📄 보안 설계 명세 및 위협 모델링

1. 보안 설계 명세 (Security Design Specification)

보안 설계 명세는 시스템 개발 초기 단계에서 보안 요구사항을 명확하게 정의하고 이를 체계적으로 문서화하는 과정을 의미한다. 시스템이 제공해야 할 보안 기능을 사전에 구체적으로 규정함으로써, 개발 및 운영 과정에서 일관되고 신뢰할 수 있는 보안 수준을 유지하는 것을 목표로 한다.

주요 목적

- 시스템에 필요한 **입력 데이터 검증**, **세션 및 인증 관리**, **데이터 암호화 및 보호**, **접근 제어** 등을 사전에 규정한다.
- 개발자 및 운영자가 준수해야 할 **보안 기준과 지침**을 제공한다.
- 개발 및 테스트 과정 중 **보안 품질 저하를 방지**하고, 보안 결함 발생 가능성을 최소화한다.
- 제품 및 서비스가 **법적·규제적 요구사항**(예: 개인정보보호법, GDPR 등)을 충족할 수 있도록 지원한다.

주요 구성 요소

- **입력 검증 정책**: 모든 사용자 입력에 대해 길이, 형식, 허용 값 등을 검증하는 기준 수립
- **세션 관리 정책**: 안전한 로그인, 세션 유지, 세션 타임아웃 처리 방안 정의
- **암호화 기준**: 저장 및 전송 데이터에 대한 암호화 방식과 알고리즘 명시
- **취약점 대응 정책**: XSS, CSRF, SQL 인젝션 등 주요 위협에 대한 대응 방안 수립
- **접근 제어 방안**: 역할 기반 권한 관리(RBAC), 관리자 기능 접근 통제 등
- **로깅 및 모니터링**: 보안 이벤트 기록 및 이상 행위 탐지 방안 마련

기대 효과

- **초기 설계부터 보안이 내재된 시스템 구축 가능**
- **보안 이슈 대응 비용 절감**
- **개발-운영 간 일관성 확보**
- **컴플라이언스(법적 요구사항) 충족 용이**

우리 중고거래 플랫폼 - 위협 모델링

1. 시스템 이해

- **구성 요소**: 사용자(USERS), 상품(PRODUCTS), 채팅(CHAT_ROOMS, CHAT_MESSAGES), 결제(Stripe 연동), 신고(REPORTS), 관리자 대시보드
- **주요 데이터 흐름**: 회원 가입 → 상품 등록 → 검색/구매 → 채팅 → 결제 → 신고/차단 관리

2. 자산 식별

- 사용자 개인정보 (아이디, 닉네임, 프로필 사진, 평점 등)
- 로그인 인증 정보 (비밀번호, 세션 토큰)
- 상품 데이터 (제목, 가격, 설명, 이미지)
- 채팅 메시지 내용
- 결제 정보 (Stripe 결제 토큰)
- 신고 및 차단 기록

3. 위협 식별 (STRIDE 기반)

범주	예상 위협 시나리오	설명
Spoofing	다른 사용자의 세션을 탈취하여 가장	세션 하이재킹, 세션 고정 공격
Tampering	상품 정보 조작	가격, 설명, 상태를 악의적으로 변경
Repudiation	악성 사용자가 거래 부정	로그 미기록 시 분쟁 발생 가능
Information Disclosure	개인 정보 유출	프로필 정보, 채팅 내용, 결제 정보 노출
Denial of Service	대량의 채팅 메시지 전송	서버 과부하 유발, 정상 서비스 방해
Elevation of Privilege	일반 사용자가 관리자 기능 접근	인증 우회 또는 취약점 공격

4. 위험 평가 (예: DREAD 모델 간단 적용)

- **세션 하이재킹**: 매우 높은 위험도 (Damage 높음, Exploitability 높음)
- **상품 정보 조작**: 중간 위험도 (사업 신뢰성에 영향)
- **개인정보 유출**: 매우 높은 위험도 (법적 문제 발생 가능)
- **서비스 거부 공격(DoS)**: 중간 위험도 (일시적 서비스 장애)

5. 대응 방안 수립

위협 시나리오	대응 방안
세션 하이재킹	HTTPS 강제 사용, Secure/SameSite 쿠키 설정, 세션 타임아웃 짧게 유지
상품 정보 조작	수정/삭제 시 사용자 인증 재확인, 변경 내역 로깅
개인정보 유출	최소 정보만 저장, 민감 정보 암호화 저장, 접근 제어 강화
DoS 공격	API Rate Limiting 적용, 채팅 메시지 빈도 제한
권한 상승 공격	관리자 기능 접근 시 이중 인증(MFA) 적용

6. 문서화 및 검토

- 위 모든 분석 결과를 **보안 설계 문서**와 함께 보관하고, 개발 중, 배포 전, 운영 중 정기적으로 검토 및 업데이트
- 신규 기능 추가 시마다 위협 모델 재수행