

Waris Damkham

Bangkok, Thailand | waris.dam@outlook.com | +66-63-954-4447

waris-damkham.netlify.app | linkedin.com/in/waris-damkham | github.com/Waariss

About Me

Offensive Security Engineer and AI Security Researcher with hands-on experience in web, mobile, API, and network penetration testing, red team engagements, and security automation. **Black Hat Asia 2026 Arsenal Speaker** and **15× CVE contributor**. I deliver offensive assessments and build automation to improve response efficiency and executive visibility. My research spans AI-driven diagnostics, OAuth 2.0 vulnerabilities in Android applications, and applied identity and access security, with work presented at IEEE QRS, InCIT, and TENCON. Holder of 20+ industry certifications, including OSCP, PNPT, CPTS, CRTP, eWPTX, and BSCP.

Skills

Programming Languages: JavaScript, Python, Java, Bash	Cloud & Infrastructure: AWS, Azure, GCP, Huawei Cloud
Web Development: HTML, CSS, React, Node.js, Flask	Artificial Intelligence: Machine & Deep Learning
DevOps & CI/CD: Git, Docker, GitHub Actions, Jenkins	Languages: Thai (Native), English (Intermediate)
Security Tools: Kali Linux, Burp Suite, Nmap, Nessus, Wireshark, Metasploit, MobSF, OpenVAS, NamicSoft, SysReptor	

Experience

Offensive Security Engineer, KASIKORN Business-Technology Group – Bangkok, Thailand Nov 2024 – Present

- Delivered 38 penetration tests across annual assessments and major-change projects, and contributed as a core member of advanced Red Team engagements, translating findings into remediation actions.
- Produced 30+ executive and technical summaries and delivered 24 security briefings (18 Penetration Testing: 15 Thai / 3 English; 6 Red Team), aligning stakeholders on risk impact, priorities, and action plans.
- Led AI pentesting and AI security workstreams across readiness, research, and automation tooling, using OWASP LLM Top 10 to translate emerging risks into actionable guidance and presentation-ready materials.
- Led PwnDoc-ng implementation, achieving 50% reduction in operational effort and 25% reduction in review workload, and drove reporting standard upgrades through 2025 report redesign and issue write-up rewrites aligned with modern security standards.
- Built security automation to scale recurring operations, including monthly subsidiary reporting extraction (34.7% manual-effort reduction), email-driven Critical CVE follow-up ($\geq 50\%$ time reduction and $\geq 80\%$ mitigation artifact tracking), and BitSight WAS daily scan automation supporting a BitSight rating of 800.

Cybersecurity Consultant, ALPHASEC – Bangkok, Thailand Jun 2024 – Oct 2024

- Performed penetration testing across Web, Mobile, and Infrastructure platforms for 16 projects, delivering remediation-focused reports aligned with OWASP and industry standards to strengthen clients' security posture.

Cybersecurity Consultant Intern, KPMG – Bangkok, Thailand Jan 2024 – Apr 2024

- Supported 3 security projects: Penetration Testing, AppSec reviews, and Vulnerability Assessments.
- Applied OWASP & Nessus to assess internal systems and secure web apps by identifying vulnerabilities.

Research Intern, Ritsumeikan University – Shiga, Japan May 2023 – July 2023

Project Title: Detecting Vulnerable OAuth 2.0 Implementations in Android Applications

- Analyzed OAuth 2.0 vulnerabilities in Android apps, emphasizing CSRF attacks, and developed an app to examine OAuth 2.0 protocols, proposing enhancements for improved security.
- Presented at the 23rd IEEE International Conference on Software Quality, Reliability, and Security (QRS 2023).

Research Intern, National Central University – Taoyuan, Taiwan June 2022 – July 2022

Project Title: Automated COVID-19 Screening Framework Using a Deep CNN with Medical Chest X-Ray

- Developed an AI-based COVID-19 diagnostic system using chest X-rays, applying transfer learning for improved accuracy and Grad-CAM for interpretability, supporting rapid clinical decision-making.
- Presented at the 6th International Conference on Information Technology (InCIT 2022).

Education

Mahidol University, Thailand Aug 2020 – May 2024
Bachelor of Science (B.S.): Information and Communication Technology (International Program)

Publications

- Practical Mobile Based Services for Identification of Chicken Diseases from Fecal Images** Mar 2025
Piyanuch S., Ananta S., **Waris D.**, Pattanan K., Kanokpitch S.
10.1109/TENCON61640.2024.10902790
- Detecting Vulnerable OAuth 2.0 Implementations in Android Applications** Feb 2024
Waris D., Shingo K., Songpon T., Tetsutaro U.
10.1109/QRS-C60940.2023.00024
- Automated COVID-19 Screening Framework Using Deep CNN With Chest X-Ray Medical Images** Mar 2023
Waris D., Tipajin T., Akara S., Jidapa K., Pattanasak M., Jja-Ching W.
10.1109/InCIT56086.2022.10067528

Projects

- Oblivion Token: M365 Conditional Access Policy Bypass OST (Offensive Tooling)**
- Built an offensive research utility for practical, repeatable, and scriptable Microsoft 365 Conditional Access (CAP) policy-bypass testing, systematizing token-centric workflows to exercise edge cases and validate enforcement gaps across Microsoft first-party applications.
 - Selected for Black Hat Asia 2026 Arsenal (Cloud Security Track).
- CHICKENME: Classification Of Chicken Diseases From Fecal Images Via Line Office Account**
- Developed a mobile-based service for poultry farmers to diagnose common chicken diseases from fecal images via a Line account, achieving 86.49% segmentation precision and 95.93% classification accuracy.
 - Presented at IEEE Region 10 Conference 2024 (TENCON 2024).

Selected Certifications

- Cyber Security 101 (SEC1) Feb 2026
- OffSec Certified Professional+ (OSCP+) Oct 2025 - Oct 2028
- OffSec Certified Professional (OSCP) Oct 2025
- Hack The Box Certified Junior Cybersecurity Associate (CJCA) Sep 2025
- Junior Penetration Tester (PT1) July 2025
- Practical SOC Analyst Associate (PSAA) July 2025
- Cloud Digital Leader Certification (CDL) June 2025 - June 2028
- API Security Certified Professional (ASCP) May 2025
- APIsec Certified Practitioner (ACP) Apr 2025
- Web Application Penetration Tester eXtreme (eWPTX) Mar 2025 - Mar 2028
- Practical Network Penetration Tester (PNPT) Feb 2025
- Hack The Box Certified Penetration Testing Specialist (CPTS) Jan 2025
- Certified Red Team Professional (CRTP) Dec 2024 - Dec 2027
- Burp Suite Certified Practitioner (BSCP) Dec 2024 - Dec 2030
- Practical Mobile Pentest Associate (PMPA) Nov 2024
- Certified AI/ML Pentester (C-AI/MLPen) Nov 2024
- GitHub Foundations (GHF) Sep 2024 - Sep 2027
- Hack The Box Certified Web Exploitation Specialist (CWES) Aug 2024