NEHAL PILLAI

(+1) 240-351-4934 | nehalp10@umd.edu | LinkedIn | Website

EDUCATION

University of Maryland, College Park *(Aug'23-Present)*
Masters of Engineering in Cybersecurity **[CGPA: 3.95]** Maryland, United States

Savitribai Phule Pune University (formerly University of Pune) *(Aug'18-Jul'22)*
Bachelor of Engineering in Computer Engineering **[GPA: 3.67]** Maharashtra, India

TECHNICAL SKILLS AND CERTIFICATIONS

- **Languages:** Python, Assembly x86, Solidity, C, Bash Scripting
- **Tools:** Burp Suite, OWASP ZAP, Nessus, Nikto, Nmap, Metasploit, SQLMap, Hydra, John the Ripper, BloodHound, Gobuster, DirBuster, Mimikatz, Gophish, Shodan, Wireshark, Aircrack-ng, Volatility, Autopsy, Splunk, GDB
- **Cloud and Virtualization Platforms:** AWS (EC2, S3, IAM, CloudWatch/CloudTrail), Basics of Azure & GCP, Basics of Docker & Kubernetes
- **Vulnerability Assessment:** Penetration Testing **(Web/Mobile/Network/API/Cloud)**, Smart Contract Auditing, Source Code Review, SAST/DAST, OWASP Top 10, CWE Top 25
- **Compliance Frameworks & Standards:** NIST Cybersecurity Framework, HIPAA, SOC 2
- **Additional Skills:** Threat Modelling, Technical Content Writing
- **Certifications**: Offensive Security Certified Professional **(OSCP)**, Certified Professional Penetration Tester **(eCPPTv2)**, Web Application Penetration Tester eXtreme **(eWPTXv2)**, EC-Council Certified Ethical Hacker **(CEH v11)**, The SecOps Group - Certified AppSec Practitioner **(CAP)**, Certified Cloud Security Practitioner – AWS**(CCSP-AWS)**, Certified Network Security Practitioner **(CNSP)**.

EXPERIENCE

CredShields Technologies PTE. LTD.
Security Research Intern *(June'24-Aug'24)*

- Conducted comprehensive **vulnerability assessment and penetration testing (VAPT)** for web and mobile applications, significantly enhancing client security.
- Contributed to the research and development of QuickScan, a groundbreaking tool delivering threat reports and rug pull scores in under 60 seconds.
- Contributed to **the OWASP Foundation's** Smart Contract Top 10, Smart Contract Security Standards, and Testing Guide.
- Conducted extensive research leading to **the creation of Hackerboard**, a detailed repository containing Web3 hacks dating back to 2011.

Security Researcher *(Dec'22-Aug'23)*

- Performed in-depth **Solidity-based smart contract audits**, identifying and mitigating vulnerabilities to secure Web3 environments.
- Developed over **200 vulnerability detectors for SolidityScan**, a flagship product of CredShields. These detectors identify and flag vulnerabilities in smart contracts. Researched and created the logic for the detectors and supported their development, testing, and deployment.
- Led and collaborated with a team of security researchers in the **research and development of ThreatScan**, a tool for smart contract analysis designed to detect potential rug pull scams by inspecting critical code elements.
- **Authored and published weekly technical blogs**, providing insights on the latest Web3 hacks and cybersecurity trends.

Independent Security Researcher *(Aug'22-Dec'22)*

- Achieved a **HackerOne reputation score of 647**, reflecting a track record of identifying vulnerabilities such as Broken Authentication, Broken Access Control, Cross-Site Scripting, Open Redirects, and Business Logic Issues in web and mobile applications.
- Recognized as one of the **top researchers** on HackerOne private bug bounty programs, including Restream and Aftership.
- **Secured more than 75 renowned companies** by reporting vulnerabilities through crowdsourcing platforms like **HackerOne, Bugcrowd,** and **Vulnerability Disclosure Programs**. Excelled in **Bug Bounty**, showcasing advanced skills in identifying and exploiting security vulnerabilities.

PROJECTS

Don't Push Your Ad Around [In association with University of Maryland, College Park] *(Oct'23-Dec'23)*

- Analyzed web-based push notifications and malicious ads using insights from PushAdMiner, identifying key patterns and the need for real-time detection. Developed machine learning methods for identifying malicious ads and authored a research paper on improving advertising security.

HONORS & INVOLVEMENT

- Represented India at the **BlackHat MEA 2022 CTF World Finals** held in Riyadh, Saudi Arabia.
- Awarded "**Honourable Mentions**" by **Google LLC** for discovering an Insecure Direct Object Reference (IDOR) issue resulting in PII leakage on one of their web applications and for identifying a content spoofing vulnerability in the Google Photos mobile application.
- Awarded **"Hall of Fame"** by **Apple Inc.** for finding an HTML injection vulnerability on one of their web applications.
- **Discovered and published over 33 CVEs** by identifying vulnerabilities in open-source software (OSS) projects, with releases registered under MITRE and NIST NSD. **[CVE-2022-4866, CVE-2022-4849 are two of them]**