# 이현규 (Hyeongyu Lee) Portfolio

## 📋 Profile

**AI & Security Research**


- **Email**: ktechq2003@korea.ac.kr / gtechq2003@gmail.com
- **Phone**: 010-3838-6382
- **Birth**: 2003.04.30
- **Website**: https://hy30nq.com
- **Blog**: hyeonql.tistory.com
- **GitHub**: github.com/hy30nq


## 🎓 Education

- **2023 - Present**: 고려대학교 인공지능사이버보안학과
- **2024 - Present**: 고려대학교 개인정보보호융합전공

## 🏢 Affiliations

- **Rubiyalab** (https://rubiyalab.team/) - 해킹팀, 보안 스터디 진행
- **Knights of the SPACE** (https://hspace.io/) - CTF 문제 출제 및 대회 운영, 기술 블로그 작성, 세미나 진행 및 발표
- **KUality** (https://kuality.kr/) - 고려대학교 인공지능사이버보안학과 소속 동아리

## 🏆 Awards & Achievements

### 2025

- **장려상** - 제2회 개인정보보호/보안 정책 아이디어 공모전 (2025.02.07)
  - 수상작: 개인정보 익명화 인증 제도 도입을 통한 데이터 활용과 개인정보보호의 균형 정책 제안

## 2024

- **최우수 수료생 (과학기술정보통신부 장관상)** - AI보안 기술개발 교육과정 (2024.12.20)
- **최우수상 (과학기술정보통신부 장관상)** - 제2회 KISIA 정보보호 개발자 해커톤 (2024.08.21)
  - 관련 기사: https://www.boannews.com/media/view.asp?idx=132213&direct=mobile
- **TOP 20 (과학기술정보통신부 장관 인증서)** - KITRI 화이트햇 스쿨 (Pre-BoB) 1기 (2024.03.22)
  - 공식 발표: https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&bbsSeqNo=94&nttSeqNo=3184227

# 🎤 Presentations

- **2024 정보보호 인재양성 교육사업 성과교류회** 발표 (2024)

# 📅 Experience & Activities

## 2025

- **한국인터넷진흥원(KISA)** - 버그헌팅 실습 훈련 초급과정 (2025.03.04 - 2025.03.15)
- **화이트햇 스쿨 3기 조교** - 1단계 멘토링 및 교육생 지원 (2025.03 - 2025.05)
- **고려대학교** - 싱가포르 해외 연수 (2025.01.12 - 2025.01.16)

## 2024

- **구름톤 유니브 3기** - kakao, goorm (2024.09 - 2025.01)
- **블록체인 누리단** - 과학기술정보통신부, KISA (2024.07 - 2024.12)
- **KnockOn Q&A 멘토** (2024.06 - Present)
- **개인정보 불법유통 대응 대학생 모니터링단** - 개인정보보호위원회, KISA (2024.07.22 - 2024.12.03)
- **중부정보보호지원센터** - 웹취약점 점검 실습 (2024.10.08)
- **한국정보보호산업협회 한국정보보호교육원** - 융합보안 인력양성 교육 (블록체인 기초) (2024.09.04 - 2024.09.06)
- **POC Security** - 29회 하계 해킹캠프 (2024.08.17 - 2024.08.18)
- **코멘토 진로부트캠프** - 현업 보안 담당자와 함께 정보보안, 개인정보 보호 실무체험하기 (2024.05.09 - 2024.06.30)

## 2023

- **국가과학기술인력개발원(KIRD)** - 사이버보안 하계 직무연계 교육과정(정보보호특성화대학) (2023.08.16 - 2023.08.18)
- **한국정보보호교육센터(KISEC)** - Start-Up K-Shield Jr. (2023.07.01 - 2023.07.31)

#  Security Vulnerabilities

## CVE-2024-11950

- **Title**: XnSoft XnView Classic RWZ File Parsing Integer Underflow Remote Code Execution Vulnerability
- **ID**: ZDI-24-1640
- **Impact**: Remote Code Execution
- **Description**: XnView Classic의 RWZ 파일 파싱 과정에서 발생하는 정수 언더플로우 취약점 발견 및 보고
- **참조**: https://www.zerodayinitiative.com/advisories/ZDI-24-1640/

#  Technical Skills

## Programming Languages

- **Proficient**: Python
- **Intermediate**: C/C++, JavaScript, HTML/CSS, PHP, SQL
- **Familiar**: Assembly, Java

## Security Tools

- **Web**: Burp Suite, OWASP ZAP, SQLMap, Dirb, Gobuster, Wfuzz
- **Binary**: IDA, GDB, x64dbg, WinDbg, OllyDbg
- **Network**: Wireshark, Nmap, Metasploit, Netcat, Masscan
- **Fuzzing**: WinAFL
- **Penetration Testing**: Kali Linux, BloodHound

## OS & Virtualization

- **Operating Systems**: Linux (Ubuntu, Kali), Windows, macOS
- **Virtualization**: VMware, VirtualBox, Docker

## Web Technologies & Cloud Infrastructure

- **Frontend Development**: HTML5/CSS3, JavaScript (ES6+), Vue.js, Bootstrap, Responsive Web Design
- **Backend Frameworks**: Python Flask, FastAPI, Node.js, Express.js, RESTful API Development
- **Database Management**: MySQL, SQLite, Database Design & Optimization
- **DevOps & Cloud**: Docker, Microsoft Azure, AWS (기초), CI/CD Pipeline, Git/GitHub
- **Web Security**: OWASP Top 10, Secure Coding Practices, Authentication & Authorization
- **Additional**: JSON/XML Processing, Web Scraping, API Integration, Microservices Architecture

# 📜 Certificates

- **정보처리기능사** (2024)
- **HSK 4급** (Chinese)
- **HSKK 초급** (Chinese Speaking)

# 🌐 Languages

- **Korean**: Native
- **English**: Intermediate (논문 읽기 가능)
- **Chinese**: HSK 4급 (Level 4), HSKK 초급 (Elementary Speaking)

# 💼 Projects (상세 설명)

## Earth CTF 사이트 개발 (2024)

**역할**: Full-Stack Developer & CTF Challenge Designer

**주요 기여사항**:

- NodeJS 기반 CTF 플랫폼 백엔드 아키텍처 설계 및 구현
- Docker를 활용한 격리된 문제 환경 구성 및 자동화 배포 시스템 구축
- SQLAlchemy ORM을 사용한 데이터베이스 설계 (사용자, 문제, 제출 기록 관리)
- JWT 기반 사용자 인증 시스템 및 세션 관리 구현
- 실시간 스코어보드 업데이트를 위한 WebSocket 통신 구현
- XSS, SQL Injection 등 웹 취약점 방어 코드 작성

**기술 스택**: Python, NodeJS, MySQL, Docker, WebSocket

## WordPress Plugin Vulnerabilities Research (2024)

**역할**: Security Researcher & Vulnerability Analyst

**주요 기여사항**:

- WordPress 플러그인 1000개 이상 대상 자동화 취약점 스캐닝 도구 개발
- 코드 구조 분석을 통한 SQL Injection, XSS 취약점 탐지
- 발견한 취약점에 대한 PoC(Proof of Concept) 코드 작성
- CVE 등록을 위한 상세 취약점 보고서 작성
- 학술제에서 연구 결과 발표

**성과**: 3개의 0-day 취약점 발견, 2개 CVE 후보 제출

## AI Powered Malicious URL Checker (2024)

**역할**: Full-Stack Developer & AI Model Developer

**주요 기여사항**:

- 웹 애플리케이션 프론트엔드 전체 개발 (Vue.js 기반)
- 악성 URL 검사 결과를 시각화하는 대시보드 개발
- 백엔드 API와 프론트엔드 간의 연동 및 통신 구현
- 사용자 친화적인 UI/UX 설계 및 반응형 웹 디자인
- 실시간 URL 검사 결과 표시 기능 구현
- 검사 이력 및 통계 대시보드 개발
- 악성 URL 탐지를 위한 데이터 전처리 파이프라인 설계 및 구현
- Random Forest, XGBoost, Neural Network를 결합한 앙상블 모델 설계 및 개발
- 모델 성능 최적화 및 하이퍼파라미터 튜닝

**기술 스택**: Vue.js, JavaScript, HTML/CSS, Chart.js, Axios, Python, scikit-learn, XGBoost, TensorFlow
**지원**: 한국정보보호산업협회(KISIA)
**GitHub**: github.com/racheliee/kisia-project

## Food AI 개인화 추천 솔루션 고도화 (2024)

**역할**: Data Engineer & Web Scraper Developer

**주요 기여사항**:

- 주요 쇼핑몰 대상 식품 데이터 수집을 위한 웹 스크래퍼 개발 및 구현
- Python을 활용한 자동화 데이터 수집 시스템 구축
- 다양한 온라인 쇼핑몰(마트, 식품 전문몰 등)의 상품 정보 크롤링
- 수집된 데이터의 전처리 및 정제 작업
- 데이터셋 구축 및 품질 관리

**기술 스택**: Python, BeautifulSoup, Selenium, Requests
**지원**: 고용노동부 일자리경험 프로그램

## LAMP Stack 웹 사이트 구현 및 취약점 실습 (2024)

**역할**: Web Developer & Penetration Tester

**주요 기여사항**:

- Linux, Apache, MySQL, PHP 환경에서 전자상거래 웹사이트 풀스택 개발
- 의도적으로 OWASP Top 10 취약점을 포함한 웹 애플리케이션 구현
- SQL Injection, XSS, CSRF, File Upload 등 10개 이상 취약점 시나리오 제작
- Burp Suite를 활용한 취약점 진단 및 익스플로잇 코드 작성
- 각 취약점에 대한 시큐어 코딩 가이드라인 문서 작성
- ModSecurity WAF 규칙 작성 및 적용

**교육**: KnockOn bootcamp 1st
**GitHub**: github.com/hy30nq/myWebsiteWithKnock

## 윈도우 소프트웨어 버그헌팅 (2023-2024)

**역할**: Vulnerability Researcher & Static Code Analyst

**주요 기여사항**:

- WinAFL을 활용한 Windows 바이너리 퍼징 환경 구축
- IDA, x64dbg를 사용한 정적 코드 분석 및 크래시 분석
- 소스코드 수준에서의 취약점 패턴 분석 및 식별
- 퍼징 하네스 작성 및 테스트 케이스 개발 지원
- 크래시 결과 분석 및 취약점 검증 프로세스 수행
- Python으로 자동화된 크래시 검증 및 크래시 분석을 위한 구조화 도구 개발
- 20개 이상의 크래시 발견, 5개 취약점 벤더 리포트

**성과**: CVE-2024-11950 등록 (XnView Classic RWZ 파일 파싱 취약점)
**교육**: KITRI 화이트햇 스쿨

## API 활용 영화 추천 프로그램 (2023)

**역할**: Backend Developer & Data Analyst

**주요 기여사항**:

- TMDB API를 활용한 영화 데이터 수집 및 전처리
- 사용자 시청 기록 기반 협업 필터링 알고리즘 구현
- SQLite 데이터베이스 설계 및 쿼리 최적화
- Tkinter를 활용한 데스크톱 GUI 애플리케이션 개발
- 멀티스레딩을 통한 API 호출 최적화로 응답속도 80% 개선

**과목**: 파이썬프로그래밍 (고려대학교)

# 🎓 주요 교육 이수 (상세 설명)

## KITRI 차세대 보안리더 양성프로그램 화이트햇 스쿨 1기 (2023.09.01 - 2024.03.22)

**과학기술정보통신부 장관 인증 TOP 20**

**교육 내용**:

- 시스템 해킹: Buffer Overflow, ROP, Heap Exploitation
- 웹 해킹: SQL Injection, XSS, CSRF 등 웹 취약점 분석
- 리버싱: PE 구조 분석, 안티 디버깅 우회, 악성코드 분석
- 네트워크: 패킷 분석, 프로토콜 취약점, MITM 공격

- 디지털 포렌식: 메모리 포렌식, 파일시스템 분석

**프로젝트**: 윈도우 소프트웨어 취약점 분석 프로젝트 수행
**성과**: 최종 평가 TOP 20

## KISIA AI 보안기술개발 네트워크반 (2024.07.08 - 2024.10.25)

**과학기술정보통신부 장관상 최우수 수료생**

**교육 내용**:

- AI 보안 위협: Adversarial Attack, Model Inversion, Data Poisoning
- AI 기반 보안: 악성코드 탐지, 이상징후 탐지, 위협 인텔리전스
- MLOps 보안: 모델 배포 시 보안 고려사항, 파이프라인 보안
- 프라이버시 보호 기술: Federated Learning, Differential Privacy

**프로젝트**: AI 기반 악성 URL 탐지 시스템 개발
**성과**: 개인 최우수 수료생 선정, KISIA 해커톤 최우수상 수상

## KnockOn Elite Whitehacker Bootcamp 1st (2024.02.17 - 2024.05.30)

**TOP 7 수료**

**교육 내용**:

- 고급 웹 해킹: Blind SQL Injection, XXE, SSRF 등
- 모의해킹 실습: 실제 기업 환경 모의 침투 테스트

**프로젝트**: LAMP Stack 취약 웹 애플리케이션 개발 및 분석
**성과**: 최종 평가 TOP 7

## 한국인터넷진흥원(KISA) 버그헌팅 실습 훈련 초급과정 (2025.03.04 - 2025.03.15)

**교육 내용**:

- 버그헌팅 방법론 및 도구 활용법
- 웹 애플리케이션 취약점 분석 실습
- 취약점 보고서 작성 및 제보 프로세스

# 📫 Contact

더 자세한 정보나 협업 제안은 아래 연락처로 문의해 주세요:


- **Email**: ktechq2003@korea.ac.kr / gtechq2003@gmail.com
- **Phone**: 010-3838-6382
- **Website**: https://hy30nq.com
- **Blog**: hyeonql.tistory.com
- **GitHub**: github.com/hy30nq