Nehal Pillai (OSCP)

(+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 **[CGPA: 3.67]** — Maharashtra, India

TECHNICAL SKILLS AND CERTIFICATIONS

- **Languages:** Python, Solidity, C, Assembly x86, Bash
- **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, Ghidra
- **Cloud and Virtualization Platforms:** AWS, Azure, Basics of Docker and 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
- **Additional Skills:** Threat Modeling, Technical Content Writing
- **Certifications:** Offensive Security Certified Professional (**OSCP**), Web Application Penetration Tester eXtreme **(eWPTXv2)**, Burp Suite Certified Practitioner (**BSCP**), Certified Professional Penetration Tester (**eCPPTv2**), 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** — Singapore, Remote

Security Researcher Intern (Returning) — *(May'24-Aug'24)*

- Collaborated with a team of security researchers on the development of ThreatScan (currently in development), a smart contract analysis tool designed to detect potential scams by examining critical code elements
- Co-authored and served as a top contributor to the **OWASP Smart Contracts Security** project, including the Smart Contract Security Top 10, Security Standards and Testing Guide.
- Conducted research to create **Web3 HackHub**, a detailed repository documenting Web3 hacks since 2011.

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

- Performed in-depth Solidity based **smart contract audits** and **conducted vulnerability assessments and penetration testing (VAPT) for web and mobile applications**, identifying and addressing vulnerabilities to enhance client security.
- 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.
- Contributed to the research and development of **QuickScan**, a tool delivering threat reports and rug pull scores in under 60 seconds.

➢ **Independent Security Researcher [Freelance]** — *(Aug'21-Dec'22)*

- Achieved a **HackerOne reputation score** of **719**, 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 some HackerOne private bug bounty programs, including **Restream** and **Aftership**.
- Reported vulnerabilities and secured over **75 renowned organizations** through crowdsourcing platforms like HackerOne and Vulnerability Disclosure Programs demonstrating advanced skills in identifying and exploiting security vulnerabilities in Bug Bounty programs.

RESEARCH

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

- Proudly represented India at the **BlackHat MEA 2022 CTF World Finals** held in Riyadh, Saudi Arabia.
- Secured the **2nd runner-up** position at the **Amazon Security x WiCyS Capture the Flag 2024** competition held across the United States.
- 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 discovering a **Blind XSS vulnerability** in one of their web applications and successfully bypassing their fix twice.
- Discovered over 33 vulnerabilities in Open Source Software, which have been assigned CVEs and registered under MITRE and NIST NVD. Notable ones include **CVE-2022-4866** and **CVE-2022-4849**.