

Affiliations

EDUCATION & COMMUNITIES

2023–Present **Korea University · AI Cybersecurity** · Integrated B.S.-M.S. Program · Privacy & Security Convergence

Present **Science & Technology Specialist Officer Program Candidate** · Cohort 3

SeeCure Lab · KUality · Knights of the SPACE · Rubiyalab · Security Research & CTF Communities

Publication

RESEARCH PAPER

2026 **Analysis and Validation of Access Control Vulnerabilities in MCP Management APIs: A Dify MCP Case Study**
Jun-Yong Lee, Hyeongyu Lee, Nurihan Kim (co-first authors); Jungmin Kang · CISC-W 2026
Analyzed missing role checks in Dify MCP management APIs and compared API responses and stored state between the original and role-protected implementations.

Awards

RECOGNITION

2025 **Encouragement Prize** · Privacy & Security Policy Idea Contest · Korea University

2024 **Excellence Award · KISIA Chairman's Award** · AI Security Essay Contest · KISIA

2024 **Minister of Science and ICT Award · Top Graduate** · KISIA AI Security Program · Top overall evaluation

2024 **Grand Prize (1st) · Minister of Science and ICT Award** · KISIA Hackathon · Malicious-URL detection extension

2024 **Top 20 · Minister of Science and ICT Certificate** · WhiteHat School · Cohort 1 · Top 20 of 320

CTF Finals

COMPETITION RESULTS

- 2026 · DEF CON 34 CTF · Finalist · Team SSS
- 2025 · WhiteHat Contest · Finalist · 5th in the qualifier · Team KUality
- 2025 · Black Hat MEA CTF · Finalist · 41st in the qualifier · Team PPU-AENG Overflow

CTF Challenge Authoring

OPERATIONS & REVIEW

- 2026 · KCTF 2026 (KUality) · Challenge authoring · Liberation Signal 1–3
- 2026 · CSKWS Joint Seminar CTF · Event operations and challenge authoring · Ghost Display, Black Cache
- 2026 · HACKTHEON Sejong Student Cybersecurity Festival · CTF operations and challenge authoring
- Aug 2026 · Information Security Fundamentals Program · Introductory instruction and Mini CTF operations
- Feb 2026 · INCOGNITO FESTIVAL CTF · Event operations and qualifier/final challenge authoring · Project Incoherence
- Feb 2026 · 5th Hanyang Hacking Defense Contest, HCTF with HSPACE · Challenge authoring
- Aug 2025 · SSD CTF · Challenge authoring

Projects

SECURITY ENGINEERING

2026–Present	Adversarial Attacks and Incident Traceability for AI Systems · Participating Researcher · Ongoing
2026–Present	Security Analysis of Remote Device-Management Protocols (TR-069) II · Participating Researcher · Ongoing
2026–Present	AI-Based Future-Threat Scenario Prediction from Threat-Actor Campaigns and MITRE D3FEND-Based Countermeasure Enhancement · Participating Researcher · Ongoing
2026	Tool/MCP Call Gateway for Securing AI IDEs Project Semester · Vulnerability Research Reproduced shell-command execution from untrusted Cursor project Hook settings, prepared a PoC and disclosure, and designed a Verify–Restrict–Log gateway.
Jun–Jul 2025	HSPACE Penetration-Testing Curriculum Content Developer · Knights of the SPACE Built a mock e-commerce service and tiered attack scenarios for a repeatable beginner lab.
Jun–Aug 2025	CTF Platform Based on Real Bug-Bounty Cases Backend Developer · FinderGap Built the backend for a platform that turns bug-bounty cases into reproducible CTF challenges.
2024	Automated WordPress Plugin Vulnerability Analysis Korea University AI Cybersecurity Symposium Co-developed an automated plugin scanner, implemented its SQL injection module, and presented the work at a departmental symposium.
2024	AI-Powered Malicious URL Classifier Frontend · Data Preprocessing · KISIA AI Security Network Cleaned phishing-URL data, supported model training, and built a malicious-URL detection extension frontend.

Vulnerability Disclosure

ZDI / CVE

2026	ZDI-CAN-30890 · Anysphere · Pending public disclosure · Co-discovered with Nurihan Kim (HanTul) · ZDI-listed CVSS 7.8
2024	CVE-2024-11950 · XnSoft XnView Classic RWZ Integer Underflow Independent Vulnerability Research · ZDI-24-1640 · High Severity Discovered and disclosed an RWZ parser integer underflow and memory corruption. ZDI published the issue as CVE-2024-11950 with remote-code-execution impact.

Other

ADDITIONAL EXPERIENCE

Mar–Aug 2025	Teaching Assistant · KITRI WhiteHat School Cohort 3 · Labs, presentations, and feedback
2024–Present	KnockOn Q&A Mentor · Web security and vulnerability-analysis practice
2024	Information Processing Craftsman · National Technical Qualification Languages · Korean (native) · English (reading/writing) · Chinese (HSK 4, HSKK Elementary) · Languages

Vulnerability Research

CTF Engineering

Security Education

Python · Docker · Git