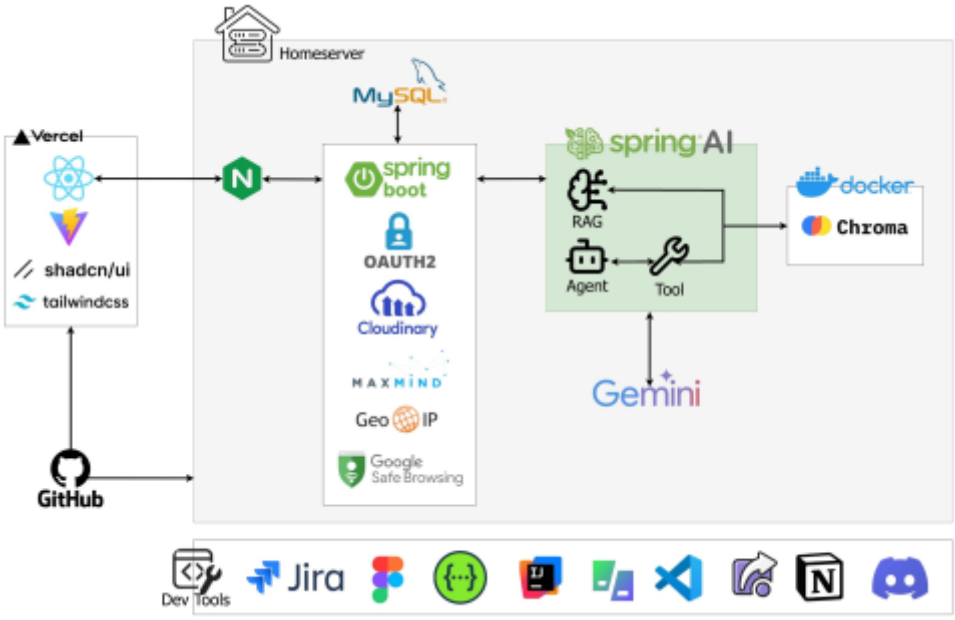
시스템 정의서(프로젝트 요약서)

(404 Found) **팀**

<table>
<tr><td rowspan="2">작품명
(주제)</td><td colspan="3">(국문) QREX: RAG 기반 QR코드 피싱 방지 서비스</td></tr>
<tr><td colspan="3">(영문) QREX: RAG-based QR code phishing prevention service</td></tr>
<tr><td rowspan="3">책 임 자
(팀장)</td><td>성 명</td><td colspan="2">김여민</td></tr>
<tr><td>소 속</td><td colspan="2">소프트웨어학부</td></tr>
<tr><td>학 번</td><td colspan="2">2024042053</td></tr>
<tr><td>개발기간</td><td colspan="3">2022 년 9 월 1 일 ~ 2022 년 12 월 11 일</td></tr>
<tr><td rowspan="4">참여학생</td><td>학번</td><td>이름</td><td>전공</td></tr>
<tr><td>2024042050</td><td>심연우</td><td>소프트웨어학부</td></tr>
<tr><td>2024042016</td><td>최수연</td><td>소프트웨어학부</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>지도교수</td><td colspan="3">강재구</td></tr>
<tr><td colspan="4">작품(주제)에 대한 요약</td></tr>
<tr><td>작품 설명</td><td colspan="3">QREX는 피싱 여부가 의심되는 QR을 스캔하여, QR 속 사이트가 유해한 사이트인지를 판별하는 웹 서비스입니다.
사용자는 자신이 검사한 결과를 다시 확인할 수 있으며, 게시판을 통해 피싱 사례를 공유하고 의견을 나눌 수 있습니다. QR 코드에 포함된 URL을 분석 대상으로 하여 피싱 가능 여부를 판단합니다. 명확한 악성 URL은 즉시 분류하고, 추가 판단이 필요한 경우에는 RAG 기반 분석을 수행합니다.</td></tr>
<tr><td>작품의
주요 기능</td><td colspan="3">1. 카메라 또는 갤러리의 QR 이미지를 인식한다.
2. 인식한 URL 정보를 서버로 전달한다.
3. 서버에서 URL을 분석하여 피싱 여부를 판별한다.
4. 판별 결과와 URL의 기본 정보를 사용자에게 제공한다.
5. 사용자가 검사한 QR 코드 결과를 저장하고 다시 확인할 수 있도록 한다.
6. 게시판을 통해 사용자들이 피싱 사례를 공유할 수 있도록 한다.
7. 회원가입 시 입력한 개인정보를 수정할 수 있도록 한다.
8. 댓글 신고 기능을 제공하여 건전한 게시판 문화를 형성한다.
9. Spring AI 기반 RAG 분석 ChatBot Agent는 사용자와의 상호작용을 담당하며, 사용자의 서비스 경험을 원활하게 지원한다.</td></tr>
</table>

작품(주제)에 대한 요약 (계속)

운영개념	 - 본 서비스는 React 기반 프론트엔드, Spring Boot 기반 통합 백엔드, 그리고 Spring Boot 내부에 내장된 Spring AI 기반 RAG 분석 모듈로 구성된 다층 아키텍처로 운용됩니다. - 사용자가 업로드한 QR 정보는 Spring Boot 서버에서 전처리되며, 추가 판단이 필요한 경우 Spring AI RAG 분석 모듈이 외부 지식과 내부 URL 패턴 정보를 결합하여 판별을 수행합니다. - 최종 분석 결과는 통합 서버를 통해 저장 및 제공되어 사용자가 UI를 통해 확인할 수 있습니다.
기타 개발 시 고려사항	1. 피싱 여부 판별 결과를 신뢰할 수 있도록 RAG 기반의 지식 검색 및 최신 피싱 사례 데이터를 결합하여 분석 정확도를 높인다. URL 구조 분석, 사례 기반 비교, 외부 지식 참조 등을 통하여 위험도 평가를 수행하며, 서비스의 설명 가능성을 높이는 요소로 활용된다. 2. QR 스캔 URL과 사용자 정보의 보안 관리를 철저히 수행한다. 3. 단순 차단 여부만 제공하는 방식이 아닌, 판단 근거를 함께 제공하여 사용자가 결과를 이해할 수 있도록 설계한다.
오픈소스활용 및 기여 방안	**1. 오픈 소스 활용** **1) 프론트엔드 및 UI (Frontend & Design)** 1.1) React & Vite: 컴포넌트 기반의 SPA개발 환경 구축 및 빠른 렌더링 최적화. 1.2) Tailwind CSS & shadcn/ui: 유틸리티 클래스와 사전 제작된 컴포넌트를 활용. 1.3) Lucide-react & Sonner: 직관적인 아이콘 인터페이스 구성 및

	사용자 알림 메시지 구현. **2) 백엔드 및 보안 (Backend & Security)** 2.1) Spring Boot & JPA: 안정적인 RESTful API 서버 구축 및 객체 지향적 데이터베이스(DB) 접근 처리. 2.2) Spring Security & JJWT: JWT(JSON Web Token) 기반의 인증 시스템을 구축하여 안전한 로그인 유지 관리. 2.3) Lombok: 반복되는 Java 코드를 자동화하여 서버 코드의 가독성과 유지보수성 향상. **3) 핵심 기능 및 AI (Core Tech & AI)** 3.1) jsQR : 브라우저(jsQR)에서 QR 이미지를 디코딩하여 URL 및 데이터 추출. 3.2) Spring AI & OpenAI API: 자바 환경에서 LLM과 벡터 DB를 연동한 RAG 시스템 구축. 2. **양성 및 악성 QR 코드 데이터셋을 활용하여 학습 및 검증을 수행한다.**
선행기술 조사 분석	**<특허>** 1. KR101115250B1(김광태, 안영택, 강유진) / 1020110080168 : QR코드의 안전도 검사 장치 및 방법 2. 1020170097491 (2017.08.01.) / 주식회사 에프원시큐리티 머신러닝을 이용한 악성코드 유포지 위험도 분석 시스템
	<논문> 1. 김영준, 이재우, 「URL 주요특징을 고려한 악성URL 머신러닝 탐지모델 개발」, 한국정보통신학회논문지 제26권 제12호, 2022, pp. 1786–1793. 2. 양형규, 「QR 코드의 보안 취약점과 대응 방안 연구」, 한국인터넷방송통신학회 논문지 v.12 no.1, 2012, pp. 83–89. 3. 이동건, 황규준, 김동오, 황진석, 「큐싱(Qshing) 해킹 대응 방안 연구」, 한국IT정책경영학회 논문지, 2024, pp. 37–42. 4. 신현창, 이주형, 김종민, 「큐싱(Qshing) 공격 탐지를 위한 시스템 구현」, 융합보안논문지, 한국융합보안학회, 2023, pp. 55–61.
	<상용 제품> 1. askurl: https://www.nurilab.com/kr/products/askurl.html 2. KT '안심 QR 서비스' 3. 싹다잡아: https://play.google.com/store/apps/details?id=com.ps.wb&hl=ko 4. 블랙 쏘세지: https://play.google.com/store/apps/details?id=io.xrium.blacksawsage&hl=ko
Key Words (5개) : **#QR, #피싱 예방, #Agent, #판별 신뢰도, #RAG**	
지도 교수	강재구 (서명)