Noah Brown

Software Engineer

+1 (555) 901-1098 | noah.brown.secure@email.com | linkedin.com/in/noahbrownsec | Washington, D.C.

SUMMARY

A security-conscious Software Engineer with 4 years of experience dedicated to building secure, reliable, and robust applications. Proficient in Python and Go, with a strong focus on secure coding practices, threat modeling, and integrating security into the CI/CD pipeline. Believes in a "security by design" philosophy to proactively mitigate vulnerabilities.

STRENGTHS

Secure Software Development Lifecycle (SSDLC): Expertise in integrating security practices into every phase of development, from design and coding to testing and deployment.

Threat Modeling: Skilled at identifying potential security threats and architectural weaknesses in system designs and proposing effective mitigations.

Secure Coding Practices: Deep understanding of common vulnerabilities (OWASP Top 10) and best practices for writing code that is resilient to attacks.

DevSecOps: Experience in automating security testing (SAST, DAST) and integrating it into CI/CD pipelines to catch vulnerabilities early.

TECHNICAL SKILLS

Languages: Python, Go, SQL

Security Tools: Snyk, Checkmarx (SAST), OWASP ZAP (DAST), Trivy, GitGuardian

Cloud & DevOps: AWS (IAM, KMS, Security Groups), Docker, Kubernetes, Jenkins, Terraform

Databases: PostgreSQL, MySQL

PROFESSIONAL EXPERIENCE

Software Engineer | SecureAuth Solutions | August 2021 - Present

- Develops backend services for an identity and access management (IAM) platform, with a primary focus on security and reliability.

- Conducts threat modeling exercises for all new features and services to proactively identify and address potential security risks.

- Led the initiative to integrate static application security testing (SAST) into the Jenkins CI/CD pipeline, reducing the number of vulnerabilities reaching production by 70%.

- Performs security-focused code reviews, mentoring other engineers on secure coding patterns and the avoidance of common pitfalls.

- Responded to and helped remediate findings from third-party penetration tests and internal security audits.

PROJECTS

Secure REST API in Go: Developed a sample RESTful API in Go that implements security best practices from the ground up, including proper authentication/authorization, input validation, parameterized queries, and secure headers. The project is well-documented with the rationale for each security decision.

EDUCATION

Bachelor of Science in Cybersecurity | George Mason University | 2017 - 2021

CERTIFICATIONS

GIAC Certified Web Application Defender (GWEB) | 2024