Seungpyo Hong

Offensive Security Researcher

newbiepwner@kakao.com | Seoul, South Korea | phantomn.github.io | phantomn | ph4nt0m

Summary

NATO CCDCOE Locked Shields 2025 DFIR CTF #1 · 21 CVEs (OS Kernel 16 + IoT 5). Offensive Security Researcher with 6 years across financial Web/App pentesting and OT/ICS security. Built an AI Orchestration Framework (IDA · Burp Suite · Frida · CodeQL via MCP + A2A) that auto-identifies Low–Medium vulnerabilities on live targets.

Experience

CoreSecurity, ICS Security Researcher (Senior) — Seoul, South Korea
June 2021 – present
5 years 1 month

- IEC 62443-4-2 Threat Modeling & pentesting — contributed to LS ELECTRIC Achilles Level 2 certification
- FDA eSTAR security consulting & medical device penetration testing
- Smart building IoT vulnerability detection tool development & field deployment
- ELECCON (KEPCO cyber warfare exercise) 2021–2024: 4-year operations & challenge development
- **NATO CCDCOE Locked Shields 2025** (Korea-Canada DFIR blue team) — overall 6th, **DFIR CTF 1st place**
- APEX CTF 2025 DFIR challenge development (May–Sep 2025)
- **NATO CCDCOE Locked Shields 2026** (Korea-Hungary Special System blue team) — overall 9th

A3 Security, Web/App Pentester — Seoul, South Korea
June 2020 – June 2021
1 year 1 month

- 12 financial/public-sector electronic finance infrastructure pentests — avg. 1–2 high-risk findings per site
- Non-standard system reviews: KT GiGA Genie AI speaker, NH RPA, IoT thermal sensor
- ISMS/ISO 27001 certification consulting (Coway)
- Clients: Cham Savings Bank, Acuon Capital, SBI Savings Bank, Hyundai HKMC

Education

BS **Kongju National University**, Computer Science — Chungnam, South Korea
Feb 2012 – Feb 2020

Cheonan Commercial High School, Information Processing — Chungnam, South Korea
Mar 2009 – Feb 2012

Vulnerability Research

OS Kernel CVEs (16) — Best of the Best 8th Cohort: Designed & implemented a custom File System Fuzzer; derived 16 CVEs (0-day + 1-day) from Linux kernel. Presented at **CodeBlue 2019** (Tokyo) & **Hack In The Box 2019** (Amsterdam). CVE-2019-18885, 19036, 19037, 19039, 19318, 19319, 19377, 19378, 19447, 19448, 19449, 19813, 19814, 19815, 19816, 19927

IoT CVEs (5) — Independent Research: Embedded/IoT device vulnerability analysis. CVE-2024-33788 (CVSS 8.0 HIGH), CVE-2024-33789 (CVSS 9.8 CRITICAL), CVE-2024-33791 (CVSS 4.6 MEDIUM), CVE-2024-33792 (CVSS 9.8 CRITICAL), CVE-2024-33793 (CVSS 5.3 MEDIUM)

Projects

AI Orchestration Framework for Security 2024 – present

- Orchestrates IDA Pro, Burp Suite, Frida, CodeQL via MCP + A2A protocol
- LLM-driven pipeline auto-identifies Low–Medium vulnerabilities on live pentest targets
- RAG pipeline (n8n · pgvector) indexes IEC 62443, ISO 27001 standards for contextual lookup

ELECCON — KEPCO Cyber Warfare Exercise 2021 – 2024

- 4-year consecutive operation of Korea's premier OT/ICS red-vs-blue exercise
- SCADA/PLC-based attack scenario design and blue team evaluation metrics

File System Fuzzer Jan 2019

- Custom fuzzer design & implementation → 16 Linux kernel CVEs
- Conference talks: CodeBlue 2019 (Tokyo), Hack In The Box 2019 (Amsterdam)

Skills

Offensive Security: Web/App Pentesting, OT/ICS Pentesting, Red Teaming, Exploit Development, Vulnerability Research, Fuzzing

OT / ICS: IEC 62443-4-2, FDA 510(k)/eSTAR, Achilles Level 2, Industrial Protocol Analysis (Modbus, DNP3, PROFINET)

AI Security Automation: MCP + A2A orchestration, n8n, LangGraph, VoltAgent, RAG (pgvector), Claude Code

Tools: IDA Pro, Burp Suite, Frida, CodeQL, pwndbg, Wireshark, Metasploit, Nmap

Languages & Certifications: Korean (Native), English (Conversational) · Linux Master 2nd Grade · Network Administrator 2nd Grade