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, AWS Solutions Architect (*Working*), Offensive Security Certified Professional (OSCP) (*Working*)
Coding Languages: Python, Javascript, Java, C, Bash
Security Skills & Tools: SAST/DAST, Web Vulnerability Analysis (OWASP Top 10), Scripting (*Python/Bash*), AWS, Incident Response, Penetration Testing, Threat Modeling
Miscellaneous Interests: Bug bounties, E-sports, Sim Racing, Snowboarding, Quidditch

Experience

Verisk | *Jersey City, NJ*
A global data analytics company for the insurance claims market
Application Security Specialist | *Mar 2021 - Present*

- Revamped application architecture review process, enforcing pre-final review vulnerability scanning, which eliminated redundant post-review code security and architecture assessments
- Piloted company's first bug bounty program, which involved reproducing and triaging vulnerabilities; successfully resolved one critical vulnerability, and several lower severity issues in three applications
- Migrated SAST and DAST infrastructure to AWS, integrated SSO (Okta), and incorporated scanning into multiple development pipelines which provided essential automation for development and security 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
- 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
- Overhauled code repository infrastructure by using authentication through HTTPS instead of SSH, allowing the implementation of a WAF which strengthened security by enabling HTTP auditing and logging
- Conducted internal application penetration tests, uncovering and addressing several high severity vulnerabilities in customer-facing applications, such as insecure access controls and privilege escalations
- Piloted threat modeling effort to some applications, employing the PASTA framework, and identified missing or improper security controls in application architectures
- Handled application-related security incidents, such as analyzing anomalous scripts and websites

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 patched recurring vulnerabilities
- Extracted metrics from security tools and leveraged Power BI to build dashboards, allowing quantification of application security measures, such as the number of vulnerabilities found over time
- Developed custom in-house scripts, including a Python Lambda function which integrated the WAF with AWS S3 to enable logging and auditing of WAF events

IBM | *Research Triangle Park, NC*
An American multinational technology corporation
Security Developer Intern | *Jun 2019 – Aug 2019*

- Streamlined asset vulnerability publication process (PSIRT) by automating the REST handshake between ServiceNow and Content Management Systems (Drupal and WordPress)
- Contributed to an Agile team, presenting tangible deliverables to executives and stakeholders biweekly

Education

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