Bùi Trường An

IT Engineer

Cybersecurity graduate from USTH with hands-on development experience building SIDERIS — a multi-service system in Node.js and React, using Redis for real-time event handling, deployed with Docker. Comfortable with backend logic, REST APIs, and working across a full JavaScript stack. Security-focused background gives a practical edge for systems that need to be built with real threats in mind. A quick, active learner, seeking a junior IT engineering role

EXPERIENCE

Cybersecurity Intern — ICTLab USTH

April 2026 - July 2026

SIDERIS | *Creator of Sidecar Integrated Detection, Event Reporting, and Intelligence System*

Stack: Node.js/Express (Backend) | React/Vite (Frontend) | PostgreSQL & Redis (Data) | Docker (DevOps)

Link: github.com/Ann-BT/SIDERIS

- Built a sidecar-deployed web attack detection and mitigation system requiring zero changes to the protected application's source code, deployed transparently as a reverse proxy in front of the target site.
- Detected 7 categories of web attacks — injection (SQLi, XSS, command injection, SSTI, XXE, SSRF), authentication attacks, reconnaissance /scanning, bot and headless-browser automation, DoS/volumetric abuse, and session hijacking — by combining user behavioral signals with server-side traffic log analysis.
- Implemented automated response (rate limiting, CAPTCHA challenge, blocking) using Redis to track and enforce threat state in real time, without manual intervention.
- Built a React dashboard consuming a REST API to give non-technical site owners a SOC-style view into detected threats and system status.

PROJECTS

- **Developing Phishing Detection Solution**

Group project - Leader

Develop Phish Shield a browser extension that combines traditional whitelists/blacklists with an Machine learning layer (**Random Forest**) to automatically scan and alert phishing URLs on browser.

- **Secure two-factor authentication system**

Designed and developed a secure and reliable SMS-based OTP system using Python Flask, Redis, and Twilio

- **Anonymous FTP Login Reporting**

IDS/IPS course work

<CVE-1999-0497> Setting up VM environment, perform scan and configure firewall for prevent vulnerability

INFORMATION

- 0397677835
- Cau Giay, Ha Noi
- merlinthemage.me
- anbt.personal@gmail.com
- Available for full-time work

EDUCATION

University of Science and Technology of Hanoi

- Bachelor in Cyber Security
- Classification: Very Good
- Achieved Top 3 academic ranking in first year
- Awarded scholarship for 3 years

SKILLS

Languages:

- English (B2 - certified by USTH)
- French (A2 - TCF)

Technical skills:

- Operating Systems: Linux (daily user - Fedora/Cachy/Arch), Windows, and some VMs
- Networking: TCP/IP fundamentals, HTTP/HTTPS, DNS, common network protocols
- Programming: JavaScript, Python (basic), TypeScript, Node.js
- Web Technologies: Next.js, React, Express.js, REST APIs, CSS Modules, WebSockets

- **Penetration Testing**

Setting up environment and perform testing on Chronos VulnHub, scan and attempt pentesting then find:

  - Broken access control via user-agent header
  - OS command injection can execute unauthenticated remote code
  - Sudo misconfiguration lead to allows root shell

- **Personal Portfolio Website**

Stack: Next.js, React, Tailwind CSS, TypeScript, Supabase, Framer Motion
Site: merlinthemage.me
Built a type-safe frontend using Next.js, React, and TypeScript, styled with custom CSS Modules, and enhanced with Framer Motion animations. Integrated Supabase (PostgreSQL & Realtime) for cloud data persistence and automated deployment to GitHub Pages.

- **Others course projects:**
  - TCP/RPC/MPI File transfer (Distributed system)
  - Networked Word Chain Game (Network Programming)
  - Multi-user WordPress server (Administration of Computer Systems)
  - Application of SHA-256 in Bitcoin (Introduction to Cryptography)
  - Cloud service with Docker and Kubernetes (Cloud Computing)

COURSES

- **EC-Council | Computer Hacking Forensic Investigator (CHFI)**

Learn in Digital Forensic course, i have learn fundamental concept of Forensic investigation, Data acquisition, Anti-forensics, Windows/Linux forensics and Network forensics.

- **Malware analysis**

Learning about malware, investigate and do some reports about basic malwares provided in course Malware analysis on REMnux VM.

- **Web security**

Learning about security of website and perform attack on course lab with some type of basic attacks for OWASP Top 10

- Tools & Platforms: Docker, Redis, Supabase, PostgreSQL, GitHub
- Security Tools: Wireshark, Burp Suite, OWASP ZAP, Wazuh, IDA Pro, Process Monitor, PEStudio
- Security Knowledge: Web Security, Malware Analysis Fundamentals, Digital Forensics

Soft skills:

- Quick learner and adaptable to new tools and workflows
- Problem-solving mindset
- Experience working in teams and leading academic projects
- Technical documentation and reporting
- Comfortable working in English
- Responsible and punctual

CERTIFICATIONS

- Google Cybersecurity Professional Certificate
- Fortinet Certified Associate in Cybersecurity
- Cisco: Network Defense