reshmi14@uw.edu | +1 (206) 446 0216 | linkedin.com/in/reshmimehta

EDUCATION

University of Washington | Seattle, Washington **March 2025**
Master of Science in Information Management (Specialization in Cybersecurity & Artificial Intelligence) *CGPA 3.98 /4*

NMIMS Mukesh Patel School of Technology Management & Engineering| Mumbai, India **July 2023**
Bachelor of Technology in Computer Engineering *CGPA 3.80/4*

SKILLS AND CERTIFICATES

- **Certifications:** ISC2 Certified in Cybersecurity, AWS Cloud Practitioner, Security+ (In Progress)
- **Skills:** Python, SQL, SIEM (Microsoft Sentinel, Splunk), Incident Response, Threat Hunting, PenTesting, NIST, ISO, HIPAA, AWS (GuardDuty, CloudTrail, Security Hub), Azure, IAM, Firewalls, Wireshark, Docker, Kubernetes, TLS/SSL, Web App Security (XSS, SQL Injection), Burp Suite, Metasploit, OWASP ZAP, Cryptography (AES, RSA, SHA), Adversarial AI Red Teaming (Prompt Injection, Jailbreak)
- **Achievements:** Top 10 – Amazon x WiCys CTF, Top 15 – Palo Alto x WiCys-UW CTF, 3rd Rank in GitHub Code Review

PROFESIONAL EXPERIENCE

Security Analyst **June 2024-Present**
Alcon *Fort Worth, TX, USA*

- Enhanced security monitoring and incident detection by developing 20+ custom KQL rules in Microsoft Sentinel, increasing threat detection accuracy by 40% and reducing false positives by 30% through targeted query optimizations and log analysis.
- Researched and formulated the security framework for AWS Landing Zone Accelerator (LZA) to support HIPAA compliance. Conducted cloud security assessments using AWS Security Hub and GuardDuty, recommending 20+ security controls that reduced compliance gaps.
- Defined and enforced a SIEM policy framework based on NIST 800-53 controls, aiming to improve threat detection consistency across cloud infrastructure. Standardized logging, alerting, and monitoring processes, resulting in a 35% improvement in response time.

Research Assistant (Gen AI) **February 2024-April 2024**
University of Washington *Seattle, WA, USA*

- Developed a secure text generation model using Hugging Face Transformers with an interactive Gradio-based UI, implementing API access controls and request rate limiting to prevent unauthorized use, improving model security by 40%.
- Conducted AI Red Teaming and custom adversarial test suites, identifying 5+ exploits (e.g., encoding bypasses, role-playing attacks). Implemented context filtering and regex sanitization, reducing adversarial success rates from 80% to 20%.
- Implemented model output validation using regex filtering and payload inspection to detect potential data leakage, prompt reversals, and unintended system responses, strengthening model security.

Data Security Analyst Intern **December 2020 – May 2021**
Granuler CIO Consulting *Mumbai, India*

- Developed Power BI dashboards to visualize security-related CRM data, identifying anomalies and inefficiencies in workflows, which improved risk analysis and operational transparency by 25%.
- Utilized SQL to extract and analyze security logs, identifying patterns in unauthorized access attempts and data inconsistencies, optimizing data validation and compliance tracking.
- Automated data pipeline processes using UiPath RPA, streamlining security event logging and report generation, reducing manual effort by 25% and ensuring data accuracy in compliance reports.

PROJECTS

HusKey Secure: Cybersecurity-Enhanced Password Manager

- Designed a secure password manager using Docker (MySQL, Nginx, PHP), improving deployment consistency and scalability by 40%.
- Implemented HTTPS encryption with OpenSSL-generated SSL certificates to mitigate man-in-the-middle (MITM) attacks, significantly reducing the exposure of sensitive credentials by 90%.
- Strengthened authentication and session security mechanisms, migrating from insecure cookies to PHP session identifiers, effectively preventing session hijacking, unauthorized access, and replay attacks.

OWASP Juice Shop Penetration Testing

- Performed full-stack penetration testing on OWASP Juice Shop, exploiting SQL Injection, Cross-Site Scripting (XSS), and Broken Authentication vulnerabilities to assess application security.
- Utilized Burp Suite, OWASP ZAP, and manual testing techniques to discover and exploit business logic flaws and access control misconfigurations, uncovering 10+ critical security issues.
- Designed remediation strategies using OWASP Top 10, enhancing input validation, authentication mechanisms, and API security.

Adversarial AI prompt detection system

- Built an AI-driven adversarial prompt detection system using Random Forest and GPT-powered analysis to mitigate cyber threats with 98% accuracy, enhancing AI resilience against prompt injection, data exfiltration, and code execution.
- Designed a real-time AI security operations dashboard with Streamlit for actionable threat intelligence visualization, reducing incident response time by 40% and providing insights into malicious activity patterns.
- Conducted comprehensive AI red team simulations using GPT-generated adversarial prompts to stress-test AI defenses, improving cybersecurity posture by 30% and mitigating vulnerabilities against AI manipulation and social engineering attacks.

AI Red Teaming & Model Security Testing

- Conducted adversarial testing on DeepSeek, Copilot and Grok AI, identifying 8+ security vulnerabilities including encoding bypass, jailbreak exploits, and system role manipulation.
- Developed adversarial prompts and tested defensive fine-tuning strategies, reducing model susceptibility to prompt injection by 60%.