1. 소프트웨어 개발 보안 설계

* 소프트웨어 개발 보안 설계

1. SW 개발 보안의 개념

소스 코드 등에 존재하는 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 일련의 보안 활동을 말한다

요구사항 명세 -> 설계 -> 구현 -> 테스트 -> 유지 보수

1. SW 개발 보안의 구성요소

정보보안의 세 가지 요소인 기밀성, 무결성, 가용성을 지키고 서버 취약점을 사전에 방지하여 위협으로부터 위험을 최소화 하는 구축 방법

1. SW 개발 보안의 3대 요소

* 기밀성 : 인가되지 않은 개인 혹은 시스템 접근에 따른 정보 공개 및 노출을 차단하는 특성, 인가된 사용자에 대해서만 자원 접근이 가능해야 하는 특성
* 무결성 : 정당한 방법을 따르지 않고선 데이터가 변경될 수 없으며, 데이터의 정확성 및 완전성과 고의/악의로 변경되거나 훼손 또는 파괴되지 않음을 보장하는 특성, 인가된 사용자에 대해서만 자원 수정이 가능하며 전송 중인 정보는 수정되지 않아야함
* 가용성 : 권한을 가진 사용자나 애플리케이션이 원하는 서비스를 지속 사용할 수 있도록 보장하는 특성, 인가된 사용자는 가지고 있는 권한 범위 내에서 언제든 자원 접근이 가능해야 하는 특성

1. SW 개발 보안 용어

* 자산 : 조직의 데이터 또는 조직의 소유자가 가치를 부여한 대상
* 위협 : 조직이나 기업의 자산에 악영향을 끼칠 수 있는 사건이나 행위
* 취약점 : 위협이 발생하기 위한 사전 조건으로 시스템의 정보 보증을 낮추는데 사용되는 약점
* 위험 : 위협이 취약점을 이용하여 조직의 자산 손실 피해를 가져올 가능성

1. SW 개발 보안을 위한 공격기법의 이해
2. DoS 공격

* 개념

시스템을 악의적으로 공격해서 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격

특정 서버에 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나 서버의 TCP 연결을 소진 시키는 등의 공격이다

* 종류

SYN 플러딩 : TCP 프로토콜의 구조적인 문제를 이용한 공격, 서버의 동시 가용 사용자 수를 SYN 패킷만 보내 점유하여 다른 사용자가 서버를 사용 불가능하게 하는 공격

UDP 플러딩 : 대량의 UDP 패킷을 만들어 임의의 포트 번호로 전송하여 응답 메시지 ICMP 를 생성하게 하여 지속해서 자원을 고갈 시키는 공격

스머프 / 스머핑 : 출발지 주소를 공격 대상의 IP로 설정하여 네트워크 전체에게 ICMP Echo 패킷을 직접 브로드캐스팅하여 마비시키는 공격

죽음의 핑 : ICPM 패킷을 정상적인 크기보다 아주 크게 만들어 전송하면 다수의 IP 단편화가 발생하고, 수신 측에서는 단편화된 패킷을 처리 하는 과정에서 많은 부하가 발생하거나, 재조합 버퍼의 오버플로가 발생하여 정상적인 서비스를 하지 못하도록 하는 공격 기법

랜드 어택 : 출발지 IP 와 목적지 IP 를 같은 패킷 주소로 만들어 보냄으로써 수신자가 자기 자신에게 응답을 보내게 하여 시스템의 가용성을 침해하는 공격기법

티어 드롭 : IP 패킷의 재조합 과정에서 잘못된 Fragment Offset 정보로 인해 수신시스템이 문제를 발생하도록 만드는 DoS 공격

공격자는 IP Fragment Offset 값을 서로 중첩되도록 조작하여 전송하고, 이를 수신한 시스템이 재조합하는 과정에서 오류가 발생, 시스템의 기능을 마비시키는 공격 방식

봉크 : 패킷을 분할하여 보낼 때 처음 패킷을 1번으로 보낸 후 다음 패킷을 보낼 때도 순서번호를 모두 1번으로 조작하여 전송하는 DoS 공격

보잉크 : 처음 패킷을 1번으로 보낸 후 다음 패킷을 100번, 다음 패킷을 200번, 20번째 패킷을 2002번, 21번째 패킷을 100번, 22번째 패킷을 다시 2002번 등으로 중간에 패킷 시퀀스 번호를 비정상적인 상태로 보내서 부하를 일으키게 하는 공격 기법

1. DDoS 공격
2. DRDoS 공격
3. 세션 하이재킹
4. 애플리케이션 공격
5. 네트워크 공격
6. 시스템 보안 위협