VIBHEK SONI

Security Research Engineer | Backend Developer | System Architect

Queens, NY | (646) 684-9436 | vibheksoni@engineer.com
LinkedIn: linkedin.com/in/vibheksoni | GitHub: github.com/vibheksoni
Portfolio: vibhek.com | Security Research Blog: insecuremind.xyz

PROFESSIONAL SUMMARY

Security Research Engineer and Backend Developer with 5+ years of applied research experience in cybersecurity, system architecture, and scalable backend systems. Currently pursuing Computer Science degree (Expected 2027) while maintaining active research portfolio through InsecureMind.xyz security blog. Demonstrated expertise in vulnerability assessment, penetration testing, and security protocol implementation across diverse computing environments.

Research Focus: API security vulnerabilities, browser security research, real-time threat detection systems, and distributed system hardening. Published research on AI model security risks and advanced Chrome browser manipulation techniques.

Technical Leadership: Architected high-performance systems serving 50,000+ requests monthly with 99.9% uptime. Implemented security measures reducing vulnerability exposure by 80% across multiple production environments. Specialized in Python-based security tooling, C-level system programming, and cloud infrastructure security.

Academic Contributions: Active security researcher with published technical documentation and proof-of-concept frameworks. Experienced in collaborative research methodologies, technical writing, and knowledge dissemination through digital publications.

PUBLICATIONS & RESEARCH

Security Research Publications

InsecureMind.xyz - Independent Security Research Blog

Soni, V. (2024). "Exposing the Risks of Open Ollama APIs: Secure Your System Now." *InsecureMind.xyz*. Available: https://insecuremind.xyz

- Comprehensive analysis of Ollama API service vulnerabilities when exposed to internet access
- Detailed risk assessment methodology for identifying exposed AI model endpoints
- Practical implementation guide for securing local AI model deployments
- Impact: Educational resource for AI security practitioners and system administrators

Soni, V. (2024). "EvilChrome: Advanced Chrome Security Research PoC." *InsecureMind.xyz*. Available: https://insecuremind.xyz

- Advanced proof-of-concept framework demonstrating critical Chrome browser security vulnerabilities
- Novel approach to undetectable browser manipulation and real-time session hijacking techniques
- Multi-threaded event monitoring system with domain-specific action triggers
- Comprehensive analysis of browser profile access, data exposure, and session hijacking attack vectors
- Impact: Educational framework for browser security research and defensive strategy development

Technical Research Projects

Open Source Security Research: EvilChrome Framework, Security Assessment Tools, AI Security Research

Research Methodologies: Vulnerability assessment, Security protocol analysis, Proof-of-concept development, Technical documentation

TECHNICAL SKILLS & RESEARCH COMPETENCIES

Programming Languages & Frameworks: C (Linux kernel modules, low-level security implementations), Python (Django, FastAPI, Flask), PostgreSQL (advanced queries, performance optimization), MySQL, MongoDB, Redis, Bash (security automation, system administration), SQL (database security analysis)

Security Research & Analysis: Penetration Testing, Security Protocols (SSL/TLS, JWT authentication, cryptographic protocol analysis), Vulnerability Research (Zero-day discovery, exploit development), Network Security (Firewall configuration, intrusion detection systems, traffic analysis)

Research Methodologies: Technical Documentation (Academic writing, research paper preparation), Proof-of-Concept Development, Data Analysis (Security metric analysis, performance benchmarking), Open Source Research (Community-driven security research, collaborative development)

System Architecture & Infrastructure: Cloud Security (AWS security implementation, containerization security with Docker/Kubernetes), System Hardening (VPS security configuration, server hardening protocols), Load Balancing & Scaling (High-availability system design, performance optimization), DevOps Security (CI/CD security implementation, infrastructure as code security with Terraform)

Research Tools & Platforms: Security Testing (Selenium automated security testing, Chrome DevTools, browser automation frameworks), Development Environments (Git version control, Docker Compose, Linux administration), AI/ML Security (Model security assessment, API vulnerability testing), Web Technologies (Nginx reverse proxy security, Cloudflare DDoS protection, WebSocket security)

Academic & Professional Development: Technical Writing (Research publication, technical blog maintenance), Presentation Skills (Technical concept communication, research findings dissemination), Collaborative Research (Cross-functional team research, peer review participation), Continuous Learning (Security trend analysis, emerging threat research)

RESEARCH & PROFESSIONAL EXPERIENCE

Security Research Engineer | Freelance Software Developer

Macan Studios | Remote | June 2025 - Present

- Conducted applied research in web application security, implementing performance optimization methodologies that improved client system response times by 35% while maintaining security integrity
- Developed automated security assessment tools using Python and Bash, creating reusable research frameworks that streamlined vulnerability detection across 12+ client environments
- Designed and implemented secure API architectures with PostgreSQL integration, contributing to research on database security optimization and reducing data processing vulnerabilities by 30%
- Collaborated with distributed research teams using agile methodologies, maintaining 98% project success rate while contributing to security best practices documentation

Security Research Specialist | Full-Stack Developer

Tesseract | Remote | September 2023 - Present

- Led comprehensive security research initiatives, developing secure web applications and automated security assessment tools serving 10,000+ users with 99.5% security uptime
- Conducted systematic penetration testing and cybersecurity assessment research across 15+ client systems, developing methodologies that reduced identified security risks by 80%
- Implemented experimental blockchain security protocols and decentralized system research, contributing to emerging technology security frameworks with 40% efficiency improvements
- Authored technical documentation and research findings for SEO and digital marketing security, resulting in 60% improvement in secure implementation practices

Independent Security Researcher | Backend Developer

Freelance Research | Remote | 2019 - Present

- Architected and implemented scalable security research infrastructure using Django/FastAPI and AWS, supporting 25+ research projects with comprehensive testing frameworks that reduced security vulnerabilities by 40%
- Engineered secure research environments and VPS security configurations, developing hardening methodologies that achieved 99.9% uptime across experimental systems
- Designed microservices-based security research architectures implementing Redis caching and load balancing, improving research system performance by 60% and reducing analysis response times from 200ms to 80ms
- Developed automated CI/CD security research pipelines using Docker and GitHub Actions, creating reproducible research environments that reduced deployment time by 50%

RESEARCH PROJECTS & TECHNICAL CONTRIBUTIONS

LlmEndpoint: Distributed AI Security Research Platform

Research Areas: AI Model Security, Load Balancing, Distributed Systems

Technologies: Python, Django, JWT, Docker, Redis, MySQL, Load Balancer | Duration: 2024 - Present

Research Objectives: Investigation of secure AI model deployment architectures and cost-effective access methodologies for open-source language models.

Methodology: Engineered a distributed AI API research platform providing secure access to open-source models through Ollama integration, serving 50,000+ authenticated monthly requests with 99.8% uptime reliability.

Technical Contributions: Developed sophisticated load balancing algorithms and intelligent routing systems across 8 distributed nodes with automatic failover capabilities; Implemented comprehensive node management research framework with real-time health monitoring and dynamic request distribution; Created security-first architecture maintaining optimal resource utilization during peak traffic scenarios.

Research Impact: Advanced understanding of AI model security deployment patterns and contributed to open-source AI infrastructure security methodologies.

CyberShield: Real-Time Threat Detection Research System

Research Areas: Network Security, Kernel-Level Programming, DDoS Mitigation

Technologies: C, Linux Kernel Modules, iptables, VPS Management | Duration: 2023 - 2024

Research Objectives: Development of high-performance, kernel-level security systems for real-time threat detection and mitigation.

Methodology: Implemented C-based firewall system using Linux kernel-level packet inspection techniques, successfully defending against simulated DDoS attacks up to 8 Gbps with sub-millisecond processing latency.

Technical Contributions: Developed dynamic rule generation algorithms and system hardening protocols using custom UFW/iptables configurations; Architected real-time threat detection system processing 1M+ packets per second with automated response capabilities; Reduced successful penetration testing attack rates by 95% through advanced security implementations.

Research Impact: Contributed to understanding of kernel-level security implementations and real-time threat response systems.

ProxyIt: Infrastructure Security Research Platform

Research Areas: Network Security, IP Cloaking, Attack Pattern Analysis

Technologies: Python, Django, Redis, Nginx, Cloudflare | Duration: 2023 - Present

Research Objectives: Investigation of backend infrastructure protection methodologies and attack pattern recognition systems.

Methodology: Developed secure proxy service research platform enabling IP cloaking techniques for backend infrastructure protection, successfully securing 500+ client services from direct exposure.

Technical Contributions: Implemented real-time attack detection and automated blocking mechanisms with comprehensive analytics framework; Developed Redis-based caching optimization and custom Nginx configurations achieving 99.9% proxy availability; Created attack pattern analysis system preventing 10,000+ unauthorized access attempts daily.

Research Impact: Advanced knowledge of network security patterns and contributed to proxy-based security architecture research.

EDUCATION

Bachelor of Science in Computer Science

Queens College, City University of New York (CUNY) | Queens, NY | Expected Graduation: May 2027

Relevant Coursework:

- Data Structures & Algorithms
- Database Systems Design and Implementation
- Computer Networks and Security
- Software Engineering Methodologies
- Cybersecurity Fundamentals
- Computer Systems Architecture
- Advanced Programming Techniques

Academic Focus: Security research methodologies, system architecture design, and advanced programming applications with emphasis on cybersecurity implementations.

Research Interests: Network security, vulnerability assessment, distributed systems security, and AI/ML security frameworks.

High School Diploma with Computer Science Concentration

Richmond Hill High School | Queens, NY | Graduated: 2023

Specialized Curriculum: Advanced computer science coursework with focus on programming fundamentals, system administration, and early security concepts.

ADDITIONAL INFORMATION

Languages: English (Native proficiency), Hindi (Conversational)

Availability: Full-time positions available, Open to research collaborations, Security consulting available for specialized projects

Security Clearance: Eligible for security clearance (US Citizen, US Born)

Professional References: Available upon request, Client testimonials available through portfolio website