

# 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 Cloud Practitioner

**Languages:** Python, Javascript, Java, C, Bash

**Security Skills & Tools:** SAST/DAST, Web Vulnerability Analysis, Incident Response, AWS, Penetration Testing, Threat Modeling, Scripting (*Python/Bash*)

**Miscellaneous Interests:** Bug bounties, E-sports, Formula 1, Snowboarding, Quidditch

## Experience

**Verisk** | *Jersey City, NJ*

**Application Security Specialist** | *Mar 2021 - Present*

- Restructured enterprise application architecture review process to implement vulnerability scanning before final board review, eliminating the need to have related meetings after the “final review” - thus increasing efficiency of the enterprise security team
- Piloted threat modeling effort to select Verisk applications, based off the PASTA framework which includes architecture review, technology enumeration, attack trees, and network, data, and trust diagrams
- Socialized developer cybersecurity training to the enterprise and member companies; metrics demonstrated a positive correlation between training participation and fewer SAST & DAST findings
- Contributed to a major restructure of code repository architecture which allowed a WAF to be implemented, and heightened the overall security posture of the authentication process
- Managed SAST and DAST solutions and integrated them into member company development processes, and manually reviewed and validated findings, as well as contributing to vulnerability remediations
- Migrated SAST and DAST infrastructure to the AWS cloud, and cleaned up our team’s AWS environment along the way, which included tasks such as deleting insecure permissions/roles and standardizing naming
- Performed an internal application penetration test to fulfill an internal audit requirement, which involved the test itself, the reporting process and delivery, and the follow-up remediations and re-test
- Trained developers in basic security testing using tools such as Burp Suite, including Burp Proxy, Repeater, and Intruder, which benefited their dev-ops capabilities and efficiencies

**Application Security Consultant** | *Consultant Sep 2020 – Mar 2021, Intern Oct 2019 – Aug 2020*

- Created and deployed a software assurance maturity model for Verisk and its 60+ member companies, enabling management, quantification, and metrics development of enterprise application security
- Helped design Incident Response workflows and developed scripts in ServiceNow, which automated parts of the IR process to increase efficiency and productivity for SOC security analysts
- Spearheaded a project to strengthen Verisk’s external attack surface, utilizing vulnerability management tools and OSINT, resulting in the patching of recurring critical vulnerabilities
- Built application security metrics into PowerBI, allowing management and monitoring of enterprise and member company statistics, such as training participation and vulnerability finding trends
- Developed various in-house scripts, such as a Python Lambda function to connect the WAF solution to AWS S3 for logging and auditing functionalities

**IBM** | *Research Triangle Park, NC*

**Security Developer Intern** | *Jun 2019 – Aug 2019*

- Automated majority of IBM’s asset vulnerability publication process (PSIRT) by developing a REST handshake between ServiceNow and Content Management Systems (Drupal and WordPress)
- Developed in an Agile team, presenting biweekly deliverables to executives and stakeholders

## Education

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