|  |  |
| --- | --- |
| Suphawith PhusanbaiAssumption UniversityBachelor of Information TechnologyCyber Security Consultant | **Email**: [suprawitch123@gmail.com](mailto:suprawitch123@gmail.com)**LinkedIn:** [Suphawith P.](https://www.linkedin.com/in/suphawith-phusanbai-39304628b/) **GitHub:** [Yamerooo123](https://hackerone.com/resurrect20?type=user)**HackeOne:** [Suphawith P](https://bugcrowd.com/SuphawithPhusanbai)**.****Phone number**: (+66) 92 496 5301Samut Prakan, Bangbo 10560 |

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

#### **PwC Thailand, Full-time**

**April 1, 2025 – Present**

**Penetration Tester**

* Web Application Penetration Testing
* Mobile Application Penetration Testing
* Network Penetration Testing
* Wi-Fi Penetration Testing
* The first RCE finder in PwC Thailand

#### **Siam Thanat Hack, Full-time**

**Nov 1, 2024 – Feb 25, 2025**

**Penetration Tester**

* Web Application Penetration Testing
* Mobile Application Penetration Testing
* Malware Analysis
* Incident Response
* CTF Creator for Women Thailand Cyber Top Talent 2024

# Key Achievements

* **Authored a CVE (CVE-2024-57276)** for a Local Privilege Escalation vulnerability in Electronic Arts' *Dragon Age: Origins*, discovered through reverse engineering and analysis of the insecure DAUpdaterSVC Windows service.
* **Selected as a CTF Challenge Creator** for the inaugural Women Thailand Cyber Top Talent event, developing complex web application challenges using Django, Node.js, and Java Spring Boot to test competitor skills in secure coding and exploitation.
* **Discovered 2 valid vulnerabilities** in HackerOne vulnerability disclosure programs, contributing to the security of partner organizations. The link is provided in [here](https://hackerone.com/resurrect20?type=user).
* **Discovered 9 valid vulnerabilities** across various BugCrowd programs, demonstrating consistent proficiency in identifying security flaws in diverse applications. The link is provided in [here](https://bugcrowd.com/SuphawithPhusanbai).
* **Formally recognized by ThaiCERT** with a Letter of Appreciation for significant contributions to enhancing Thailand's national cybersecurity posture. The link is provided in [here](https://github.com/yamerooo123/ResearchNBugBountyEncyclopedia/blob/main/Contributions/LoA_ThaiCERT.jpg).
* **Authored an ExploitDB entry for CVE-2024-48827 (Watcharr 1.43.0)**, documenting a **JWT misconfiguration** that allowed privilege escalation via blank secret validation. The link is provided in [here](https://www.exploit-db.com/exploits/52130).

# CVE Record

For detailed records of my contributions to OSS projects and findings, please visit my [GitHub](https://github.com/yamerooo123) profile.

Currently, I possess 9 CVE in total.

* Dragon Age Origins 1.0.5 Local Privilege Escalation (CVE-2024-57276)
* Watcharr 1.43.0 Privilege Escalation (CVE-2024–48827)
* Operately 0.1.0 Remote Code Execution (CVE-2024–48093)
* Watcharr 1.43.0 Authentication Bypass (CVE-2024–50634)
* PyMOL 2.5.0 Remote Code Execution (CVE-2024–50636)
* UnoPIM 0.1.3 Stored Cross-Site Scripting (CVE-2024–50637)
* UnoPIM 0.1.4 Stored Cross-Site Scripting (CVE-2024–52305)
* Ever® Traduora 0.20.0 Authentication Bypass (CVE-2024–53484)
* InnoShop 0.3.8 Stored Cross-Site Scripting (CVE-2024-57277)

# Technical Blog

**GitBook blog:** <https://suphawith-phusanbai.gitbook.io/book-of-suphawith/>

* A repository of my security research, featuring in-depth write-ups on malware analysis, CVEs, and vulnerability discoveries.

# Certifications

1. Offensive Security Certified Professional (OSCP)



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

1. Certified Penetration Testing Specialist (CPTS)

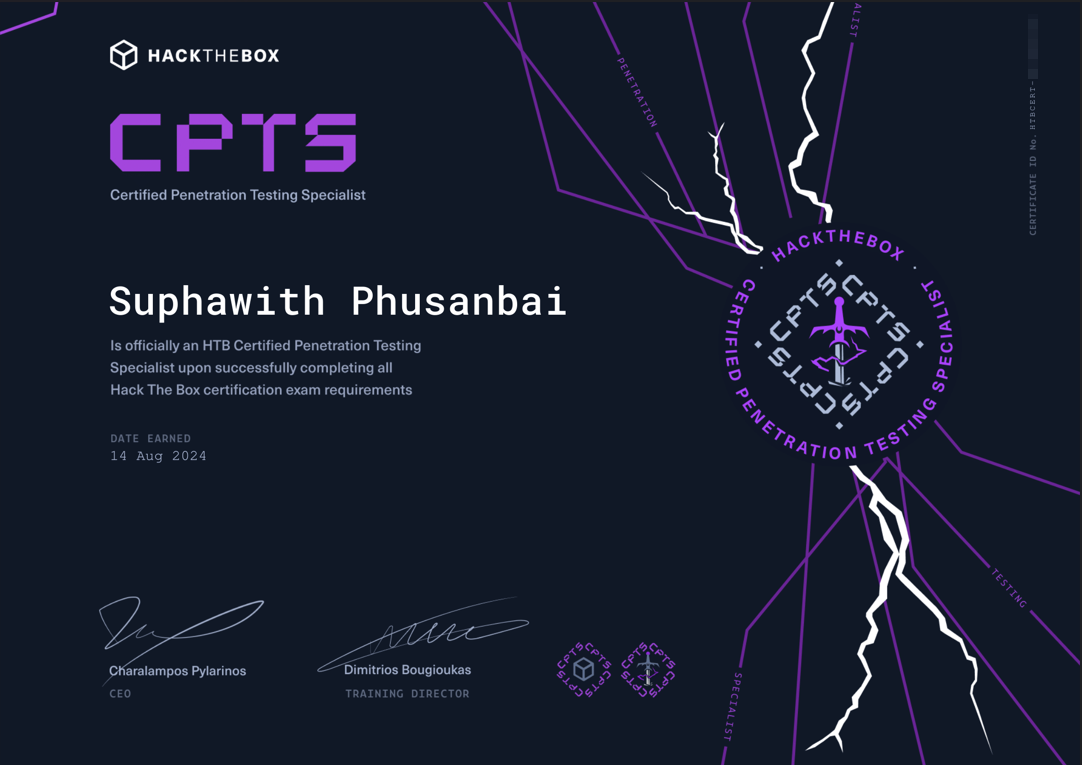


Figure 2: Certified Penetration Testing Specialist

1. Practical Network Penetration Tester (PNPT)



Figure 3: Practical Network Penetration Tester

1. eLearning Junior Penetration Tester Certificate (eJPT)

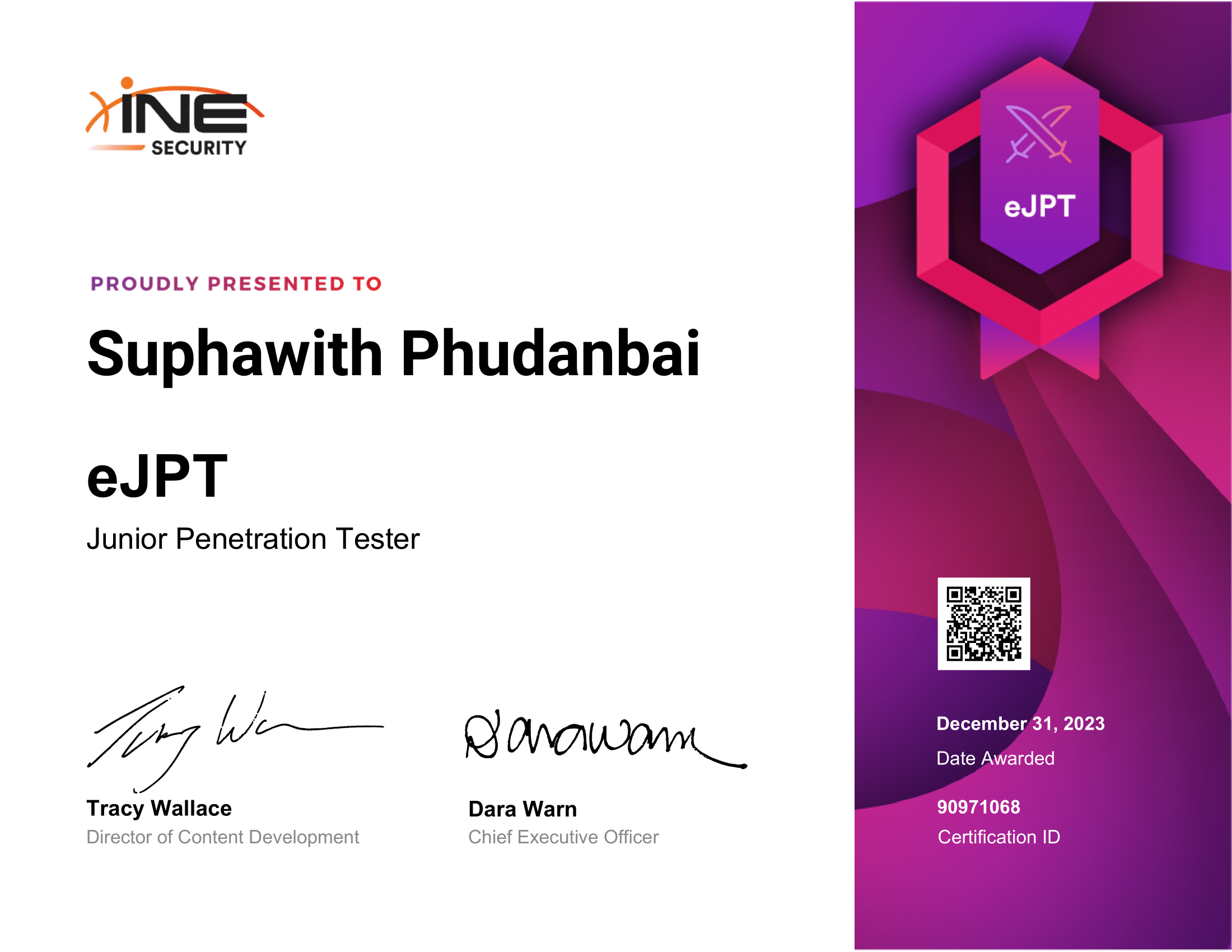


Figure 4: e-Learning Junior Penetration Tester

|  |  |
| --- | --- |
|  | |
|  |
|  | |
|  | |