# SECURITY RESEARCHER

## PERSONAL DETAILS

Name: Truong Nguyen Long

Date of Birth: 30-01-2007

Linkedin: LongTruong

Mail: longbinhquoitay8@gmail.com

Address: Ho Chi Minh City

My Blog: Thewindghost

GitHub: Thewindghost

Language: Vietnamese, English

## OVERVIEW

Security Researcher with one year of combined internship and full–time experience in bug bounty, pentest, CTFs, and exploit research. Seeking to contribute advanced vulnerability research and exploit development skills to strengthen organizational security posture

## WORK-EXPERIENCE

Penetration Tester & Security Researcher in CodeToanBug 20/07/2024 - 20/05/2025

- Designed and Developed Web CTF challenges for labs.codetoanbug.com
- Configured and Secured Ubuntu Servers following Essential Security Practices, Including Nginx Security Hardening, Fail2Ban, Docker Networking, and Least Privilege Permissions.
- Join the real pentest project of penetration testing company for IIS server system

## SKILLS

Technical and Techniques:

- Proven ability to identify and exploit real–world OWASP Top 10 vulnerabilities.
- Primary Strengths - Broken Access Control, Business Logic Error and Cross-Site Scripting (XSS) proven in PoCs and Pentests.
- Develop automation scripts and tools in Python/Go to streamline vulnerability scanning, triage, and exploit proof-of-concept generation.

Tools:

- Nuclei, Katana, Burp Suite Pro (+ extensions), Ghauri; Kali/Parrot OS; Drozer, APKTool, ADB, JADX–GUI.

Programming Languages:

- Python(Flask), NodeJs, Golang, PHP.

## CERTIFICATE

- Completed The HTB Certified Penetration Testing Specialist Path Learning
- Completed The Web Pentesting 101–102 – CyberJutsu Academy
- Completed The Python Developer, Intermediate, Introduction – SoloLearn
- Cybersecurity Foundations – LinkedIn Learning
- Certified Associate Penetration Tester (CAPT) – Hackviser

## ACHIEVEMENTS AND AWARDS

- Top 1 Bug Bounty Hunter – Trip Security Response Center (Feb 2025)
- Top 6 Finalist – CSAW'2024 Red Team Competition (Nov 2024)

## CVES TABLE

- CVE-2025-23001 Host Header Injection Reset Password Poisoning – CTFd
- CVE-2025-29419 Man-In-The-Middle Attack (Waiting – Mitre)
- SSL Downgrade – HTTP (Waiting – Mitre)
- CVE-2025-10295 XSS Stored – Forced File Download – kayapati
- CVE-2025-62674 Missing Authentication for Critical Function – iCam365
- CVE-2025-64770 Missing Authentication for Critical Function – iCam365
- Insecure Broadcast Receiver – Android App (Waiting – CISA)

## CTFS PARTICIPATED

- Top 14 – Interlogica CTF 2024
- Top 37 – Fetch The Flag Snyk 2025
- Top 90 – Apoorv CTF 2025
- Top 170 – Hack The Box Apocalypse 2025
- Top 485 – Hack The Box Apocalypse 2024
- Top 533 – Hack The Boo 2024
- Advent of Cyber 2024

## PROJECTS

- Re-Hawk Scanning Tool – In Process
- Bug Bounty Web(Python Flask) – In Process
- Contributing to and Building Web CTF for Shielded Skies CTF 2024

## Education

Self-Taught / Independent Researcher:

- Portswigger Academy
- CTF Hack The Box
- Hack The Box Academy
- Root Me
- Mobilehackinglab
- Bugcrowd University
- Hacksplaining