[정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

1. 다음은 무엇에 대한 설명인가?

SW개발과정에서 개발자의 실수, 논리적 오류 등으로 인해 발생될 수 있는 보안 취약점, 보안 약점들을 최소화하여 사이버 보안위협에 대응할 수 있는 안전한 SW를 개발하기 위한 일련의 보안활동을 의미한다. 목적은 각 단계별로 요구되는 보안활동을 수행함으로써 안전한 소프트웨어를 만들 수 있도록 한다.

① Secure Coding Guide
② Secure Software
③ Secure SDLC
④ Secure Algorithm

[기출 예상 문제]

2. 다음 중 MS-SDL(MicroSoft-Secure Development Lifecycle)의 7단계 절차에 속하지 않는 것은?

① 교육 ② 설계
③ 대응 ④ 수정

[기출 예상 문제]

3. 다음 중 소프트웨어 개발 보안 생명주기(Secure SDLC) 방법론 유형 중 Seven Touchpoints에 대한 설명으로 가장 적절한 것은?

① 5개의 보안강화 활동을 정의한다.
② 실무적으로 검증된 개발 보안 방법론 중 하나이다.
③ 소프트웨어 개발 생명주기 초기단계에 보안강화를 목적으로 한다.
④ 보안강화 활동에 교육, 설계, 운영이 포함된다.

[기출 예상 문제]

4. 다음 중 CLASP(Comprehensive, Lightweight Application Security Process)의 5가지 관점에 포함되지 않는 것은?

① 역할 기반 관점 ② 취약성 관점
③ 유지보수 관점 ④ 개념 관점

[기출 예상 문제]

5. SW결함의 한 종류로 보안 취약점을 유발하는 원인을 의미하는 용어로 가장 적절한 것은?

① 보안약점 ② 보안문제
③ 보안원인 ④ 보안결함

[정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

6. 주요 보안 항목에 대한 설명으로 가장 거리가 먼 것은?

① 기밀성(Confidentiality)은 인가된 사용자만 정보 자산에 접근할 수 있는 것이다.
② 가용성(Availability)은 정보 자산에 대해 적절한 시간에 접근 가능한 것을 의미한다.
③ 부인 방지(non-repudiation)는 시스템이 각 사용자를 정확히 식별하고자 할 때 사용하는 방법이다.
④ 무결성(Integrity)은 적절한 권한을 가진 사용자에 의해 인가된 방법으로만 정보를 변경할 수 있도록 하는 것이다.

[기출 예상 문제]

7. 다음은 무엇에 대한 설명인가?

서버로 요청하는 쿼리를 임의로 조작하여 실행하게 하는 공격으로 피해자의 권한을 이용하여 공격도 가능하다. 피해자의 권한을 이용하여 피해자가 조작된 패킷을 전송하고 이 결과로 공격자가 이득을 얻는 형태의 공격이다. 예로는 홈페이지 자동 가입이 있다.

① 크로스사이트 요청 위조(CSRF)
② SQL 삽입(SQL Injection)
③ 크로스사이트크립트(XSS)
④ 분산 서비스 거부 공격(DDoS)

[기출 예상 문제]

8. 다음 중 프로그램 입력 값에 대한 부적절한 검증 등으로 인해 발생할 수 있는 보악 약점의 예시로 가장 거리가 먼 것은?

① SQL 삽입
② 크로스사이트스크립트
③ 스니핑
④ 자원 삽입

[기출 예상 문제]

9. 다음 중 크로스사이트스크립트(XSS)를 해결하기 위한 방법으로 가장 적절한 것은?

① 입력 데이터에 예약어 및 특수문자가 입력되지 않게 필터링한다.
② HTML 태그 사용을 제한한다.
③ 업로드 되는 파일의 확장자를 제한한다.
④ 경로 조작에 사용될 수 있는 문자를 필터링한다.

[기출 예상 문제]

10. SW가 실행환경, 사용자, 관련 데이터에 대한 민감한 정보를 포함하는 오류메시지를 보여줌으로써 공격자의 악성 행위를 도와줄 수 있는 보안약점을 의미하는 용어로 가장 적절한 것은?

① 사용자 중요 정보 평문 전송
② 하드코드로 되어있는 패스워드
③ 불충분한 세션관리
④ 오류 메시지를 통한 정보 노출

[정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

11. 다음은 무엇에 대한 설명인가?

웹 서버에 명령을 실행하여 관리자 권한을 획득해 행하는 공격 방법이다. 파일 업로드 취약점을 이용하며 서버 명령을 실행할 수 있는 asp, cgi, php, jsp 등이 있다.

① SQL 삽입(SQL Injection)
② 웹셸 공격(Webshell Attack)
③ 크로스사이트크립트(XSS)
④ 랜섬웨어(Ransomware)

[정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

1. 다음 중 블록 암호화 방식에 대한 설명으로 가장 거리가 먼 것은?

① 블록 암호화 방식 종류에는 DES, AES, SEED가 있다.
② 한 번에 하나씩 데이터 블록을 암호화하는 방식이다.
③ 비트/바이트/단어들을 순차적으로 암호화한다.
④ 현재의 출력 블록은 현재의 입력 블록에만 영향을 받는 방식의 알고리즘이다.

[기출 예상 문제]

2. 다음은 무엇에 대한 설명인가?

2001년 미군 표준 기술 연구소(NIST)에서 발표한 개인키 암호화 알고리즘이다. 128, 192, 256비트의 암호/복호키를 이용하여 128비트의 평문(블록)을 암호화, 복호화하는 방식이다.

① DES ② SEED
③ AES ④ RSA

[기출 예상 문제]

3. 다음 중 서로 다른 키를 사용하는 비대칭 암호화 방식으로 보안 수준이 높지만 속도가 느리고 알고리즘이 복잡한 특징을 가진 암호화 알고리즘은?

① AES ② SHA-256
③ RSA ④ DES

[기출 예상 문제]

4. 다음 중 코드 오류의 형태에 대한 설명으로 가장 거리가 먼 것은?

① 랜덤 에러: 입력시 한 자리를 더 추가하여 기록한 에러
② 이중 에러: 전위에러가 2개 이상 발생한 에러
③ 전위 에러: 입력시 좌우자리가 바뀌어 발생한 에러
④ 생략 에러: 입력시 한 자리를 더 빠뜨리고 기록한 에러

[기출 예상 문제]

5. 데이터항목의 지정된 범위(최소치와 최대치)를 검사하는 오류 검출 방법으로 가장 적절한 것은?

① 공란 검사 ② 유효 범위 검사
③ 대조 검사 ④ 균형 검사

[정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

6. 오류 검출 방법에 대한 설명으로 가장 거리가 먼 것은?

① 순차 검사: 입력데이터 코드가 중복되어 있는지를 검사한다.
② 크기 검사: 데이터 필드에 나타난 문자의 개수가 정확한가를 검사한다.
③ 코드 검사: 패리티 검사에 의해서 코드의 오류를 검사한다.
④ 타당성 검사: 수신한 데이터를 송신측에 되돌려 보내서 원래의 데이터와 비교하여 오류를 검사한다.

[기출 예상 문제]

7. 코드오류 보안약점에 대한 설명으로 가장 거리가 먼 것은?

① Null Pointer 역참조: Null로 설정되지 않은 모든 변수의 주소값을 참조했을 때 발생하는 보안약점
② 부적절한 자원 해제: 사용된 자원을 적절히 해제하지 않아 새로운 입력을 처리할 수 없게 되는 보안약점
③ 해제된 자원 사용: 해제된 자원을 참조하여 예기치않은 오류가 발생될 수 있는 보안약점
④ 초기화되지 않은 변수 사용: 변수를 초기화하지 않고 사용하여 예기치 않은 오류가 발생될 수 있는 보안약점

[기출 예상 문제]

8. 다음 설명의 (ㄱ)에 들어갈 용어로 가장 적절한 것은?

> 보안약점 중 (ㄱ)은(는) 중요한 데이터 또는 기능성을 불충분하게 (ㄱ)하였을 때 인가되지 않는 사용자에게 데이터 누출이 가능해지는 보안약점이다. 예를 들어 제거되지 않고 남은 디버거 코드, 시스템 데이터 정보 노출, Private 배열에 Public 데이터 할당 등이 있다.

① 추상화 ② 클래싱
③ 캡슐화 ④ 패키징

[기출 예상 문제]

9. 다음 중 보안약점의 종류 중 캡슐화와 관련된 예시가 아닌 것은?

① 잘못된 세션에 의한 데이터 정보 노출
② 초기화되지 않은 변수 사용
③ 제거되지 않고 남은 디버그 코드
④ Private 배열에 Public 데이터 할당

[정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

10. 다음은 무엇에 대한 설명인가?

DNS 요청에 대한 변조 공격을 수행하는 방식으로 피해자는 정확한 URL을 요청했음에도 다른 IP를 응답 값으로 받게 된다.

① DNS Spoofing 공격
② 악성코드를 이용한 파밍 공격
③ SQL 삽입공격
④ ARP Sniffing 공격

[기출 예상 문제]

11. 다음 중 API 오용과 관련된 예시로 가장 적절한 것은?

① Public 메소드부터 반환된 Private 배열
② DNS Lookup에 의존한 보안 결정
③ Null Pointer 역참조
④ 잘못된 세션에 의한 데이터 정보 노출

[정답] [정보시스템 구축관리>소프트웨어 개발 보안 구축]

1. SW개발 보안 설계

1	2	3	4	5	6	7	8	9	10	11									
3	4	2	3	1	3	1	3	2	4	2									

2. SW개발 보안 구현

1	2	3	4	5	6	7	8	9	10	11									
3	3	3	1	2	4	1	3	2	1	2									

[정답 및 해설] [정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 설계]

SW개발 보안 설계 1. ③

소프트웨어 개발 보안 생명주기(Secure SDLC)에 대한 설명이다.

SW개발 보안 설계 2. ④

MS-SDL 절차
- 교육(Training)
- 계획·분석(Requirement)
- 설계(Design)
- 구현(Implementation)
- 시험·검증(Verification)
- 배포·운영(Release)
- 대응(Response)

SW개발 보안 설계 3. ②

① 7개의 보안강화 활동을 정의한다.
③ CLASP에 대한 설명이다.
④ MS-SDL에 대한 설명이다.

SW개발 보안 설계 4. ③

CLASP는 개념, 역할 기반, 활동 평가, 활동 구현, 취약성의 5가지 관점에 따라 개발보안 프로세스를 수행할 것을 제안한다.

SW개발 보안 설계 5. ①

보안 약점(Weakness)에 대한 설명이다.

SW개발 보안 설계 6. ③

③ 인증(Authentication)에 대한 설명이다.
- 부인 방지(non-repudiation)
: 메시지의 송수신이나 교환 후, 또는 통신이나 처리가 실행된 후에 그 사실을 증명함으로써 사실 부인을 방지하는 보안 기술.

SW개발 보안 설계 7. ①

크로스사이트 요청 위조(CSRF)에 대한 설명이다.

SW개발 보안 설계 8. ③

③ 스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다.

SW개발 보안 설계 9. ②

XSS는 웹페이지에 악의적인 스크립트를 포함시켜 사용자 측에서 실행되게 유도하므로, HTML 태그 사용을 제한하여, 악의적인 스크립트를 포함시키지 못하게 막는다.

[정답 및 해설] [정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 설계]

SW개발 보안 설계 10. ④

오류 메시지를 통한 정보 노출에 대한 설명이다.

SW개발 보안 설계 11. ②

웹셸 공격(Webshell Attack)에 대한 설명이다.

[정답 및 해설] [정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 구현]

SW개발 보안 구현 1. ③

③ 스트림 암호화 방식에 대한 설명이다.

SW개발 보안 구현 2. ③

AES(Advanced Encryption Standard)에 대한 설명이다.

SW개발 보안 구현 3. ③

공개키(Public) 암호화 방식에 대한 설명으로 대표적인 알고리즘에는 RSA가 있다.

SW개발 보안 구현 4. ①

① 추가 에러에 대한 설명이다.
- 랜덤 에러: 에러가 두 가지 이상 결합되어 발생한 에러(일정한 규칙 없이 발생)

SW개발 보안 구현 5. ②

유효 범위 검사(range check)에 대한 설명이다.

SW개발 보안 구현 6. ④

④ 반향 검사(echo check)에 대한 설명이다.
- 타당성 검사(feasibility check): 어떤 규정된 제한 내에 데이터가 들어 있는 것을 논리적인 측면에서 확인하는 검사.

SW개발 보안 구현 7. ①

① Null Pointer 역참조: Null로 설정된 변수의 주소값을 참조했을 때 발생하는 보안약점

SW개발 보안 구현 8. ③

캡슐화에 대한 설명이다.

SW개발 보안 구현 9. ②

② 코드오류에 대한 예시이다.
* 보안약점 중 캡슐화 예시
- 잘못된 세션에 의한 데이터 정보노출
- 제거되지 않고 남은 디버그 코드
- 시스템 데이터 정보 노출
- Public 메소드부터 반환된 Private 배열
- Private 배열에 Public 데이터 할당

[정답 및 해설] [정보시스템 구축관리>소프트웨어 개발 보안 구축>SW개발 보안 구현]

SW개발 보안 구현 10. ①

DNS Spoofing 공격에 대한 설명이다.

SW개발 보안 구현 11. ②

① 캡슐화에 관련된 예시이다.
③ 코드오류에 관련된 예시이다.
④ 캡슐화에 관련된 예시이다.
* 보안 약점 중 API 오용 예시
- DNS Lookup에 의존한 보안결정
- 취약한 API 사용