

M.O. Haque

QA Engineer — 5 Years+ Experience | E-mail: Secure.at3137312055@gmail.com | Phone: 313-731-2055
US Citizen — Orlando, FL | [LinkedIn: secure-at-whitehat](#) | [GitHub: oscpprep.github.io](#) / [Global-Aid.github.io](#)

SUMMARY

I'm a QA Automation Engineer passionate about simplifying complex testing processes. I focus on developing and running automated tests to ensure software and systems function as intended. I enjoy exploring creative approaches to enhance testing and thrive in collaborative environments where we work together to solve challenges and build great products.

WORK HISTORY

Sineris March 2023 – Present, Orlando, FL

QA Automation Tester Consultant

- Designed and implemented test plans, performing smoke and regression tests for CRM software.
- Developed automated test scripts using WebdriverIO with Cucumber BDD and Selenium WebDriver.
- Executed security, performance, and mobile compatibility tests; tested integrations with external systems.
- Created and maintained feature files covering extensive UI elements, navigation, and workflows.
- Collaborated with developers to identify and resolve issues, enhancing system stability and reliability.

BA Soft Tech Dec 2023 – June 2024, Orlando, FL

QA Automation Engineer

- Developed automated test scripts using Python, Selenium, and Capybara.
- Conducted API testing for RESTful services and automated Android application testing with Espresso.
- Created and maintained test scripts with WebdriverIO and Cucumber BDD; enhanced Cypress test automation.
- Integrated test scripts with TestRail and built interactive consoles for WebdriverIO development.
- Configured Jenkins for CI/CD, improving build and deployment efficiency by 30%.

Quantum IT Services Feb 2021 – Dec 2023, New York, NY

Security Analyst Intern

- Monitored and analyzed real-time alerts using SIEM tools; responded to security incidents and collaborated with incident response teams.
- Managed and tuned security tools (antivirus, IDS/IPS, firewalls) to enhance threat detection and reduce false positives.
- Conducted vulnerability assessments, prioritized patches, and integrated threat intelligence into daily operations.
- Performed detailed analysis of security logs, leveraged forensics tools for incident investigations, and contributed to security awareness programs.

IIE Inc Aug 2019 – Jun 2023, Elgin, IL

Network Security Engineer Intern

- Utilized threat investigation frameworks and applied MITRE resources for Cyber Threat Intelligence.
- Conducted threat analysis using Yara, OpenCTI, and managed the MISP Threat Sharing Platform.
- Performed memory and disk forensics, executed malware analysis, and developed infrastructure hunting methodologies.
- Engaged in threat emulation, phishing defense, and buffer overflow exploitation; proficient in real-time threat detection with Snort and Zeek.

EDUCATION / CERTIFICATION

Microsoft Administrative Associate 2023 – 2024

New Horizons of NE Florida, Jacksonville, FL USA

CompTIA Security+ CE Certification Issued Jul 2022 - Expires Jul 2025

Credential ID: a9080fea-d1d4-4b12-b7ab-0e65488759be

Master of Arts/Science in Religious and Social Sciences 2014 – 2020

IIE.inc, Elgin, IL USA

SKILLS & TOOLSETS

QA Test Automation & Development

Languages: Python (Selenium, Appium), JavaScript, Selenium, Ruby (Capybara)
Test Frameworks: WebDriverIO, Cypress, JUnit, BDD: Cucumber
Database: CRUD operations with SQL in MongoDB
Version Control: Git, GitHub, Bitbucket; CI/CD: Jenkins, GitLab CI/CD, CircleCI
Test Management: Jira, Azure Boards, TestRail, Tools: Docker, Postman, Allure, Selenium Grid, Sauce Labs

Penetration Testing & Exploitation

Tools: Aircrack-ng, BeEF, Burp Suite, Hydra, John the Ripper, Metasploit, Sqlmap, Wireshark, Nikto, Nmap, Recon-ng, Gobuster

Cyber Defense

Endpoint Monitoring: Osquery, Wazuh; Firewalls: pfSense, FortiGate
Network Monitoring: Splunk, Zeek, Snort, ELK Stack; OSINT: SpiderFoot, Shodan, Google Dorks, Maltego

Threat Intelligence & Incident Response

Threat Intel: MISP, OpenCTI, MITRE ATT&CK, ThreatConnect; Incident Response: Cyber Kill Chain, Pyramid of Pain, Unified Kill Chain, NIST
Forensics: Memory leaks, Disk (Autopsy, FTK Imager); Malware Analysis: Yara