BEN LOEMHENG

Phone: +855 66 470 422
Email: benloemheng.it@gmail.com
Portfolio: benloemheng.vercel.app
Github: loemheng840

SUMMARY

Motivated Computer Science student and Web Security Researcher with interest in penetration testing, application security, and backend development. Passionate about building security tools, identifying vulnerabilities, and improving application security through practical research and development, while continuously learning modern cybersecurity techniques and secure software engineering practices.

PROJECT EXPERIENCE

Auto Offensive - Built an automated scanning platform (Team Project)

Auto Offensive is an automated offensive security scanning platform that orchestrates security tools through a REST API backed by a gRPC execution engine, Redis job queue, and sandboxed Docker + gVisor containers. Users submit Unix-style pipeline commands (e.g., subfinder -d example.com | httpx | naabu), and the system parses them into sequential steps, runs each tool in isolated containers, pipes output between steps, streams logs in real-time, and persists structured findings to PostgreSQL. It also integrates AI-driven analysis and SonarQube code quality scanning.

Key features:

- Pipeline-based scanning with Unix-style pipe chaining between tools
- 7+ integrated security tools (subfinder, httpx, naabu, nmap, nuclei, gobuster, gitleaks)
- Real-time log streaming via Server-Sent Events (SSE) and Redis pub/sub
- Sandboxed execution using Docker + gVisor kernel-level isolation
- Three scan modes: Basic, Medium, and Advanced (full pipeline)
- JWT authentication via Keycloak (OAuth2/OIDC) with role-based access control
- Structured findings with automatic parsing and deduplication
- Extensible tool registry add new tools via JSON definitions without code changes
- SonarQube integration for code quality scanning
- AI-powered security analysis engine (MCP-based agent orchestration)
- PDF report generation for scan results
- API key management with scoping and revocation

Technologies: FastAPI, Go + gRPC, PostgresSQL, Docker + gVisor, Redis, Docker Compose,Anthropic API, MCP, Protocol Buffers, sqlc, Goose migrations

Stack Quiz - Online Game Challenge (Team Project)

Stack Quiz is a real-time interactive quiz platform inspired by Kahoot!, designed for classrooms, training sessions, and online learning environments. The platform allows teachers to create live quizzes, students to join sessions instantly, and administrators to manage educational content efficiently. It includes analytics dashboards, leaderboard systems, and real-time communication features to enhance engagement and track learning performance through an interactive and scalable web application experience.

Key features:

- Real-time multiplayer quiz sessions
- Live leaderboard and scoring system
- Quiz creation and management
- Session PIN/join system
- Analytics and performance tracking
- Timer-based quiz questions
- Dashboard for quiz statistics
- Authentication and user management

Technologies: React, Spring Boot, PostgreSQL, WebSocket communication, JWT Authentication

EDUCATION

Bachelor of Information Technology **2024 - 2026**

Norton University

- Computer science

Short Courses **2024 - 2026**

ISTAD Institute

- Java & Spring boot (Short courses)
- Full-Stack Development
- IT Professional - Cybersecurity (In Progress)

ADDITIONAL INFORMATION

- **Technical Skills:**
  - Spring Boot
  - Frontend
  - Web Pentesting
  - Microservices (Basic)
  - Database
  - Linux command line & basic server management
  - SDLC Understanding
  - Shell Scripting
- **Tools:**
  - Docker
  - Burp Suite
  - OWASP ZAP
  - Nmap
  - Wireshark
  - Metasploit
  - Nikto
  - Gobuster
  - SQLmap
  - ffuf
  - Hydra
  - John the Ripper
  - Hashcat
  - Postman
  - Docker
  - Sonarqube, Trivy
  - Google Cloud Platform
  - WebSocket
  - Keycloak exposure
- **Languages:**
  - Khmer (Native)
  - English (Medium — conversational to technical)
- **Certifications:**
  - Full-Stack Development
  - ITP-Web Security Engineering
- **Awards/Activities:**
  - Top 3 Team project — Full-Stack Development (ISTAD)
- **Reference:**
  - **Name**
    - Instructor of ISTAD
    - Phone:
    - Email :

Dear Hiring Manager,

I am writing to apply for the Web Security / Web Penetration Testing position at your company. Although my academic background includes general history and cultural studies, I have developed strong technical skills and hands-on experience in cybersecurity, backend development, and web application security through study course, self-study, labs, and team projects.

My background trained me to think critically, conduct detailed research, analyze patterns, and communicate findings clearly. These skills became highly valuable as I transitioned into cybersecurity, where investigation, problem-solving, and attention to detail are essential.

I have actively built practical experience through platforms such as Hack The Box and TryHackMe, where I practiced web exploitation, privilege escalation, reconnaissance, and vulnerability analysis in realistic lab environments. I regularly study OWASP Top 10 vulnerabilities and have hands-on experience identifying and understanding issues such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, IDOR, insecure APIs, and misconfigurations.

In addition, I use tools such as Burp Suite, Nmap, Linux environments, and web debugging tools during CTF challenges, security labs, and personal testing projects. I also write technical reports and vulnerability writeups to document findings, explain attack paths, and improve my understanding of security concepts.

Beyond security testing, I have experience in backend and API development using technologies such as Python, Java, Spring Boot, FastAPI, PostgreSQL, gRPC, and REST APIs. Building backend systems has strengthened my understanding of authentication, authorization, API security, and how vulnerabilities emerge in real-world applications.

Recently, I have been working on projects involving API architecture, gateway services, automation tools, and security-focused backend systems, which further increased my interest in offensive security and secure application design.

What attracts me most to cybersecurity is the continuous learning process and the challenge of understanding how systems work internally. I enjoy researching vulnerabilities, solving technical problems, and improving application security through ethical and responsible testing.

I would welcome the opportunity to contribute my analytical mindset, technical dedication, and growing hands-on security experience to your team. Thank you for considering my application. I look forward to discussing my qualifications further.

Sincerely,
Ben Loemheng