고영훈

정보보안 컨설팅
소프트웨어 개발

koyo@koyo.kr
koyo.kr
github.com/koyokr

기술

- Security
  - Pen Testing
  - Web Hacking
  - Reversing
- DevSecOps
  - Jenkins, Docker
  - AWS, Linux
- Programming
  - Python, Java, C++
  - TypeScript, Shell Script
- Development
  - Git, SQL
  - Spring, Django

소개

저는 컴퓨터를 좋아하는 사람입니다.

집념을 갖고 목표에 도전하며 더 나은 방법을 찾아 고민하고 문제 해결에 최선을 다합니다.

강력한 소속감과 책임감을 갖고 기대에 부응해 결과로 보답합니다.

잘 부탁드립니다.

경험

보안컨설팅 교육
시큐리티아카데미
안랩 트랙
2024. 7. – 2024. 10.

- 역량평가 1등
- 주요정보통신기반시설 점검 가이드 학습
- 취약점 진단/모의해킹/버그바운티 수행
- Burp Suite, XSS, SQL Injection

인턴
한국인터넷진흥원
디지털서명인증팀
2024. 5. – 2024. 7.

- 알뜰폰 인증 관련 보안조치 취합 및 검증
- 디지털인증확산센터 구축 행사 지원

개발 교육
삼성 청년 SW 아카데미
자바 트랙
2023. 7. – 2024. 5.

- 커피 단체주문 서비스 백엔드/인프라 담당
- 암표 방지 티케팅 서비스 블록체인 담당
- 테이스팅노트 서비스 백엔드/인프라 담당
- Spring Boot, Jenkins, Solana, Nuxt

학사
전남대학교
컴퓨터정보통신공학전공
2015. 3. – 2022. 2.

- 정보보호119 동아리 회장
- 대학정보보호동아리연합회(KUCIS) 발표
- 사이버위기대응 모의훈련 자문위원
- 시스템보안연구센터 연구보조 근로장학생
- KCI 정보보호학회논문지 제2저자 게재
- 사이버명예경찰 누리캅스 활동
- 대학생금융보안캠프 수료
- Pen Test, Pandas, Keras, PyTorch

보안 관제
공군 사이버작전센터
정보보호병
2017. 6. – 2019. 5.

- IDS/IPS, WAF, SIEM 관제
- 업무 자동화 도구 개발
- Python, JavaScript, Shell Script

보안 교육
차세대 보안 리더 양성 프로그램
정보보호특기병 트랙
2016. 7. – 2017. 2.

- Top 30
- IoT 신규 취약점 버그바운티 포상금 수령
- KISA Whistl 개선 웹셸 탐지 도구 개발
- UART, C++, Qt, Regex

수상

2024	2024 블록체인 경진대회 ESG 해커톤	우수상
	삼성 청년 SW 아카데미 특화 프로젝트	우수상
2023	2023 제5회 K-디지털 트레이닝 해커톤 대회	장려상
	삼성 청년 SW 아카데미 1학기	성적우수상
2020	2020년 대학정보보호동아리 프로젝트부문	우수상
	이달의 전남대인	표창
	제7회 소프트웨어 개발보안 경진대회	우수상
	한전KDN 뉴딜 선도 혁신 해커톤	장려상
2019	IoT 보안위협 시나리오 공모전	최우수상
	2019년 TS 보안 허점을 찾아라!	우수상
	2019년 대학정보보호동아리 활동실적부문	우수상
	2019년 대학정보보호동아리 프로젝트부문	호남권 최우수상
	제6회 소프트웨어 개발보안 경진대회	장려상
2017	2017년 육군 해킹방어대회	우수

자격

2022	AWS Certified Developer – Associate
	AWS Certified Solutions Architect – Associate
2021	정보처리기사
2019	한국사능력검정시험 1급

프로젝트명	민간기업 취약점 점검		
수행 기관	미래창조과학부, 한국인터넷진흥원	기간	2020. 5. 11. ~ 5. 20.
팀 구성 및 담당 역할	2인 / 모의침투 자문위원	주요 기술	XSS, SQLi

■ **미래창조과학부, 한국인터넷진흥원 주관 민간분야 사이버위기대응 모의훈련**

○ 사이버위기대응 참여업체 웹페이지 취약점 점검

■ **담당 업무**

○ 웹사이트 점검 및 취약점 54개 보고

- 입력 값 검증 부재 48건, 취약한 인증 1건
- 취약한 정보저장 방식 1건, 부적절한 환경설정 3건, 취약한 접근통제 1건

■ **성과/배운점**

○ 수동 점검을 통해 실전 취약점을 탐지하는 경험

○ 취약점 리포트를 작성하고 적합한 조치방안을 제시하는 역량

프로젝트명	공공기관 취약점 점검		
수행 기관	전남대학교	기간	2020. 5. 22. ~ 5. 28.
팀 구성	4인	주요 기술	XSS

■ **공공기관 취약점 점검**

○ 5개 공공기관 161개 웹페이지 취약점 점검

■ **담당 업무**

○ 웹사이트 점검 및 취약점 150개 보고

- 입력 값 검증 부재 102건, 취약한 인증 13건
- 취약한 정보저장 방식 23건, 부적절한 환경설정 12건

■ **성과/배운점**

○ 공공기관의 보안 요구사항과 법적 규제를 준수해 취약점을 탐지하는 경험

프로젝트명	TS 보안 허점을 찾아라!		
수행 기관	한국교통안전공단	기간	2019. 11. 30. ~ 12. 1.
팀 구성	4인	주요 기술	XSS, CSRF

■ **한국교통안전공단 취약점 점검 경진대회**

○ 대상: 한국교통안전공단 홈페이지

■ **성과/배운점**

○ 2019년 TS 보안 허점을 찾아라! - 우수상 (한국교통안전공단)

프로젝트명	육군 해킹방어대회		
수행 기관	육군	기간	2017. 2. 23.
팀 구성	2인	주요 기술	침해사고분석

■ **육군 해킹방어대회**

○ 침해사고를 당한 윈도우 PC에서 디지털 포렌식을 수행해 침해사고 요인 분석

■ **성과/배운점**

○ 2017년 육군 해킹방어대회 - 우수 (육군 정보화기획참모부)

프로젝트명	IoT 신규 취약점 버그바운티		
수행 기관	차세대 보안 리더 양성 프로그램 (Best of the Best)	기간	2017. 2.
팀 구성	개인	주요 기술	IoT, UART

■ 계기/목적

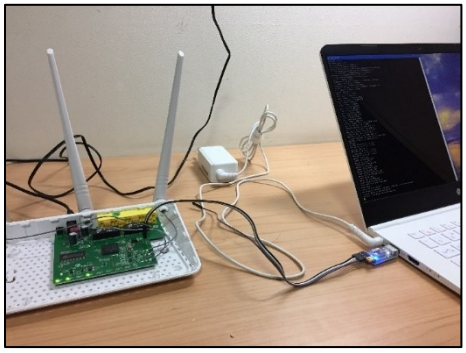
○ 시중에 판매되는 IoT 기기의 신규 취약점을 찾아 신고하는 과정을 실제로 함으로써 역량을 쌓기 위함

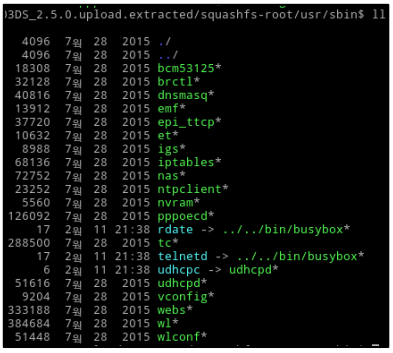
■ 담당 업무

○ 펌웨어 파일시스템 추출 및 UART 통신을 통해 웹페이지의 파라미터를 검증하고 정적 바이너리 분석

○ 로그인 인증 우회, 커맨드인젝션, 버퍼오버플로 등 신규 취약점 다수 발견

○ 발견 방법, 발생 원인, 검증 방법, 악용 시나리오, 조치 방안을 보고서로 작성하여 한국인터넷진흥원에 제출





■ 성과/배운점

○ 한국인터넷진흥원 S/W 취약점 신고포상제 2017년 1분기 포상금 수령

○ 파라미터 값을 검증하지 않거나 안전하지 않은 함수를 사용해 취약점이 발생하는 실제 사례 학습

프로젝트명	스마트초인종부터 시작하는 스마트시티 해킹		
팀 구성	5인	기간	2019. 11.
담당 역할	공격 기술 담당	주요 기술	IoT, UART

■ 계기/목적

○ 스마트초인종은 홈 네트워크에 연결된 IoT 기기 중 유일하게 집 외부에 노출된 기기

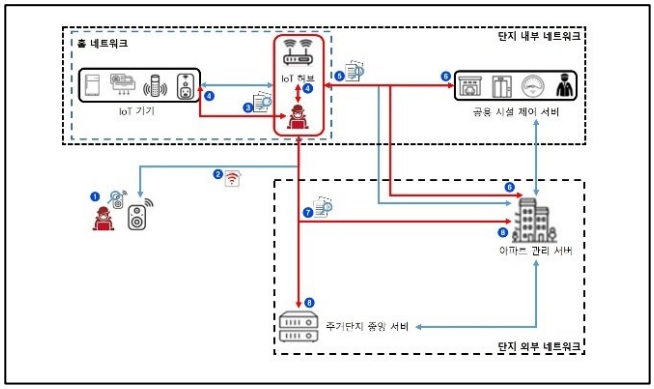
○ 외부에 노출된 IoT 기기를 통한 내부 네트워크 침투 시나리오 제시

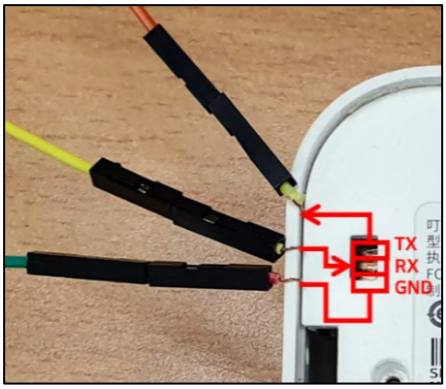
■ 담당 업무

○ 시중에 판매되는 스마트초인종을 구매해 UART 통신 가능성을 확인하고 펌웨어에서 파일시스템 추출

○ 커맨드 인젝션을 통해 파일 내용을 화면에 출력하는 방법을 통해 와이파이 자격증명 탈취

○ 홈 네트워크에 접속 후 Scanning, ARP Spoofing 등의 기법을 적용해 단계별로 네트워크 장악





■ 성과/배운점

○ IoT 보안위협 시나리오 공모전 – 최우수상 (한국인터넷진흥원)

○ 이전 IoT 신규취약점 버그바운티 과정에서 학습한 지식을 응용하고 악용 시나리오 작성 능력을 기름

프로젝트명	정규식 기반의 웹셸 탐지 도구 (WHISTL)		
수행 기관	차세대 보안 리더 양성 프로그램 (Best of the Best)	기간	2016. 9. ~ 2016. 12.
팀 구성 및 담당 역할	4인 / 개발	주요 기술	C++, Qt, 정규표현식

■ **계기/목적**

○ 한국인터넷진흥원의 웹셸 탐지 프로그램 WHISTL 개선 과제 수행

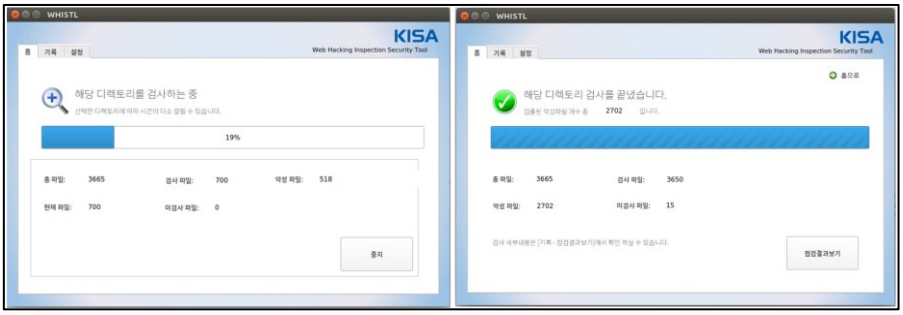
○ 윈도우에서 허용하지 않는 파일경로의 웹셸을 탐지하지 못하는 문제 해결

■ **담당 업무**

○ `//./` UNC Path Prefix를 사용해 경로 길이가 260자를 넘거나 비허용 문자를 포함하는 파일 스캔

○ 수집한 웹셸 샘플을 대상으로 기존 정규식 패턴의 성능을 평가하고 탐지율을 기준으로 최적화

○ C++로 프로그램을 새로 작성하고 re2와 같은 정규식 라이브러리를 도입해 탐지 속도 향상



■ **성과/배운점**

○ **윈도우 미탐지 문제 해결, 탐지율 32.6%에서 74%로, 탐지속도 8분 8초에서 29초로 성능 향상**

○ **후속 연구로 PHP 엔진의 바이트코드 실행 단계에서 함수명을 감시해 웹셸을 탐지하는 프로그램 제시**

○ **C++, Git, 정규식을 프로젝트에서 처음 사용하는 과정에서 문제를 정의하고 해결법을 찾는 사고방식을 키움**

프로젝트명	인터넷에 노출된 내 개인정보 탐색 앱 (님아 그것은 제 정보입니다)		
팀 구성	4인	기간	2019. 7. ~ 2019. 8.
담당 역할	백엔드 개발	주요 기술	Spring, Swift

■ **계기/목적**

○ 인터넷에 노출된 내 개인정보를 간편하게 찾아주는 앱을 통해 경각심 유도

■ **담당 업무**

○ 본인인증 후 주요 포털에 노출된 개인정보 탐색 결과를 제공하는 API 및 관리자페이지 작성

○ 삭제 요청, 온라인/오프라인 개인정보 관련 분쟁조정 신청, 개인정보 침해 신고 기능 제공

○ Azure와 Heroku에 API 서버와 관리자 페이지 배포

■ **성과/배운점**

○ **제6회 소프트웨어 개발보안 경진대회 - 장려상 (한국정보보호학회)**

○ **클라우드 환경을 처음 접하고 삭제와 신고 기능을 기획하면서 개인정보 관련 제도를 학습함**

비고	https://github.com/corykim0829/thats-my-info https://github.com/koyokr/thats-my-info-server

프로젝트명	크로스플랫폼 PE/ELF 보안 속성 점검 도구 (checksec.py)		
팀 구성	7인	기간	2019. 6. ~ 2019. 11.
담당 역할	Windows, PE 부문 개발	주요 기술	Python, ELF, PE

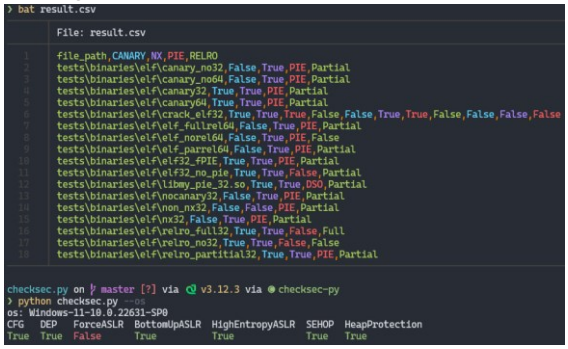
■ 계기/목적

○ Linux/ELF의 보안 속성만 출력하는 도구 checksec.sh에서 Windows/PE 영역으로 확장해 편의 제공

■ 담당 업무

○ 파이썬 모듈 pefile을 사용해 입력된 경로의 PE 파일의 메모리 보안 속성 출력

○ 파워셀 명령어 Get-ProcessMitigation을 통해 Windows 운영체제의 메모리 보안 속성 출력



■ 성과/배운점

○ 2019년 대학 정보보호 동아리 프로젝트부문 호남권 - 최우수상 (한국인터넷진흥원)

○ 컴파일러에서 설정할 수 있는 실행파일 메모리 보안 옵션과 운영체제에서 제공하는 보안 기능을 학습함

비고	https://github.com/is119/checksec.py

프로젝트명	페이로드 임베딩 사전학습 기반의 웹 공격 분류 연구		
수행 기관	전남대 사이버보안연구센터	기간	2020. 2. ~ 2020. 7.
담당 역할	데이터 전처리, AI 모델 구현	주요 기술	Python, Keras, NLP

■ 계기/목적

○ 전통적인 웹방화벽과 자연어 처리 기법보다 좋은 성능의 웹공격 분류 모델 제안

■ 담당 업무

○ 오픈소스 웹방화벽 modsecurity를 참고해 카테고리를 정의하고 악성 페이로드 데이터셋 분류

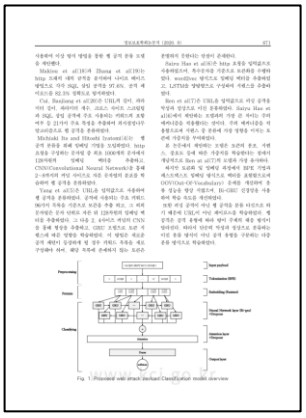
○ 토큰화, 임베딩, 신경망에 대해서 후보군 및 파라미터별로 데이터 처리 및 모델 학습

○ BPE 토큰화, FastText 임베딩, Bi-GRU, Attention 모델링 구현 및 파라미터 조정

○ Accuracy, Precision, Recall, F1-Score 평가 지표 시각화


페이로드 임베딩 사전학습 기반의 웹 공격 분류 모델

Web Attack Classification Model Based on Payload Embedding Pre-Training



■ 성과/배운점

○ 정보보호학회논문지 게재 및 KCI 등재 (제2저자)

○ 논문 리뷰 방법, 인공지능 모델 기초, 악성URL 관련 도메인 지식을 학습함

비고	https://doi.org/10.13089/JKIISC.2020.30.4.669

프로젝트명	변조 방지와 투명성 제공을 위한 개인정보처리방침 블록체인 서비스		
팀 구성	3인	기간	2024. 8. 28. ~ 2024. 8. 30.
담당 역할	블록체인(이더리움), 프론트엔드	주요 기술	Solidity, Web3, Vue

■ 계기/목적

○ ESG 경영에서 '개인정보보호·데이터 보안'은 중요한 요소로 개인정보보호 중심 설계가 필요

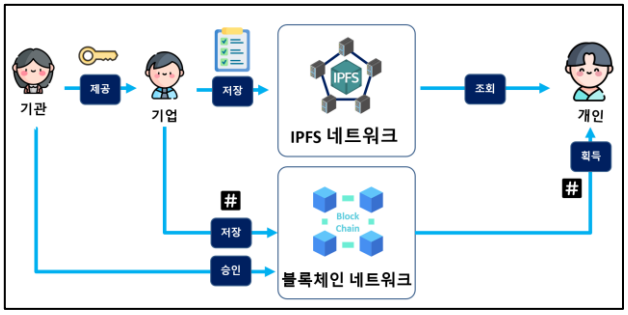
○ 개인정보처리방침이 변경되면 사용자에게 필수로 고지해야 하며, 개인정보처리방침 과거 이력 제공을 권고

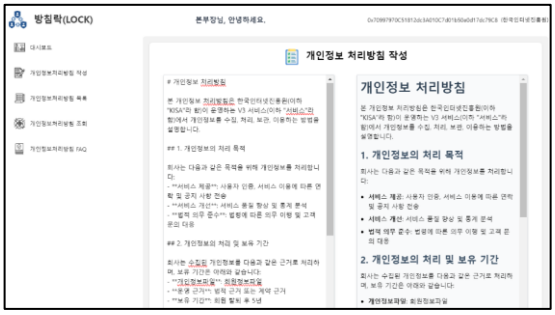
■ 담당 업무

○ IPFS에 개인정보처리방침을 저장하고 블록체인 스마트 컨트랙트로 이력을 관리하는 시스템 개발

○ 기관은 기업 목록을 관리하고 기업의 개인정보처리방침 갱신 요청을 확인하고 승인

○ 기업은 개인정보처리방침 이력을 관리하고 개인정보처리방침을 갱신





■ 성과/배운점

○ 2024 블록체인 경진대회 「BEST Challenge」 ESG 해커톤 - 우수상 (한국인터넷진흥원)

비고	https://github.com/koyokr/ppc

프로젝트명	웹캠을 이용한 실시간 거북목 자세 탐지 시스템 (거북목 탈출 넘버원)		
팀 구성	4인	기간	2020. 7. ~ 2020. 8.
담당 역할	데이터, AI 모델, 백엔드	주요 기술	PyTorch, Django, PyQt

■ 계기/목적

○ 사회적 거리두기의 장기화로 국민의 평균 PC 사용 시간이 증가함에 따른 거북목 질환 증가 대응

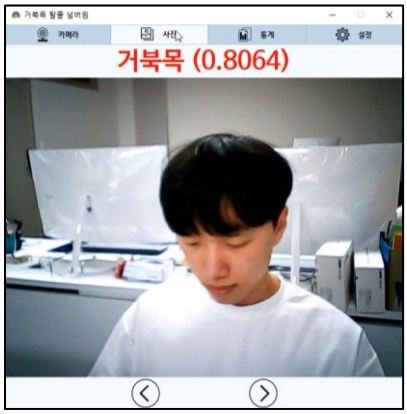
■ 담당 업무

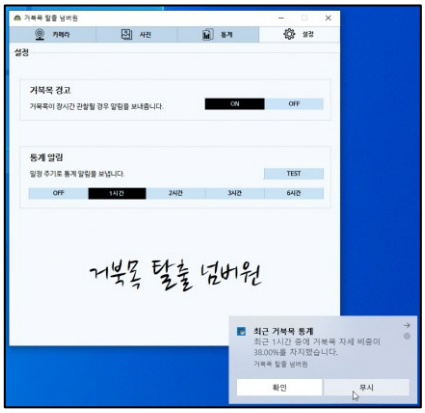
○ 웹캠을 통해 PC 사용자의 거북목 자세를 실시간으로 판별하고 알림을 보내는 서비스(서버, 클라이언트) 개발

○ 다양한 환경에서 웹캠으로 촬영한 1,930개 이미지 데이터셋 구축

○ 사전학습된 자세 추정 모델로 이미지를 structured 데이터로 변환하고 XGBoost 모델 학습

○ Gunicorn 및 Supervisord를 도입해 Django 인스턴스 수를 증가시켜 스케일업





■ 성과/배운점

○ 제7회 소프트웨어 개발보안 경진대회 - 우수상 (행정안전부)

○ 0.8986의 정확도(accuracy)와 0.9026의 F1-Score(0.9026)의 성능을 보이는 실시간 판별 모델 구현

비고	https://github.com/koyokr/ihunch-escape

프로젝트명	블록체인 기반의 암표 방지 티케팅 서비스 (conting)		
수행 기관	삼성 청년 SW 아카데미	기간	2024. 2. ~ 2024. 4
담당 역할	블록체인(솔라나), 스프링 배치	주요 기술	Spring, React Native, Rust

■ 계기/목적

○ 암표를 막는 방법 중 하나로 1인1매가 정착되면서 가족과 함께 공연을 관람하기가 어려워짐

○ 암표를 효과적으로 막는 동시에 검증 가능한 가족 간 표 구매를 가능하게 하고 값싼 NFT 티켓 생태계 구현

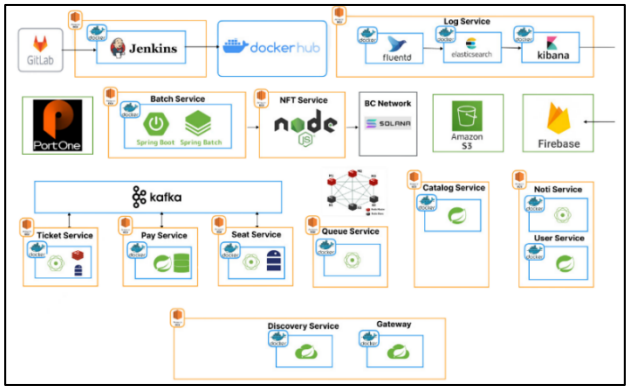
■ 담당 업무

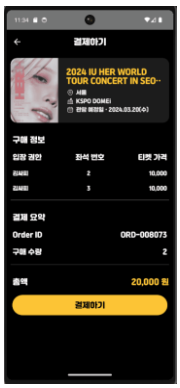
○ 구매 시 생체인증으로 비대칭키를 생성하고 공개키를 서버에 전송하여, 검표 시 개인키 서명을 통해 동일 검증

○ Solana Program(스마트 컨트랙트)를 작성해 NFT 티켓의 발행/거래/팬추첨 및 가족인증 구현

○ React Native 환경에서 호환되지 않는 관련 web3 라이브러리 문제에 대응해 대체 함수 작성

○ Spring Batch를 통해 새로 생성된 공연에 대해 NFT 티켓 민팅





■ 성과/배운점

○ 삼성 청년 SW 아카데미 특화 프로젝트 – 우수상 (삼성전자주식회사)

○ 디지털 환경에서만 가능한 디지털서명의 이점을 강력하게 체감하고 블록체인과 Web3 생태를 학습함

비고	https://github.com/con-ting/conting

프로젝트명	기부단체 정보 제공 플랫폼 (GIVE1004)		
팀 구성	6인	기간	2023. 11.
담당 역할	데이터, DB, AI 챗봇	주요 기술	Spring, React Native, LLM

■ 계기/목적

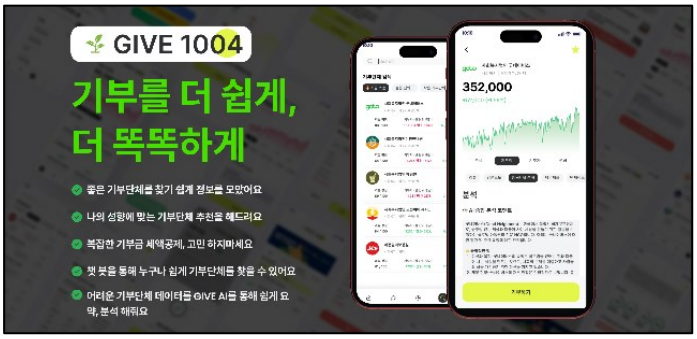
○ 국내 기부율이 30%대에서 20%대로 대폭 감소함에 따라 대응 필요성을 느낌

○ 기부 안하는 이유로 61%가 '믿을 수 없어서', 기부 경험자 중 57%가 '기부금 사용 내역을 모른다'고 답함

■ 담당 업무

○ 국내에서 활동하는 기부단체들을 검색, 필터, 정렬, 추천 등으로 빠르게 찾을 수 있음

○ 기부단체의 기부내역, 사용내역, 재무분석, 감사내역, 관련뉴스, 사용자평점, AI분석 제공



■ 성과/배운점

○ 2023 제5회 첨단산업 디지털 핵심 실무인재 양성훈련 해커톤 대회 – 장려상 (직업능력심사평가원)

비고	https://github.com/GIVE1004

프로젝트명	단체 커피 주문 서비스 (SSAFEE)		
수행 기관	삼성 청년 SW 아카데미	기간	2024. 1. ~ 2024. 2
담당 역할	인프라, 백엔드, 프론트엔드	주요 기술	Spring, Vue, Nuxt.js

■ 계기/목적

○ 삼성 광주공장 내부에 위치해 있는 SSAFY 광주캠퍼스 특성상 단체 커피 주문이 매우 활성화됨

○ 주문을 취합해서 하나씩 입력하는 교육생과 주문배달 플랫폼의 수수료를 지불하는 사장님간 상호이익을 노림

■ 담당 업무

○ 소셜 로그인을 하면 카페를 선택하고 방을 생성하고 공유링크를 통해 로그인 없이 접속 및 메뉴 추가 가능

○ 사내 메신저 연동으로 참가자에게 알림 제공, 실시간 메뉴 주문, 실시간 채팅, 주문 접수

○ OAuth2 로그인, Jwt, WebSocket 실시간채팅 구현

○ Jenkins 구성을 통해 빌드 및 Docker Compose 배포 자동화

■ 성과/배운점

○ 지역 카페와 협력해 시연 당일 교육생들의 주문을 직접 전달하고 배달하는 데 성공

○ Spring Boot 3 MVC 및 JPA 환경으로 REST API를 Vue 3로 CSR을 구현하는 경험을 얻음

비고	https://github.com/ssafee-team/ssafee

프로젝트명	온라인 기사 조회수 예측 모델 연구		
팀 구성	개인	기간	2020. 4. ~ 2020. 6.
담당 역할	데이터 처리, AI 모델	주요 기술	Python, Keras, NLP

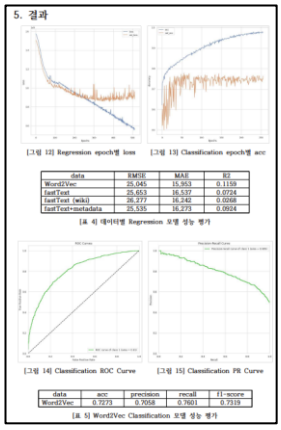
■ 계기/목적

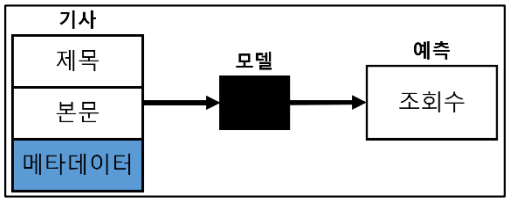
○ 기사의 제목과 본문만으로 조회수를 예측하는 아이디어 실험

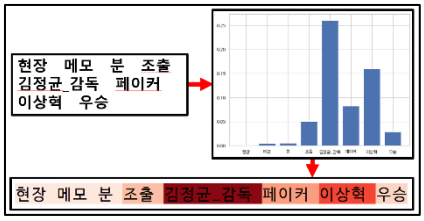
■ 담당 업무

○ 기존 연구 2개를 리뷰하고 한계점을 짚고 개선된 연구 결과를 제시

○ 51,816개의 수집된 데이터셋에 대해 한국어 형태소와 명사 추출 및 음정별 초중종성 분리 후 토큰화 적용







■ 성과/배운점

○ 회귀 모델 R2 0.1159, 분류 모델 Accuracy 0.7273, F1-Score 0.7319

○ 악성 페이로드를 분류하는 AI 모델 연구에서 배운 방법론을 타 도메인에 적용해 목표 달성

비고	https://github.com/koyokr/news-prediction

프로젝트명	공군 사이버작전센터 보안관제 업무 자동화		
수행 기관	공군 사이버작전센터	기간	2017. 11. ~ 2018. 10.
담당 역할	알림, 전파, 일지 자동화	주요 기술	Python, JavaScript, Shell

■ **계기/목적**

○ 동시다발적으로 발생하는 관제 대응 업무 간소화

■ **담당 업무**

○ 유형별 매뉴얼 제시, 일지 작성, 타 부대 전파 자동화
- COM 객체를 사용해 한셀 갱신, 윈도우 클립보드 형식을 이용해 HWP 문서 갱신
- 지정된 유형이 아니거나 예외가 발생하면 상태를 로깅하고 수작업 명시

○ 중요한 탐지 건 발생 시 음성 알림 전파

○ 데이터 취합, 점검 보조 등 단순 반복 작업 자동화

○ Git 버전 관리를 도입하고 기능별로 모듈화하여 전역 후에도 손쉽게 유지보수될 수 있도록 함

■ **성과/배운점**

○ 단순 반복 작업에 소모되는 시간을 대폭 줄여 상황관제반의 업무 속도와 정확도를 향상시킴

○ 기능별로 업무 기여도에 따라 포상 수령

프로젝트명	사이버지식정보방 개발환경 구축 자동화		
팀 구성	개인	기간	2018. 7. ~ 2018. 10.
담당 역할	개발	주요 기술	Go, Shell, DNS

■ **계기/목적**

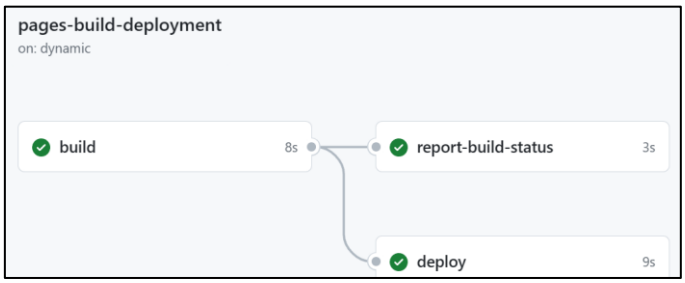
○ 172.0.0.0/8, 192.0.0.0/8 대역 차단으로 인한 GitHub, Google 등 특정 사이트 접속 불가 문제

■ **담당 업무**

○ 글로벌 서비스는 1개 도메인에 여러 IP를 연결하는 경우가 흔함
- 라운드 로빈, 지리적 기반 부하 분산, 국가 규제 등의 이유

○ Heroku 인스턴스에 DNS 수집 프로그램을 배포해 해외 리전 IP를 PostgreSQL에 기록

○ hosts 파일을 수정하고 필요한 프로그램을 한 번에 설치하는 스크립트 배포
- 템플릿을 수정하면 빌드하여 스크립트 다운로드 페이지를 생성하는 CI/CD 파이프라인 생성



■ **성과/배운점**

○ VPN, SSH 터널링을 배제한 방법으로 특정 대역 차단 문제 해결

○ 빠른 사용자 환경 구축을 통해 초기 세팅 시간 단축

비고	https://github.com/koyokr/sjb-init https://github.com/koyokr/sjb-host