SECURITY RESEARCHER

PERSONAL DETAILS

Name: Truong Nguyen Long

Date of Birth: 30-01-2007

Linkedin: LongTruong

Mail: longbinhquoitay8@gmail.com

Address: Ba Ria - Vung Tau City

My Blog: Thewindghost

GitHub: Thewindghost

Language: VietNam, English

OVERVIEW

Focused on Web Security, Bug Bounty, and Vulnerability Research Through Intensive Internship and Self-Directed Study Within 1 year.
Participated in Bounty Programs (GOV, HackerOne, Bugcrowd, private), Direct Collaboration, CTF Competitions, and Real-World Exploit Research.

WORK-EXPERIENCE

Web Security Analyst CodeToanBug 20/07/2024 Internship(Present)

- 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.

SKILLS

- Nuclei, Katana, Tool-Pentesting in Kali Linux, Burp Suite Pro Extension, Ghauri, Parrot OS.
- Python-Flask Programming, NodeJs, Golang.

Blog POC Bug Bounty

- HHI Reset Password Poisoning(Advance Technical - Direct Collaboration)
- Open Redirect via Remote SVG Fetch-Variant(BugCrowd)
- Unauthenticated cache purging(Hackerone)
- Cross-Site-Scripting Steal Cookie + Low-Risk XSS(Hackerone)
- Observable Timing Discrepancy - Timing Attack(Hackerone)
- Cross-Site-Scripting Via Prototype Pollution(Private Web Penetration Project)
- Cross-Site-Scripting Severity-Low(Private Web Penetration Project)
- Iframe Injection Full Page(Private Program)
- Cross-Site-Scripting Steal Cookie + Low-Impact(Private Program)
- HTML Injection Full Page - Phishing Attack(BugCrowd)
- Cache Poisoning - Import File Malicious For Attack(BugCrowd)
- Forced File Download Attack(BugCrowd)
- Server-Side Request Forgery + External Service Interaction(BugCrowd)
- Insecure Direct Object Reference - Username Admin(BugCrowd)

ACHIEVEMENTS

- Top 37 Fetch The Flag Snyk 2025
- CVE-2025-23001 Host Header Injection Reset Password Poisoning CTFd (Server-Side)
- CVE-2025-29419 Man-in-the-Middle Attack Discloses Sensitive Information CTFd (Network)
- Top 14 Interlogica CTF 2024
- Top 170 Hack The Box Apocalypse 2025
- Hack The Boo 2024
- Top 90 Apoorv CTF 2025
- Top 485 Hack The Box Apocalypse 2024
- CSAW'2024 RED Team Finalist

CERTIFICATE

- Completed the CPTS Path Learning(finished) - Exam Scheduled: 20/07/2025
- CBJS Web Pentesting 101–102 (in progress) - Exam Scheduled: 15/05/2025
- Completed The Python Developer, Intermediate, Introduction SoloLearn

PROJECTS

- Developing a Flask-based Framework that integrates Server-Side Vulnerabilities for Learning and Research Purposes. GitHub
- Contributing to and Building Web CTF for Shielded Skies CTF 2024. GitHub
- File Upload Attack, XSS Via Prototype Pollution, Iframe Injection, Open Redirection, XSS Steal Cookie (ASP.Net FrameWork - Windows- Private Project Penetration Testing CodeToanBug)