홍승표

Offensive Security Researcher

newbiepwner@kakao.com 서울특별시 phantomn.github.io phantomn ph4nt0m

요약

NATO CCDCOE Locked Shields 2025 DFIR CTF 1위 · CVE 21건 (OS Kernel 16 + IoT 5). 금융권 Web/App 모의해킹 1년, OT/ICS 보안 약 5년 경력의 Offensive Security Researcher. IDA · Burp Suite · Frida · CodeQL을 MCP + A2A로 연결한 AI Orchestration Framework를 구현해 실제 점검 대상에서 Low~Medium 취약점을 자동 식별.

경력

코어시큐리티 (CoreSecurity), ICS 보안연구팀 주임 연구원 — 서울, 6월 2021 – 현재

- IEC 62443-4-2 기반 Threat Modeling 및 모의해킹 — LS ELECTRIC 자동화기기 Achilles Level 2 인증 취득 기여
- FDA eSTAR 보안 컨설팅 및 의료기기 모의해킹
- 스마트빌딩 IoT 취약점 탐지 기술 개발 및 실증, IoT/CCTV 침해사고 조사 도구 개발
- 한국전력 실전형 사이버 공방 훈련(ELECCON) 2021~2024 4회 운영 및 문제 개발
- **NATO CCDCOE Locked Shields 2025** 한국-캐나다 연합 DFIR 블루팀 — 훈련 종합 6위, **DFIR CTF 1위**
- APEX CTF 2025 DFIR 문제 개발 참여 (2025.05 ~ 2025.09)
- **NATO CCDCOE Locked Shields 2026** 한국-헝가리 연합 Special System 블루팀 — 훈련 종합 9위

A3 Security, 보안기술팀 사원 — 서울, 6월 2020 – 6월 2021

- 금융권 및 공공기관 전자금융기반시설 모의해킹 12개 사이트 — 고위험 취약점 평균 1~2건/사이트 식별
- KT 기가지니 AI 스피커, 농협중앙회 RPA, IoT 열감지 장비 등 비정형 시스템 보안성 검토
- ISMS/ISO 27001 인증 취득 지원 컨설팅 (코웨이)
- 참저축은행, 애큐온캐피탈, SBI저축은행, 현대자동차 HKMC 등 모의해킹

학력

학사 **공주대학교 (Kongju National University)**, 컴퓨터공학부 — 충남, 2월 2012 – 2월 2020

천안상업고등학교, 정보처리과 — 충남, 3월 2009 – 2월 2012

취약점 연구

OS Kernel CVE 16건 — Best of the Best 8기: 커스텀 File System Fuzzer 설계·구현으로 Linux Kernel CVE 16건 (0-day 포함) 도출. **CodeBlue 2019** (도쿄) · **Hack In The Box 2019** (암스테르담) 발표. CVE-2019-18885, 19036, 19037, 19039, 19318, 19319, 19377, 19378, 19447, 19448, 19449, 19813, 19814, 19815, 19816, 19927

IoT CVE 5건 — 개인 연구: 임베디드/IoT 장비 취약점 분석. 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)

프로젝트

AI Orchestration Framework for Security — 2024 – 현재

- IDA Pro, Burp Suite, Frida, CodeQL을 MCP + A2A 프로토콜로 연결한 취약점 분석 자동화 파이프라인
- LLM 기반 오케스트레이션으로 실제 점검 대상에서 Low~Medium 취약점 자동 식별
- n8n · pgvector RAG 파이프라인으로 IEC 62443, ISO 27001 표준 문서 검색 적용

ELECCON — 한국전력 사이버 공방 훈련 2021 – 2024

- 국내 최대 OT/ICS 실전형 사이버 공방 훈련 4년 연속 운영
- SCADA/PLC 기반 공격 시나리오 설계 및 방어팀 평가 지표 수립

File System Fuzzer (BoB 8기) 1월 2019

- 커스텀 Fuzzer 설계·구현 → Linux Kernel CVE 16건 도출
- CodeBlue 2019 (도쿄), Hack In The Box 2019 (암스테르담) 발표

기술

Offensive Security: Web/App 모의해킹, OT/ICS 모의해킹, Red Teaming, 익스플로잇 개발, 취약점 연구, Fuzzing

OT / ICS: IEC 62443-4-2, FDA 510(k)/eSTAR, Achilles Level 2, 산업용 프로토콜 분석 (Modbus, DNP3, PROFINET)

AI 보안 자동화: MCP + A2A 오케스트레이션, n8n, LangGraph, VoltAgent, RAG (pgvector), Claude Code

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

자격 및 언어: 한국어 (모국어), 영어 (일상 회화) · 리눅스 마스터 2급 · 네트워크 관리사 2급