**아래 그림은 KoreaIT 네트워크에서 웹서버 악성코드 탐지 서비스 구축의 한 예로**

**웹서버와 연결된 데이터베이스 서버로의 SQL Injection 공격으로 인한 침해사고가 발생하였다.**

**이에 대해 테스트를 진행하고 조치 사항과 대응 방안에 대해 본인 이름의 보고서를 작성하고**

**앞으로의 SQL Injection공격에 대한 정보보호 정책 교육 내용 및 유지보수를 담당하는 외부자 보안을 강화하는 방법에 관련하여 서술하시오.**

**보고서 형식으로 문서화(Word 파일)**

**1. 침해사고 보고서(70점)**- 보고서 작성 완성도에 따라 차등 점수

   : 침해사고 시연 시 50점 / 조치 및 개선방안 20점

     SQL Injection (시기, 방법, 등) - 조치사항 - 개선방안 서술

**1. 사고 개요**

KoreaIT 네트워크에서 발생한 침해사고는 웹서버와 연결된 데이터베이스 서버로의 SQL Injection 공격으로 인해 중요 정보가 유출된 사건이다. 본 보고서는 침해사고의 시연, 조치사항 및 향후 개선 방안을 포함한다.

**2. 보안사고분석**

**2.1 공격 방식**

- 공격자는 웹 애플리케이션의 입력 필드에서 SQL Injection 취약점을 발견

- ‘OR ‘1’=’1’-- 등의 페이로드를 이용하여 인증 우회

- 데이터베이스에서 민감한 정보를 무단 조회 및 수정

**3. 조치 사항**

긴급 차단 조치:

- 웹 애플리케이션 방화벽(Web Firewall) 설정 강화 : 의심스러운 IP 차단

- SQL Injection 탐지 및 제거: 데이터베이스 로그 분석을 통해 공격자의 접근 이력 확인

취약한 SQL 쿼리 수정 및 Prepared Statement 적용

- 보안 패치 적용: 웹 애플리케이션 및 데이터베이스의 최신 보안 패치 적용

웹사이트 입력값 검증 로직 추가

**4. 개선 방안**

**4.1 개발 보안 강화**

- Prepared Statement 및 ORM(Object-Relational Mapping) 사용

- 입력 값 검증: 화이트리스트 기반의 입력 필터링 적용

- 에러 메시지 제한: 데이터베이스 오류 정보를 최소화하여 공격자가 내부 구조를 유추하지 못하도록 설정

**4.2 보안 모니터링 및 대응**

- 실시간 보안 모니터링 시스템 도입 (SIEM, IDS/IPS)

- 정기적인 보안 점검 및 취약점 분석 수행

**4.3 접근 제어 강화**

- 최소 권한 원칙 적용: 불필요한 DB 접근 권한 제한

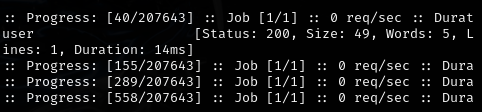
- 관리자 계정 보호: 강력한 비밀번호 정책 및 다중 인증(MFA) 적용한다.

**5. 침해사고 시연**

**1. FuFF(매개변수를 퍼징하는 도구)를 이용해 취약점을 찾는다**



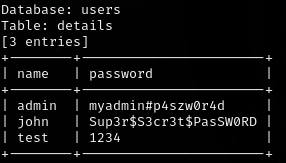
**2. 결과로 user를 확인**



**4. FUZZ 부분을 user로 바꾼 후 접속 확인하고sqlmap(SQL Injection을 자동으로 탐지, 공격하는 도구)을 사용하여 데이터 추출, 덤프 시도**



**5. 취약점을 이용해 보여선 안 될 데이터베이스 안 유저들의 정보가 그대로 노출됐음을 확인**



**2. 정보보호 정책 교육 내용 간단히 서술(10점)**

정보보호 정책 교육 내용은 조직 내 보안 의식을 높이고, 직원들이 정보보호 규정을 준수할 수 있도록 돕는 중요한 교육이다. 이 교육은 직원들이 정보보호 정책을 실천하고, 보안 위협으로부터 조직을 보호하는 데 필수적인 역할을 한다.

- 정보보호 정책 이해: 조직의 정보보호 정책 및 절차를 설명하고, 이를 준수하는 이유를 이해시킨다.

- 비밀번호 관리: 강력한 비밀번호 설정, 주기적인 변경, 공유 금지 등을 교육한다.

- 데이터 보호: 중요한 정보의 보안 유지 방법과 데이터 암호화, 백업 절차를 -설명한다.

- 피싱 및 사회 공학 공격 예방: 이메일, 전화 등으로 시도되는 피싱 공격을 식별하고 방어하는 방법을 교육한다.

- 인터넷 및 이메일 사용 규정: 안전한 인터넷 사용과 이메일 첨부파일 처리 방법에 대해 교육한다.

- 물리적 보안: 컴퓨터, 문서 등 물리적 자산을 안전하게 관리하는 방법을 설명한다.

- 사고 발생 시 대응 절차: 보안 사고 발생 시 즉시 신고하고, 대응 절차를 따르는 방법을 안내한다.

**3. 외부자 보안에 대한 관리 방안에 대하여 서술(10점)**

**외부자 보안 관리 방안은 기업이나 조직의 정보 자산을 보호하고 외부로부터의 공격을 예방하기 위해 중요한 요소이다. 외부자 보안은 종종 네트워크, 시스템, 애플리케이션에 대한 외부 공격이나 데이터 유출을 막는 데 집중하기도 한다.**

**- 보안 정책 설정: 외부 협력업체와의 계약에 보안 요구사항을 포함하고, 최소한의 권한만 부여한다.**

**- 네트워크 보안 강화: 방화벽과 침입 탐지 시스템(IDS/IPS)을 사용하고, VPN 및 암호화를 통해 외부 접속을 보호한다.**

**- 멀티팩터 인증(MFA): 외부 접속 시 MFA를 요구하고, 강력한 비밀번호 정책을 적용한다.**

**- 로그 모니터링: 외부 접속 활동을 기록하고 비정상적인 활동을 탐지한다.**

**- 서드파티 보안 관리: 외부 업체와의 보안 요구사항을 명확히 하고, 보안 취약점을 점검한다.**

**- 사회 공학 공격 대비 훈련: 직원에게 피싱 및 스피어 피싱에 대한 교육을 한다.**

**- 패치 관리: 최신 보안 패치를 적용하고, 자동화된 시스템을 사용해 빠르게 업데이트한다.**

**- 사고 대응 계획: 공격 시 신속히 대응할 수 있는 계획을 마련한다.**