9장 소프트웨어 개발 보안 구축

109 Secure SDLC

- 보안상 안전한 소프트웨어를 개발하기 위해 SDLC에 보안강화를 위한 프로세스를 포함하 것

대표적 방법론 CLASP / SDL / Seven Touchpoints

단계별 보안 활동

요구사항 분석 단계 -> 설계 단계 -> 구현 단계 -> 테스트 단계 -> 유지보수단계

소프트웨어 개발 보안 요소 – 기밀성 / 무결성 / 가용성 / 인증 / 부인 방지

시큐어 코딩 – 구현 단계에서 발생할 수 있는 보안 취약점들을 최소화하기 위해 보안 요소들을 고려하며 코딩하는 것

110 입력 데이터 검증 및 표현

- 입력 데이터로 인해 발생하는 문제들을 예방하기 위해 구현 단계에서 검증해야 하는 보안 점검 항목들

입력 데이터 검증 및 표현의 보안 약점

SQL 삽입 / 경로 조작 및 자원 삽입 / 크로스사이트스크립팅 / 운영체제 명령어 삽입 / 위험한 형식 파일 업로드 / 신뢰되지 않는 URL 주소로 자동접속 연결 / 메모리 버퍼 오버플로

111 보안기능

- 소프트웨어 개발의 구현 단계에서 코딩하는 기능인 인증, 접근제어, 기밀성, 암호화 등을 올바르게 구현하기 위한 보안 점검 항목들

보안 기능의 보안 약점

적절한 인증없이 중요 기능 허용 / 부적절한 인가 / 중요한 자원에 대한 잘못된 권한 설정 / 취약한 암호화 알고리즘 사용 / 중요정보 평문 저장 및 전송 / 하드코드 된 암호화 키

112 코드 오류

- 개발자들이 코딩 중 실수하기 쉬운 형 변환, 자원 반환 등의 오류를 예방하기 위한 보안 점검 항목들

코드 오류의 보안 약점

널 포인터 역참조 / 부적절한 자원 해제 / 해제된 자원 사용 / 초기화되지 않은 변수 사용

스택 가드 – 주소가 저장되는 스택에서 발생하는 보안 약점을 막는 기술

113 캡슐화

- 정보 은닉이 필요한 중요한 데이터와 기능을 불완전하게 캡슐화하거나 잘못 사용함으로써 발생할 수 있는 문제를 예방하기 위한 보안 점검 항목들

캡슐화의 보안 약점

잘못된 세션에 의한 정보 노출 / 제거되지 않고 남은 디보그 코드 / 시스템 데이터 정보 노출 / Public 메소드로부터 반환된private 배열 / Private 배열에 public 데이터 할당

접근 제어자 – 외부로부터의 접근을 제한하기 위해 사용되는 예약어

114 암호 알고리즘

- 중요 정보를 보호하기 위해 평문을 암호화된 문장으로 만드는 절차 또는 방법

개인키 암호화 기법 – 동일한 키로 데이터를 암호화하고 복호화하는 암호화 기법

스트림 암호화 방식 / 블록 암호화 방식

공개키 암호화 기법 – 데이터를 암호화할 때 사용하는 공개키는 사용자에게 공개하고 비밀키는 관리자가 비밀리에 관리하는 암호화 기법

양방향 알고리즘 종류 – SEED / ARIA / DES / AES / RSA / IDEA / Skipjack / TKIP

해시 – 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환하는 것

SHA 시리즈 / MD5 / N-NASH / SNEFRU

115 서비스 공격 유형

서비스 거부 공격 – 대량의 데이터를 한 곳의 서버에 집중적으로 전송함으로써 서버의 정상적인 기능을 방해하는 것

Ping of Death – 패킷의 크기를 인터넷 프로토콜 허용 범위 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격 방법

스머핑 – IP나 ICMP의 특성을 악용하여 엄청난 양의 데이터를 한 사이트에 집중적으로 보냄으로써 네트워크를 불능 상태로 만드는 공격 방법

SYB Flooding – 3-way-handshake과정을 의도적으로 중단시킴으로써 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하도록 공격하는 방법

TearDrop – Offset 값을 변경시켜 수신 측에서 과부하를 발생시킴으로써 시스템이 다운되도록 하는 공격 방법

LAND Attack – 패킷을 전송할 때 송신 IP 주소와 수신 IP 주소를 모두 공격 대상의 IP 주소로 하여 자신에 대해 무한히 응답하게 하는 공격

DDOS – 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 서비스거부 공격을 수행하는 것

Trin00 / TFN / TFN2K / Stacheldraht

116 서버 인증

보안 서버 – 개인정보를 암호화하여 송신, 수신할 수 있는 기능을 갖춘 서버

인증 – 로그인을 요청한 사용자의 정보를 확인하고 접근 권한을 검증하는 보안 절차

지식 기반 인증 – 사용자가 기억하고 있는 정보를 기반으로 인증을 수행하는 것

고정된 패스워드 / 패스 프레이즈 / 아이핀

소유 기반 인증 – 사용자가 소유하고 있는 것을 기반으로 인증을 수행하는 것

신분증 / 메모리 카드 / 스마트 카드 / OTP

생체 기반 인증 – 사용자의 고유한 생체 정보를 기반으로 인증을 수행하는 것

행위 기반 인증 – 사용자의 행동 정보를 이용해 인증 수행

위치 기반 인증 – 인증을 시도하는 위치의 적절성 확인

117 보안 솔루션

- 외부로부터 불법적인 침입을 막는 기술 및 시스템

방화벽 – 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용, 거부, 수정하는 기능을 가진 침입 차단 시스템

침입 탐지 시스템 – 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 드응ㄹ 실시간으로 탐지하는 시스템

오용 탐지 / 이상 탐지

침입 방지 시스템 – 비정상적인 트래픽을 능동적으로 차단하고 격리하는 보안 솔루션

데이터 유출 방지 – 내부 정보의 외부 유출을 방지하는 보안 솔루션

웹 방화벽 – 웹 기반 공격을 방어할 목적으로 만들어진 웹 서버에 특화된 방화벽

VPN – 공중 네트워크와 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션

NAC – 네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록한 후 일관된 보안 관리 기능을 제공하는 보안 솔루션

SIEM – 로그 및 보안 이벤트를 통합하여 관리하는 보안 솔루션

118 데이터 입력 출력

- 키보드로부터 데이터를 입력받아 화면이나 파일로 출력하는 것

C언어 – scanf, printf

Java – scanner, nextint, print, printf, println

119 제어문

- 서술된 순서에 따라 무조건 위에서 아래로 실행되는 프로그램의 순서를 변경할 때 사용하는 명령문

배열, If, Switch, For, While