━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

\*\*데이터베이스 보안 사고 사례 및 대응 전략 보고서\*\*

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

과목명 : DB 기초 및 실습

강사 : 강사님

과정 : AI를 활용한 보안전문가 양성과정

이름 :

제출일 : 2025년 7월 7일

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

1. 개인정보 침해 사고 사례 조사 및 분석

|  |  |
| --- | --- |
| 항목 | 내용 |
| 누가(Who) | 신원미상의 자(이하 ‘해커’) |
| 언제(When) | 2025년 2월경 |
| 어디서(Where) | 비즈니스온커뮤니케이션(스마트빌), NHN위투(가방팝) |
| 무엇을(What) | SQL 인젝션 공격을 통한 DB 접근 및 개인정보 유출 |
| 어떻게(How) | 에러 기반 및 UNION 기반 SQL 인젝션을 통한 웹 애플리케이션 공격 |
| 왜(Why) | 입력값 검증 미흡하고 웹 방화벽이 작동하지 않는 상태였거나, 접근 IP 제한이 없는 등 보안 정책 미준수로 인한 DB 취약점 노출됨. |

개인정보보호위원회 보도자료에 따르면, 25년도 2월 26일 전체회의에서 안전조치 의무를 위반한 2개 사업자에 대해 과징금 및 과태료를 부과하고 아울러 시정명령과 공표명령을 하였다. 구체적인 내용은 아래와 같다.

이에 따라 개인정보보호 법규를 위반한 2개 사업자\*에 대해 총 1억 9,810만 원의 과징금 및 1,230만 원의 과태료를 부과하고 아울러 시정명령과 공표명령을 하기로 의결하였다.

해당 사례에서 발견된 문제점은 다음과 같다.

|  |  |  |
| --- | --- | --- |
| 항목 | 스마트빌((주)비즈니스온커뮤니케이션) | 가방팝(엔에이치엔위투(주)) |
| 유출 정보 | 이름, 아이디, 비밀번호, 이메일, 연락처 등 **총 179,386건** | 판매자 및 고객 정보, **주민등록번호 포함** **총 534,903건** |
| 공격 기법 | SQL 인젝션 (에러 기반 + UNION 기반) | SQL 인젝션 (에러 기반 + UNION 기반) |
| 주요 원인 | - SQLi 방어 미흡 - 시스템 접근 IP 제한 없음 - 유출 신고 지연 | - WAF(웹방화벽) 비활성화 - SQLi 취약점 방치 - 개인정보 파기 미이행 |
| 법적 위반 사항 | - 개인정보 보호조치 미흡 - 유출 통지 지연 | - 보호조치 미흡 - 파기 의무 위반 - 과잉보관(주민등록번호) |

1. 시나리오에 따른 위협 방어 전략 및 정책 제시

해당 보안 취약점(위 표의 ‘주요 원인’)에 대해 다음과 같이 개인정보 유출 방지 전략을 제안한다.

1. 취약점 진단

| **전략** | **설명** |
| --- | --- |
| 정기적 보안 취약점 점검 | KISA의 ‘소프트웨어 보안약점 진단 가이드’를 활용하여 정기적으로 SQLi, XSS, 인증 우회 등 보안 취약점 점검 |
| 코드 수준 취약점 진단 | SAST(정적 분석 도구)를 통해 코드 내 쿼리 구성 방식 확인 |
| 취약점 자동 진단 툴 도입 | SQLMap, Vega, Burp Suite 등으로 자동 진단 수행 |

1. 접근 통제

| **전략** | **설명** |
| --- | --- |
| IP 기반 접근 제한 | 관리자 및 백엔드 시스템에 접근 가능한 IP를 화이트리스트 방식으로 제한 |
| 최소 권한 원칙 적용 | DB 계정별 접근 권한을 최소화하고 RBAC 적용 |
| 관리자 이중 인증 적용 | DB 및 관리 시스템 접속 시 OTP 등 MFA 적용 |
| 외부 접근 분리 | 개발/운영/테스트 DB를 물리적 혹은 논리적으로 분리하여 운영 |

1. 암호화 적용

| **전략** | **설명** |
| --- | --- |
| 개인정보 암호화 저장 | 이름, 주민등록번호, 연락처 등은 AES-256,RSA 등 기반으로 DB 내 암호화 저장 |
| 비밀번호 해시 처리 | 비밀번호는 단방향 해시(SHA-256 이상 + Salt)로 저장 |
| 데이터 전송 암호화 | SSL/TLS 기반으로 DB 접근 및 API 호출 시 데이터 전송 구간 암호화 |
| 키 관리 체계 구축 | 암호화 키는 HSM 또는 키 관리 솔루션을 통해 안전하게 관리 |

1. 로그 추적 및 모니터링

| **전략** | **설명** |
| --- | --- |
| DB 접근 로그 수집 | 모든 SELECT, UPDATE, DELETE, INSERT, LOGIN 등 SQL 로그를 저장 |
| 이상 징후 탐지 시스템 | IDS/IPS 또는 SIEM 연동하여 의심스러운 DB 접근 실시간 탐지 |
| 비인가 접속 경고 시스템 | 야간/비정상 패턴의 DB 접속이 감지될 경우 관리자 경고 및 자동 차단 |
| 로그 보존 정책 | 주요 DB 접근 로그는 최소 1년 이상 보관하며 위·변조 방지 적용(개인정보 보호법 및 정보통신망법 참조) |

1. 전략 별 주요 개념

| **용어** | **정의** |
| --- | --- |
| XSS(Cross-Site Scripting) | 공격자가 웹사이트에 악성 스크립트를 삽입하여, 사용자 브라우저에서 해당 스크립트가 실행되도록 하는 **클라이언트 측 공격 방식**입니다.  주로 쿠키 탈취, 세션 하이재킹 등에 악용됩니다. |
| SAST(Static Application Security Testing) | 소스 코드, 바이트 코드 등을 실행하지 않고 분석하여 보안 취약점을 탐지하는 **정적 분석 기법**입니다. 개발 초기 단계에서 취약점을 찾는 데 유리합니다. |
| RBAC(Role-Based Access Control) | 사용자의 역할(Role)에 따라 시스템 자원 접근 권한을 제어하는 방식으로, **최소 권한 원칙**을 실현하는 대표적인 접근 제어 모델입니다. |
| MFA(Multi-Factor Authentication) | 사용자의 인증 시 **두 개 이상의 인증 수단**(예: 비밀번호 + OTP)을 요구하여 보안을 강화하는 인증 방식입니다. 계정 탈취 방지에 효과적입니다. |
| SIEM(Security Information and Event Management) | 다양한 보안 로그와 이벤트 데이터를 통합 수집·분석하여 **보안 위협을 실시간 탐지 및 대응**하는 시스템입니다. 조직의 보안 가시성과 위협 대응력을 높입니다. |

마치며

SQL 인젝션은 코드 한 줄, 필터 하나의 부재로도 발생할 수 있으며, 특히 DB에 직접 연결되는 웹 시스템은 지속적인 점검과 정책적 대비가 필수적이다.

보안은 단기 대응이 아닌 **지속적 프로세스**이다.

한국인터넷진흥원(KISA)의 보안 점검 도구와 가이드라인을 적극 활용하시기를 권장한다.

참고자료 :

개인정보보호위원회의 보도자료: <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=11019>

KISA의 소프트웨어 보안약점 진단가이드 :

<https://www.kisa.or.kr/2060204/form?postSeq=9&page=1>

KISA의 보안취약점 및 침해사고 대응 가이드라인 :

<https://www.kisa.or.kr/2060204>