Email: suprawitch123@gmail.com

LinkedIn: Suphawith P.

GitHub: Yamerooo123

BugCrowd: Suphawith P.

Phone number: (+66) 92 496 5301

Samut Prakan, Bangbo 10560

Suphawith Phusanbai

Assumption University

Bachelor of Information Technology

Major of Information Technology

I consistently find ways to polish and improve both my penetration testing skills and soft skills to be 1% better every day. My goal is to become a cybersecurity professional who contributes to the greater good of the cybersecurity field.

Professional Experience

Siam Thanat Hack, Full-time

Nov 1 2024 - Present

Penetration Tester

- Performed web application penetration testing using OWASP framework and CVSS Score for the assessment.
- Used to be part of incident response and malware analysis projects.
- Used to research to reproduce 0-day exploits proof of concept.

BUGCROWD PLATFORM, Remote

Present

Security Researcher

Freelance Security Researcher at BUGCROWD Platform

Used to report 3 valid vulnerabilities in Bug Bounty Programs and Vulnerability Disclosure Programs

Certifications

1. Offensive Security Certified Professional (OSCP)

Figure 1: https://www.credential.net/6c571871-4cbb-4bee-b996-e28476632b87#acc.DOuw915E

2. Certified Penetration Testing Specialist (CPTS)

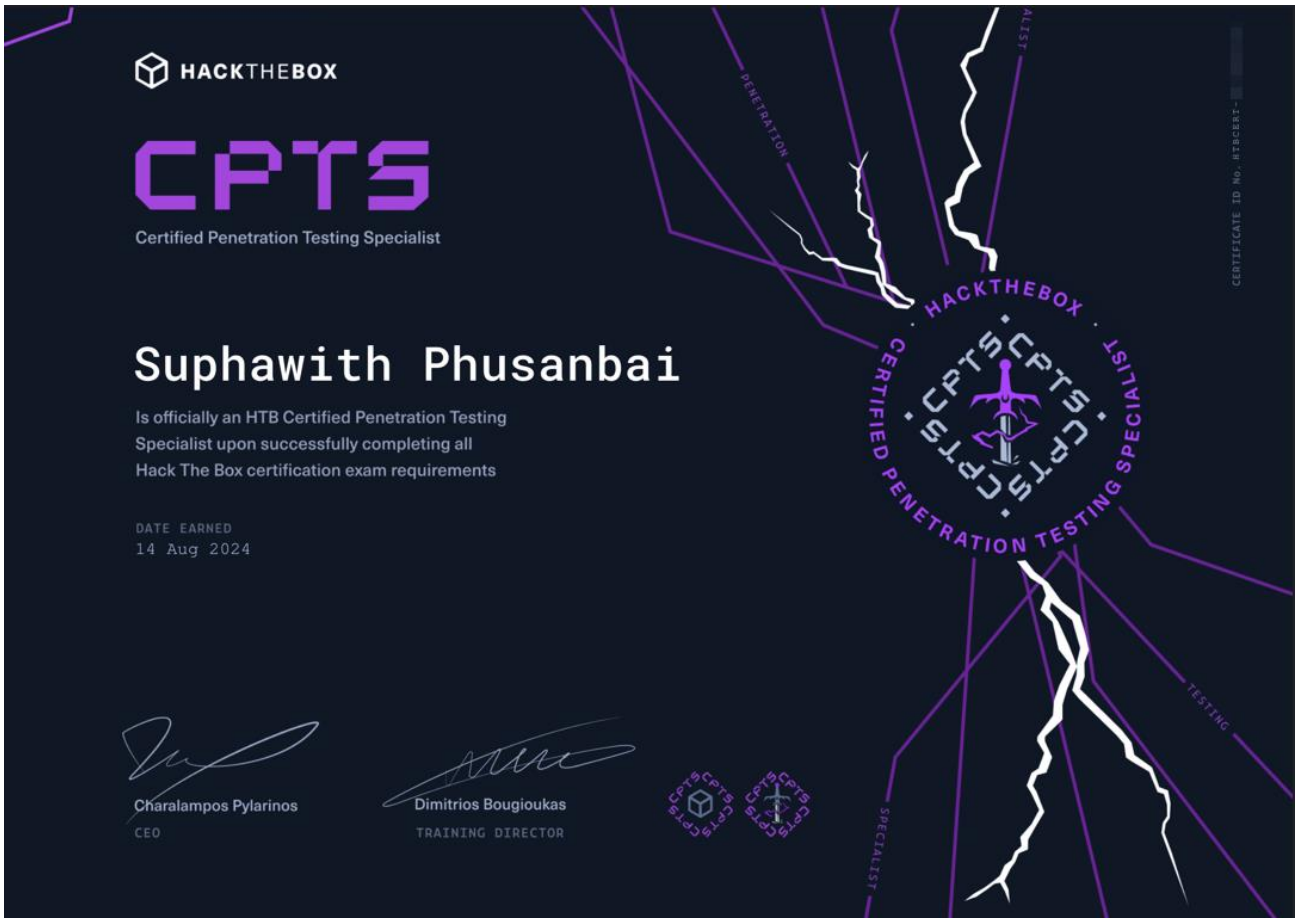

Figure 2: Certified Penetration Testing Specialist

3. Practical Network Penetration Tester (PNPT)

Figure 3: Practical Network Penetration Tester

4. eLearning Junior Penetration Tester Certificate (eJPT)

Figure 4: e-Learning Junior Penetration Tester

CVE Record

For detailed records of my contributions and findings, please visit my GitHub profile.

Currently, possessed 9 CVE in total.

1. Watcharr 1.43.0 Privilege Escalation (CVE-2024–48827)
2. Operately 0.1.0 Remote Code Execution (CVE-2024–48093)
3. Watcharr 1.43.0 Authentication Bypass (CVE-2024–50634)
4. PyMOL 2.5.0 Remote Code Execution (CVE-2024–50636)
5. UnoPIM 0.1.3 Stored Cross-Site Scripting (CVE-2024–50637)
6. UnoPIM 0.1.4 Stored Cross-Site Scripting (CVE-2024–52305)
7. Ever® Traduora 0.20.0 Authentication Bypass (CVE-2024–53484)
8. Dragon Age Origins 1.0.5 Local Privilege Escalation (CVE-2024-57266)
9. InnoShop 0.3.8 Stored Cross-Site Scripting (CVE-2024-57267)

Professional Achievements

For detailed records of my contributions and findings, please visit my GitHub profile.

[Electronic Arts] Dragon Age Origins - Local Privilege Escalation (CVE-2024-57266).

CVE-2024-57266

In Electronic Arts Dragon Age Origins 1.05, the DAUpdaterSVC service contains an unquoted service path vulnerability. This service is configured with insecure permissions, allowing users to modify the executable file path used by the service. The service runs with NT AUTHORITY\SYSTEM privileges, enabling attackers to escalate privileges by replacing or placing a malicious executable in the service path.

Women Thailand Cyber Top Talent CTF Creator 2024

[Web application] CTF Challenge Creator

Create web application CTF challenges using multiple web development frameworks such as Django, NodeJS and Java Spring Boot for 1st qualification event.

Bug Bounty Program

Sensitive Data Exposure Finding - Monash University (P4 vulnerability finding)

Identified a misconfiguration in a URL query parameter that allowed enumeration of valid usernames and email addresses, potentially exposing users to social engineering attacks.

Vulnerability Disclosure Program

Server Misconfiguration Finding – Anheuser-Busch InBev company (P5 vulnerability finding)

Found unrestricted under developing page on the production website which exposed to the public. This finding is informational but may affect the reputation of the company which possessed an impact in terms of business and reputation.

Open-source Project Contributions

Privilege Escalation - Watcharr v.1.43.0 (Streaming application)

Participated in security testing and discovered a critical vulnerability which affected version 1.43.0 and below.

- The issue and mitigation can be reviewed here
- The vulnerability is patched in later version v1.44.0
- The vulnerability was found in design flaw where it allows attackers to crafted JWT token to escalate privilege.

Remote Command Execution via Arbitary File Upload - Operately v.0.1.0 (The Open-Source Startup Operating System)

Participated in security assessment

- **Remote Command Execution via File Upload** – The file upload function doesn't validate the file extension, allowing any privileged user to upload any malicious file through the API. To trigger the vulnerability an employee needs to execute the malicious file to success the attack.