Rebecca Turner

Tacoma, WA • b\_l\_turner@yahoo.com • github.com/Mystshara

## 💡 Professional Summary

DevSecOps and Security Automation Engineer with a project-driven approach to infrastructure security and vulnerability management. Specialized in static and dynamic analysis tooling, container orchestration, secrets management, and CI/CD pipelines. Designed and deployed automated security platforms using Kubernetes, Terraform, and Vault. Gained foundational knowledge through formal study, then deepened expertise through real-world builds and security engineering projects. Collaborative, fast-learner who thrives in fast-paced, technical environments focused on building secure, automated infrastructure.

## 🧰 Technical Skills

Kubernetes • Vault • Terraform • Docker • GitHub Actions • Celery • Redis • Python • Bash • Trivy • Nikto • ZAP • PostgreSQL • NGINX • CI/CD • Security Automation

## 🛠 Projects

**PTaaS Security Demo**  
Public simulation of a modular, automated penetration testing platform.  
• Integrated secrets management, containerized scanning, task orchestration, and triage workflows  
• GitHub: https://github.com/Mystshara/ptaas-security-demo

**Bug Bounty Automation System (Private Repository)**Comprehensive toolkit for automating vulnerability discovery and validation.  
• Modular containers, Celery-based scheduling, and multi-scanner orchestration  
• Integrated Vault, Trivy, Nikto, ZAP, PostgreSQL, Redis, Nginx, Ingress Controllers and GitHub CI/CD

**Game & Web Hosting Platform (In Progress)**  
Infrastructure for dynamically provisioning game and web servers using Proxmox, Kubernetes, and automation tools like Terraform and Ansible.

**Popular Game Website Collaboration**  
Contributed to a full-stack game website project. Developed front-end components, styled layouts, and wrote interactive page logic. Supported MySQL database integration and dynamic UI behavior.

## 💼 Experience

**Independent Security Automation Engineer – Remote | 2024–Present**• Architected a scalable, containerized PTaaS pipeline using Vault, Redis, and GitHub Actions  
• Deployed secure infrastructure workflows using Terraform and managed build automation  
• Designed and documented cloud-native security solutions with GitHub-hosted public demos

## 🎓 Education & Applied Learning

Cybersecurity AAST Program (In Progress)  
Bates Technical College – Tacoma, WA | 2022–2024  
Completed 90+ credits in a hands-on cybersecurity program focused on security fundamentals, networking, scripting, and threat detection.  
Relevant Coursework:  
• Information Security I & II, Ethical Hacking, Python for Security, Cybersecurity Analyst I & II  
• Network Defense, Cisco Networking, IT Systems, SQL Fundamentals, Capstone Security Project  
• Applied working knowledge of Server Administration and Cloud/Virtualization through active project work

## 🚀 Applied Infrastructure & Security Development

• Built scalable security pipelines for vulnerability scanning, secrets management, and infrastructure provisioning  
• Developed and deployed cloud-native services with Kubernetes, Docker, and CI/CD workflows  
• Proficient in scripting, infrastructure-as-code, and container security validation  
• Contributor to open-source tooling and public demos on GitHub

## 🔹 Additional Experience (Optional)

Community Infrastructure & Collaboration  
Supported online communities through collaboration, project planning, and digital event operations.