

Atharva Shirude

College Park, MD • sec.atharvashirude@gmail.com • www.linkedin.com/in/atharvashirude • (240) 398-7708 • [GitHub](#) • [Blog](#)

SKILLS

- **Knowledge Areas:** Incident Response, Risk Management, IAM, AV, Firewall, TCP/IP, IDS/IPS, EDR, OWASP Top 10, OSINT, Web Application Security, API, Active Directory, TLS, SSH, HTTPS, Network Security, Cloud Security, Technology Platforms
- **Tools & Frameworks:** Nmap, Burp Suite, Wireshark, Nessus, Shodan, Kali Linux, Splunk, KQL, Elasticsearch, Kibana, Yara, Docker
- **Technical Skills:** Shell/Bash, Python, PHP, JavaScript, Golang, Vulnerability Assessment, Security Architecture, Network Analysis

EXPERIENCE

Ameeba Labs LLC – Security Engineer | USA

June 2025 – Present

- Built automated workflows and detection pipelines in Python and Golang, leveraging security tools, to identify and triage anomalous activity across AI agent logs, improving insider threat visibility and detection accuracy by 40% in alignment with security policies.
- Engineered scalable security controls and automation scripts integrated into CI/CD pipelines to auto-remediate vulnerabilities and streamline incident response, reducing manual intervention time by 25%.
- Partnered with software and infrastructure teams to enhance telemetry, logging, and forensics capabilities for AI-driven systems.

University of Maryland – Security Researcher | USA

November 2023 – May 2025

- Engineered automated pipelines using Python, Selenium, and NLP to process 10,000+ cybersecurity filings, improving analysis efficiency by 40% and data accuracy by 30%.
- Built a Retrieval-Augmented Generation (RAG) framework on a 10K-document vector database, increasing contextual retrieval precision by 45% for insider risk and governance analysis.

PKF Algosmic Pvt Ltd – Security Engineer | India

February 2022 – July 2023

- Performed comprehensive web and thick-client penetration testing across 25+ applications, uncovering critical vulnerabilities (SQLi, IDOR, insecure storage) and safeguarding data for 2M+ users.
- Executed Active Directory assessments involving enumeration, Kerberoasting, and privilege escalation simulations achieving consistent domain compromise in controlled tests and driving policy hardening for 5+ enterprise clients.
- Enhanced detection and response capabilities by developing custom SIEM correlation rules and alert logic, improving threat detection accuracy by 15% and reducing false positives by 20%.
- Collaborated with Blue Team and IT operations to integrate detection workflows and automate log analysis.
- Delivered security awareness sessions and authored 10+ technical blogs on threat modeling, malware analysis, and secure coding.

HACKX Security – Security Engineer | India

July 2020 – January 2022

- Performed OWASP Top 10 web application assessments (SQLi, XSS, IDOR, CSRF, auth bypass), uncovering 20+ high-severity vulnerabilities and collaborating with developers to verify remediations and reduce exploitable risk.
- Built prototype automation tools and workflows to scale offensive emulation and vulnerability discovery, cutting manual testing effort by 40% and accelerating time-to-find for repeatable weaknesses.
- Assessed cryptography and transport security across 20+ systems (TLS, SSH, AES, RSA), remediating 15+ misconfigurations and protocol weaknesses and improving data-in-transit posture by 30%.
- Supervised and mentored a team of 5 interns on VAPT engagements for financial-sector clients, improving remediation throughput and contributing to a 30% reduction in high-risk findings.
- Delivered client-facing reports and remediation playbooks with prioritized remediation steps, risk ratings, and test evidence to support compliance and secure-by-design fixes.

CERTIFICATIONS

CEH Master, Junior Penetration Tester v2, Offensive Security Certified Professional (OSCP) (Targeting December 2025), AWS Certified Solutions Architect - Associate (Targeting November 2025)

ACHIEVEMENTS

- Achieved 9th place in the in-person Amazon CTF 2024 (Seattle, Washington DC, NY) and 1st place at the Army Institute of Technology CTF, Pune, India.
- Designed and developed cloud-based CTF challenges and AWS IAM misconfiguration labs for Cloud Village at DEFCON 2025, focusing on cloud security best practices.

EDUCATION

University of Maryland, College Park | USA

May 2025

Master of Engineering, Cybersecurity

Penetration Testing, Cloud Security, Information Assurance, Incident Response, Virtualization and Container

University of Pune | India

June 2022

Bachelor of Technology, Computer Science and Engineering