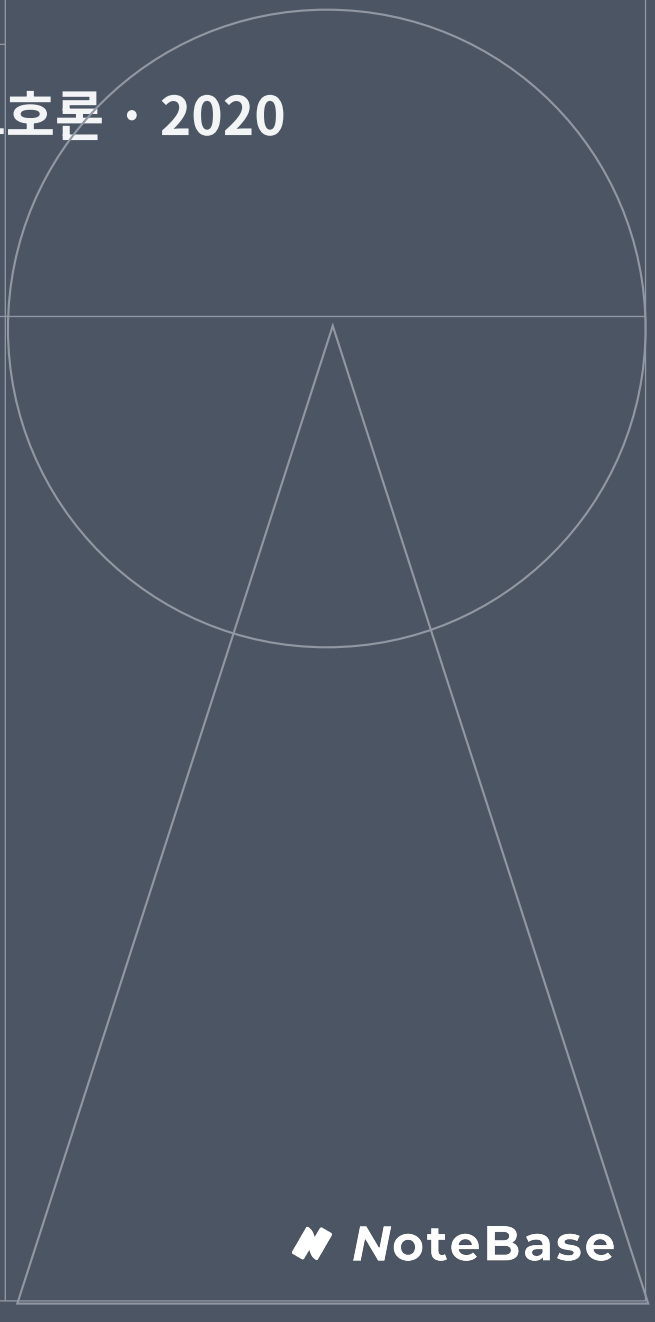
기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2020



NoteBase

기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2020

공무원/국회직/9급 · 정보보호론 · 2020

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 3번

출제 포인트

전자서명이 제공하는 인증·무결성·부인방지 기능과 암호화가 제공하는 기밀성 기능을 구별하는 문제이다.

핵심 개념

전자서명은 서명자의 신원을 확인하고 전자문서가 서명 후 변경되지 않았음을 검증하며, 서명 사실의 부인을 어렵게 하는 기술이다. 전자서명 자체는 문서 내용을 숨기지 않으므로 기밀성이 필요하면 별도의 암호화를 적용한다. 인증서는 공개키와 소유자의 신원 정보를 인증기관이 전자서명으로 결합한 전자문서이고, 인증서 폐기 목록(CRL)은 폐기된 인증서의 식별 정보를 담은 목록이다.

선지별 해설

① O — 인증서의 전자서명을 검증하면 인증서와 공개키의 진위를 확인할 수 있으므로, 인증서 로그인에서 사용자의 신원을 증명하는 데 활용할 수 있다.
② O — 배포자가 소프트웨어에 코드 서명을 하면 다운로드한 파일이 서명 후 변경되거나 위조되었는지 검증할 수 있다.
③ X — 전자서명은 이메일의 작성자와 무결성을 확인하지만 이메일 내용을 숨기지는 못한다. 틀린 표현은 '이메일 내용이 중간 메일서버에 노출되지 않도록 한다'이며, 올바르게는 '이메일 내용을 중간 메일서버에 노출하지 않으려면 내용을 암호화한다'이다.
④ O — 웹서버 인증서에 대한 인증기관의 전자서명을 검증하면 인증서가 신뢰할 수 있는 기관에서 발급되었는지와 통신 상대 서버의 사이트가 유효한지 확인할 수 있다.
⑤ O — 인증기관은 폐기된 인증서의 식별 정보를 인증서 폐기 목록(CRL)으로 발행하고 전자서명하여 목록의 출처와 무결성을 검증할 수 있게 한다.

NoteBase

오답 포인트

③은 전자서명과 암호화를 혼동하게 만든 선지이다. 전자서명은 누가 보냈는지와 내용이 바뀌지 않았는지를 검증하지만, 제3자가 내용을 읽지 못하게 하는 기능은 암호화가 담당한다.

다시 나오면 이렇게 판단

‘신원 확인·변조 검증·서명 부인 방지’가 핵심이면 전자서명의 활용이고, ‘내용을 보이지 않게 함·노출 방지·비밀 유지’가 핵심이면 암호화의 활용으로 판단한다.

암기 포인트

전자서명은 인증·무결성·부인방지, 암호화는 기밀성이다.

NoteBase

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 2번

출제 포인트

NAC가 수행하는 네트워크 접근 통제와 데이터 통신 내용의 암호화를 구별하는 문제이다.

핵심 개념

NAC(Network Access Control)는 네트워크에 접속하려는 사용자와 단말을 식별하고 보안 정책 준수 여부를 검사하여 접속을 허용·제한·차단하는 체계이다. 핵심은 '누가 어떤 상태로 네트워크에 들어오는가'를 통제하는 것이며, 데이터 패킷 자체를 암호문으로 바꾸는 것은 VPN, IPsec, TLS 같은 암호화 기술의 역할이다.

선지별 해설

① O — NAC는 PC와 네트워크 장치의 접속 상태를 확인하고, 정책에 맞지 않는 장치의 네트워크 이용을 제한하거나 격리할 수 있다.
② X — 틀린 표현은 '데이터 패킷 암호화'이다. NAC는 접속 주체와 단말의 상태를 검사하여 접근을 통제하는 시스템이며, 올바르게는 데이터 패킷 암호화는 VPN, IPsec, TLS 등 암호화 통신 기술의 기능이다.
③ O — 접근 제어는 인증 결과와 보안 정책에 따라 네트워크 접속을 허용하거나 차단하는 NAC의 핵심 기능이다.
④ O — NAC는 보안 정책을 위반했거나 웜 등에 감염된 단말을 탐지하여 격리하고, 해당 단말에서 발생하는 유해한 네트워크 접근을 차단할 수 있다.
⑤ O — NAC는 사용자·단말의 신원을 확인하는 인증 절차를 접근 허용 판단과 연계한다.

오답 포인트

'정보보호 시스템이므로 암호화도 수행한다'고 넓게 생각하면 ②를 놓치기 쉽다. NAC의 중심은 접속 전후의 인증·검사·접근 통제이고, 패킷의 기밀성을 확보하는 암호화는 별도의 보안 통신 기능이다. 또한 ④는 NAC가 모든 침입을 패킷 내용으로 분석한다는 뜻이라기보다, 위험 단말을 탐지·격리하여 그 단말의 트래픽을 차단한다는 의미로 판단한다.

NoteBase

다시 나오면 이렇게 판단

선지가 사용자·단말 인증, 보안 상태 점검, 접속 허용·차단, 격리에 관한 것이면 NAC 기능으로 판단한다. 데이터 내용의 암호화·복호화처럼 통신 기밀성 자체를 제공하는 기능이면 NAC의 고유 기능이 아닌 것으로 판단한다.

암기 포인트

NAC는 접속을 통제하고, VPN·IPsec·TLS는 통신 내용을 암호화한다.

NoteBase

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 5번

출제 포인트

X.509 인증서의 주요 필드가 누구와 무엇을 나타내는지 구분하는 문제이다.

핵심 개념

X.509 인증서는 공개키와 그 소유자의 신원 정보를 결합하고, 발급자인 인증기관이 그 결합 내용을 전자서명하여 신뢰성을 보증하는 전자 문서이다. Version은 인증서 형식의 버전, Serial number는 발급 인증기관이 부여한 인증서 식별번호, Issuer는 발급자, Subject는 공개키가 귀속되는 주체, Signature는 발급자의 개인키로 생성한 전자서명에 해당한다.

선지별 해설

① O — Version은 해당 인증서가 따르는 X.509 인증서 형식의 버전 정보를 나타낸다.
② O — Serial number는 인증기관이 발급한 인증서를 구별하기 위해 부여하는 고유번호이다. 동일한 발급 인증기관이 발급한 인증서들 사이에서 유일해야 한다.
③ O — Issuer name은 인증서를 발급하고 서명한 인증기관의 식별 정보를 나타낸다.
④ O — Subject name은 인증서에 담긴 공개키가 누구에게 귀속되는지를 나타내는 공개키 소유 주체의 식별 정보이다.
⑤ X — 틀린 표현은 '공개키 소유자가 생성한 서명 정보'이다. Signature는 원칙적으로 인증서 발급자인 인증기관이 인증서 본문을 자신의 개인키로 서명하여 생성한 값이다. 따라서 '인증기관이 자신의 개인키로 생성한 서명 정보'로 고쳐야 한다.

오답 포인트

인증서에 들어 있는 공개키의 소유자와 인증서에 전자서명하는 주체를 혼동하기 쉽다. 공개키의 소유자는 Subject이고, 인증서의 서명자는 Issuer인 인증기관이다.

NoteBase

다시 나오면 이렇게 판단

각 필드를 '발급자·소유자·식별번호·서명자'로 나누어 판단한다. Issuer는 발급자, Subject는 공개키 소유 주체, Serial number는 발급자가 부여한 인증서 번호, Signature는 발급자가 개인키로 만든 전자서명이다.

암기 포인트

Issuer가 발급하고 서명하며, Subject가 공개키를 소유한다.

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 2번

출제 포인트

이 문제는 버퍼가 할당된 메모리 영역과 길이 검사가 없는 문자열 복사의 결과를 바탕으로 버퍼 오버플로우 유형을 구별하는 문제이다.

핵심 개념

힙 버퍼 오버플로우는 동적 메모리 영역인 힙에 할당된 버퍼의 경계를 넘어 데이터를 쓰는 취약점이다. 이 프로그램의 buf가 가리키는 256바이트 공간은 malloc으로 힙에 할당되며, strcpy는 목적지 버퍼의 크기를 확인하지 않고 argv[1]의 문자열과 널 종료 문자를 복사한다. 따라서 입력 문자열이 버퍼에 들어갈 수 있는 길이를 넘으면 힙 영역의 경계를 침범한다.
스택 버퍼 오버플로우는 스택에 놓인 배열 등의 경계를 넘는 경우이고, 힙 버퍼 오버플로우는 malloc 등으로 동적 할당한 공간의 경계를 넘는 경우이다. 취약점의 유형은 포인터 변수 자체의 위치가 아니라 실제 복사 대상 버퍼가 할당된 위치로 판단한다.

NoteBase

선지별 해설

① X — buf라는 포인터 변수는 지역변수이지만, strcpy의 실제 목적지인 buf가 가리키는 256바이트 버퍼는 malloc으로 힙에 할당된다. 틀린 표현은 '스택 버퍼 오버플로우'이며, 올바르게는 '힙 버퍼 오버플로우'이다.
② O — 힙에 할당된 고정 크기 버퍼에 길이를 검사하지 않는 strcpy로 외부 입력 argv[1]을 복사하므로 힙 버퍼 오버플로우가 발생할 수 있다.
③ X — 형식 문자열을 해석하는 printf 계열 함수나 사용자 입력을 형식 문자열로 사용하는 코드가 없다. 틀린 표현은 '포맷 스트링 공격'이며, 올바르게는 '힙 버퍼 오버플로우 공격'이다.
④ X — 공격자가 제어하는 정수의 산술 연산이 넘쳐 할당 크기가 작아지는 구조가 아니다. 틀린 표현은 '정수 오버플로우 공격'이며, 올바르게는 '길이 검사가 없는 문자열 복사에 의한 힙 버퍼 오버플로우 공격'이다.
⑤ X — 여러 실행 흐름이 공유 자원에 접근하며 실행 순서에 따라 결과가 달라지는 동시성 구조가 없다. 틀린 표현은 '레이스 컨디션 공격'이며, 올바르게는 '힙 버퍼 오버플로우 공격'이다.

오답 포인트

buf가 main 함수 안에 선언된 지역 포인터라는 점만 보고 ①을 고르기 쉽다. 그러나 넘치는 대상은 포인터 변수 buf 자체가 아니라 malloc이 반환한 메모리 공간이다. 또한 strcpy의 핵심 위험은 형식 문자열이나 정수 연산이 아니라 목적지 크기를 확인하지 않는 복사이다.

다시 나오면 이렇게 판단

먼저 쓰기 대상 버퍼가 어디에 할당되었는지 확인한다. 지역 배열이면 스택, malloc·calloc 등으로 동적 할당된 공간이면 힙으로 본다. 그다음 strcpy처럼 입력 길이를 제한하지 않는 함수가 버퍼 크기를 넘겨 쓸 수 있는지를 판단한다.

암기 포인트

malloc 버퍼에 무제한 strcpy 복사 → 힙 버퍼 오버플로우이다.

NoteBase

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 3번

출제 포인트

CBC 모드에서 초기벡터의 사용, 블록 간 연쇄성, 오류 전파, 처리 순서, 암호화·복호화에 필요한 연산을 구별하는 문제이다.

핵심 개념

CBC는 현재 평문 블록 P_i를 직전 암호문 블록 C_{i-1}과 결합한 뒤 암호화하여 현재 암호문 블록 C_i를 만드는 운영모드이다. 첫 블록에는 직전 암호문 대신 초기벡터(IV)를 사용한다.

ㄱ O: IV는 같은 키로 여러 메시지를 암호화할 때마다 새로 생성하여 사용해야 하며, 일반적으로 무작위이고 예측하기 어려워야 한다.

ㄴ X: 같은 평문 블록이라도 직전 암호문 블록이 다르면 암호화 입력이 달라지므로 대응하는 암호문 블록은 같지 않을 수 있다.

ㄷ O: 암호화 전에 평문 블록 P_2에 생긴 오류는 C_2를 바꾸고, 변경된 암호문이 다음 블록의 입력에 연쇄적으로 사용되므로 이후 암호화 결과에도 파급된다.

ㄹ O: 각 블록의 암호화에는 직전 암호문 블록이 필요하므로 P_1부터 P_n까지 순차적으로 암호화한다.

ㅁ X: CBC 복호화에는 블록 암호의 복호화 연산이 필요하므로 암호화 알고리즘만으로 암호화와 복호화를 모두 수행할 수 없다. 따라서 옳은 것은 ㄱ, ㄷ, ㄹ이다.

NoteBase

선지별 해설

① X: ㄱ과 ㄹ은 옳지만 ㄴ이 틀렸다. 같은 평문 블록이라도 직전 암호문 블록이 다르면 대응하는 암호문 블록도 달라질 수 있다. 올바른 조합은 ㄱ, ㄷ, ㄹ이다.
② X: ㄱ은 옳지만 ㄴ과 ㅁ이 틀렸다. 같은 평문 블록이 같은 암호문 블록을 만든다고 단정할 수 없고, CBC 복호화에는 블록 암호의 복호화 연산이 필요하다. 올바른 조합은 ㄱ, ㄷ, ㄹ이다.
③ O: ㄱ은 새로운 IV의 사용, ㄷ은 평문 오류의 후속 암호화 전파, ㄹ은 연쇄 구조에 따른 순차 암호화를 정확히 설명한다.
④ X: ㄷ과 ㄹ은 옳지만 ㄴ이 틀렸고 옳은 ㄱ이 빠져 있다. 같은 평문 블록이라도 연쇄 입력이 다르면 암호문 블록은 달라질 수 있으며, 올바른 조합은 ㄱ, ㄷ, ㄹ이다.
⑤ X: ㄷ과 ㄹ은 옳지만 ㅁ이 틀렸고 옳은 ㄱ이 빠져 있다. CBC의 암호화와 복호화에는 각각 블록 암호의 암호화 연산과 복호화 연산이 필요하며, 올바른 조합은 ㄱ, ㄷ, ㄹ이다.

오답 포인트

ㄴ은 ECB처럼 같은 평문 블록이 같은 암호문 블록을 만든다고 착각하게 하는 함정이다. CBC에서는 직전 암호문이 다음 블록에 섞인다. 또한 ㄷ은 암호화 전 평문 P_2의 오류를 묻는다. 전송 중 암호문 블록에 생긴 오류의 복호화 전파와 혼동하면 안 된다. ㅁ은 CFB·OFB처럼 블록 암호의 암호화 연산만 사용하는 모드의 성질을 CBC에 잘못 적용한 표현이다.

다시 나오면 이렇게 판단

CBC는 '새 IV 사용 → 직전 암호문과 결합 → 순차 암호화'의 연쇄 구조로 판단한다. 평문 오류가 암호화 입력에서 생기면 뒤의 암호문까지 연쇄적으로 달라지고, CBC 복호화에는 블록 암호의 복호화 연산이 필요하다는 점을 함께 확인한다.

암기 포인트

CBC는 새 IV, 암호문 연쇄, 순차 암호화, 복호화 연산 필요로 기억한다.

NoteBase

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 3번

출제 포인트

TLS 세션을 처음 설정할 때 인증, 암호 알고리즘 협상, 세션 키 생성에 필요한 정보 교환을 담당하는 하부 프로토콜을 구별하는 문제이다.

핵심 개념

Handshake 프로토콜은 클라이언트와 서버가 TLS 버전과 암호 스위트 등 보안 매개변수를 협상하고, 서버 인증 및 필요한 경우 클라이언트 인증을 수행하며, 세션 키를 만들기 위한 정보를 교환하는 절차이다.
Change Cipher Spec 프로토콜은 협상된 암호 명세를 이후 통신에 적용한다는 전환 신호를 전달한다.
두 프로토콜의 결정적 차이는 Handshake가 보안 조건을 협상하고 키를 수립하는 반면, Change Cipher Spec은 이미 협상된 조건의 적용 전환을 알린다는 점이다.

NoteBase

선지별 해설

① X
One Time Password 프로토콜은 한 번만 사용할 수 있는 비밀번호를 이용하는 인증 방식이므로, TLS 세션의 암호 스위트 협상과 세션 키 수립을 담당하지 않는다. 틀린 표현은 'One Time Password 프로토콜'이며, 올바르게는 'Handshake 프로토콜'이다.

② X
Secure Electronic Transaction 프로토콜은 전자상거래의 카드 결제를 보호하기 위해 설계된 보안 프로토콜이므로, TLS 세션 설정을 담당하는 하부 프로토콜이 아니다. 틀린 표현은 'Secure Electronic Transaction 프로토콜'이며, 올바르게는 'Handshake 프로토콜'이다.

③ O
Handshake 프로토콜은 TLS 세션 시작 시 통신 상대를 인증하고 암호 스위트 등 암호 관련 정보를 협상하며 세션 키 생성에 필요한 정보를 교환한다.

④ X
Document Object Model은 HTML·XML 문서를 객체 트리로 표현하고 조작하기 위한 문서 모델이므로, TLS 보안 프로토콜이 아니다. 틀린 표현은 'Document Object Model 프로토콜'이며, 올바르게는 'Handshake 프로토콜'이다.

⑤ X
Change Cipher Spec 프로토콜은 협상된 암호 명세를 이후 레코드에 적용한다는 사실을 상대방에게 알리는 역할을 하며, 인증·알고리즘 협상·세션 키 수립 자체를 담당하지 않는다. 틀린 표현은 'Change Cipher Spec 프로토콜'이며, 올바르게는 'Handshake 프로토콜'이다.

오답 포인트

⑤의 Change Cipher Spec도 TLS 하부 프로토콜이어서 혼동하기 쉽다. 그러나 문제의 핵심 표현인 '상호 인증', '암호 메커니즘 정보 교환', '세션 키 생성'은 협상과 키 수립을 수행하는 Handshake를 가리킨다.

다시 나오면 이렇게 판단

TLS 연결 초기에 인증, 암호 스위트 협상, 키 교환 또는 세션 키 수립이 제시되면 Handshake로 판단한다. 협상된 암호 명세를 이제부터 적용한다는 전환 통지라면 Change Cipher Spec으로 판단한다.

암기 포인트

Handshake는 협상·인증·키 수립, Change Cipher Spec은 협상 결과의 적용 전환이다.

NoteBase

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 4번

출제 포인트

이 문제는 PGP의 전자서명, 혼합 암호화, 이메일 연동 방식과 공개키 알고리즘을 구분하는 문제이다.

핵심 개념

PGP는 이메일과 파일을 암호화하고 전자서명하는 보안 방식이다. 기밀성에는 빠른 대칭키 암호와 키 전달을 위한 공개키 암호를 함께 사용하고, 전자서명으로 송신자 인증·무결성·송신 부인방지를 제공한다. 또한 이메일 응용 프로그램과 연동하거나 독립 프로그램으로 사용할 수 있다.

선지별 해설

① O — 전자서명은 송신자의 개인키로 생성되므로 송신자가 보낸 사실을 부인하기 어렵게 한다. 그러나 수신자가 실제로 메시지를 받았거나 읽었다는 사실까지 증명하지는 않으므로 수신 부인방지는 지원하지 않는다.
② O — 실제 메시지는 처리 속도가 빠른 대칭키로 암호화하고, 그 대칭키는 수신자의 공개키를 이용해 보호하는 혼합 암호 방식을 사용한다.
③ O — PGP는 메시지나 파일의 해시값을 송신자의 개인키로 서명하고, 수신자가 송신자의 공개키로 이를 검증하여 서명자의 신원과 내용의 무결성을 확인한다.
④ X — 틀린 표현은 '플러그인 기능으로 확장 불가능'이다. 올바르게는 PGP를 이메일 응용 프로그램의 플러그인 또는 연동 기능으로 확장하여 사용할 수 있다.
⑤ O — PGP의 공개키 처리에는 RSA를 사용하는 방식과 Diffie-Hellman 계열의 키 관리 방식을 사용하는 버전이 존재한다.

오답 포인트

④의 '확장 불가능'이라는 단정이 함정이다. PGP는 이메일과 별개인 독립 도구로만 작동하는 것이 아니라 이메일 응용 프로그램에 연동하여 암호화와 전자서명 기능을 제공할 수 있다.

NoteBase

다시 나오면 이렇게 판단

PGP 문항에서는 전자서명은 송신자 인증·무결성·송신 부인방지, 혼합 암호화는 대칭키로 본문 암호화·공개키로 세션키 보호, 사용 형태는 이메일 연동 가능으로 나누어 판단한다.

암기 포인트

PGP는 서명과 혼합 암호화를 제공하며 이메일에 연동할 수 있다.

NoteBase

8. 리눅스 시스템에서 사용자 로그인 실패 정보가 저장되는 파일은?

① btmp
② extmp
③ wtmp
④ utmp
⑤ atmp

정답 1번

출제 포인트

리눅스의 로그인 기록 파일 중 로그인 실패 기록을 저장하는 btmp와 현재 로그인 상태를 기록하는 utmp, 로그인·로그아웃 이력을 기록하는 wtmp를 구분하는 문제이다.

핵심 개념

btmp: 실패한 로그인 시도를 기록하는 파일이며 lastb 명령으로 확인할 수 있다.
utmp: 현재 로그인한 사용자의 세션 정보를 기록한다.
wtmp: 로그인과 로그아웃의 누적 이력을 기록한다.

선지별 해설

① O — btmp는 로그인 실패 정보를 저장하므로 문제의 조건에 정확히 해당한다.
② X — 틀린 표현은 extmp이다. extmp는 리눅스의 표준 로그인 실패 기록 파일이 아니며, 올바른 파일명은 btmp이다.
③ X — 틀린 표현은 wtmp이다. wtmp는 로그인과 로그아웃의 누적 이력을 저장하며, 로그인 실패 정보는 btmp에 저장된다.
④ X — 틀린 표현은 utmp이다. utmp는 현재 로그인 중인 사용자와 세션 상태를 기록하며, 로그인 실패 정보는 btmp에 저장된다.
⑤ X — 틀린 표현은 atmp이다. atmp는 리눅스의 표준 로그인 실패 기록 파일이 아니며, 올바른 파일명은 btmp이다.

오답 포인트

btmp, utmp, wtmp는 이름이 비슷하다. 특히 wtmp도 로그인 관련 이력을 저장하지만, 실패한 로그인 시도만을 묻는 경우에는 btmp를 선택해야 한다.

다시 나오면 이렇게 판단

실패한 로그인은 btmp, 현재 로그인 상태는 utmp, 로그인·로그아웃 누적 이력은 wtmp로 구분한다.

NoteBase

암기 포인트

btmp의 b는 bad login, utmp는 현재 사용자, wtmp는 누적 로그인 이력으로 연결한다.

NoteBase

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 1번

출제 포인트

최근 보안 위협의 명칭과 공격 대상·동작 방식을 올바르게 연결할 수 있는지를 묻는 문제이다.

핵심 개념

BlueKeep은 원격 데스크톱 프로토콜(RDP) 서비스의 취약점으로, 인증 전 단계에서 원격 코드 실행이 가능하다.
Dark Web은 일반 검색 엔진으로 접근하기 어렵고 전용 소프트웨어나 설정을 이용해 접속하는 비공개성 인터넷 영역이다.
Deepfake는 인공지능으로 사람의 얼굴·음성·영상 등을 실제처럼 합성하거나 변조하는 기술이다.
Emotet은 주로 피싱 메일의 악성 첨부 파일이나 링크로 유포되는 악성코드이며, 다른 악성코드를 내려받는 로더로도 활용되었다.
Sodinokibi는 REvil로도 불리는 랜섬웨어로, 파일을 암호화하고 금전을 요구한다.

NoteBase

선지별 해설

① O — BlueKeep은 취약한 Windows의 원격 데스크톱 서비스에서 사용자 인증 없이 원격 코드 실행을 가능하게 하는 취약점이다. 따라서 제시된 설명은 옳다.
② X — 틀린 부분은 'Dark Web'을 피싱 메일로 유포되는 금융정보 탈취 악성코드라고 한 것이다. 올바르게는 Dark Web은 전용 소프트웨어나 설정을 통해 접근하는 비공개성 인터넷 영역이다. 피싱 메일을 통한 유포와 정보 탈취는 악성코드의 공격 방식에 해당한다.
③ X — 틀린 부분은 'Deepfake'를 특정 웹브라우저를 통해 익명성이 보장되는 인터넷 영역이라고 한 것이다. 올바르게는 Deepfake는 인공지능으로 음성·얼굴·영상을 실제처럼 합성하거나 변조하는 기술이며, 익명성이 강조되는 인터넷 영역은 Dark Web이다.
④ X — 틀린 부분은 'Emotet'을 한글 메일 속 정상 파일로 위장한 랜섬웨어라고 한 것이다. 올바르게는 Emotet은 피싱 메일의 악성 첨부 파일이나 링크 등으로 유포되는 악성코드로, 정보 탈취나 다른 악성코드 설치에 활용된다. 랜섬웨어 자체를 뜻하지 않는다.
⑤ X — 틀린 부분은 'Sodinokibi'를 인공지능 기반의 음성·영상 조작이라고 한 것이다. 올바르게는 Sodinokibi는 파일을 암호화하고 몸값을 요구하는 랜섬웨어이며, 인공지능으로 음성·영상을 합성·조작하는 것은 Deepfake이다.

오답 포인트

선지들은 실제 보안 용어의 정의를 서로 바꾸어 배치했다. 특히 ③은 Dark Web의 설명을 Deepfake에 붙였고, ⑤는 Deepfake의 설명을 Sodinokibi에 붙였다. ④에서는 피싱 메일로 유포된다는 특징만 보고 Emotet을 랜섬웨어로 오인하기 쉽지만, Emotet의 핵심은 악성코드 유포·정보 탈취·추가 악성코드 설치에 활용되는 악성코드라는 점이다.

다시 나오면 이렇게 판단

각 용어를 '취약점·인터넷 영역·합성 기술·악성코드·랜섬웨어'로 먼저 분류한다. BlueKeep은 RDP 취약점, Dark Web은 익명성 중심의 인터넷 영역, Deepfake는 AI 합성, Emotet은 피싱 기반 악성코드, Sodinokibi는 파일 암호화 랜섬웨어로 판단한다.

암기 포인트

BlueKeep=RDP 취약점, Dark Web=비공개성 인터넷 영역, Deepfake=AI 합성, Emotet=피싱 기반 악성코드, Sodinokibi=REvil 랜섬웨어이다.

NoteBase

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 4번

출제 포인트

이 문제는 블록체인의 무결성 구조, 작업증명 채굴, 주소와 공개키의 관계, 전자서명의 역할을 구분하는 문제이다.

핵심 개념

머클 루트는 블록에 담긴 거래들을 해시 트리로 요약한 최상위 해시값이며 블록 헤더에 기록된다. 채굴은 블록 헤더의 해시값이 난이도 목표를 만족하도록 논스 등을 반복해서 바꾸어 찾는 작업이다. 개인키는 거래에 전자서명하여 자금 사용 권한을 증명하는 데 쓰이며, 이미 확정된 블록체인 원장을 임의로 수정하는 열쇠가 아니다. 원장 무결성은 이전 블록 해시의 연결과 네트워크 합의로 유지된다.

NoteBase

선지별 해설

① O — 각 거래의 해시를 머클 트리로 결합한 최상위 값이 머클 루트이며, 블록 헤더에 포함되어 거래 내역의 무결성을 확인하는 데 사용된다.

② O — 작업증명 방식의 채굴은 논스 등을 바꾸어 가며 주어진 난이도 목표를 만족하는 해시값을 찾는 과정이다. 즉, 목표 조건에 맞는 해시 입력을 반복 탐색한다는 취지의 설명이다.

③ O — 일반적인 암호화폐 주소는 공개키 자체 또는 공개키를 해시한 값을 바탕으로 만들어지며, 자금을 주고받을 목적지 식별자로 사용된다.

④ X — 틀린 표현은 '블록체인 내의 원장을 수정하기 위해서는 개인키를 사용해야 한다'이다. 개인키는 거래를 전자서명하여 해당 자금의 사용 권한을 증명할 때 사용한다. 블록체인 원장을 바꾸려면 해당 블록과 뒤따르는 블록의 해시 연결을 다시 구성하고 네트워크의 합의 조건까지 충족해야 하므로, 개인키만으로 기존 원장을 임의 수정할 수 없다.

⑤ O — 송신자는 자신의 주소에 대응하는 개인키로 거래의 전자서명을 생성한다. 노드는 서명을 검증하여 정당한 소유자의 거래인지 확인하고, 이미 사용된 자금을 다시 쓰는 거래는 원장 상태와 합의 규칙에 따라 배제하므로 이중 지불을 방지한다.

오답 포인트

④는 개인키가 거래를 승인하는 수단이라는 사실을 원장 자체를 수정하는 수단으로 바꾸어 놓았다. 또한 ⑤의 전자서명은 사용 권한을 증명하고, 실제 이중 지불 여부는 노드가 원장 상태와 합의 규칙으로 함께 검증한다는 점을 구분해야 한다.

다시 나오면 이렇게 판단

개인키가 등장하면 먼저 '거래 서명과 소유권 증명'에 관한 설명인지 확인한다. 기존 원장의 변경 방지는 해시 연결과 합의의 역할이고, 주소 생성은 공개키 또는 그 해시값, 거래 승인은 개인키 전자서명의 역할로 구분한다.

암기 포인트

공개키의 해시는 주소, 개인키는 서명, 머클 루트는 거래 요약, 해시 연결과 합의는 원장 무결성이다.

NoteBase

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 1번

출제 포인트

대칭키 암호의 키 사용 방식과 성질, 대표 알고리즘을 구별하는 문제이다.

핵심 개념

대칭키 암호는 송신자와 수신자가 공유한 동일한 비밀키로 암호화와 복호화를 수행하는 방식이다. 연산이 비교적 단순하여 비대칭키 암호보다 빠르지만, 양쪽이 같은 키를 알고 있으므로 누가 암호문이나 인증값을 만들었는지를 제3자에게 독점적으로 증명할 수 없어 부인방지를 제공하지 못한다. IDEA는 대칭키 블록 암호이고, RC4는 대칭키 스트림 암호이다.

선지별 해설

① X — 틀린 표현은 '부인방지 기능을 제공한다'이다. 대칭키는 송신자와 수신자가 같은 비밀키를 공유하므로 어느 쪽이 데이터를 생성했는지 제3자에게 독점적으로 증명할 수 없다. 올바르게는 '대칭키 암호만으로는 부인방지를 제공할 수 없으며, 부인방지에는 개인키로 서명하고 공개키로 검증하는 전자서명과 같은 비대칭키 기반 방식이 사용된다'이다.
② O — 대칭키 암호는 비대칭키 암호보다 연산이 단순하여 일반적으로 암호화와 복호화 속도가 빠르다.
③ O — 대칭키 암호에서는 송신자와 수신자가 사전에 공유한 동일한 비밀키를 사용한다. 이 공유키의 안전한 분배와 관리가 핵심 과제이다.
④ O — IDEA는 64비트 블록과 128비트 키를 사용하는 대칭키 블록 암호 알고리즘이다.
⑤ O — RC4는 키로부터 의사난수 키스트림을 만들고 평문과 결합하는 대칭키 스트림 암호 알고리즘이다.

오답 포인트

①의 '부인방지'를 대칭키 암호가 제공하는 기밀성과 혼동하기 쉽다. 공유키를 아는 당사자 모두가 같은 결과를 만들 수 있으므로 대칭키 방식만으로는 특정 송신자만 생성했다는 사실을 증명하지 못한다.

NoteBase

다시 나오면 이렇게 판단

‘같은 비밀키 공유·빠른 처리·블록 또는 스트림 암호’는 대칭키의 특징으로 판단한다. ‘송신자만 생성 가능함을 공개적으로 증명·부인방지’가 나오면 개인키와 공개키를 구분하는 전자서명의 성질인지 확인한다.

암기 포인트

대칭키는 같은 키로 빠르게, 전자서명은 개인키로 서명하여 부인방지를 제공한다. IDEA는 블록, RC4는 스트림이다.

NoteBase

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 5번

출제 포인트

OSI 7계층에서 VPN 관련 프로토콜이 동작하는 계층을 구분하는 문제이다. PPTP와 L2TP는 모두 2계층인 데이터 링크 계층의 터널링 프로토콜로 분류된다.

핵심 개념

PPTP: PPP 프레임을 IP 네트워크를 통해 전달하도록 터널링하는 데이터 링크 계층 프로토콜이다.
L2TP: L2F와 PPTP의 특성을 결합하여 PPP 프레임을 터널링하는 데이터 링크 계층 프로토콜이다. 자체적으로 기밀성을 제공하지 않아 실제 VPN에서는 흔히 IPsec과 함께 사용된다.
IPsec: IP 패킷을 보호하는 네트워크 계층 프로토콜이다.
SSL/TLS: 응용 프로그램과 전송 계층 사이에서 통신 보안을 제공하므로 데이터 링크 계층 프로토콜이 아니다.

선지별 해설

① X — PPTP는 2계층이지만 SSL은 2계층이 아니다. 틀린 표현은 'SSL'이며, 2계층 프로토콜로 고치면 'PPTP - L2TP'가 된다.
② X — PPTP는 2계층이지만 IPsec은 IP 패킷을 보호하는 3계층 프로토콜이다. 틀린 표현은 'IPsec'이며, 2계층 프로토콜로 고치면 'PPTP - L2TP'가 된다.
③ X — L2TP는 2계층이지만 IPsec은 3계층이다. 틀린 표현은 'IPsec'이며, 2계층 프로토콜로 고치면 'L2TP - PPTP'가 된다.
④ X — L2TP는 2계층이지만 SSL은 2계층이 아니다. 틀린 표현은 'SSL'이며, 2계층 프로토콜로 고치면 'L2TP - PPTP'가 된다.
⑤ O — PPTP와 L2TP는 모두 PPP 프레임을 캡슐화하여 전달하는 2계층 터널링 프로토콜이다.

오답 포인트

L2TP가 실제로 IPsec과 함께 사용되는 경우가 많다는 점 때문에 두 프로토콜을 같은 계층으로 착각하기 쉽다. L2TP는 2계층 터널링을 담당하고, IPsec은 3계층에서 IP 패킷의 인증·기밀성·무결성을 제공한다.

NoteBase

다시 나오면 이렇게 판단

PPP 프레임을 터널링하는 PPTP·L2TP는 2계층, IP 패킷 자체를 보호하는 IPsec은 3계층으로 판단한다. SSL/TLS는 데이터 링크 계층이 아니므로 2계층 묶음에서 제외한다.

암기 포인트

2계층 터널링은 PPTP·L2TP, 3계층 보안은 IPsec이다.

NoteBase

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 4번

출제 포인트

접근 권한을 결정하는 기준이 사용자·그룹의 신원인지, 보안 등급인지, 역할인지, 규칙인지 구분하는 문제이다.

핵심 개념

임의적 접근 제어(DAC)는 객체의 소유자가 사용자 또는 그룹의 신원(ID)을 기준으로 해당 객체의 접근 권한을 자율적으로 부여·변경하는 방식이다. 객체마다 권한을 세밀하게 설정할 수 있어 유연성이 높다.
강제적 접근 제어(MAC)는 보안 등급과 보안 레이블에 따라 중앙 정책이 접근을 강제한다. 규칙 기반 접근 제어는 미리 정한 규칙과 조건으로 접근을 결정하고, 역할 기반 접근 제어(RBAC)는 직무·역할에 권한을 부여한다.
래티스 기반 접근 제어(LBAC)는 보안 등급 사이의 격자형 지배 관계를 이용한다.

선지별 해설

① X — 틀린 표현은 '강제적 접근 제어'이다. 강제적 접근 제어는 사용자·그룹 ID에 따른 소유자의 재량이 아니라 주체와 객체의 보안 등급·레이블 및 중앙 정책에 따라 접근을 통제한다. 제시문의 방식은 임의적 접근 제어이다.
② X — 틀린 표현은 '규칙 기반 접근 제어'이다. 규칙 기반 접근 제어는 시간, 위치, 요청 유형 등 미리 정한 규칙이나 조건을 기준으로 접근을 결정한다. 사용자·그룹 ID를 기준으로 객체별 권한을 유연하게 설정하는 제시문은 임의적 접근 제어이다.
③ X — 틀린 표현은 '역할 기반 접근 제어'이다. 역할 기반 접근 제어는 개별 사용자 ID가 아니라 직무나 역할에 권한을 묶고 사용자를 그 역할에 배정한다. 제시문의 방식은 임의적 접근 제어이다.
④ O — 임의적 접근 제어는 객체 소유자의 재량 아래 사용자 또는 그룹의 ID를 기준으로 객체별 접근 권한을 세분화한다. 유연한 권한 설정이 가능하다는 제시문의 특징과 일치한다.
⑤ X — 틀린 표현은 '래티스 기반 접근 제어'이다. 래티스 기반 접근 제어는 사용자·그룹 ID 자체가 아니라 보안 등급과 범주가 이루는 격자형 지배 관계를 기준으로 접근을 판단한다. 제시문의 방식은 임의적 접근 제어이다.

NoteBase

오답 포인트

‘접근 제한을 설정한다’는 표현만 보고 통제가 강하다는 뜻의 강제적 접근 제어를 고르기 쉽다. 그러나 결정적 단서는 ‘주체 또는 소속 그룹의 ID’, ‘객체별로 세분화’, ‘유연한 접근 제어’이며, 이는 임의적 접근 제어의 특징이다.

다시 나오면 이렇게 판단

권한 결정 기준을 먼저 찾는다. 사용자·그룹 신원과 소유자의 재량이면 DAC, 보안 등급·레이블이면 MAC, 직무·역할이면 RBAC, 사전 규칙·조건이면 규칙 기반 접근 제어, 보안 등급의 격자형 지배 관계이면 LBAC로 판단한다.

암기 포인트

DAC는 ID와 소유자 재량, MAC는 등급과 강제, RBAC는 역할, LBAC는 격자이다.

NoteBase

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 5번

출제 포인트

ECDSA의 안전성 근거, 메시지 해시 사용, 타원곡선 암호의 효율성, 블록체인에서의 용도, 서명용 난수의 조건을 구별하는 문제이다.

핵심 개념

ECDSA는 타원곡선 이산대수 문제의 어려움에 기반한 전자서명 알고리즘이다. 메시지의 해시값과 개인키, 서명마다 새로 선택한 비밀 난수(논스)를 이용해 서명을 만들고, 공개키로 서명의 유효성을 검증한다. 특히 논스는 예측하기 어려워야 하며 같은 개인키로 두 서명에 재사용해서는 안 된다.

선지별 해설

① O — ECDSA의 안전성은 타원곡선 위에서 공개된 점들로부터 비밀 스칼라를 구하는 타원곡선 이산대수 문제의 계산상 어려움에 근거한다.
② O — ECDSA는 원문 전체를 직접 서명하는 방식이 아니라, 서명할 메시지를 해시한 결과를 서명 연산에 사용한다.
③ O — 타원곡선 암호는 같은 수준의 보안을 목표로 할 때 RSA보다 훨씬 짧은 키를 사용할 수 있어 저장·전송 부담과 연산 자원 측면에서 유리하다. 다만 ECDSA 자체는 암호화·복호화 알고리즘이 아니라 서명·검증 알고리즘이므로, 선지의 '복호화'는 타원곡선 공개키 연산의 효율성을 가리키는 취지이다.
④ O — 블록체인에서는 거래 작성자가 해당 개인키의 소유자임을 전자서명으로 확인하고, 서명 이후 거래 내용이 바뀌지 않았는지를 검증하는 데 ECDSA가 사용될 수 있다.
⑤ X — 틀린 표현은 '메시지에 관계없이 동일하게 사용해야 안전하다'이다. 올바르게는 서명 생성에 쓰는 논스를 서명마다 새롭고 예측하기 어렵게 생성해야 하며, 같은 개인키로 논스를 재사용하면 여러 서명값의 관계를 통해 개인키가 노출될 수 있다.

NoteBase

오답 포인트

⑤의 논스를 암호 알고리즘의 고정 매개변수처럼 생각하기 쉽다. ECDSA의 논스는 고정값이 아니라 각 서명에만 한 번 쓰는 비밀값이며, 동일 논스의 재사용은 보안을 높이는 것이 아니라 개인키 유출 위험을 만든다. 또한 ③의 '복호화'는 엄밀한 ECDSA 기능명이 아니라는 점과 문항이 의도한 타원곡선 암호의 효율성 설명을 구분해야 한다.

다시 나오면 이렇게 판단

ECDSA 선지에서는 '타원곡선 이산대수의 어려움', '메시지 해시', '짧은 키', '서명과 공개키 검증'은 기본 특성으로 판단한다. 반면 논스를 고정하거나 재사용한다는 표현은 개인키 유출로 이어지므로 틀린 설명으로 판단한다.

암기 포인트

ECDSA는 메시지는 해시하고, 논스는 서명마다 새로 사용한다. 논스 재사용은 곧 개인키 유출 위험이다.

NoteBase

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 3번

출제 포인트

공개키 인증 절차에서 키 쌍 생성, 인증기관의 인증서 발급, 상대방의 인증서 검증이 어떤 선후관계로 이루어지는지를 묻는 문제이다.

올바른 순서

1. ㄹ — Alice가 자신의 공개키와 개인키를 생성한다.
2. ㄴ — Alice가 자신의 공개키를 인증기관에 보낸다.
3. ㅁ — 인증기관이 Alice의 공개키에 대응하는 인증서를 발급한다.
4. ㄱ — Alice가 자신의 공개키와 발급받은 인증서를 Bob에게 전송한다.
5. ㄷ — Bob이 인증기관의 공개키로 Alice의 인증서를 검증한다.

왜 이 순서: 인증기관은 Alice의 공개키를 받아야 그 공개키에 대한 인증서를 발급할 수 있고, Bob은 발급된 인증서를 전달받은 뒤에야 인증기관의 공개키로 이를 검증할 수 있다.

NoteBase

선지별 해설

① X — ㄹ-ㄱ-ㄴ-ㄷ-ㅁ은 인증서가 발급되기 전에 Alice가 인증서를 Bob에게 보내고 Bob이 이를 검증하는 순서이므로 성립하지 않는다. 틀린 부분은 ㄱ·ㄷ을 ㅁ보다 앞에 둔 것이며, 올바르게는 ㄹ-ㄴ-ㅁ-ㄱ-ㄷ이다.

② X — ㄹ-ㄴ-ㄷ-ㄱ-ㅁ은 Bob의 인증서 검증이 인증서 발급과 전달보다 먼저 놓여 있으므로 성립하지 않는다. 틀린 부분은 ㄷ을 ㅁ·ㄱ보다 앞에 둔 것이며, 올바르게는 ㄹ-ㄴ-ㅁ-ㄱ-ㄷ이다.

③ O — ㄹ에서 키 쌍을 생성하고, ㄴ에서 공개키를 인증기관에 제출한 뒤, ㅁ에서 인증서를 발급받는다. 이어 ㄱ에서 Bob에게 공개키와 인증서를 보내고 ㄷ에서 Bob이 인증서를 검증하므로 선후관계가 모두 맞는다.

④ X — ㅁ-ㄹ-ㄱ-ㄷ-ㄴ은 Alice가 키 쌍을 만들고 공개키를 인증기관에 보내기 전에 인증기관이 인증서를 발급하는 순서이므로 성립하지 않는다. 틀린 부분은 ㅁ을 ㄹ·ㄴ보다 앞에 둔 것이며, 올바르게는 ㄹ-ㄴ-ㅁ-ㄱ-ㄷ이다.

⑤ X — ㅁ-ㄹ-ㄷ-ㄱ-ㄴ은 공개키 제출 전에 인증서를 발급하고, Bob이 인증서를 전달받기 전에 검증하는 순서이므로 성립하지 않는다. 틀린 부분은 ㅁ을 ㄹ·ㄴ보다 앞에 두고 ㄷ을 ㄱ보다 앞에 둔 것이며, 올바르게는 ㄹ-ㄴ-ㅁ-ㄱ-ㄷ이다.

오답 포인트

인증기관의 인증서 발급과 Bob의 인증서 검증을 혼동하기 쉽다. ㅁ은 Alice가 공개키를 인증기관에 제출한 뒤에 이루어지고, ㄷ은 Alice가 발급된 인증서를 Bob에게 전달한 뒤에 이루어진다.

다시 나오면 이렇게 판단

절차형 문제는 각 단계의 입력이 어디서 생기는지 확인한다. 공개키를 먼저 생성해야 인증기관에 보낼 수 있고, 인증기관이 인증서를 발급해야 Alice가 이를 전달할 수 있으며, Bob은 인증서를 받은 뒤 검증한다.

암기 포인트

키 생성 → 공개키 제출 → 인증서 발급 → 상대방에게 전달 → 인증서 검증의 흐름으로 기억한다.

NoteBase

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 1번

출제 포인트

OWASP의 웹 애플리케이션 10대 보안 위험 항목과 클라우드 컴퓨팅 분야의 위협을 구분하는 문제이다.

핵심 개념

OWASP Top 10은 웹 애플리케이션에서 빈번하고 영향이 큰 보안 위험을 분류한 목록이다. 문항에 제시된 Injection, XML External Entities, Broken Authentication, Sensitive Data Exposure는 이 목록의 항목이지만, Abuse of Cloud Computing은 클라우드 서비스의 악용을 뜻하는 별도의 클라우드 보안 위협이다.

선지별 해설

① O — Abuse of Cloud Computing은 클라우드 자원을 스팸 발송, 악성코드 유포, 공격 수행 등에 악용하는 위협을 가리키며, 문항이 묻는 OWASP 웹 애플리케이션 10대 보안 위험의 항목이 아니다. 따라서 '속하지 않는 것'에 해당한다.
② X — Injection은 신뢰할 수 없는 입력이 명령어나 질의의 일부로 해석되어 발생하는 웹 애플리케이션 취약점으로, OWASP 목록에 속한다. 틀린 판단은 이를 '속하지 않는 것'으로 보는 것이며, 올바르게는 'OWASP 목록에 속하는 것'이다.
③ X — XML External Entities(XXE)는 취약한 XML 처리기가 외부 엔터티를 처리하면서 파일 노출이나 서버 측 요청 등의 피해가 생기는 취약점으로, OWASP 목록에 속한다. 틀린 판단은 이를 '속하지 않는 것'으로 보는 것이며, 올바르게는 'OWASP 목록에 속하는 것'이다.
④ X — Broken Authentication은 인증과 세션 관리의 결함 때문에 계정 탈취나 사용자 위장이 가능해지는 취약점으로, OWASP 목록에 속한다. 틀린 판단은 이를 '속하지 않는 것'으로 보는 것이며, 올바르게는 'OWASP 목록에 속하는 것'이다.
⑤ X — Sensitive Data Exposure는 암호화나 접근 보호가 충분하지 않아 민감정보가 노출되는 위험으로, OWASP 목록에 속한다. 틀린 판단은 이를 '속하지 않는 것'으로 보는 것이며, 올바르게는 'OWASP 목록에 속하는 것'이다.

NoteBase

오답 포인트

①도 보안 위협을 나타내는 표현이어서 OWASP 항목처럼 보이는 것이 함정이다. 그러나 OWASP 목록은 웹 애플리케이션 취약점 분류이고, ①은 클라우드 컴퓨팅 자원의 악용이라는 더 넓은 클라우드 보안 위협이다. 또한 문제의 부정형 표현인 '속하지 않는'을 놓치면 ②~⑤를 답으로 고르기 쉽다.

다시 나오면 이렇게 판단

선지의 대상 영역을 먼저 구분한다. 입력값 처리, XML 처리, 인증, 민감정보 보호처럼 웹 애플리케이션의 구현 취약점을 가리키면 OWASP 항목으로 보고, 클라우드 서비스 자체의 악용처럼 다른 보안 영역을 가리키면 범주 밖의 항목으로 판단한다.

암기 포인트

Injection · XXE · Broken Authentication · Sensitive Data Exposure는 웹 애플리케이션 위험이고, Abuse of Cloud Computing은 클라우드 악용 위협이다.

NoteBase

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 2번

출제 포인트

IPsec의 전송모드와 터널모드, ESP의 보안 기능, IKE의 키 교환 역할을 구분하는 문제이다.

핵심 개념

IPsec은 IP 계층에서 통신 내용을 보호하는 보안 프로토콜 체계이다. 전송모드는 원래 IP 헤더를 유지한 채 주로 상위 계층 데이터 부분을 보호하고, 터널모드는 원래 IP 패킷 전체를 보호한 뒤 새로운 외부 IP 헤더를 붙인다. ESP는 기밀성을 중심으로 무결성·인증 기능도 제공할 수 있으며, IKE는 통신 상대를 인증하고 보안 연관과 암호 키를 협상한다.

선지별 해설

① O — IPsec 통신을 설정할 때는 보호할 통신의 양 끝점 또는 상대 피어를 식별해야 하므로 송신자와 수신자는 상대방의 IP 주소를 설정한다.
② X — 틀린 표현은 '전송모드는 원래의 IP 헤더에 새로운 IP 헤더를 추가한다'이다. 새로운 IP 헤더를 추가하는 것은 터널모드이며, 전송모드는 원래 IP 헤더를 그대로 사용한다.
③ O — ESP는 IP 패킷의 페이로드를 암호화하여 기밀성을 제공하고, 선택적으로 인증 데이터를 사용하여 무결성과 출처 인증도 제공할 수 있다.
④ O — IKE는 인증된 Diffie-Hellman 방식으로 공유 비밀을 만들고, IPsec에서 사용할 보안 연관과 키를 협상한다.
⑤ O — IPsec은 공용망에서 사설망처럼 안전한 통신 경로를 만드는 VPN을 구현하는 대표적인 방법 중 하나이다.

오답 포인트

②는 전송모드와 터널모드의 헤더 구조를 뒤바꾼 선지이다. '새로운 IP 헤더 추가'라는 표현이 나오면 전송모드가 아니라 터널모드에 해당한다. 또한 ESP의 무결성 제공은 필수 기능이 아니라 선택적으로 사용할 수 있는 기능이라는 점도 함께 구분한다.

NoteBase

다시 나오면 이렇게 판단

원래 IP 헤더를 유지하면 전송모드, 원래 IP 패킷을 감싸고 새 IP 헤더를 붙이면 터널모드로 판단한다.
암호화·무결성은 ESP의 기능이고, 상대 인증과 키·보안 연관 협상은 IKE의 역할로 구분한다.

암기 포인트

전송모드＝원래 헤더 유지, 터널모드＝새 헤더 추가, ESP＝암호화·무결성, IKE＝인증·키 협상이다.

NoteBase

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 5번

출제 포인트

기호 권한 rwsr--r--를 특수 권한 비트와 소유자·그룹·기타 사용자 권한의 8진수로 변환하는 문제이다.

조건 정리

주어진 권한: rwsr--r--
구해야 할 값: chmod에 사용할 4자리 8진수 권한
주의할 조건: 소유자 실행 위치의 소문자 s는 소유자 실행 권한 x와 setuid가 모두 설정되었다는 뜻이다.

사용할 공식

4자리 chmod 권한은 [특수 권한][소유자 권한][그룹 권한][기타 사용자 권한] 순서로 적는다.
특수 권한은 setuid=4, setgid=2, sticky bit=1이고, 일반 권한은 r=4, w=2, x=1을 더해 구한다.
이 기준을 쓰는 이유는 제시된 문자열에 일반 읽기·쓰기·실행 권한뿐 아니라 setuid를 나타내는 s가 포함되어 있기 때문이다.

계산 과정

1. 소유자 권한 rws에서 r+w+x=4+2+1=7이고, s에 의해 setuid 특수 비트는 4이다.
2. 그룹 권한 r--는 4, 기타 사용자 권한 r--도 4이다.
3. [setuid 4][소유자 7][그룹 4][기타 4]를 결합하면 4744이다.
따라서 명령어는 chmod 4744 first이다.

NoteBase

선지 판단

① X — chmod 1644 first는 sticky bit와 일반 권한 644를 설정하므로, setuid와 소유자 실행 권한이 있는 rwsr--r--가 되지 않는다. 틀린 1644는 4744로 고쳐야 한다.
② X — chmod 1744 first는 sticky bit와 일반 권한 744를 설정한다. 소유자 실행 권한은 생기지만 setuid가 아니므로 틀렸다. 틀린 1744는 4744로 고쳐야 한다.
③ X — chmod 2744 first는 setgid와 일반 권한 744를 설정한다. 제시된 s는 그룹 실행 위치가 아니라 소유자 실행 위치에 있으므로 setuid를 써야 한다. 틀린 2744는 4744로 고쳐야 한다.
④ X — chmod 4644 first는 setuid를 설정하지만 소유자 실행 권한 x가 없다. 이 경우 소유자 실행 위치는 소문자 s가 아니라 대문자 S로 표시되므로 틀렸다. 틀린 4644는 4744로 고쳐야 한다.
⑤ O — chmod 4744 first는 setuid 4와 소유자 rwx=7, 그룹 r--=4, 기타 사용자 r--=4를 설정하므로 rwsr--r--와 정확히 일치한다.

오답 포인트

핵심 함정은 소문자 s와 대문자 S의 차이이다. 소문자 s는 setuid와 소유자 실행 권한이 모두 켜진 상태이므로 4644가 아니라 4744이다. 또한 첫째 자리는 일반 실행 권한이 아니라 setuid·setgid·sticky bit를 나타내는 특수 권한 자리이다.

다시 나오면 이렇게 판단

먼저 s의 위치로 setuid와 setgid를 구분하고 대소문자로 해당 실행 권한의 존재 여부를 확인한다. 그다음 특수 권한, 소유자, 그룹, 기타 사용자 순서로 각 값을 계산해 네 자리를 결합한다.

암기 포인트

소유자 위치 s는 setuid 4, 그룹 위치 s는 setgid 2, 기타 사용자 위치 t는 sticky bit 1이다. 소문자는 실행 권한 있음, 대문자는 실행 권한 없음을 뜻한다.

NoteBase

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 등을 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 1번

쟁점

이 문제는 2020년 개정으로 도입된 목적의 합리적 관련성에 따른 추가 이용·제공과 가명정보 처리 특례에 관한 문제이다. 핵심은 동의 없는 처리를 전면 금지하는 경우와 법이 일정한 요건 아래 허용하는 경우를 구별하는 것이다.

용어 풀이

가명처리란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로, 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리하는 것이다. 이렇게 처리된 개인정보가 가명정보이다.

핵심 구분

개인정보 보호법 제15조 제3항과 제17조 제4항은 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체의 불이익 여부와 암호화 등 안전성 확보조치 여부 등을 고려하여, 대통령령으로 정하는 바에 따라 동의 없이 개인정보를 이용하거나 제공할 수 있도록 한다. 또한 제28조의2부터 제28조의4까지는 통계작성·과학적 연구·공익적 기록보존을 위한 가명정보의 동의 없는 처리, 결합전문기관을 통한 결합, 안전성 확보조치를 규정한다.

NoteBase

선지별 해설

① X
동의 없는 이용·제공을 전면 금지한 부분이 틀렸다. 법은 당초 수집 목적과 합리적으로 관련된 범위인지, 정보주체에게 불이익이 발생하는지, 암호화 등 안전성 확보조치를 하였는지 등을 고려하여 대통령령으로 정하는 바에 따라 동의 없이 이용하거나 제공할 수 있도록 한다.
틀린 표현: '정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 없도록 함'
올바른 표현: '위 사항들을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 있도록 함'

② O
개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하여 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리하는 것은 가명처리의 법정 정의에 해당한다.

③ O
개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

④ O
서로 다른 개인정보처리자 간의 가명정보 결합은 개인정보보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

⑤ O
가명정보를 처리하는 개인정보처리자는 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 기술적·관리적·물리적 안전조치를 하여야 한다.

오답 포인트

①의 '고려하여'라는 말 뒤에 금지 결론이 이어지는 점이 함정이다. 법은 해당 사정들을 고려하더라도 언제나 금지하는 것이 아니라, 정해진 요건을 충족하면 동의 없는 추가 이용·제공을 허용한다.

다시 나오면 이렇게 판단

목적의 합리적 관련성, 정보주체의 불이익, 암호화 등 안전성 확보조치가 함께 제시되면 동의 없는 추가 이용·제공의 허용 요건을 묻는 것으로 판단한다. 가명정보 문항에서는 정의, 허용 목적, 결합 주체, 안전조치 의무를 차례로 확인한다.

NoteBase

암기 포인트

합리적 관련 범위의 추가 이용·제공은 조건부 허용이고, 가명정보는 목적 제한·전문기관 결합·안전조치가 핵심이다.

NoteBase

20. 다음 설명에서 제시하는 공격 유형은?

> 게시판의 글에 원본과 함께 악성 코드를 삽입하여 글을 읽을 경우 악성코드가 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 2번

출제 포인트

게시판에 저장된 악성 코드가 다른 사용자의 브라우저에서 실행되는 공격을 XSS로 식별하는 문제이다.

핵심 개념

XSS(Cross Site Scripting)는 공격자가 웹 페이지에 악성 스크립트를 삽입하여 그 페이지를 보는 사용자의 브라우저에서 실행되게 하는 공격이다.
이 지문처럼 악성 코드가 게시판 글에 저장되었다가 사용자가 글을 읽을 때 실행되는 형태는 저장형 XSS이다.
핵심 키워드는 '입력값 미필터링', '웹 페이지에 악성 코드 삽입', '다른 사용자의 브라우저에서 실행'이다.

NoteBase

선지별 해설

① X — SQL Injection은 입력값에 악성 SQL 구문을 넣어 데이터베이스 질의를 변조하는 공격이다. 틀린 표현은 'SQL Injection'이며, 지문의 공격은 웹 페이지에 삽입된 스크립트가 사용자의 브라우저에서 실행되는 저장형 XSS이다.
② O — XSS는 웹 페이지에 악성 스크립트를 삽입하여 사용자의 브라우저에서 실행되게 한다. 게시판에 저장된 코드가 글을 읽을 때 실행된다는 지문의 설명과 일치한다.
③ X — 파일 업로드 취약점은 확장자·형식·실행 권한 검증이 미흡한 업로드 기능을 이용해 악성 파일을 서버에 올리는 취약점이다. 틀린 표현은 '파일 업로드 취약점'이며, 지문은 파일 업로드가 아니라 게시글 입력값에 삽입된 악성 스크립트의 실행을 설명하므로 저장형 XSS이다.
④ X — CSRF(Cross Site Request Forgery)는 로그인된 사용자의 인증 상태를 악용하여 사용자가 의도하지 않은 요청을 서버에 보내게 하는 공격이다. 틀린 표현은 'CSRF'이며, 사용자의 브라우저에서 삽입 스크립트가 실행되어 정보를 유출하는 지문의 공격은 XSS이다.
⑤ X — 쿠키/세션 위조는 세션 식별자나 쿠키 값을 탈취·변조하여 다른 사용자로 가장하거나 인증 상태를 악용하는 공격이다. 틀린 표현은 '쿠키/세션 위조'이며, 지문은 게시판에 저장된 악성 코드가 열람 시 실행되는 저장형 XSS를 설명한다.

오답 포인트

지문에 '클라이언트의 정보 유출'이 제시되어 쿠키/세션 위조와 혼동하기 쉽다. 그러나 공격의 결과보다 실행 방식이 중요하다. 게시판 입력값이 필터링되지 않아 악성 코드가 페이지에 포함되고, 다른 사용자가 글을 읽을 때 브라우저에서 실행된다는 표현이 XSS의 결정적 단서이다.

다시 나오면 이렇게 판단

악성 SQL로 데이터베이스 질의를 바꾸면 SQL Injection, 웹 페이지에 삽입된 스크립트가 사용자의 브라우저에서 실행되면 XSS, 로그인된 사용자가 원치 않는 요청을 보내게 되면 CSRF로 구분한다. 특히 게시판에 코드가 저장되었다가 열람 시 실행되면 저장형 XSS로 판단한다.

암기 포인트

DB 질의 변조는 SQL Injection, 브라우저의 악성 스크립트 실행은 XSS, 인증된 사용자의 원치 않는 요청은 CSRF이다.

NoteBase