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 Informatics and Data Science

A fresh graduate from Assumption University, I am currently pursuing a career in cybersecurity. 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 an ethical hacker who contributes to the greater good of the cybersecurity field.

Training and Certifications

- Offensive Security Certified Professional (OSCP)
- Certified Penetration Testing Specialist (CPTS)
- Practical Network Penetration Tester Certificate (PNPT)
- eLearning Junior Penetration Tester Certificate (eJPT)
- AWS Academy Graduate - AWS Academy Cloud Foundations

CVE Record

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

- CVE-2024-48093
- CVE-2024-48827
- CVE-2024-50634
- CVE-2024-50636
- CVE-2024-50637
- CVE-2024-53484

Professional Experience

Siam Thanat Hack, Hybrid

Present

Penetration Tester

- Worked as a professional penetration tester at Siam Thanat Hack company. I am specialized in web application penetration testing and network penetration testing.

BUGCROWD PLATFORM, Remote

Present

Security Researcher

Freelance Security Researcher at BUGCROWD Platform

- Submitted and reported vulnerabilities in both Bug Bounty and Vulnerability Disclosure Programs, including successful identification of P4 and P5 level vulnerabilities.

SCIENCE IN EP CLASSROOM AND แบบฝึกหัดการอ่านออกเสียงภาษาอังกฤษ

Facebook Pages, Samut Prakan Bang Bo

Present

Website Administrator

A website administrator at LearnSciAtHome

- Regularly post and update contents
- Secure the website by ensuring plugins are up-to-date, creating a security configuration to disallow users for specific pages, implementing firewall and 2FA using security plugins and code snippets, scanning website with NESSUS and WPScan.

Professional Achievements

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

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 Contribution

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 File Upload and No Rate Limitation Vulnerabilities - Operately v.0.1.0 (The Open-Source Startup Operating System)

Participated in software testing as an alpha tester

- **No Rate Limitation** – Users can create an unlimited number of channels with the same name, potentially leading to denial of service."
- **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.

Practical Projects

For detailed records of my contributions and findings, please visit my GitHub profile. If you need to see the live website, I would gladly share it for showcase.

Full stack e-Commerce web application - University Graduation Project

Using Django framework with the combination of Bootstrap 5 and JavaScript. The web site also integrated with a recommender system using Cosine Similarity for the model development.

Responsibilities:

-Frontend development: Created UX/UI and designed page layout using Bootstrap 5 and jQuery

-Backend development: Created necessary website functions using Django framework

-Database configuration: Created and designed database architecture using MySQL

-Deployment: Deployed the website from GitHub repository on Heroku.

Political Fake News Detector – Research Project

The project aims to make an improvement on the existing project by using LSTM model and experimenting with different model configurations to find the model that has the highest accuracy.

Responsibilities:

-Data Preprocessing: Ensured datasets are cleaned by removing rows with empty and null values, removing stop-words, removing punctuation, tokenization and lemmatization.

-Baseline Model Training: Trained baseline model for experimenting with prepared datasets which will be used in developing a better model.

Hobbies

- Practice source code reviewing on open-source projects available in GitHub
- Pursue more advanced knowledges by completing more certifications offered by OffSec, INE, Hack The Box, TryHackMe, PortSwigger, Hacktricks etc.
- Participate in webinars organized by security researchers to absorb and understand their mindset and open myself to new perspectives.