

소속

AFFILIATIONS

2023-현재 고려대학교 인공지능사이버보안학과 · 개인정보보호융합전공 · 학·석사 연계과정생

현재 과학기술전문사관 제3기 후보생 · Science & Technology Specialist Officer Program

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

논문

PUBLICATION

2026 MCP 관리 API의 접근통제 취약점 분석 및 검증연구: Dify MCP 사례
이준용 · 이현규 · 김누리한(공동 제1저자), 강정민 · 한국정보보호학회 동계학술대회(CISC-W 2026)
Dify MCP 관리 API의 역할 검증 누락을 분석하고, 원본과 역할 검증을 추가한 환경의 API 응답 및 저장 데이터 변화를 비교·검증했습니다.

수상

AWARDS

2025 장려상 · 제2회 개인정보보호·보안 정책 아이디어 공모전 · 고려대학교 정보보호대학원

2024 우수상 · 한국정보보호산업협회장상 · AI보안 기술개발 참여수기 공모전 · 한국정보보호산업협회

2024 과학기술정보통신부 장관상 · 최우수 수료생 · KISIA AI보안 기술개발 교육과정 · 교육·실습·프로젝트 종합 평가

2024 1등 · 과학기술정보통신부 장관상 · KISIA 정보보호 개발자 해커톤 · 크롬 확장 프로그램 기반 악성 URL 탐지 서비스

2024 Top 20 · 과학기술정보통신부 장관 인증서 · 화이트햇 스쿨 1기 · 320명 중 상위 20인

CTF 본선 참가

CTF FINALS

- 2026 · DEF CON 34 CTF · 본선 진출 · Team SSS
- 2025 · 화이트햇콘테스트 · 본선 진출 · 예선 5위 · Team KUality
- 2025 · Black Hat MEA CTF · 본선 진출 · 예선 41위 · Team PPU-AENG Overflow

CTF 출제

CHALLENGE AUTHORING & OPERATIONS

- 2026 · KCTF 2026 (KUality) · 문제 출제 · Liberation Signal 1-3
- 2026 · CSKWS 연합 세미나 CTF · 대회 운영 및 문제 출제 · Ghost Display, Black Cache
- 2026 · 핵테온 세종 초·중·고 사이버보안 한마당 · CTF 운영 및 문제 출제
- 2026.08 · 정보보호 실무기초 교육과정 · 기초 과정 교육 및 Mini CTF 운영
- 2026.02 · INC0GNITO FESTIVAL CTF · 대회 운영 및 예선·본선 문제 출제 · Project Incoherence
- 2026.02 · 제5회 한양 해킹방어대회 HCTF with HSPACE · 문제 출제
- 2025.08 · SSD CTF · 문제 출제

2026-현재	AI 시스템 대상 적대적 공격·사고 추적 기술 연구 · 참여 연구원 · 수행 중
2026-현재	원격 장비관리 통신 프로토콜 보안성 분석(TR-069) II · 참여 연구원 · 수행 중
2026-현재	Threat Actor 캠페인 기반 미래 위협 시나리오 예측 AI 기술 및 MITRE D3FEND 기반 대응 기법 고도화 · 참여 연구원 · 수행 중
2026	AI IDE 보안 강화를 위한 Tool/MCP 호출 게이트웨이 기반 방어 방법론 프로젝트 학기제 · Vulnerability Research Cursor IDE의 비신뢰 프로젝트 Hook 설정이 워크스페이스 신뢰 검증과 샌드박스 없이 셸 명령을 실행하는 문제를 분석하고 재현했습니다. 재현 가능한 PoC와 책임 있는 제보 문서를 정리하고, Verify·Restrict·Log 게이트웨이 관점의 방어 방법론을 설계했습니다.
2025.06-07	HSPACE 침투 테스트 교육 콘텐츠 Content Developer · Knights of the SPACE 입문자가 단계적으로 공격 흐름을 이해할 수 있도록 가상 쇼핑몰과 난이도별 침투 테스트 시나리오를 구성하고, 반복 실행 가능한 실습 환경을 제작했습니다.
2025.06-08	실전 버그바운티 사례 기반 CTF 플랫폼 Backend Developer · FinderGap 실제 버그바운티 사례를 재현 가능한 CTF 문제로 전환하는 교육 플랫폼의 백엔드를 구현했습니다.
2024	WordPress 플러그인 취약점 분석 자동화 고려대학교 인공지능사이버보안학과 학술제 WordPress 플러그인을 대상으로 한 자동 취약점 탐지 도구를 공동 개발하고 SQL Injection 분석 모듈을 담당했습니다. 분석 결과와 구현 내용을 교내 학술제에서 발표했습니다.
2024	AI 기반 악성 URL 분류기 Frontend · Data Preprocessing · KISIA AI Security Network 피싱 URL 데이터 정제와 모델 학습 파이프라인 구축에 참여하고, 크롬 확장 프로그램 형태의 악성 URL 탐지 서비스 프론트엔드를 개발했습니다.

취약점 제보

2026	ZDI-CAN-30890 · AnySphere · 공개 예정 · 김누리한(HanTul)과 공동 발견 · ZDI 표기 CVSS 7.8
2024	CVE-2024-11950 · XnSoft XnView Classic RWZ 정수 언더플로우 Independent Vulnerability Research · ZDI-24-1640 · High Severity 조작된 RWZ 파일 처리 과정의 정수 언더플로우와 메모리 손상을 분석·재현하고 책임 있게 보고했습니다. 해당 취약점은 원격 코드 실행 영향으로 ZDI 권고문과 CVE로 공개되었습니다.

기타

2025.03-08	KITRI 화이트햇 스쿨 3기 조교 · 실습·중간발표 운영 및 학습자 피드백 지원
2024.06-현재	KnockOn Q&A 멘토 · 웹 보안·취약점 분석 학습 지원
2024	정보처리기사 · 국가기술자격 언어 · 한국어(모국어) · 영어(읽기·쓰기) · 중국어(HSK 4급, HSKK 초급) · Languages

Vulnerability Research

CTF Engineering

Security Education

Python · Docker · Git