Zhongyang Zhu

New York, NY • 201-800-6173
zhongyang.zyz.zhu@gmail.com
linkedin.com/in/zhongyang-zhu/

Technical Proficiencies

Certifications: Burp Suite Certified Professional, Security+, AWS (Certified Security Specialty, Solutions Architect, Certified Cloud Practitioner)
Coding Languages: Python, Javascript, Bash, Java, C
Security Skills & Tools: SAST + DAST, Web Vulnerability Testing & Analysis (OWASP Top 10), Application Penetration Testing, Scripting (*Python/Bash*), Cloud Security
Miscellaneous Interests: Bug bounties and browser security, E-sports, Sim Racing, Snowboarding

Experience

Verisk | *Jersey City, NJ*

A global data analytics company for the insurance claims market

Application Security Specialist | *Mar 2021 - Present*

- Overhauled and formalized application security review process by enforcing proactive vulnerability scanning during development, strengthening the overall security posture of the application and SDLC and eliminating the necessity for previously redundant post-development code security assessments.
- Piloted Verisk’s first bug bounty program, which involved reproducing and triaging vulnerabilities; successfully identified multiple critical vulnerabilities and directly contributed to code fixes with development teams for flagship applications.
- Migrated SAST and DAST infrastructure to AWS, integrated SSO (Okta), and incorporated scanning into multiple development pipelines which provided essential security automation to various dev teams.
- Conducted manual review and validation of SAST & DAST findings, actively contributing to vulnerability remediation efforts, such as completely removing SQL injection from one flagship application.
- Conducted internal penetration tests, uncovering and addressing several high severity vulnerabilities in customer-facing applications, such as insecure access controls and privilege escalations.
- Helped overhaul code repository infrastructure by replacing SSH authentication with HTTPS authentication, following security best practices and enabling a WAF to be implemented.
- Handled application and web-related security incidents, such as analyzing anomalous code, scripts, and websites.
- Piloted threat modeling effort to some applications, employing the PASTA framework, and identified missing or improper security controls in application architectures.
- Managed and promoted secure coding training across the enterprise and its business units, resulting in a positive correlation in teams between training participation and reduced SAST scan findings.

Application Security Consultant | *Aug 2020 – Mar 2021*

- Contributed to the design of Incident Response workflows and developed ServiceNow scripts to automate parts of the IR process, enhancing efficiency and productivity for SOC security analysts.
- Spearheaded a project to fortify the company's external attack surface by leveraging vulnerability management tools and OSINT, which successfully identified recurring vulnerabilities.
- Extracted metrics from security tools and leveraged Power BI to build dashboards, allowing quantification of application security initiatives, such as the number of vulnerabilities found over time.
- Developed custom scripts to automate application security efforts, such as a Python Lambda function which integrated the WAF with AWS S3 to enable logging and auditing of previous WAF events.

Education

- **New York University** | B.A. Computer Science, Cybersecurity Minor | *Aug 2016 – May 2020*