

Chu Quoc Khanh

Fresher SOC

Email: khanhcqhe170425@gmail.com

Phone: 0987061908

Address: 286, Van Giang, Hung Yen

Github: <https://github.com/KhanhCQ1511>

LinkedIn: <https://www.linkedin.com/in/khanhchu-k0i3n>

CAREER OBJECTIVE

Fresher SOC looking for a position in an organization that encourages hands-on and skill enhancement. Hoping to apply my technical skills and knowledge of security testing to effectively complete assigned tasks and deliver high-quality results for the company. My short-term goal is to become a full-time employee of the company after completing my probationary period and become a security engineer in the long run.

EDUCATION

FPT UNIVERSITY HANOI | 2021 - NOW

Majors: Information Assurance

Current GPA: 7.55/10

KEY COMPETENCIES

Technical Skills

Programing Language:

- C, Java, Python, SQL at fundamental level

Tools:

- Burp Suite, Metasploit, Nmap, HxD, FTK, PwDump7, Ophcrack, OSXPMem, Wireshark, FOG, ClamAV, Yara, ...

Linux:

- Basic usage with common commands, Bash scripts at basic level
- Platform: Kali

OS:

- Basic understanding about Linux, Window Server

Networking:

- Understanding about OSI model, TCP/IP, common protocols, ...

Vulnerability:

- Basic understanding 10 common website security vulnerabilities

Languages:

- English: Pre-Intermediate level
- Japanese: Basic level

EXPERIENCES

VTC Digicom - Intern Cyber Security

April 2024 - July 2024

- Learn about computer networks and networks devices
- Learn about logs, SIEM, IDS
- Perform scanning, vulnerability detection and penetration testing of Web applications according to OWASP
- Analysis test result and provided detail report
- Find Bug Bounty on Prebuilt CMS and build PoC exploit

PROJECT

DynamicPHPCode Filtering Bypass leads to Remote Code Execution

July, 2024

Conducted a review and testing on the latest version of Dolibarr CMS and discovered a bypassable vulnerability to inject PHP code into the system leading to Remote Code Execution.

Link: The vendor has not allowed the vulnerability to be publicly disclosed

CVSSv3: 8.9

Store XSS in ConcreteCMS

July, 2024

Concrete5 in latest version was affected by multiple cross-site scripting vulnerabilities that could allow an attack to execute JavaScript in the browsers of targeted users.

Link: The vendor has not allowed the vulnerability to be publicly disclosed

CVSSv3: 3.8

CERTICATIONS

Applied Cryptograph | Feb 2024

<https://www.coursera.org/account/accomplishments/specialization/BSNG7WK6JR22>

Python for Everybody | Mar 2024

<https://www.coursera.org/account/accomplishments/specialization/WR7VSXPJRH2S>

HORNORS & AWARDS

Good Students semester Summer | 2023

Good Students semester Fall | 2023

Excellent Students semester Spring | 2024