2020 정보처리기사 필기 - 5.3 소프트웨어 개발 보안 구축(1)

2020. 4. 17. 21:37

#2020정보처리기사필기정리

Secure SDLC

Secure SDLC의 개요

- 보안상 안전한 소프트웨어를 개발하기 위해 SDLC(소프트웨어 개발 생명주기)에 보안 강화를 위한 프로세스를 포함한 것
- 유지보수 단계에서 보안 이슈를 해결하기 위해 소모되는 비용을 최소화하기 위함
- Secure Software 사의 CLASP, Microsoft 사의 SDL 등

요구사항 분석 단계에서의 보안 활동

- 보안 항목에 해당하는 요구사항을 식별하는 작업 수행
- 보안 수준을 보안 요소별로 등급을 구분하여 분류
- 보안 요소 : 기밀성, 무결성, 가용성, 인증, 부인 방지

설계 단계에서의 보안 활동

- 식별된 요구사항을 소프트웨어 설계서에 반영하고 보안 설계서 작성
- 네트워크, 서버, 물리적 보안, 개발 프로그램 등 환경에 대한 보안통제 기준을 수립하여 설계에 반영

구현 단계에서의 보안 활동

- 표준 코딩 정의서 및 소프트웨어 개발 보안 가이드를 준수하여 설계서에 따라 보안 요구 사항 구현
- 단위 테스트 실행
- 시큐어 코딩 : 구현 단계에서 발생할 수 있는 보안 취약점을 최소화하기 위해 보안 요소들을 고려하여 코딩

테스트 단계에서의 보안 활동

- 작성된 보안 설계서를 바탕으로 보안 사항들이 정확히 반영되고 동작되는지 점검

유지보수 단계에서의 보안 활동

- 이전 과정을 모두 수행했음에도 발생할 수 있는 보안사고들을 식별하고 발생 시 해결하고 보안 패치 실시

세션 통제

세션 통제의 개요

- 서버와 클라이언트의 연결인 세션 간의 연결로 인해 발생하는 정보를 관리
- 요구사항 분석 및 설계 단계에서 진단해야 하는 보안 점검 내용

불충분한 세션 관리

- 일정한 규칙이 존재하는 세션ID가 발급되거나 타임아웃이 너무 길게 설정되어 있는 경우 발생
- 세션 하이재킹(세션 정보를 가로채는 공격)을 통해 획득한 세션 ID로 접근할 수 있음

잘못된 세션에 의한 정보 노출

- 다중 스레드 환경에서 멤버 변수에 정보를 저장할 때 발생
- 변수의 범위를 제한하는 방법으로 방지 가능
- 싱글톤 패턴에서 발생하는 레이스컨디션으로 인해 동기화 오류가 발생하거나 멤버 변수의 정보가 노출될 수 있음
- 레이스컨디션 : 두 개 이상의 프로세스가 공용 자원을 획득하기 위해 경쟁하고 있는 상태

세션 설계 시 고려사항

- 로그아웃 요청 시 할당된 세션이 완전히 제거되도록 함
- 이전 세션이 종료되지 않으면 새로운 세션이 생성되지 못하도록 함

입력 데이터 검증 및 표현

입력 데이터 검증 및 표현의 개요

- 입력 데이터로 인해 발생하는 문제들을 예방하기 위해 구현 단계에서 검증해야 하는 보안 점검 항목
- 개발 단계에서 유효성 검증 체계를 갖추고 검증되지 않은 데이터가 입력될 시 처리할 수 있도록 구현해야 함
- 일관된 언어셋을 사용하여 코딩

입력 데이터 검증 및 표현의 보안 약점

종류	보안 약점	해결 방법
SQL 삽입	입력란에 SQL을 삽입하여 무단으로 DB를 조회, 조작	동적 쿼리에 사용되는 입력 데이터에 입력되지 않게 필터링 되도록 설정
경로 조작 및 자원 삽입	데이터 입출력 경로를 조작하여 서버 자원을 수정 삭제	경로 순회 공격을 막는 필터 사용
크로스사이트 필터링 (XSS)	웹페이지에 악성 스크립트를 삽입하여 방문자의 정보 탈취, 비정상적 기능 수행 유발	HTML 태그 사용을 제한 <,>,& 등의 문자를 다른 문자로 치환
운영체제 명령어 삽입	외부 입력값을 통해 시스템 명령어 실행을 유도하여 권한을 탈취하거나 시스템 장애 유발	웹 인터페이스를 통해 시스템 명령어 전달 방지 외부 입력값을 검증없이 내부 명령어로 사용하지 않음
위험한 형식 파일 업로드	악의적인 명령어가 포함된 스크립트 파일을 업로드하여 시스템에 손상을 입히거나 제어	업로드 되는 파일의 확장자 제한 파일명의 암호화 웹사이트와 파일 서버의 경로 분리 실행 속성 제거
신뢰되지 않는 URL 주소로 연결	입력값으로 사이트 주소를 받는 경우 이를 조작하여 피싱 사이트로 유도	연결되는 외부 사이트의 주소를 화이트 리스트로 관리

보안 기능

보안 기능의 개요

- 코딩하는 기능인 인증, 접근제어, 기밀성, 암호화들을 올바르게 구현하기 위해 구현 단계에서의 보안 점검 항목

보안 기능의 보안 약점

종류	보안 약점	해결 방법
적절한 인가 없이 중요기능 허용	보안검사를 우회하여 인증과정 없이 중요 정보 또는 기능에 접근 및 변경 가능	중요 정보나 기능을 수행하는 페이지에는 재인증 기능을 수행
부적절한 인가	접근제어 기능이 없는 실행경로를 통해 정보 또는 권한 탈취	모든 실행 경로에 대해 접근 제어 검사 수행 사용자에게는 반드시 필요한 접근 권한만 부여
중요한 자원에 대한 잘못된 권한 설정	권한 설정이 잘못된 자원에 접근하여 임의로 사용	관리자만 자원들에 접근하도록 설정 인가되지 않은 사용자의 중요 자원 접근 여부 검사
취약함 암호화 알고리즘 사용	암호화된 환경설정 파일을 해독하여 중요정보 탈취	안전한 암호화 알고리즘 사용 IT보안인증사무국이 안정성을 확인한 암호모듈을 이용
중요정보 평문 저장 및 전송	암호화되지 않은 평문 데이터를 탈취해 중요 정보 획득	중요 정보 저장, 전송 시 암호화 과정을 거침 보안 채널 이용
하드코드된 비밀번호	소스코드 유출 시 내부에 하드코드된 패스워드 이용	패스워드를 암호화하여 별도 파일 저장 기본 설정 패스워드나 키의 사용을 피함

시간 및 상태

시간 및 상태의 개요

- 동시 수행을 지원하는 병렬 시스템이나 다수의 프로세스가 동작하는 환경에서 시간과 실행 상태를 관리하여 원활하게 동작되도록 하기 위한 보안 검증 항목

TOCTOU 경쟁 조건

- 검사 시점과 사용 시점을 고려하지 않고 발생하는 보안 약점

종료되지 않은 반복문 또는 재귀 함수

- 조건이나 논리 구조를 잘못 구성하여 종료할 수 없게 되는 경우 시스템 자원을 끊임없이 사용하

인한 서비스 또는 시스템 장애 발생

필기 정리

'2020 정보처리기사 > 5과목 : 정보시스템 구축 관리' 카테고리의 다른 글

2020 정보처리기사 필기 - 5.4 시스템 보안 구축 (4)	2020.04.19
2020 정보처리기사 필기 - 5.3 소프트웨어 개발 보안 구축(2) (0)	2020.04.17
2020 정보처리기사 필기 - 5.3 소프트웨어 개발 보안 구축(1) (0)	2020.04.17
2020 정보처리기사 필기 - 5.2 IT 프로젝트 정보 시스템 구축 관리(3) (0)	2020.04.17
2020 정보처리기사 필기 - 5.2 IT 프로젝트 정보 시스템 구축 관리(2) (0)	2020.04.17
2020 정보처리기사 필기 - 5.2 IT 프로젝트 정보 시스템 구축 관리(1) (0)	2020.04.17

1D1C 구독하기

SECRET WRITE

PREV 1 2 3 4 5 6 7 8 NEXT

Recent posts