
Anthony Rice III

CSP/DevOps/AppSec

890 Union Station Pkwy

Lewisville, TX 75057

(404) 427-5153 / [linkedin.com/in/anthony-rice-iii-733227177](https://www.linkedin.com/in/anthony-rice-iii-733227177)

Rnarice3@gmail.com / anthony-rice3-3d7x.vercel.app

github.com/AnthonyRice3

SUMMARY

Security+ certified web developer with a strong foundation in modern application development and a growing specialization in web application security. Skilled in identifying and mitigating common vulnerabilities (OWASP Top 10), performing secure code reviews, and integrating security into the SDLC. Proficient in front-end and back-end development, RESTful APIs, OAuth2/JWT, and CI/CD practices. Seeking to contribute to secure web applications through a hybrid role in development and security.

SKILLS / TOOLS

- OWASP Top 10, Secure Coding, Threat Modeling - Web Technologies (HTML, CSS, JavaScript, React, Node.js) - API Security (RESTful, GraphQL), OAuth2, JWT - DevSecOps Fundamentals, CI/CD Integration -
- Burp Suite - OWASP ZAP - Wireshark - NetworkMiner - Terraform - Active Directory - Adobe - Windows/Linux/Apple OS

RELATIVE PROFESSIONAL EXPERIENCE

Tri Star Labs, Atlanta, GA - *Lead Web Developer* - AUG 2020 - PRESENT

- Designed and implemented secure, scalable web app architectures, improving product stability and reducing deployment risks.
- Conducted code reviews focusing on performance, security, and quality, which led to a noticeable decrease in bugs and improved team development standards.
- Integrated threat modeling and vulnerability mitigation strategies into development, reducing the likelihood of critical security incidents and improving compliance posture.
- Built and managed RESTful APIs with robust authentication/authorization flows, enabling faster development cycles and more secure third-party integrations.

PROJECTS/ LABS

SEPT 2024 - PRESENT

- Packet & Traffic Analysis with Wireshark and NetworkMiner
- Performed XSS and Injection Attacks in sandbox environments
- Deployed honeypots, enumerated hosts, and explored NTFS permissions
- Conducted reconnaissance and simulated network exploitation
- Red Team, Social Engineering Using SET
- Data Protection & Communication Security
- System Configuration & Memory/File Management
- Secure Infrastructure with IaC & Container Orchestration

EDUCATION & CERTIFICATIONS

- Springboard | Cybersecurity Career Track (Online)
CompTIA Security+ Certified
- University of Toledo | Toledo, OH
Business Management | Academic Scholarship Recipient