2020-국회직-9급-정보보호론-가형-해설-곽후근

1. 전자서명의 활용 사례로 적합하지 않은 것은?
① 인증서 로그인을 통해 사용자의 신원을 증명한다.
② 다운로드하는 소프트웨어의 위변조 여부를 확인한다.
③ 이메일 내용이 중간 메일서버에 노출되지 않도록 한다.
④ 웹브라우저로 통신하는 서버의 사이트가 유효한지 검증한다.
⑤ 폐기된 인증서들을 모아서 인증서 폐기 목록(CRL)을 발행한다.
정답 체크 :
(3) 노출을 막으려면 대칭키 또는 비대칭키를 사용해서 암호화를 수행해야 한다.
오답 체크 :
(1) 공인인증서에 활용된다.
(2) 전자서명은 서명자 인증, 무결성, 부인방지를 제공하므로 소프트웨어의 위변조 여부를 확인할 수 있다.
(4) 서버의 인증서에 전자서명이 활용된다.
(5) 전자서명은 CRL과 OCSP를 사용한다.

2. NAC(Network Access Control) 시스템의 기능이 아닌 것은?
① PC 및 네트워크 장치 통제
② 데이터 패킷 암호화
③ 접근 제어
④ 해킹, 웜, 유해 트래픽 탐지 및 차단
⑤ 접근 인증
정답 체크 :
(2) NAC은 접근 제어를 수행하는 장치로 암호화 기능을 제공하지 않는다.
오답 체크 :
(1) 백신 관리, 패치 관리, 자산 관리(비인가 시스템 자동 검출) 등을 수행한다.
(3), (5) 내부 직원에 대한 역할 기반의 접근 제어와 네트워크의 모든 IP 기반 장치의 접근을 제어 및 인증한다.
(4) 유해 트래픽 탐지 및 차단, 해킹 행위 차단, 완벽한 증거 수집 등을 수행한다.
Tip! 아래의 표는 NAC의 주요 기능을 나타낸다.

구분	기능
접근 제어 및 인증	• 내부 직원에 대한 역할 기반의 접근 제어 • 네트워크의 모든 IP 기반 장치 접근 제어
PC 및 네트워크 장치 통제(무결성 확인)	• 백신 관리 • 패치 관리 • 자산 관리(비인가 시스템 자동 검출)
해킹, 웜, 유해 트래픽 탐지 및 차단	• 유해 트래픽 탐지 및 차단 • 해킹 행위 차단 • 완벽한 증거 수집

3. X.509 인증서를 구성하는 필드에 대한 설명으로 옳지 않은 것은?

① Version: 현재 사용 중인 X.509의 버전 정보
② Serial number: 인증기관이 부여한 고유번호
③ Issuer name: 인증서를 발급한 인증기관 식별 정보
④ Subject name: 공개키의 소유자 정보
⑤ Signature: 공개키 소유자가 생성한 서명 정보
정답 체크 :
(5) 서명 알고리즘 식별자이다.
오답 체크 :
(1), (2), (3), (4) 인증서 필드를 정리하면 다음과 같다.

Version	인증서의 버전
Serial Number	CA가 할당한 정수로 된 고유 번호
Signature	서명 알고리즘 식별자
Issuer	발행자
Validity	유효기간
Subject	소유자
Subject Public Key Info	소유자의 공개키 정보
Issuer Unique Identifier (Optional)	발행자 고유 식별자
Subject Unique Identifier (Optional)	소유자 고유 식별자
Extensions (Optional)	확장

4. 다음 프로그램이 취약한 공격 유형은?

```
#define BUFSIZE 256
int main(int argc, char **argv) {
  char *buf;
  buf = (char *)malloc(sizeof(char)*BUFSIZE);
  strcpy(buf, argv[1]);
}
```

① 스택 버퍼 오버플로우 공격
② 힙 버퍼 오버플로우 공격
③ 포맷 스트링 공격
④ 정수 오버플로우 공격
⑤ 레이스 컨디션 공격
정답 체크 :
(2) malloc을 통해 힙에 메모리가 할당되었으므로 힙 버퍼 오버플로우 공격이 된다.
오답 체크 :
(1) 동적 메모리 할당(malloc)이 아닌 정적 메모리 할당(배열로 할당)되었다면 스택에 메모리가 할당되어 스택 버퍼 오버플로우 공격이 된다.
(3) printf() 사용된 %s와 같은 문자열을 가리켜 포맷 스트링이라 한다. 포맷 스트링을 조작하면(%n을 사용) 임의의 메모리 주소의 쓰기 혹은 복귀 주소를 변경할 수 있다.
(4) 정수값이 증가하면서 허용된 가장 큰 값보다 더 커져서 실제 저장되는 값은 의도하지 않게 아주 작은 수이거나 음수가 되어 프로그램이 예기치 않게 동작하는 것을 의미한다.

(5) 한정된 자원을 동시에 이용하려는 여러 프로세스가 자원의 이용을 위해 경쟁을 벌이는 현상이다. 레이스 컨디션을 이용하여 root 권한을 얻는 공격을 의미한다.

5. 대칭키 암호 운영모드로서 평문 블록 $(P_1, P_2, \ldots, P_n)$을 암호화 하는 CBC(Cipher Block Chaining) 모드에 대한 설명으로 옳은 것만을 〈보기〉에서 모두 고르면?

〈보 기〉

ㄱ. 평문이 달라지면 초기벡터는 매번 새롭게 랜덤으로 생성된다.
ㄴ. 평문 블록이 동일하면 대응하는 암호문 블록도 동일하다.
ㄷ. P_2에 발생한 에러는 P_2블록 이후의 모든 암호화 과정에 파급된다.
ㄹ. 암호화 과정은 평문 블록 P_1부터 P_n까지 순차적으로 진행된다.
ㅁ. 암호화 및 복호화를 하는데 암호화 알고리즘만 있어도 된다.

① ㄱ, ㄴ, ㄹ
② ㄱ, ㄴ, ㅁ
③ ㄱ, ㄷ, ㄹ
④ ㄴ, ㄷ, ㄹ
⑤ ㄷ, ㄹ, ㅁ
정답 체크 :
(3)
ㄱ : 초기벡터가 같으면 공격의 대상이 된다.
ㄷ : 구조적 특징으로 인해 에러가 전파된다.
ㄹ : P_1이 끝나야 P_2가 진행되고, P_2가 끝나야 P_3가 진행된다.
오답 체크 :
(1), (2), (4), (5)
ㄴ : 평문 블록이 동일해도 대응하는 암호문 블록은 동일하지 않다.
ㅁ : 별도의 복호화 알고리즘이 필요하다.

6. TLS(Transport Layer Security) 프로토콜에서 TLS 세션을 처음 시작할 때 클라이언트와 서버 간에 안전한 연결을 위하여 상호 인증을 수행하고 암호 메커니즘의 정보를 교환하여 세션키를 생성하는 하부 프로토콜은?
① One Time Password 프로토콜
② Secure Electronic Transaction 프로토콜
③ Handshake 프로토콜
④ Document Object Model 프로토콜
⑤ Change Cipher Spec 프로토콜
정답 체크 :
(3) 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유키를 결정한다. 인증서를 이용한 인증을 수행한다.
오답 체크 :
(1) 고정된 비밀번호 대신 사용되는 매번 새롭게 바뀌는 일회용 비밀번호이다. S/KEY 방식, 시간 동기화 방식, 챌린지/응답 방식, 이벤트 동기화 방식 등이 있다.
(2) 전자상거래 당사자들에게 신뢰성과 안전성을 제공하기 위하여 인증, 비밀성 등의 보안 기능과 지불 기능을 제

공하는 전자상거래 전용 프로토콜이다.
(4) 객체 지향 모델로써 구조화된 문서를 표현하는 형식이다(플랫폼/언어 중립적).
(5) SSL/TLS에서 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.

7. 이메일 보안을 위하여 사용하는 PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?
① 송신 부인방지는 지원하지만 수신 부인방지는 미지원
② 기밀성 제공을 위하여 대칭키 방식과 공개키 방식 사용
③ 인증받을 메시지나 파일에 전자서명을 생성, 확인 작업을 수행
④ 이메일 어플리케이션에 플러그인 기능으로 확장 불가능
⑤ 공개키에는 RSA 버전과 Diffie-Hellman 버전이 존재
정답 체크 :
(4) 플러그인 기능으로 확장이 가능하다.
오답 체크 :
(1) 송신 부인방지는 전자서명을 통해 지원하나 수신 부인방지는 별도로 지원하지 않는다.
(2) 기밀성을 위해 대칭키와 공개키를 사용한다.
(3) PGP는 전자서명을 사용한다.
(5) 공개키는 RSA, Diffie-Hellman, ElGamal을 사용한다.

8. 리눅스 시스템에서 사용자 로그인 실패 정보가 저장되는 파일은?
① btmp
② extmp
③ wtmp
④ utmp
⑤ atmp
정답 체크 :
(1) 리눅스에서 사용자 로그인 실패 정보가 저장된다.
오답 체크 :
(2) 해당 로그는 존재하지 않는다.
(3) 유닉스에서 사용자들의 로그인, 로그아웃, 시스템 재부팅 정보를 로그로 남긴다.
(4) 유닉스에서 현재 시스템에 로그인한 사용자의 상태를 출력한다(로깅).
(5) 해당 로그는 존재하지 않는다.

9. 최근 발생한 보안 위협에 대한 설명으로 옳은 것은?
① 블루킵(Bluekeep): 원격 데스크톱 서비스를 인증 없이 조작할 수 있는 취약점
② 다크웹(Dark Web): 피싱 메일을 통해 유포되며 금융정보 탈취를 시도하는 악성코드
③ 딥페이크(Deepfake): 특정 웹브라우저를 통해 익명성이 보장되는 인터넷 영역
④ 이모텟(Emotet): 한글로 작성된 메일 내부에 정상파일로 위장한 랜섬웨어
⑤ 소디노키비(Sodinokibi): 인공지능을 기반으로 실제처럼 조작한 음성, 영상 등을 통칭함
정답 체크 :
(1) 윈도우 원격 데스크톱 서비스를 이용해 정상적인 인증 단계를 거칠 필요 없이 원격에서 임의의 코드를 실행하는 취약점이다.

오답 체크 :
(2) 해당 설명은 이모텟을 나타내고, 다크웹은 특정 웹브라우저를 통해 익명성을 보장하는 인터넷 영역이다.
(3) 해당 설명은 다크웹을 나타내고, 딥페이크는 인공지능을 기반으로 실제처럼 조작한 음성, 영상 등을 통칭한다.
(4) 해당 설명은 소디노키비를 나타내고, 이모텟은 피싱 메일을 통해 유포되며 금융정보 탈취를 시도하는 악성코드이다.
(5) 해당 설명은 딥페이크를 나타내고, 소디노키비는 한글로 작성된 메일 내부에 정상파일로 위장한 랜섬웨어이다.

10. 암호화폐를 주고 받는 블록체인 네트워크에 대한 설명으로 옳지 않은 것은?
① 거래 내역들의 최상위 해시값은 머클 루트(Merkle Root)로서 블록 헤더에 포함된다.
② 채굴(Mining)은 주어진 난이도에 따라 해시값의 역상을 구하는 과정이다.
③ 공개키의 해시값이 암호화폐를 주고 받는 주소값으로 사용된다.
④ 블록체인 내의 원장을 수정하기 위해서는 개인키를 사용해야 한다.
⑤ 이중 지불을 방지하기 위해 송신자는 자신의 주소값에 대응하는 전자서명을 생성한다.
정답 체크 :
(4) 블록체인 내의 원장을 기존 내용을 수정할 수는 없다. 다만, 수정을 하게 되면 기존 내용은 보존되고 변경된 내용이 추가되는데 이때는 PoW 또는 PoS를 사용한다(개인키를 사용하지 않는다).
오답 체크 :
(1) 머클 루트는 해당 블록에 저장되어 있는 모든 거래의 요약본(해시값)으로 블록 헤더에 포함된다.
(2) 채굴은 특정한 해시값을 산출해 내는 것인데, 이는 해시값의 역상을 구하는 과정(해시값으로부터 원래의 메시지를 구함)과 동일하다.
(3) 암호화폐를 주고 받는 주소값은 공개키의 해시 값으로부터 작성한다.
(5) 송신자는 자신이 보낸 것을 증명하기 위해 전자서명(디지털서명)을 사용한다. 그리고 해당 정보와 PoW(작업증명) 또는 PoS(지분 증명)를 사용하여 이중 지불을 방지한다.

11. 대칭키 암호에 대한 설명으로 옳지 않은 것은?
① 부인방지 기능을 제공한다.
② 비대칭키 암호에 비해 속도가 빠르다.
③ 송신자와 수신자가 동일한 비밀키를 사용한다.
④ IDEA는 대칭키 암호 알고리즘이다.
⑤ RC4는 스트림 암호 알고리즘이다.
정답 체크 :
(1) 대칭키는 기밀성 또는 무결성, 인증을 제공할 수 있지만 부인방지 기능을 제공하지 않는다.
오답 체크 :
(2) 수학 연산에 기반하지 않기 때문에 속도가 빠르다.
(3) 송신자와 수신자가 동일한 비밀키를 사용한다.
(4) Lai-Massey가 개발하였고, 블록 길이가 64비트, 키 길이는 128비트, 라운드 수는 8.5이다.
(5) Rivest가 개발하였고, 40비트에서 2048비트의 키 길이를 가진다.

12. OSI 7계층 중 2계층 암호화 프로토콜로 짝지어진 것은?
① PPTP - SSL
② PPTP - IPSec

③ L2TP - IPSec
④ L2TP - SSL
⑤ PPTP - L2TP
정답 체크 :
(5) 터널링 프로토콜로서 2계층이다.
오답 체크 :
(1), (4) SSL은 4계층이다.
(2), (3) IPSec는 3계층이다.

13. 다음 설명에서 제시하는 접근 제어 정책은?

> 주체 또는 소속 그룹의 아이디(ID)에 근거하여 객체에 대한 접근 제한을 설정한다. 객체별로 세분화된 접근 제어가 가능하고, 유연한 접근 제어 서비스를 제공할 수 있어 다양한 환경에서 폭넓게 사용되고 있다.

① 강제적 접근 제어(Mandatory Access Control)
② 규칙 기반 접근 제어(Rule Based Access Control)
③ 역할 기반 접근 제어(Role Based Access Control)
④ 임의적 접근 제어(Discretionary Access Control)
⑤ 래티스 기반 접근 제어(Lattice Based Access Control)
정답 체크 :
(4) 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스(그룹 개념을 사용) 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
오답 체크 :
(1) 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어 시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
(2) 규칙에 기반한 접근 제어이다. 여기서 규칙이란 “어떤 데이터는 3:00부터 6:00까지만 접근이 허용된다”와 같은 것을 의미한다.
(3) 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.
(5) 객체들(자원, 컴퓨터, 어플리케이션)과 주체들(개인, 그룹, 조직) 사이의 상호작용에 기반을 둔 복잡한 접근 제어 모델이다. 주체가 접근할 수 있는 상위와 하위의 경계를 설정하여 해당 범위 내 임의 객체의 접근을 제한한다.

14. 전자서명 알고리즘 중 하나인 ECDSA(Elliptic Curve Digital Signature Algorithm)에 대한 설명으로 옳지 않은 것은?
① 타원곡선 상에서 이산대수 문제가 어렵다는 사실에 안전성의 근거를 두고 있다.
② 서명할 메시지를 해싱(Hashing)한 후 그 해시값을 ECDSA 서명 알고리즘에 입력한다.
③ 동일한 비도에서 RSA 전자서명보다 공개키 길이가 짧고 복호화가 빠르다는 장점을 갖는다.
④ 블록체인 환경에서 거래의 진위 여부를 검증하기 위해 사용된다.
⑤ 서명 생성 시 사용되는 난수는 메시지에 관계없이 동일하게 사용해야 안전하다.
정답 체크 :
(5) 메시지에 따라 서로 다른 난수를 사용해야 한다.

오답 체크 :
(1) 타원곡선 이산대수 문제(ECDLP)라고 한다.
(2) 서명 속도를 높이기 위해 해시값을 사용한다.
(3) RSA에 비해 키 길이가 짧고 이로 인해 복호화가 빠르다.
(4) 거래의 진위 여부를 검증하기 위해 전자서명을 사용한다.

15. Bob이 Alice의 공개키를 인증하는 과정이다. 순서대로 나열한 것은?

ㄱ. Alice는 자신의 공개키와 인증서를 Bob에게 전송한다.
ㄴ. Alice는 자신의 공개키를 인증기관에 보낸다.
ㄷ. Bob은 인증기관의 공개키로 Alice의 인증서를 검증한다.
ㄹ. Alice는 자신의 공개키와 개인키를 생성한다.
ㅁ. 인증기관은 Alice의 공개키에 대응하는 인증서를 발급한다.

① ㄹ - ㄱ - ㄴ - ㄷ - ㅁ
② ㄹ - ㄴ - ㄷ - ㄱ - ㅁ
③ ㄹ - ㄴ - ㅁ - ㄱ - ㄷ
④ ㅁ - ㄹ - ㄱ - ㄷ - ㄴ
⑤ ㅁ - ㄹ - ㄷ - ㄱ - ㄴ
정답 체크 :
(3)
ㄹ : Alice는 자신의 공개키와 개인키를 생성한다.
ㄴ : Alice는 자신의 공개키를 인증기관에 보낸다.
ㅁ : 인증기관은 Alice의 공개키에 자신의 개인키로 서명을 붙여 인증서를 발급한다(저장소에 보관).
ㄱ : Alice는 자신의 공개키와 인증서를 Bob에게 전송한다. (저장소에 있는 인증서를 Bob이 가져간다)
ㄷ : Bob은 인증기관의 공개키로 Alice의 인증서를 검증한다.

16. OWASP(Open Web Application Security Project) 2020에서 발표된 10가지 보안 위협에 속하지 않는 것은?
① Abuse of Cloud Computing
② Injection
③ XML External Entities
④ Broken Authentication
⑤ Sensitive Data Exposure
정답 체크
(1) 2019년도에 조사된 클라우드 컴퓨팅의 10가지 위협 중의 하나이다(wire19.com).
오답 체크
(2), (3), (4), (5) 2020년에 공식적으로 발표되지는 않았고, 2017년도에 발표된 것을 그대로 사용한다.
Injection
Broken Authentication
Sensitive Data Exposure
XML External Entities (XXE)

Broken Access control
Security misconfigurations
Cross Site Scripting (XSS)
Insecure Deserialization
Using Components with known vulnerabilities
Insufficient logging and monitoring

17. IPsec 보안 프로토콜에 대한 설명으로 옳지 않은 것은?
① IPsec 설정 시 송·수신자가 상대방의 IP 주소를 입력해야 한다.
② 전송모드는 원래의 IP 헤더에 새로운 IP 헤더를 추가한다.
③ ESP 프로토콜은 IP 패킷을 암호화하고 무결성까지 보장할 수 있다.
④ IKE 프로토콜은 인증된 Diffie-Hellman 키 교환 방식을 사용한다.
⑤ VPN(Virtual Private Network)을 구성하는 한 가지 방법이다.
정답 체크 :
(2) 전송모드는 기존 패킷을 사용하므로 원래의 IP 헤더를 사용한다.
오답 체크 :
(1) 정책 설정 과정에서 송•수신자의 IP 주소를 입력한다.
(3) ESP는 암호화, 인증, 무결성을 제공한다.
(4) IKE는 Diffie-Hellman을 사용한다.
(5) VPN은 IPSec 또는 SSL 등을 이용하여 구성할 수 있다.

18. 리눅스 서버에 저장된 first 파일의 접근 권한을 다음과 같이 설정하기 위한 명령어는?

rwsr--r--	1	test	test	8980	4월 18	14:18	first

① chmod 1644 first
② chmod 1744 first
③ chmod 2744 first
④ chmod 4644 first
⑤ chmod 4744 first
정답 체크 :
(5) setuid가 설정된 경우이다.
rws : 47 (참고로 rwx는 7)
r-- : 4
r-- : 4
정답 체크 :
(1), (2) sticky bit가 설정된 경우이다.
(3) setgid로 rwxr-sr--에 해당한다.
(5) rws는 rwx에 setuid가 설정된 것을 의미하므로 46으로 해석되지 않는다.

19. 2020년 8월 5일 개정된 「개인정보 보호법」에 대한 설명으로 옳지 않은 것은?
① 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위 내에서 정보주체에게 불이익이 발생하는지 여부 등

을 고려하여 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 없도록 함
② 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정개인을 알아볼 수 없도록 처리하는 것을 가명처리로 정의함
③ 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 함
④ 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행하도록 함
⑤ 개인정보처리자는 가명정보를 처리하는 경우 해당 정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적, 관리적 및 물리적 조치를 하도록 함
정답 체크)
(1) 제15조(개인정보의 수집 · 이용) ③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.
제17조(개인정보의 제공) ④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.
오답 체크)
(2) 제2조(정의) 1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
(3) 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
(4) 제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.
(5) 제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관 · 관리하는 등 해당 정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.

20. 다음 설명에서 제시하는 공격 유형은?

> 게시판의 글에 원본과 함께 악성 코드를 삽입하여 글을 읽을 경우 악성 코드가 실행되도록 하여 클라이언트의 정보를 유출하는 공격기법이다. 웹 페이지가 사용자로부터 입력 받은 데이터를 필터링하지 않고 그대로 동적으로 생성된 웹 페이지에 포함하여 사용자에게 재전송할 때 발생한다.

① SQL Injection
② XSS(Cross Site Scripting)
③ 파일 업로드 취약점
④ CSRF(Cross Site Request Forgery)
⑤ 쿠키/세션 위조
정답 체크 :

(2) 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

오답 체크 :

(1) 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.

(3) 어플리케이션 개발/운영 환경과 동일한 언어로 작성된 공격 파일을 웹 서버 측에 업로드 한 후, 원격으로 해당 파일에 접근하여 실행시키는 취약점으로, 작성된 공격 파일의 기능에 따라서 위험도가 다양해진다.

(4) 웹 사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹 사이트에 요청하게 하는 공격이다. 즉, 일단 사용자가 웹 사이트에 로그인한 상태에서 CSRF 공격 코드가 삽입된 페이지를 열면, 이후에는 사용자의 행동과 관계없이 사용자의 웹 브라우저와 공격 대상 웹 사이트 간의 상호 작용이 이루어진다.

(5) 적절히 보호되지 않은 쿠키를 사용하면 Cookie Injection 등과 같은 쿠키값 변조를 통하여 다른 사용자로의 위장 및 권한 사항 등의 문제가 생길 수 있다. 또한 쿠키 및 세션은 Cookie Sniffing 및 XSS를 통한 Cookie Hijacking 등과 같은 쿠키 값 복사를 통해 현재 활성화된 사용자의 권한 복제 위험성이 존재한다.