporting of web application penetration tests.
- Created Yara rules for SIEM and developed automation for SOAR playbooks.
- Enhanced penetration testing documentation, checklists, and formats to improve efficiency and accuracy.

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

EXTERNAL SECURITY RESEARCHER (FREELANCE)

Apr 2022 - Aug 2023 | Least Authority

- Conducted manual code reviews on blockchain protocols, Web3 applications and browser extensions, working with languages including Solidity, TypeScript, Rust, Golang, Clarity, and Python.
- Collaborated with client teams to address remediation efforts and resolve false positive issues.
- Performed security design reviews of protocol implementation designs to ensure robust security measures.
- Investigated and researched new attack vectors within the Web3 ecosystem for new emerging threats.

Main technologies used: Visual Studio Code, Github, Solidity, Typescript, Rust, Golang, Clarity and Python

DEVSECOPS ANALYST (FULL-TIME)

Aug 2021 - Oct 2022 | 3PillarGlobal (Tripwire)

- Monitored cloud alerts and incidents using Alert Logic.
- Developed remediation plans for Cloud vulnerabilities in collaboration with the Operations team.
- Created automated jobs to sort and filter vulnerability reports from Docker images hosted in our internal image registry to then publish the filtered results in a DB.
- Implemented a vulnerability management program for third-party vulnerabilities, utilizing Artifactory, Jira, and Confluence documentation.
- Developed an API and an internal portal plugin to aggregate and display vulnerability reports from our DB.
- Conducted both SAST and DAST testing using BurpSuite and OWASP's Manual Code Review Guide.

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 policies and procedures to ensure alignment with ISO 27001 requirements.
- Created an information security awareness program, including training courses and evaluations.
- Participated in daily SecOps activities, monitoring and addressing alerts from CloudWatch, AWS GuardDuty, and Alert Logic.
- Audited cloud security controls, ensuring alignment with AWS best practices and the AWS Well-Architected Framework.
- Conducted web application penetration testing on internal applications, following OWASP ASVS and OWASP Top 10 guidelines.

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 an internal methodology based on the OSSTMM and the PTES.
- Executed red teaming exercises tailored to client needs, using the MITRE ATT&CK matrix to identify and address security issues.
- Developed exploits and automation tools for penetration testing tasks, primarily using Python scripting.
- Performed web application pentesting and developed an internal methodology based on OWASP ASVS.
- Established a streamlined process for documenting penetration testing activities, enhancing efficiency and accuracy.

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 implemented an internal MySQL database to effectively manage application vulnerabilities.
- Monitored and responded to security incidents using Palo Alto Firewall, Exabeam SIEM, and Symantec AV console.
- Created threat hunting patterns within the network using Exabeam SIEM to proactively identify and address potential security threats.
- Developed Proof of Concept (PoC) tests to evaluate the efficiency of various Endpoint Detection and Response (EDR) solutions in detecting malware.
- Assisted the application security team by validating vulnerabilities and helping in the reporting process.

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, PHP
- 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 (Malware PoC Tests)

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