

18. SW 개발 보안의 3대 요소 중에서 인가되지 않은 개인 혹은 시스템 접근에 따른 정보의 노출을 차단하는 특성이 무엇인지 쓰시오.

답)

해설) 수제비 정보처리기사 실기 9-3페이지 참조

36. 다음이 설명하는 시큐어 코딩 가이드의 보안 약점에 대해서 쓰시오.

- * 프로그램 입력값에 대한 검증 누락, 부적절한 검증, 잘못된 형식 지정을 통해 발생한다.
- * 사용자, 프로그램 입력 데이터에 대한 유효성 검증체계를 수립하고 실패 시 처리 설계 및 구현을 통해 대응한다.

정답)

참고) 수제비 정보처리기사 실기 9-14 페이지

정답은 답글(<https://cafe.naver.com/soojebi/5172>)에 있습니다.

43. 다음 괄호에 알맞은 용어를 쓰시오

(①)은 2010년 6월에 발견된 웜 바이러스이다. 지멘스의 SCADA 시스템만을 감염시켜 장비를 제어하고 감시하는 특수한 코드를 내부에 담고 있다. (①)은 장비를 프로그램하는 데 사용되는 PLC를 감염시켜 장비의 동작을 변경한다

답)_____

정답과 해설은 답글(<https://cafe.naver.com/soojebi/7068>)에 있습니다.

45. 다음 괄호에 알맞은 용어를 쓰시오

(①)은 정보를 수집한 후, 저장만 하고 분석에 활용하고 있지 않는 다량의 데이터이다. (①)는 처리되지 않은 채 미래에 사용할 가능성이 있다는 이유로 삭제되지 않고 방치되어 있어, 저장 공간만 차지하고 보안 위험을 초래할 수 있다.

답) _____

정답과 해설은 답글(<https://cafe.naver.com/soojebi/7129>)에 있습니다.

46. 다음 괄호에 알맞은 용어를 쓰시오

- (①)은 잃어버린 스마트폰을 주문 사람이 해당 스마트폰을 켜서 이동통신망 혹은 와이파이에 접속하면 이용자(원 소유자)가 원격으로 기기를 사용 불능 상태로 만들 수 있는 기술이다.

- 워너크라이 랜섬웨어가 세계 곳곳으로 막 퍼져나가던 때에 멀웨어테크라는 영국 보안전문가가 워너크라이 내에서 발견한 도메인을 정식으로 등록하면서 랜섬웨어 확산이 멈추는 효과가 발생했기에 (①)라고 불리기 시작했다.

답)_____

정답과 해설은 답글(<https://cafe.naver.com/soojebi/7266>)에 있습니다.

47. 다음 괄호에 알맞은 용어를 쓰시오

()은/는 특수 목적은 가진 조직이 하나의 표적에 대해 다양한 IT 기술을 이용해서 지속적으로 정보를 수집하고 취약점을 파악하여 침투, 검색, 수집, 유출하는 공격 기법이다.

답)_____

정답과 해설은 답글(<https://cafe.naver.com/soojebi/7405>)에 있습니다.

50. 보안의 3요소 중 서비스가 계속 유지가 되어 인가된 대상에게 정보를 제공하는 것으로 시스템이 장애 없이 정상적으로 운영되는 능력을 무엇이라고 하는지 쓰시오.

답)_____

정답과 해설은 답글(<https://cafe.naver.com/soojebi/7570>)에 있습니다.

※ 2019년 이전 기출문제입니다.

56. 다음이 설명하는 용어를 쓰시오.

- * 기업이 재해/재난으로부터 타격을 입은 뒤 업무를 어떻게 복구하는지에 대한 계획을 말한다.
- * 전산의 단순복구 뿐 아니라 고객 비즈니스의 지속성을 보장한다.
- * 재해 복구를 포함하는 더 넓은 개념으로 쓰인다.

정답)

정답(<https://cafe.naver.com/soojebi/7959>)은 답글에 있습니다.

※ 2019년 이전 기출문제입니다.

57. 다음이 설명하는 용어를 쓰시오.

온라인 상에서 불법 활동을 조장하기 위해 만들어진 컴퓨터 프로그램이다. 공격용 톨킷이라고 불리며 보통 취약점을 이용하도록 미리 프로그램 된 악성코드 등으로 구성돼 원하는 형태로 공격을 감행하거나 공격을 자동화 할 수 있다. 인터넷에서 곧바로 사용할 수 있으며 키로거를 은밀히 설치 시켜 불법적으로 정보를 수집해 가기도 한다.

정답)

정답(<https://cafe.naver.com/soojebi/8040>)은 답글에 있습니다.

76. 다음은 보안 공격 기법에 대한 설명이다. 괄호()안에 들어갈 공격 기법을 쓰시오.

- (①) : 출발지 주소를 공격 대상의 IP로 설정하여 네트워크 전체에 ICMP Echo 패킷을 직접 브로드캐스팅(Directed Broadcasting)하여 타겟 시스템을 마비시키는 공격기법이다.

- (②) : 요청 헤더의 Content-length를 비정상적으로 크게 설정하여 메시지 바디 부분을 매우 소량으로 보내 계속 연결 상태를 유지시켜 자원을 소진시키는 공격기법이다.

- (③) : 공격자가 IP Fragment Offset 값을 서로 중첩되도록 조작하여 전송하고, 이를 수신한 시스템이 재조합하는 과정에서 오류가 발생, 시스템의 기능을 마비시키는 공격기법이다.

답)

① _____

② _____

③ _____

정답 및 해설) <https://cafe.naver.com/soojebi/11049>

112. 인증 시스템의 하나로 한 번의 인증을 통해서 여러 개의 서비스를 이용할 수 있는 시스템은 무엇인가?

정답)

정답은 답글(<https://cafe.naver.com/soojebi/23441>)에 있습니다. (참고로 2019년 이전 출제되었던 문제입니다.)

118. 다음은 IPSEC의 세부 프로토콜에 대한 설명이다. 괄호() 안에 들어갈 용어를 쓰시오.

(①) : 보안 관련 설정들을 생성, 협상 및 관리하는 프로토콜로 udp 500번 포트를 사용하는 프로토콜

(②) : 메시지 인증 코드(MAC)와 암호화를 이용하여 인증(무결성), 송신처 인증, 기밀성을 제공하는 프로토콜

(③) : 기밀성(암호화)을 제외한 메시지 인증 코드(MAC)를 이용한 인증(무결성), 송신처 인증을 제공하는 프로토콜

답)

① _____

② _____

③ _____

정답 및 해설) <https://cafe.naver.com/soojebi/24611>

121. 다음은 정해진 메모리의 범위를 넘치게 해서 원래 리턴 주소를 변경시켜 임의의 프로그램이나 함수를 실행시키는 시스템 해킹 기법인 버퍼 오버플로우 공격에 대한 대응방안이다. 괄호 () 안에 들어갈 용어를 쓰시오.

[버퍼 오버플로우 대응방안]

1. 운영체제의 주기적 최신 패치 적용
2. 입력값 검증이 가능한 안전한 함수 사용 (Strncpy())
3. (①) : 카나리(canary)라고 불리는 무결성 체크용 값을 복귀주소와 변수 사이에 삽입해 두고 버퍼 오버플로우 시 카나리값이 변하게 되면 복귀주소를 호출하지 않는 방법
4. (②) : 함수 시작 시 복귀주소를 Global RET라는 특수 스택에 저장해 두고 함수 종료 시 저장된 값과 스택의 RET값을 비교해서 다를 경우 오버플로우로 간주하고 프로그램 실행을 중단하는 방법
5. (③) : 메모리 공격을 방어하기 위해 주소 공간 배치를 난수화하고, 실행 시 마다 메모리 주소를 변경시켜 버퍼 오버플로우를 통한 특정주소 호출을 차단하는 방법

답)

① _____

② _____

③ _____

134. 다음은 SW 개발 보안과 관련된 용어이다. 괄호() 안에 들어갈 가장 올바른 용어를 쓰시오.

(①) : 조직이나 기업의 자산에 악영향을 끼칠 수 있는 사건이나 행위

(②) : 조직의 데이터 또는 조직의 소유자가 가치를 부여한 대상

(③) : 취약점을 이용하여 조직의 소유자가 가치를 부여한 대상에 손실 또는 피해를 가져올 가능성

답)

① _____

② _____

③ _____

정답 및 해설) <https://cafe.naver.com/soojebi/30327>

139. 다음은 보안 공격 기법에 대한 설명이다. 괄호 () 안에 들어갈 가장 정확한 보안 공격 기법을 쓰시오.

- (①) : 검증되지 않은 외부 입력 데이터가 포함된 웹페이지가 전송되는 경우, 사용자가 해당 웹페이지를 열람함으로써 웹페이지에 포함된 부적절한 스크립트가 실행되는 공격기법
- (②) : 응용 프로그램의 보안 취약점을 이용해서 악의적인 SQL 구문을 삽입, 실행시켜서 데이터베이스(DB)의 접근을 통해 정보를 탈취하거나 조작 등의 행위를 하는 공격기법
- (③) : 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 하는 공격기법

답)

① _____

② _____

③ _____

144. 다음은 공개키 암호화 알고리즘에 대한 설명이다. 괄호() 안에 들어갈 암호화 알고리즘을 쓰시오.

(①) : 고급 암호화 표준이라고 불리는 암호 알고리즘이며 블록 크기는 128비트이며, 키 길이에 따라 128비트, 192비트, 256비트로 분류할 수 있고, 암호화와 복호화 과정에서 동일한 키를 사용하는 대칭 키 알고리즘이다.

(②) : KISA, ETRI에서 개발하고 TTA에서 인증한 안전성, 신뢰성이 우수한 고속 블록 단위의 128비트 대칭 키 암호화 알고리즘이다.

(③) : 56bit의 키를 이용, 64bit의 평문 블록을 64bit의 암호문 블록으로 만드는 블록 방식의 암호화 알고리즘이다.

답)

① _____

② _____

③ _____

1. 다음 중 ① ~ ③의 설명에 해당하는 보안 약점을 [보기]에서 찾아서 쓰시오.

- ① SQL 삽입 공격, 크로스 사이트 스크립트(XSS) 공격을 유발할 수 있는 보안 약점
- ② 인증, 권한 관리, 암호화, 중요정보 처리를 부적절하게 구현 시 발생할 수 있는 보안 약점
- ③ 잘못된 세션에 의한 정보 노출, 제거되지 않은 디버그 코드, 시스템 정보 노출 등으로 발생할 수 있는 보안 약점

[보기]

- ㄱ. 캡슐화 보안 약점
- ㄴ. 입력데이터 검증 및 표현의 보안 약점
- ㄷ. 보안 기능에 대한 보안 약점
- ㄹ. 시간 및 상태 보안 약점
- ㅁ. 에러 처리 보안 약점

답)

- ① _____
- ② _____
- ③ _____

정답 및 해설) <https://cafe.naver.com/soojebi/8271>