[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

1. SW 개발 보안의 세 가지 요소를 쓰시오.

답:

[기출 예상 문제]

2. SW 개발 보안 항목에 대한 설명이다. ( )안에 들어갈 가장 적합한 보안 항목을 쓰시오.

보안 항목	설명
(①)	적절한 권한을 가진 사용자에 의해 인가된 방법으로만 정보를 변경할 수 있다.
(②)	시스템이 각 사용자를 정확히 식별하고자 할 때 사용한다.
(③)	정보 자산에 대해 적절한 시간에 접근 가능하다.
(④)	메시지의 송수신 사실을 부인할 수 없도록 송수신 증거를 제공한다.
(⑤)	인가된 사용자만 정보 자산에 접근할 수 있다.

답 ① ②
③ ④
⑤

[기출 예상 문제]

3. SW 개발 보안과 관련된 용어에 대한 설명이다. ( )안에 들어갈 가장 적합한 용어를 고르시오.

용어	설명
(①)	조직 자산의 파괴와 손해가 발생하는 행동을 할 수 있는 내·외부의 주체
(②)	위협이 발생하기 위한 사전 조건에 따른 상황
(③)	조직의 데이터 또는 조직의 소유자가 가치를 부여한 대상
(④)	위협원이 취약점을 사용하여 위협 행동하여 자신에 나쁜 영향의 결과를 가져올 확률과 영향도
(⑤)	조직의 자산에 대한 위협이 되는 위협원의 공격 행동

(ㄱ) 위험(Risk) (ㄴ) 위협(Threat)
(ㄷ) 자산(Asset) (ㄹ) 취약점(Vulnerability)
(ㅁ) 위협원(Threat agents)

답 ① ②
③ ④
⑤

[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

4. 소프트웨어 개발 보안 관련 기관 중 두 가지만 쓰시오.

답:

[기출 예상 문제]

5. 소프트웨어 개발 보안 관련 기관의 역할에 대한 설명이다. ( )안에 들어갈 가장 적합한 관련 기관을 쓰시오.

용어	설명
(①)	- SW 개발 보안 정책 총괄 - SW 개발 보안 가이드 공지
(②)	- SW 개발 보안 정책 및 가이드 개발 - SW 개발 보안 교육과정 운영
(③)	- SW 개발 보안 계획 수립 - SW 개발 보안 역량을 갖춘 사업자 또는 감리법인 선정
(④)	- SW 개발 보안 가이드를 참조하여 개발 - SW 보안 약점 관련 시정요구 이행
(⑤)	- 감리계획 수립 및 협의 - SW 보안약점 제거여부 진단 및 조치결과 확인

답 ①　　②
③　　④
⑤

[기출 예상 문제]

6. SecureSDLC에서 주요 보안 활동에 대한 설명이다. ( )안에 들어갈 가장 적합한 단계를 쓰시오.

단계	설명
(①) 단계	보안 사고를 식별하고, 사고 발생 시 이를 해결하고 보안 패치를 실시
(②) 단계	식별된 보안 요구사항을 소프트웨어 설계서에 반영하고 보안 설계서 작성
(③) 단계	보안 항목에 해당하는 요구사항을 식별
(④) 단계	표준 코딩 정의서 및 SW 개발 보안 가이드를 준수하며 구현
(⑤) 단계	보안 설계서를 바탕으로 보안 사항들이 정확히 반영되고 동작하는지 점검

답 ①　　②
③　　④
⑤

[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

7. 설명 중 ( )안에 들어갈 가장 적합한 용어를 쓰시오.

(①)은/는 소프트웨어 개발 과정에서 발생할 수 있는 보안 취약점을 최소화하여 보안 위협으로부터 안전한 소프트웨어를 개발하기 위한 일련의 보안 활동을 의미한다. (①)은/는 데이터의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 유지하는 것을 목표로 한다.
(②)은/는 보안상 안전한 소프트웨어를 개발하기 위해 소프트웨어 개발의 모든 과정에 보안 강화 프로세스를 포함한 것을 의미한다. (②)은/는 요구사항 분석, 설계, 구현, 테스트, 유지 보수 등 SDLC 전체 단계에 걸쳐 수행되어야 할 보안 활동을 제시한다. 대표적인 방법론에는 MS-SDL, Seven Touchpoints, CLASP 등이 있다.

답 ①
②

[기출 예상 문제]

8. 현재 시스템에서 처리하는 정보 중 중요정보로 분류되어 있는 정보의 대부분은 개인정보이다. 개인정보보호 관련 법규 중 3가지만 쓰시오.

답:

[기출 예상 문제]

9. 다음 중 특정IT 기술관련 규정에 대한 설명이다.( ) 안에 들어갈 가장 적합한 규정을 고르시오.

단계	설명
(①)	개인 바이오정보의 보호와 안전한 활용을 위한 원칙 및 조치사항
(②)	개인 위치정보의 유출 및 오남용을 방지하기 위한 법률
(③)	뉴미디어 서비스 이용 및 제공 시 개인 정보의 침해사고를 예방하기 위한 준수사항
(④)	RFID 시스템의 이용자들의 프라이버시를 보호하고 안전한 RFID 이용 환경을 조성하기 위한 가이드라인

(ㄱ) RFID 프라이버시 보호 가이드 라인
(ㄴ) 바이오 정보 보호 가이드 라인
(ㄷ) 뉴미디어 서비스 개인정보보호 가이드라인
(ㄹ) 위치정보의 보호 및 이용 등에 관한 법률

답 ①
②
③
④

[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]
10. 설명 중 ( )안에 공통적으로 들어갈 가장 적합한 용어를 쓰시오.

시스템이 처리하는 정보들 중 법적 의무사항으로 필수적인 안전조치를 해야 하는 정보들 이외에도 물리적, 기술적 접근 허용범위와 정보유출 시 예상되는 피해를 기준으로 ( )을/를 결정하거나, 정보의 자산가치를 기준으로 중요정보를 식별하고 법적 의무 사항에 준하는 보안 강도를 적용하여 정보가 처리될 수 있도록 설계되어야 한다. 아래는 정보의 ( ) 예시이다.
- 1등급: 그 자체로 개인 식별이 가능하거나, 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격히 제한된 개인정보, 유출 시 범죄에 직접적으로 이용 가능한 정보
- 2등급: 조합되면 명확히 개인의 식별이 가능한 개인정보, 유출 시 법적 책임 부담 가능한 정보
- 3등급: 개인정보와 결합하여 부가적인 정보 제공 가능 정보, 제한적인 분야에서 불법적 이용 가능 정보

답:

[기출 예상 문제]
11. 구현 단계에서 발생할 수 있는 보안 취약점들을 최소화하고, 외부 공격으로부터 안전한 소프트웨어를 개발하는 기법을 의미하는 용어를 쓰시오.

답:

[기출 예상 문제]
12. SW 개발 보안 요구공학 프로세스에 대한 설명이다. 설명 중 ( )안에 들어갈 가장 적합한 용어를 쓰시오.

SW 개발 보안요구 공학은 크게 (①)와/과 (②)로 나눠진다. (①)은/는 요구사항 도출, 요구사항 분석, 요구사항 명세, 요구사항 확인과 검증 단계로 구성되어 있고, (②)은 비즈니스 환경 변화 또는 시간의 흐름에 따라 서버 보안요구사항은 변경될 수 있으므로 서버 보안요구사항을 지속적으로 갱신하는 것을 의미한다.

답:

[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

13. 소프트웨어 개발보안 요구사항 개발에 대한 설명이다. ( )안에 들어갈 가장 적합한 단계을 쓰시오.

단계	설명
(①)	관계자들에게 요구사항이 맞는지 확인하고 검증하는 과정으로, 소프트웨어 개발보안요구사항 문제 보고서를 작성한다.
(②)	보안요구사항 분석서를 통하여 소프트웨어 개발 시스템의 목표 기술과 사업의 기능과 비기능적 요구사항을 명세화 시킨다.
(③)	보안요구사항을 내용별로 분류된 것을 토대로 분석하여 보안요구사항의 제약조건을 판별한다.
(④)	조직의 이해관계자의 상호의견을 조율하고, 협의를 통해 요구사항을 수집하고 수집된 요구사항을 정제하고 내용 별로 분류한다.

답 ① 소프트웨어 개발보안의 ( )
② 소프트웨어 개발보안의 ( )
③ 소프트웨어 개발보안의 ( )
④ 소프트웨어 개발보안의 ( )

[기출 예상 문제]

14. 설명 중 ( )안에 들어갈 가장 적합한 용어를 쓰시오.

서버 보안요구사항 관리는 이해관계자 간의 협상을 통해 기준을 정하고 상부의 정식 승인을 받아 변경을 수행해야 한다. 아무런 승인없이 서버 보안요구사항을 변경하게 되면 시간이 지나 이력을 알 수 없기 때문에 관리를 철저하게 하고 서버 보안요구사항 명세서와 아래의 서버 보안요구사항 ( )를 통해 산출물과 테스트 시나리오 등을 관리하도록한다.

<보안 요구사항 ( )>

보안 요구사항 ( )								
프로젝트 이름								
담당자								
프로젝트 설명								
ID	하부ID	요구사항 설명	비즈니스요구, 기획, 목적, 목표	프로젝트 목표	WBS인도물	보안설계	보안개발	시험사례
1.0	1.0							
	1.1							
	1.2							
	1.2.1							
2.0	2.0							
	2.1							
	2.2							
	2.1.1							
3.0	3.0							
	3.1							
	3.2							
	3.2.1							
4.0	4.0							
5.0	5.0							

답:

[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

15. SW개발보안 요구사항 명세와 설계에 대한 설명이다. ( )안에 들어갈 가장 적합한 내용을 고르시오.

* SW개발보안 요구사항 명세와 설계 수행 순서
1. 정보에 대한 보안항목을 환경 분석에 따라 법률적으로 검토한다.
: 소프트웨어 개발에 대한 보안항목의 식별을 위해 내·외부 환경 분석을 통하여 보안항목을 분석한다. 또 소프트웨어의 목적에 맞게 소프트웨어가 처리하는 정보의 분류를 조직 정보의 자산 가치에 따라 기타 중요 정보를 식별한다.
2. 보안항목의 요구사항을 수집한다.
1) (①)
: 보안 법률검토에 의한 보안의 목적과 목표 설정 이행 시스템에 대한 정확한 정보를 식별하여 보안요구사항을 분석할 수 있도록 파악한다.
2) (②)
: 보안 설계서의 작업 준비로 보안 환경에 대한 자료 수집과 자료 정리에 따라 작업을 할당하고 역할과 책임을 분류한다. 그 이후 작업 실시에 따른 일정별 작업 계획을 수립하고, 보안 환경 구축에 필요한 과업별 작업 카드 작성 및 기록과 보고체계를 구축한다.
3) (③)
: 보안 환경의 요구사항 수집과 현행 시스템의 목표를 바탕으로 보안 환경의 구축을 위해 구체적으로 필요한 적합한 환경 기술, 인력과 인력의 기술수준, 조직의 보안 성숙도를 기반으로 스펙(spec)을 기술하고 검토한다.

(ㄱ) 보안 환경의 적용 기술을 검토한다.
(ㄴ) 보안관련 법률검토 요구사항에 의한 개발 환경의 계획과 통제에 관한 정보를 식별한다.
(ㄷ) 소프트웨어 개발 PM(project manager)은 보안 요구사항을 분석하여 수행 계획을 수립한다.

답 ①
②
③

[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

16. 취약점 진단을 위한 하드웨어 환경 구성에 대한 설명이다. ( )안에 들어갈 가장 적합한 하드웨어를 고르시오.

하드웨어	설명
(①)	서버와 클라이언트를 연결해주는 연결망으로 기업 내부에서는 근거리 유선망(LAN, Local Area Network)로 구성된다.
(②)	취약점 진단을 수행하기 위해 필요한 CPU, 메모리 등 각종 하드웨어가 장착된 서버이다.
(③)	취약점 진단을 수행하기 위해 필요한 데이터를 담아두는 저장 공간으로 이러한 데이터를 취약점 진단 데이터라고 한다.

(ㄱ) 진단 서버 (ㄴ) 스토리지
(ㄷ) 네트워크

답 ①
②
③

[기출 예상 문제]

17. 다음 중 보안성이 강화된 응용프로그램 구현을 위한 환경 구축에서의 보안취약점 환경구축 기능과 취약점 모니터링 환경 기능을 분류하시오.

(ㄱ) 보안 취약점 진단 진행 중 환경에 대한 모니터링 정보를 저장
(ㄴ) 대상 시스템을 테스트 환경에 배포
(ㄷ) 보안 취약점 진단하는 환경 설정 정보를 문서화 명세 관리
(ㄹ) 보안 취약점 진단 진행 중 보안 취약점 진단 환경 인프라와 대상 시스템에 대한 모니터링 수행
(ㅁ) 보안 취약점 점검에 필요한 진단도구와 모니터링 툴을 설치 관리

답 ① 보안취약점 환경구축 기능:
② 취약점 모니터링 환경 기능:

[소프트웨어 개발 보안 구축>SW개발 보안 설계]

[기출 예상 문제]

18. 다음 제시된 보안성이 강화된 응용 프로그램 구현을 위한 일정 계획 수립 절차를 순서대로 나열하시오.

(ㄱ) 일정 계획을 위한 보안 전문가 선정
(ㄴ) 일정 계획을 위한 보안 범주 식별
(ㄷ) 보안성이 강화되었는지 취약점 점검과 함께 독립적인 테스트 계획을 기획
(ㄹ) 보안요구사항을 분석

답:

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]
1. 암호 알고리즘에 대한 설명이다. ( )안에 들어갈 가장 적합한 용어를 쓰시오.

(①) 암호화 기법은 동일한 키로 데이터를 암호화 하고 복호화 한다. (①) 암호화 기법은 대칭 암호 기법 또는 단일키 암호화 기법이라고도 한다. (①) 기법은 블록 암호화 방식과 스트림 암호화 방식으로 분류된다.
(②) 암호화 기법은 데이터를 암호화할 때 사용하는 공개키(Public Key)는 데이터베이스 사용자에게 공개하고, 복호화할 때의 비밀키(Secret Key)는 관리자가 비밀리에 관리한다. (②) 암호화 기법은 비대칭 암호 기법이라고도 한다.

답 ①
②

[기출 예상 문제]
2. 평문을 암호문으로 암호화하는 것은 가능하지만 암호문을 평문으로 복호화하는 것은 불가능한 단방향 암호화 기법의 종류 중 1가지만 쓰시오.

답:

[기출 예상 문제]
3. 개인키 암호화 기법은 한 번에 하나의 데이터 블록을 암호화 하는 블록 암호화 방식과 평문과 동일한 길이의 스트림을 생성하여 비트 단위로 암호화하는 스트림 암호화 방식으로 분류된다. 블록 암호화 방식과 스트림 암호화 방식의 종류 중 2가지만 쓰시오.

답 ① 블록 암호화 방식:
② 스트림 암호화 방식:

[기출 예상 문제]
4. 다음 설명에 가장 부합하는 암호화 알고리즘을 쓰시오.

1975년 미국 NBS(National Bureau of Standars, 미국 국립 표준국)에서 발표한 개인키 암호화 알고리즘으로 56비트 암호/복호키를 이용하여 64비트의 평문을 암호화, 복호화 하는 암호화 방식이다.

답:

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

5. 암호 알고리즘에 대한 설명이다. ( )안에 들어갈 가장 적합한 용어를 쓰시오.

(①)은/는 2001년 미국 표준 기술 연구소(NIST)에서 발표한 개인키 암호화 알고리즘이다. (②), 192, 256 비트의 암호/복호키를 이용하여 (②)비트의 평문을 암호화, 복호화 하는 방식이다.

답 ①
②

[기출 예상 문제]

6. 시큐어 코딩 점검 내용인 SW 보안약점 항목 중 두가지만 쓰시오.

답:

[기출 예상 문제]

7. 암호 알고리즘에 대한 설명이다. ( )안에 들어갈 가장 적합한 용어를 쓰시오.

알고리즘	설명
(①)	임의의 길이 메시지를 256 비트ㄴ의 축약된 메시지를 만들어내는 해시 알고리즘
(②)	1978년 MIT 공과 대학의 Rivest, Shamir, Adelman 등 3인이 공동 개발한 공개 키 암호화 알고리즘
(③)	국제표준화기구(ISO) 표준인 시드(SEED)와 함께 사용될 국가 표준 128bit 블록 암호화 알고리즘
(④)	1999년 한국인터넷진흥원(KISA)에서 개발한 블록 암호화 알고리즘

답 ①
②
③
④

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

8. SW 보안약점 항목에 대한 설명이다. ( )안에 들어갈 가장 적합한 항목를 쓰시오.

항목	설명
(①)	거의 동시에 수행되는 병렬 처리 시스템, 다수의 프로세스가 실행되는 환경에서 시간과 실행 상태의 부적절한 관리로 인해 발생 가능한 보안약점
(②)	인가되지 않은 사용자에게 프로그램 내부의 데이터 누출이 가능해지는 보안약점
(③)	프로그램 입력 값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식 지정 등으로 인해 발생되는 보안약점
(④)	보안기능을 적절하지 않게 구현 시 발생할 수 있는 보안약점
(⑤)	프로그램의 형(type)변환 오류 등과 같이 개발자가 범할 수 있는 개발 오류로 인해 발생되는 보안약점
(⑥)	의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점
(⑦)	에러를 처리하지 않거나, 불충분하게 처리하여 에러 정보에 중요정보가 포함될 때 발생할 수 있는 보안약점

답 ① ②
③ ④
⑤ ⑥
⑦

[기출 예상 문제]

9. 입력 데이터 검증 및 표현과 관련한 보안 약점 중 2가지만 쓰시오.

답:

[기출 예상 문제]

10. 입력 데이터 검증 및 표현과 관련한 보안 약점 중 사용자의 입력 값 등 외부 입력 값이 SQL 쿼리에 삽입되어 공격하는 보안 약점은 무엇인지 쓰시오.

답:

[기출 예상 문제]

11. 입력 데이터 검증 및 표현과 관련한 보안 약점 중 검증되지 않은 외부 입력 값에 의해 브라우저에서 악의적인 코드가 실행되는 보안 약점은 무엇인지 쓰시오.

답:

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

12. 설명 중 ( )안에 들어갈 가장 적합한 용어를 쓰시오.

> 입력 데이터 검증 및 표현과 관련한 보안 약점 중 사용자로부터 입력되는 값을 외부사이트의 주소로 사용하여 자동으로 연결하는 서버 프로그램은 피싱 공격에 노출되는 취약점이 있다. 해결 방법으로는 자동 연결할 외부 사이트의 URL과 도메인은 ( )(으)로 관리한다.

답:

[기출 예상 문제]

13. 입력 데이터 검증 및 표현과 관련한 보안 약점 중 경로 조작 및 자원 삽입은 데이터 입출력 경로를 조작하여 서버 자원을 수정/삭제할 수 있는 보안 약점이다. 다음 중 경로 조작 및 자원 삽입의 해결 방안을 고르시오.

> (ㄱ) 외부의 입력이 파일명인 경우에는 경로 순회를 수행할 수 있는 문자('/' 와 같은 기호)를 제거
> (ㄴ) SQL문에 쓰이는 예약어, 특수문자의 삽입을 제한
> (ㄷ) 입력한 문자열에서 <, >, &, 등을 replace 등의 문자 변환 함수를 사용하여 &lt, &gt, &amp, &quot로 치환

답:

[기출 예상 문제]

14. 시간 및 상태와 관련한 보안 약점 중 다수의 멀티 프로세스 상에서 인프라 자원을 체크하는 시점과 사용되는 시점이 달라서 발생하는 보안 약점은 무엇인지 쓰시오.

답:

[기출 예상 문제]

15. 시간 및 상태와 관련한 보안 약점 중 제대로 제어되지 않은 재귀함수에서 무한재귀가 발생하는 보안 약점의 예시이다. ( )안에 들어갈 가장 적합한 답을 쓰시오.

<안전하지 않은 코드>

```
int fac(n) {
    return n*fac(n-1);
}
```

<안전한 코드>

```
int fac(n) {
    if(n <= 0) (          ) 1;
    else return n * fac(n-1);
}
```

답:

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

16. 보안 기능에 관련한 보안 약점에 대한 설명이다. ( ) 안에 들어갈 가장 적합한 내용과 그 해결방안을 고르시오.

보안약점	설명
(①)	적절한 인증 없이 중요정보를 열람 또는 변경 가능한 보안약점
(②)	적절하지 못한 접근제어로 외부 입력 파라미터 값이 포함된 문자열로 서버 접근을 가능케 하는 보안약점
(③)	중요한 자원에 대한 적절하지 못한 접근 권한이 부여되어 의도치 않게 중요 정보가 노출, 수정되는 보안약점
(④)	중요한 민감성 정보의 기밀성이 취약한 암호화 알고리즘을 사용하여 정보가 노출되는 보안약점
(⑤)	프로그램이 보안과 관련된 민감한 데이터를평문으로 통신채널을 통해서 송·수신할 경우 스니핑을 통해 인가되지 않은 사용자에게 민감한 데이터가 노출될 수 있는 보안약점
(⑥)	프로그램 코드 내부에 민감한 데이터를 직접 입력한 후 내부 인증을 사용하거나 통신하는 경우 관리가 정보가 노출 될 수 있는 보안약점

(ㄱ) 부적절한 인가
(ㄴ) 사용자 중요정보 평문 저장 및 전송
(ㄷ) 중요한 자원에 대한 잘못된 권한 설정
(ㄹ) 적절한 인증 없는 중요기능 허용
(ㅁ) 하드코드된 비밀번호
(ㅂ) 취약한 암호화 알고리즘 사용

(a) 패스워드는 암호화하여 별도의 파일에 저장하여 사용한다.
(b) 중요한 정보가 있는 페이지는 재인증이 적용되도록 설계한다.
(c) 설정파일, 실행파일 등은 관리자에 의해서만 읽고 쓰기가 가능하도록 설정한다.
(d) 사용자 권한에 따른 접근 제어 리스트를 관리한다.
(e) 중요한 정보를 통신채널을 통해 전송할 때에 암호화한다.
(f) 취약하다고 알려진 암호 알고리즘 대신 검증된 알고리즘을 사용한다.

답 ① – ② –
③ – ④ –
⑤ – ⑥ –
⑦ –

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

17. 에러 처리에 관련한 보안 약점에 대한 설명이다. ( ) 안에 공통적으로 들어갈 가장 적합한 용어를 쓰시오.

에러를 처리하지 않거나, 불충분하게 처리하여 에러 정보에 중요정보가 포함될 때 발생할 수 있는 보안 약점 중 오류 상황 대응 부재는 시스템에서 발생되는 오류를 처리하지 못하여 프로그램 다운 등 의도하지 못하는 경우가 발생할 수 있는 보안 약점이다. 오류 상황 대응 부재의 해결 방안으로는 오류가 발생할 수 있는 부분에 대하여 제어문을 사용하여 적절하게 ( ) 을/를 해야 한다. 다만, 적절하지 않은 ( )을/를 할 경우 의도하지 않은 상황이 발생 될 수 있으므로 충분한 검사와 광범위한 ( ) 대신 구체적인 ( ) 수행하도록 한다.

답:

[기출 예상 문제]

18. 아래의 C언어를 실행하였을 때 발생할 수 있는 가장 적합한 보안 약점을 고르시오.

```
#include <stdio.h>
int main(void) {
    int a;
    printf("변수 a의 값은 %d입니다.", a);
    return 0;
}
```

(ㄱ) 널(Null) 포인터 역참조
(ㄴ) 부적절한 자원 해제
(ㄷ) 해제된 자원 사용
(ㄹ) 초기화되지 않은 변수 사용

답:

[기출 예상 문제]

19. 코드 오류와 관련한 보안 약점 중 유한한 시스템 자원이 계속 점유하고 있으면 자원 부족으로 인해 새로운 입력을 처리하지 못 하고, 자원의 누수 등이 발생할 수 있다. 해당 보안 약점을 방지하기 위한 방법을 간략히 서술하시오.

답:

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

20. 캡슐화에 관련한 보안 약점에 대한 설명이다. ( )안에 들어갈 가장 적합한 내용을 고르시오.

보안약점	설명
(①)	Public으로 선언된 메소드의 인자가 Private 선언된 배열에 저장되면, Private 배열을 외부에서 접근하여 배열 수정과 객체 속성 변경이 가능해 지는 보안약점
(②)	시스템의 내부 데이터나 내부 로직 등을 예외 처리 메시지 등을 통해 공개되는 보안약점
(③)	프로그램 디버깅을 위해 작성된 코드를 통해 권한이 없는 사용자 인증이 우회되거나, 또는 중요 정보에 접근이 가능해지는 보안약점
(④)	Private로 선언된 배열을 Public으로 선언된 메소드를 통해 반환하면, 그 배열의 주소가 외부에 공개되어 외부에서 배열 수정과 객체 속성 변경이 가능해 지는 보안약점
(⑤)	잘못된 통신 세션에 의해 권한 없는 사용자에게 데이터 노출이 일어날 수 있는 보안 약점

(ㄱ) Private 배열에 Public 데이터 할당
(ㄴ) 시스템 데이터 정보 노출
(ㄷ) 제거되지 않고 남은 디버그 코드
(ㄹ) 잘못된 세션에 의한 정보 노출
(ㅁ) Public 메소드부터 반환된 Private 배열

답 ① ② ③ ④ ⑤

[기출 예상 문제]

21. API 오용과 관련한 보안 약점에 대한 설명이다. ( ) 안에 들어갈 가장 적합한 용어를 쓰시오.

* API 오용과 관련한 보안 약점
1. (①) lookup에 의존한 보안 결정은 도메인명에 의존하여 인증 및 접근 통제 등의 보안 결정을 내리는 경우 발생하는 보안 약점으로, (①)에 의존할 경우 공격자에 의해 (①) 스푸핑 공격 등이 가능하게 된다.
2. 취약한 (②)는 보안상 금지된 함수거나, 부주의하게 사용될 가능성이 많은 (②)을/를 의미한다. (②)에 대해 확인하지 않고 사용할 때 보안 문제를 발생시킬 수 있으므로, 보안 문제로 금지된 함수(ex. gets())는 이를 대체할 수 있는 안전한 함수(ex. gets_s())를 사용한다.

답 ① ②

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]
22. SW개발보안 테스트의 결함 등급을 측정하여 보안사고 발생 시 복구 우선순위를 결정할 수 있다. 보안테스트의 결함 등급 측정 시 필요한 두 가지를 쓰시오.

답:

[기출 예상 문제]
23. SW개발보안 테스트의 종류에 대한 설명이다. ( )안에 들어갈 가장 적합한 내용을 쓰시오.

SW구현이 완료되면 조직의 보안정책의 적합 여부를 확인하기 위해 SW보안 테스트를 진행한다. 보안 정책의 기준에 합당한지 충분히 테스트 하고, 결과에 대한 증빙을 남겨 보안 감사에 대비한다. SW보안 테스트를 하여 취약점을 진단하는 방법은 다음과 같이 (①)와/과 (②)(으)로 구분할 수 있으며, 상호 보완적으로 선택할 수 있다.
- (①): SW를 실행하지 않고, 소스 코드 수준으로 보안 약점을 분석하고 SW 개발 과정에서 주로 사용된다.
- (②): SW실행환경에서의 보안약점 분석으로 SW시험단계에서 주로 사용된다.

답 ①
②

[기출 예상 문제]
24. 다음 중 SW개발보안 테스트 중 정적 분석의 특징을 모두 고르시오.

(ㄱ) 분석 시 소스 코드가 필요 없다.
(ㄴ) 컴포넌트 간 발생할 수 있는 통합된 취약점 발견에 제한적이다.
(ㄷ) SW실행 환경에서 보안 약점을 분석한다.
(ㄹ) SW개발 초기에 취약점 발견으로 수정 비용이 절감된다.

답:

[기출 예상 문제]
25. 다음 설명에 가장 부합하는 SW개발보안 테스트의 일반 원칙을 고르시오.

보안 담당자 및 보안 평가자의 테스트 결과를 서버 담당자에게 피드백하여 문제가 있는 요구사항에 기능에 대한보완이 이루어 질 수 있도록 조치를 취하게 하고, 필요 시 기술적인 제언을 수행한다.

(ㄱ) SW보안 테스트 계획서에 따른 실시
(ㄴ) SW보안 테스트의 적정성 판단
(ㄷ) SW보안 결과의 신뢰성 확인
(ㄹ) SW보안결함 발견 시 피드백 결과 확인

답:

[소프트웨어 개발 보안 구축>SW개발 보안 구현]

[기출 예상 문제]

26. SW프로그램과 보안명세서와의 차이와 불일치이고 기대하는 보안품질의 결과와 실제 관찰 결과 간의 차이라고 정의된다. 즉, SW시스템이 사용자가 기대하는 타당한 보안 기대치를 만족하지 못하는 것을 의미하는 용어를 쓰시오.

답:

[기출 예상 문제]

27. SW보안결함의 종류에 대한 설명이다. ( )안에 들어갈 가장 적합한 결함의 종류를 고르시오.

보안결함	설명
(①)	설치/운영되기 전에 발견된 소프트웨어 보안결함
(②)	설치/운영되는 환경에 전달된 소프트웨어 보안결함
(③)	소프트웨어의 운영 중에 나타나서 발생하는 하나 이상의 이상 징후들의 집합

(ㄱ) SW의 특이한 고장 (ㄴ) 발견된 보안결함
(ㄷ) 잠재적 보안결함

답 ① ②
③

[기출 예상 문제]

28. 다음 제시된 SW개발보안 테스트와 결함관리 수행 순서를 순서대로 나열하시오.

(ㄱ) 취약점 테스트를 실시할 주기와 대상을 선정한다.
(ㄴ) SW 취약점 테스트를 수행한다.
(ㄷ) SW 취약점의 지적사항을 해결한다.
(ㄹ) SW취약점 테스트의 변경요청 제기 및 테스트 일정을 수립한다.
(ㅁ) 점검이 완료된 소스코드를 관리한다.
(ㅂ) SW 취약점 테스트 보고서를 발행한다.
(ㅅ) SW 보안결함 해결사항을 보고한다.
(ㅇ) 전반적인 보안 상황을 보고한다.

답: