/chinmay-lohani
/chinmayl27.github.io/portfolio

CHINMAY LOHANI

(551) 232 - 8278
clohani1@jh.edu

OBJECTIVE

- I am a Security Engineering graduate student, skilled in Penetration Testing, Secure Code Review, Reverse Engineering, and Threat Modeling. I am technically skilled in Python, C++, Kali Linux, Burp Suite, OWASP ZAP, Ghidra, and Microsoft Threat Modeling. I have certifications including Google Cybersecurity and IBM Cybersecurity, and am looking for Summer 2024 internship opportunities to gain hands-on experience and apply my passion for learning across the cybersecurity domain.

EDUCATION

- **Master of Science in Security Informatics** | GPA: 3.84/4, Johns Hopkins University, US **Aug 2023 – Present**
  Security & Privacy in Computing, Software Vulnerability Analysis, Critical Infrastructure Protection.
- **Bachelor of Technology in Computer Science & Engineering** | GPA: 8.5/10, IIITS, India **Aug 2019 – Jun 2023**
  Cyber Security, Computer Networks, Machine Learning, Artificial Intelligence, Linear Algebra, Computer Architecture.

PROFESSIONAL EXPERIENCE

Graduate Teaching Assistant **Johns Hopkins University** **Aug 2023 – Dec 2023**

- Teaching assistant for *Full-Stack JavaScript* and *Decision Analytics* courses offered at Johns Hopkins University.
- Facilitated hands-on lab sessions and designed customized exercises to reinforce JavaScript and Data Analytics concepts for over 90 students. Conducted weekly review sessions to identify knowledge gaps and clarify challenging topics.

Software Engineer Intern **Mercedes-Benz Research & Development** **Jan 2023 – May 2023**

- Developed data warehouses using PostgreSQL to organize unstructured vehicle data, enabling optimized dashboard reporting.
- Visualized vehicle sensor data on interactive HD maps using React, trained Machine Learning models in Python validating level 3 vehicle automation requirements, and documented models and API endpoints, ensuring a smooth handoff to production engineering teams.

Core Member, GDSC **Google** **Aug 2022 – Apr 2023**

- Organized 10+ hands-on workshops and delivered lectures on full-stack development and industry practices for over 60 students.
- Led a 6-member team to build a community portal, increasing club event participation by 25%.

TECHNICAL SKILLS

- **Languages**: C++, C, Python, JavaScript, Java, Solidity, Ruby, R
- **Database and Libraries**: MERN, Django, FastAPI, Node, SQL, NoSQL, REST, Flask, MongoDB, PostgreSQL, NumPy, Pandas
- **Tools and Platforms**: VSCode, PySpark, Owasp ZAP, Burp Suite, GitHub, Docker, Azure, Ghidra, Wireshark, NMap, OpenSSL, Lynis, Microsoft Threat Modeling Tool, Valgrind, Scitools, Angr.io, Scapy, Metasploit, SQLMAP
- **Frameworks and OS**: NIST Cybersecurity Framework, MITRE, OWASP, HIPAA, Windows, Linux, Kali
- **Certifications**: Google Cybersecurity Certificate, IBM Cybersecurity Analyst, Blockchain Specialization by UB, Cryptography 1 by Stanford

PUBLICATIONS

- **"Assuring Safe Navigation and Network Operations of Autonomous Ships"**, 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), 2024, University of Nevada, Las Vegas, US.

PROJECTS

- **Penetration Testing and Vulnerability Assessment of OpenEMR** (Aug 2023 – Dec 2023): Performed security testing of OpenEMR, identifying vulnerabilities like SQLi, DoS, buffer overflows and XSS. Used tools including Burp Suite, OWASP ZAP, SQLMAP, and Wireshark to detect issues. Documented proof of exploitation along with remediation recommendations.
- **Angband** (Oct 2023 – Nov 2023): Developed proof-of-concept exploit achieving root access by reverse engineering Angband game binary to locate format string vulnerability. Used IDA Pro and GDB to analyze vulnerability and craft input to exploit stack overflow, redirect code execution flow, and open remote shell.
- **Duke Nukem II** (Sep 2023 – Oct 2023): Exploited buffer overflow in Duke Nukem game binary to achieve remote root shell access. Reverse engineered binary using Ghidra to identify vulnerable function and crafted malicious input. Developed proof-of-concept demonstrating arbitrary code execution via shellcode injection and redirecting control flow using buffer overflow technique.
- **Open-Source Web Server Security Assessment** (Aug 2023 – Sep 2023): Conducted threat modeling on an open-source web server using SciTool Understand and Microsoft Threat Modeling Tool. Produced an executive summary detailing risks and employed Ghidra and Veles for reverse engineering, bolstering the system's security posture.
- **Intrusion Detection System for IoT** (Jan 2022 – March 2022): Simulated DDoS attack in IoT devices, like flooding on CoAP network using Cooja simulator, leveraged the simulation data to train an ML model for detection of unusual traffic.

ADDITIONAL EXPERIENCE AND AWARDS

- **Software Development:** First Place Winner at HopHacks Hackathon 2023; developed Automated Insulin Titration Management application aim towards reducing patient titration errors and received best application of Google Cloud award.
- **Competitive Coding:** #1500 global Google HASH 2020, #64 global in CodeChef's September 2020 Challenge, #2 university wide at Codex competition, 5-star problem solver on HackerRank, 4-star coder on CodeChef.
- **ML/AI:** 3-star Contributor at Kaggle