J. KAVIYARASAN

CYBERSECURITY RESEARCHER & VAPT ENTHUSIAST | CSE UNDERGRADUATE

Chennai, Tamil Nadu, India · +91 63810 31772 · kaviyarasangit@gmail.com · linkedin.com/in/kaviyarasan-j27 · github.com/ARASAN011

CONTACT

Chennai, Tamil Nadu, India
+91 63810 31772
kaviyarasangit@gmail.com
linkedin.com/in/kaviyarasan-j27
github.com/ARASAN011

EDUCATION

PERI Institute of Technology
Chennai, India
B.E., Computer Science & Engineering
Expected 2027

Relevant Coursework:
Computer Networks · DBMS · Data Structures & Algorithms · Operating Systems · Information Security

CERTIFICATIONS

- Networking Devices & Initial Configuration — Cisco Badge
- Cybersecurity Analyst Job Simulation — Tata (Forage)
- Introduction to Cybersecurity — Cisco Networking Academy
- Networking Basics — Cisco Networking Academy

CORE COMPETENCIES

- Analytical & Critical Thinking
- Attention to Detail
- Ethical Judgment & Integrity
- Problem-Solving Under Pressure
- Clear Technical Documentation
- Team Collaboration
- Adaptability & Continuous Learning
- Curiosity-Driven Research
- Professional Verbal Communication

PROFESSIONAL SUMMARY

Detail-oriented Computer Science Engineering student and aspiring Cybersecurity Researcher specializing in Vulnerability Assessment and Penetration Testing (VAPT). Builds and ships open-source security tools in Kali Linux environments, including an OWASP Top 10-aligned vulnerability scanner and an ML-driven password security analyzer. Combines applied machine learning, secure database design, and network configuration skills with a proactive, defense-first mindset to identify, document, and remediate digital vulnerabilities.

My approach integrates hands-on vulnerability testing with adherence to compliance frameworks (NIST, ISO 27001) to secure critical access points, API endpoints, and enterprise identity infrastructure.

TECHNICAL SKILLS

- **Identity & Access Management (IAM):** Public Key Infrastructure (PKI), Mutual TLS (mTLS), OAuth 2.0, SAML, Role-Based Access Control (RBAC)
- **Vulnerability & Telemetry:** CVSS v3.1 Risk Scoring, Auth Log Telemetry Analysis, Incident Response Workflows
- **Frameworks & Compliance:** NIST Cybersecurity Framework, ISO 27001/27002, OWASP API Top 10
- **Cybersecurity & OS:** Kali Linux, Vulnerability Assessment, Penetration Testing (VAPT), Active Defense, OWASP Top 10, Reconnaissance Automation, Password/Credential Hygiene, Information Security
- **Programming & Scripting:** Python, Bash, JavaScript, HTML5, CSS3
- **Machine Learning:** Classification & Regression Modeling, Ensemble Methods, Applied ML for Security & Healthcare Use Cases
- **Databases & Tools:** SQL, MySQL Workbench, Relational Database Management Systems (RDBMS), Git/GitHub
- **Networking:** Device Architecture, Initial Device Configuration, Routing Protocols

SECURITY ANALYSIS & COMPLIANCE HIGHLIGHTS

- Evaluated security postures against industry standards (NIST CSF, ISO 27001) by reviewing technical specifications, access controls (ACLs), and risk assessment documentation.
- Translated manual and automated penetration testing findings into structured vulnerability reports, assigning CVSS v3.1 risk scores and outlining step-by-step developer remediation guidelines.
- Analyzed multi-source log telemetry (endpoints, identity) to isolate false positives, assess threat exposure, and recommend defensive security controls aligned with zero-trust principles.
- Articulated complex security vulnerabilities, risk metrics, and attack vectors into clear, executive-ready reports for cross-functional business and engineering teams.

TECHNICAL PROJECTS

StrikeProbe v4.0.0 — *Enterprise-Style Web Vulnerability Scanner* github.com/ARASAN011/strikeprobe-v-4.0.0
- Designed and deployed an OWASP Top 10 (2025)-aligned open-source vulnerability scanner for the Kali Linux environment, generating actionable remediation reports.
- Automated targeted web scanning phases to flag configuration weaknesses, cutting manual reconnaissance time.
- Documented tool architecture and logic transparently on GitHub to support collaborative open-source security research.

Security Improviser v1 — *ML-Driven Credential Security Tool* github.com/ARASAN011/security-improviser-v1
- Built a password breach-checking and strength evaluation tool with ML-based classification/regression to score password security levels.
- Applied secure handling practices to credential data throughout analysis and reporting.

The Self-Healing Honeypot — *Active Defense Framework (In Development)*
- Architecting an automated intrusion detection and rapid remediation framework using active defense principles.
- Designing isolation mechanisms and containerized sandboxes to intercept payloads and dynamically rebuild compromised network nodes.

IPv4 & IPv6 Categorizer — *Utility to classify and categorize IPv4/IPv6 addresses for faster network identification · Apache-2.0* github.com/ARASAN011/IPV4-and-IPV6-categorizer

Heart Disease Prediction AI — *Six-algorithm ensemble for stable, accurate prediction with secure handling of sensitive patient data · MIT* github.com/ARASAN011/heart-disease-prediction-ai

Multi-Page Client Web Application — *Re-architected a monolithic single-file site into a modular, multi-page HTML5/CSS3/JavaScript application for a laptop retail client, improving load performance and maintainability*

CAREER OBJECTIVE

Seeking to leverage hands-on VAPT experience, Python automation capabilities, and a core understanding of PKI/Identity protocols to support advanced Information Security operations and Vulnerability Assessment initiatives.