정보처리기사 실기 > 정보처리실무 > 합격을 다지는 모듈별 확인문제

09. 소프트웨어 개발 보안 구축

확인문제 1 소프트웨어 개발 보안은 소프트웨어 개발 과정중 발생할 수 있는 수많은 보안 위협으로부터 보안 취약점을 발견하고 안전한 소프트웨어를 개발하기위한 활동이다. 소프트웨어 개발 보안의 목표 3 가지를 쓰시오.

답 : 무결성, 가용성, 기밀성

확인문제 2 소프트웨어의 기획부터 폐기까지의 전 과정을 효과적으로 관리하기 위한 절차로서 소프트웨어를 개발하기 위한 작업활동, 절차, 산출물, 기법등을 체제적으로 순서에 맞게 정리한 것은?

답 : SDLC(Software Development Life Cycle)

확인문제 3 다음 보기는 소프트웨어 개발 보안에 관련된 기관이다. 소프트웨어 개발 보안 정책 가이드를 개발하고 소프트웨어 개발 보안에 대한 기술을 지원, 교육, 자격제도 운영등을 수행하는 기관명을 쓰시오.

답 : 한국 인터넷 진흥원 (KISA)

확인문제 4 개인정보의 수집 · 유출 · 오용 · 남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 하는 법령을 쓰시오.

답 : 개인정보 보호법

확인문제 5 소프트웨어 개발 보안 관련 프로세스인 Secure SDLC에 대하여 100자 내외로 서술 하시오.

답 : 안전한 소프트웨어 개발을 위하여 소프트웨어 생명주기(SDLC)에 보안을 강화한 프로세스를 의미한다. 요구사항분석, 설계, 구현, 테스트, 유지보수 등 SDLC 전과정에 걸쳐 적용되어야 할 보안 활동을 제시한다.

확인문제 6

다음이 설명하는 소프트웨어 보안관련 용어를 영문으로 쓰시오.

- 개발하는 소프트웨어가 복잡해짐으로 인해 보안상 취약점이 발생할 수 있는 부분을 보완하여 프로그래밍하는 것이다.
- 우리나라에서는 2012년 12월부터 '소프트웨어 개발 보안' 제도를 시행하여 이를 의무화 하였다.
- 서버, 네트워크 와 같은 물리적 보안부터 개발 프로그램 등 환경에 대한 보안 통제 기주늘 수립한 것이다.

답 : Secure Coding

확인문제 7

이 암호화 방식은 RFC 1321로 지정되어 있으며, 주로 프로그램이나 파일이 원본 그대로인지를 확인하는 무결성 검사 등에 사용된다. 1991년에 로널드 라이베스트가 예전에 쓰이던 MD4를 대체하기 위해 고안했으며, 임의의 길이의 메시지(variable-length message)를 입력받아, 128비트짜리 고정 길이의 출력값을 낸다. 입력 메시지는 512 비트 블록들로 쪼개진다; 메시지를 우선 패딩하여 512로 나누어떨어질 수 있는 길이가 되게 하며, 128비트 암호화 해시 함수인 암호화 방식을 쓰시오.

답 : MD5

확인문제 8

서버/클라이언트 사이의 연결을 세션이라고 한다. 세션 통제는 이 연결에서 발생하는 정보를 관리하기 위한것이며 요구사항 분석 및 설계 단계 중 진단해야 하는 보안 점검에 해당한다. 이러한 세션 설계시 고려해야 할 사항 2가지를 쓰시오

답 :
- UI 설계시 열려진 모든 페이지에서 한번에 로그아웃이 가능하게 설계한다.
- 로그아웃을 수행하면 세션이 완전에 종료되도록 설계한다.
- 이전 세션이 정상적으로 종료되지 않은 경우 새로운 세션이 생성되지 못하도록한다.
- 비밀 번호를 변경할 경우 기존의 설정된 세션을 종료하고 재할 당 하도록 한다.
- 세션의 자동 종료 타임아웃은 중요도에 따라 높은 경우 2~5분, 낮을 경우 15~30분으로 설정한다.

확인문제 9

다음 설명에 알맞은 보안 취약점을 쓰시오.

-웹사이트에 공격자에 의해 작성된 악의적 스크립트를 삽입하는 방식이다.
-다른 사용자의 웹 브라우저 내에서 적절한 검증 없이 실행된다.
-사용자의 세션을 탈취하거나, 웹 사이트를 변조하거나 혹은 악의적인 사이트로 사용자를 이동시킬 수 있다.

답: XSS(Cross Site Scripting)

확인문제 10

다음 설명에 알맞은 보안 취약점을 쓰시오.

-웹 응용 프로그램에 강제로 SQL 구문을 삽입하여 내부 데이터베이스 서버의 데이터를 유출 및 변조하고 관리자 인증을 우회할 수 있는 공격 기법이다.
-동적 쿼리에 사용되는 입력 데이터에 예약어 와 특수문자를 입력하지 못하도록 설정하여 방지할 수 있다.

답:SQL injection

확인문제 11

TOCTOU(Time Of Check Time Of Use) 경쟁 조건에 대하여 50자 내외로 서술 하시오.

답: 코딩 과정에서 검사시점과 사용시점을 가만하지 않는 경우 발행하는 보안 취약점이다.

확인문제 12

이것은 특정 사용자를 대상으로 하지않고 불특정 다수를 대상으로 로그인된 사용자가 자신의 의지와 상관없이 공격자의 의도에 따라 행위하게 만드는 공격이다.
XSS 공격과 유사하다. 유명 인터넷 쇼핑몰인 옥션에서 발생한 개인정보 유출 사건에 사용된 공격 기법이다.

답: CSRF(Cross Site Request Forgery)

확인문제 13

회원 가입시 보안에 관련된 요구사항이다. 잘못 도출된 항목을 고르시오.

가. 패스워드는 레인보우 테이블 공격 대비를 위하여 솔트를 저공하고 양방향 암호화 처리 한다.
나. 아이디 패스워드를 SSL을 통하여 암호화 한다.
다. 패스워드의 해시처리는 클라이언트가 아닌 서버에서 수행 하도록 한다.

답: 가. 패스워드는 레인보우 테이블 공격 대비를 위하여 솔트를 저공하고 단방향 암호화 처리 한다.

확인문제 14

이 공격은 최근 패스워크 크래킹 기법으로 패스워드별로 해시값을 미리 생성해 놓은 테이블을 을 사용하여 Reduction 함수의 반복 수행을 통하여 일치하는 해시 값으로 패스워드를 탈취 하는 기법이다. 이 기법의 명칭을 쓰시오.

답 : Rainbow Table Attack

확인문제 15

다음 제시된 코드의 보안 취약점을 찾아 해당 취약점명을 쓰시오.

```
String Data = request.getParameter("data") ;
cmd = new String[] { "cmd.exe", "/c", Data } ;
Runtime.getRuntime().exec(cmd) ;
```

답 : Command injection 공격

확인문제 16

다음 빈칸에 알맞은 용어를 쓰시오.

( )는 프로그램에서 일반적으로 객체가 Null이 될 수 없다는 가정을 위반했을 때 발생한다.
( )를 방지하기 위해서는 미리 해당 값이 Null 값이 아니라는 것을 체크해 주는 로직을 설계해야 한다.

실 예를 살펴보면 다음과 같다.

〈취약 코드〉

```
public void f(boolean b) {
    String cmd = System.getProperty("cmd");
    cmd = cmd.trim();
    System.out.println(cmd);
}
```

〈수정 코드〉

```
public void f(boolean b) {
    String cmd = System.getProperty("cmd");
    if (cmd != null) {
        cmd = cmd.trim();
        System.out.println(cmd);
    } else System.out.println("null command");
}
```

답 : 널 포인터 (Null Pointer) 역참조

〈취약 코드〉

```
public void f(boolean b) {
    String cmd = System.getProperty("cmd");     // cmd가 null 값인지 확인 하는 절차 누락
    cmd = cmd.trim();                            // trim 메소드 호출 시 null 포인터 예외 방생
    System.out.println(cmd);
```

〈수정 코드〉

```
public void f(boolean b) {
    String cmd = System.getProperty("cmd");
    if (cmd != null) {                          // cmd가 null 값인지 확인 하는 절차 추가
        cmd = cmd.trim();
        System.out.println(cmd);
    } else System.out.println("null command");
}
```

확인문제 17

보안상 금지된 함수이거나, 부주의하게 사용될 가능성이 높은 API를 사용하는 경우 보안상 문제가 발생할 수 있는 보안 취약점을 쓰시오.

답 : 취약한 API 사용

확인문제 18

다음 소스코드에서 발생할 수 있는 취약점을 작성하시오.

```
try{
  rd = new BufferedReader(new FileReader(new File(filename)));
}
 catch(IOExcception e) {
  e.printStackTrace();
}
```

답 : 오류메시지 노출로 인한 취약점

확인문제 19

-이 원칙은 소프트웨어 개발 보안 구축시 정보보안의 3요소중 하나이다.
-인가된 사람, 프로세스, 시스템만 필요성에 근거하여 시스템에 접근해야 하난다는 원칙이다.
-이 원칙을 보장하기 위한 보안 기술에는 접근 제어, 암화화 등이 있다.

위 문장에서 설명하는 보안 요소를 쓰시오.

답 : 기밀성

확인문제 20

다음의 보안 약점 설명에서 빈칸에 알맞은 내용을 작성하시오.

가. 신뢰되지 않는 URL 주소로 자동접속 연결 : 외부에서 입력 받은 값을 주소로 사용할 때 파라미터 값을 검증하지 않는 경우 피싱 공격에 노출될 가능성이 있다.
나. ( ) : HTTP 요청에 있는 파라미터가 HTTP Response 의 응답헤더로 다시 전달될 대 파라미터 내에 개행문자 (CR, LF) 가 존재하면 HTTP 응답이 분리될 수 있다. 이 때 공격자는 개행 문자를 이용해서 첫 번째 응답을 종료시키고 두 번째 응답에 악의적인 코드를 주입할 수 있다.
다. 크로스사이트 요청 위조 : 특정 웹 사이트에 대해 사용자가 인지하지 못한 상황에서 사용자 의도와는 무관하게 공격자가 의도한 행위를 요청할 수 있다.
라. 경로 조작 및 자원 삽입 : 입력 값 조작을 통하여 시스템이 보호하는 자원에 임의 접근이 가능하다.

답 : HTTP 응답 분할

확인문제 21

이 공격은 공격 대상 컴퓨터의 실행 속도를 느리게 하거나 동작을 마비시켜 서비스 거부상태가 되도록 하는 공격 기법이다. IP 헤더를 위조하여 공격하고자 하는 송싲나 IP 주소와 포트번호를 수신자의 IP 주소와 포트번호로 동일하게 설정하여 패킷을 전송하는 DDos 공격 기법으로 일명 자폭 공격이라 하는 공격 기법이 무엇인지 쓰시오.

답 : Land Attack