HOÀNG TUYỂN QUYỀN

Đại Kim, Hoàng Mai, Hà Nội
0936378085 | 21/01/2003 | qh6967258@gmail.com | https://github.com/quyenheu

CAREER GOALS

- Improve my skills and knowledge about pentest. From there, upgrade to become a redteam and devote myself to the company and business

EDUCATION

Academy of Cryptography Techniques - KMA Ha Noi, Viet Nam
Junior of information security 2021-2026

- Successfully complete specialized subjects

WORK EXPERIENCE

VNCERT/CC - Vietnam Cyberspace Emergency Response Center Tran Duy Hung, Ha Noi
Web Penetration Testing 7/2023-12/2023

- Perform penetration testing in real systems:
  - Apply the pentest process to perform penetration testing of websites in project
- Research and build labs on information security:
  - Build web labs that simulate common vulnerabilities using PHP and Nodejs
  - Create exploit scripts with Python, Bash and learn about new popular tools
- Participate in actual combat exercises on actual state domains:
  - Type Attack & Defense
- Participate in actual combat exercises on actual state domains:
  - Testing and technical support in the Smart Banking 2023 competition

KCSC club – Information security club of KMA Academy of Cryptography Techniques
Member of the web segment

- Learn, analyze and practice attacking web vulnerabilities from basic to advanced
- Participate in competitions organized by the club and outside
- Research and presentations according to the club's assigned topics
- Listen to other members of the club give presentations about information security

SKILLS

Technical Skills

- Information security:
  - Basic Windows/Linux privilege escalation skills
  - Have knowledge of common web vulnerabilities: Cmdi, SQLi, file upload, IDOR, path traversal, file inclusion, XSS, SSRF, CORS, CSRF, deserialize vulnerability, ...
  - Know how to approach and analyze a target: Reconnaissance, fuzzing, hypothesize, …
  - Have skills in searching and analyzing documents
- Tools:
  - Skills using recon and exploitation tools: Burpsuite, osmedeus, nuclei, nmap, metasploit, ffuf, …
  - Skills in writing exploit scripts with: Python, bash
- Program:
  - Front-end: HTML, CSS, JS
  - Back-end: PHP, Nodejs and basic Java swing
  - Database: MySQL

    - Data structure and algorithms: C/C++, Python, Java
- Soft skills:
    - Self-study, teamwork, communication and play sports well

Languages

- Reading English documents well and basic communication

Certifications

- Web penetration testing certificate of CyberJutsu
- TOEIC 550 certificate

PROJECT

Web Blog

- Summary of some my bug bounty cases, cve, write up ctf and research
- Link: https://web-blog-lime.vercel.app/

Custom tool reconnaissance and exploit based on Osmedeus

- Recon: scanning subdomain, classify http, dns, IP range, spider, fuzzing, ...
- Vulnerability: nuclei, jaeles, and custom vulnerability as SQLi, Cmdi, Pathtraversal, XSS, SSTI, …
- Link: https://github.com/quyenheu/My-Custom-Tool

ACTIVITIES

Participate in some ctf competitions

- Bách Khoa ctf - BKCTF, Sinh viên với an toàn thông tin - PTIT , KCSC recruitment and other competitions on ctftime, cookie arena

Regularly practice and write up ctf

- On platform: hackthebox, cookie arena, root me, portswigger, …

Link: https://web-blog-lime.vercel.app/CTF.html

BUG BOUNTY & CVE

- CVE-2023-45809: Disclosure of user names via admin bulk action views
- Cross-origin resource sharing in Bugcrowd
- Vulnerability in huntr: Leaked all images from a unauthorized user account
- Vulnerability in huntr: Leaked all documents from a unauthorized user account
- Link: https://web-blog-lime.vercel.app/CVE.html

COURSE

Web penetration testing – Cyberjutsu academy 4/2023-8/2023

Student

- Learn, analyze and practice attacking common web vulnerabilities
- Receive training on pentest workflow, teamwork, goal approach, and testing practices
- Participate in competitions and lab systems organized by the center
- Oriented by experts in the field of information security

IELTS - The IELTS workshop: 10/2022-3/2023

Student

- Learning 4 English skills: writing, reading, listening, speaking