

# Hritesh Sonawane

sonawane.h@northeastern.edu | +1 (781)-921-4481 | Boston, MA

<https://www.linkedin.com/in/hritesh-sonawane> | <https://github.com/hritesh-sonawane>

A highly disciplined software developer with experience in *security engineering*, who loves building new things, starting from a blank whiteboard or early-stage prototype & transforming it into something people value

## TECHNICAL SKILLS

<b>Languages/Misc</b>	Golang, Python, C++, Bash, JavaScript, Node.js, React.js, HTML, CSS, PostgreSQL, MongoDB, Git, Reverse Engineering (ROP), Malware/ CVE Analysis
<b>Framework/Tools</b>	OSINT, OWASP Top 10, Wireshark, Snort, Metasploit, Nmap, Splunk, Burp Suite
<b>Cloud/OS</b>	AWS, Google Cloud, Microsoft Azure, Terraform, Kali, Ubuntu, Arch

## EDUCATION

**Northeastern University, Khoury College of Computer Sciences**, Boston, MA May 2024  
Master of Science in Cybersecurity GPA: 3.8/4.0

- Related courses: Systems Security, Network Security, Software Vulnerabilities, Application Security
- Research: Recipient of the Khoury Research Apprenticeship under Dr. Cristina Nita-Rotaru (NDSS lab)  
Topic: Attacks against delay-based congestion control algorithms – awarded best CS Research project

**University of Mumbai**, Mumbai, India July 2022  
Bachelor of Engineering in Information Technology CGPA: 9.1/10.0 | 2<sup>nd</sup> year: 9.2/10.0 | 3rd year: 10.0/10.0

- Related courses: Computer Networks, Cryptography, Cloud Security, Operating Systems, OOP
- Research: TORSION - Web Reconnaissance using Open-Source Intelligence, Publisher: IEEE ICONAT

## PROJECTS

**Attacks against delay-based congestion control algorithms**, NDSS Lab January 2023 - April 2023

- Formulated a finite-state machine (FSM) against Meta's implementation of the QUIC protocol (facebook/mvfst) - Copa (<https://web.mit.edu/copa>)
- Leveraged Mininet to orchestrate competitive flows with loss-based (Reno, CUBIC) & delay-based (BBR) algorithms
- Devoured numerous research papers in the congestion control sphere for comprehensive insights

**Hac'KP 2021**, Grapnel – Guided Micro-Fuzzing March 2021 - August 2021

- Upgraded a Darknet Crawler for the Kerala Police Cyberdome, themed 'Demystifying the Dark Web'; 20% more effective crawling as compared to previous iteration of the crawler
- Represented nodes graphically and identified vulnerabilities and other Indicators of compromise (IOCs) present in the darknet site
- Intelligent Darknet Monitor displaying the status of onion sites (Up/Down), boosting SDLC up by 3 weeks; Used Python, GraphQL, Dgraph, AWS S3, and pytest

**IEEE Xplore – Undergrad Capstone**, Torsion April 2021 - March 2022

- Engineered a Python-based Open-Source Intelligence (OSINT) tool for collecting metadata and maintaining a dossier on an entity by username
- Used ReactJS for frontend and Docusaurus for documenting the project
- Has darknet support - onion & i2p sites scanning and uses async to optimize querying speed by 30%

**TerrafoAWS**, Terraform on AWS foundation February 2021 - June 2021

- Reference repository and framework to build highly secure and scalable platforms on AWS which leverages established best practices and paradigms to support ops developers

## WORK EXPERIENCE

---

**The Broad Institute of MIT and Harvard**, *Security Engineer*, Cambridge, MA September 2023 - Present

- Integrating alerts from Splunk, Qualys, Google SCC, SentinelOne to Slack using Tines
- Securing and improving the data pipelines organization wide using HashiCorp Vault
- Meticulously reviewing source code, identifying vulnerabilities, and implementing enhancements to fortify the security of every product utilized at the Broad Institute

**Pfizer - Zoetis, Inc (Fortune 500)**, *Security Engineer Intern* / Boston, MA May 2023 - August 2023

- Leveraged Python, Ansible, PowerShell scripts and automation frameworks, reducing manual security tasks by 30%
- Achieved 25% faster incident response by correlating 1 million daily security events with Splunk (ES and Phantom), Demisto (Palo Alto Networks), and CrowdStrike Falcon; VAPT using tools such as Nucleus, Nessus, Burp, Nmap, and Metasploit
- Implemented Azure and AWS cloud security measures, guarding assets through network security, IDAM & encryption

**Oyela Inc**, *Software Development Engineer Intern* / Mumbai, India February 2022 - April 2022

- Streamlined the blocking and reporting feature for users and posts; boosted user interaction and positive feedback by 30% after feature adoption; Engineered Golang REST APIs for MongoDB integration
- Built the prototype for a search algorithm with the ELK (Elasticsearch, Logstash, and Kibana) stack for 20% efficient query of username, product name and category name as opposed to legacy regex

**Codecademy**, *Community Chapter Lead* / New York City, NY May 2021 - May 2022

- An ethical hacker leading and empowering a thriving community of college programmers (200+) in Mumbai, India
- Goa: Solutions to popular coding challenges; SysDesign: Software Systems Design module; GoPilot: Golang with tests

**Virtually Testing Foundation**, *DevOps Intern* | Remote (Los Angeles), CA May 2021 - May 2022

- Efficient infrastructure management with VMware virtualization on VMware HOL
- Managed containerized applications with Docker and orchestrated deployments using Kubernetes for seamless scalability

## LICENSES AND CERTIFICATIONS

---

- **AWS Certified Solutions Architect Associate** - AWS
- **AlgoExpert, SystemsExpert** - *AlgoExpert*
- **Digital Forensics and Incident Response** - *Basis Technology*
- **Practical Ethical Hacking** - *TCM Security*

## ACHIEVEMENTS AND EXTRA-CURRICULARS

---

- **CrowdStrike 2023-24 NextGen Scholarship** Recipient - \$10,000  
Awarded to only 8 students in the USA studying AI and Cybersecurity
- **Google's Hackathon (Code\_Love\_Hack)** Global Finalist - *Google*
- **DEF CON** Crypto village staff - DEF CON
- **HackMIT 2023** Mentor and Principal Judge - *MIT*
- **IEEE CTF** - 1<sup>st</sup> place *IEEE Mumbai Section*
- **5X** Tech Workshops, **4X** Hackathon Finalist, **3X** Long Distance Marathons, **100+** Anime