KorealT 네트워크에서 개인정보가 유출되는 사고가 발생하였다.

DB 서버에 저장된 학생 및 교직원의 개인정보가 유출된 것으로 기본적인 분석 결과 퇴직자의 계정을 활용하여

XSS(Cross Site Script)공격에 의해 발생한 것으로 확인이 되었으며

이에 대한 관리적인 보안 구축에 대한 보고서를 작성하고 직무분리와 최소 권한 원칙에 대해 서술하시오.

정보보호 총괄 책임자 - 홍길동

정보보호 실무 책임자 - 임꺽정

보고서 형식으로 문서화(Word 파일)

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

: 침해사고 시연 시 40 점 / 조치 및 개선사항 20 점 / 인적 보안 10 점

- XSS (시기, 방법, 등) - 조치사항 - 개선방안 서술(인적 보안 포함)

1. 사고 개요

KorealT 네트워크에서 발생한 개인정보 유출 사고는 퇴직자의 계정을 활용한 XSS(Cross Site Scripting) 공격으로 인해 DB 서버에 저장된 학생 및 교직원의 개인정보가 외부로 유출된 사건이다. 본 보고서는 이와 같은 사고의 재발 방지를 위한 관리적 보안 조치를 제안한다.

2. 보안 사고 분석

2.1 공격 방식

- 퇴직자의 계정이 비활성화되지 않아 지속적으로 접근 가능

- XSS 취약점을 이용하여 사용자 세션을 탈취하거나 악성 스크립트를 삽입하여 정보 유출

- 데이터베이스 접근 권한이 불필요하게 확대되어 있어 계정을 통해 광범위한 정보 조회 가능

3. 관리적 보안 구축 방안

3.1 계정 및 접근 관리 강화

- 퇴직자 계정 즉시 비활성화 및 삭제 절차 마련

- 정기적인 계정 감사 수행 (Inactive 계정 자동 비활성화)

- 다중 인증(MFA) 적용하여 계정 탈취 위험 감소

3.2 XSS 취약점 대응 방안

- 웹 애플리케이션에서 입력 값 검증 및 필터링 적용

- Content Security Policy(CSP) 설정 강화하여 악성 스크립트 차단

- 정기적인 보안 취약점 점검 및 패치 적용

3.3 보안 로그 및 모니터링 체계 강화

- Zabbix 및 SIEM(Security Information and Event Management) 시스템 도입하여 실시간 감시

- 비정상적인 로그인 및 접근 패턴 탐지 기능 강화

- 주기적인 보안 로그 분석 및 이상 행위 탐지

3.4 인적 보안 방안

- 정기적인 보안 교육을 실시하여 직원들의 보안 인식을 강화하고, 보안 사고 사례를 공유하여 예방 의식을 높임

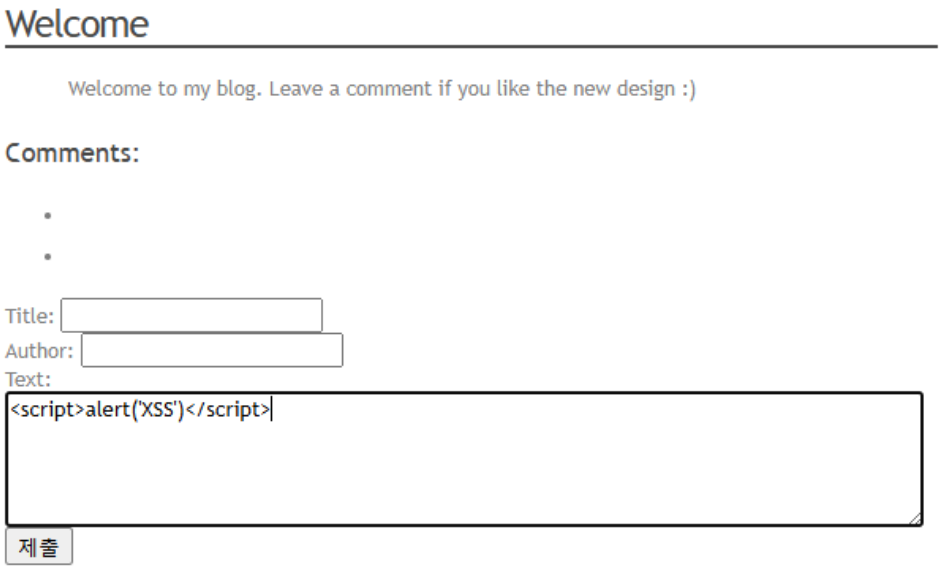
- 퇴직자 및 부서 이동 시 즉시 접근 권한을 점검하고 불필요한 권한을 회수

- 직원들의 시스템 접근 및 로그 활동을 모니터링하여 비정상적인 접근 시 즉각 대응

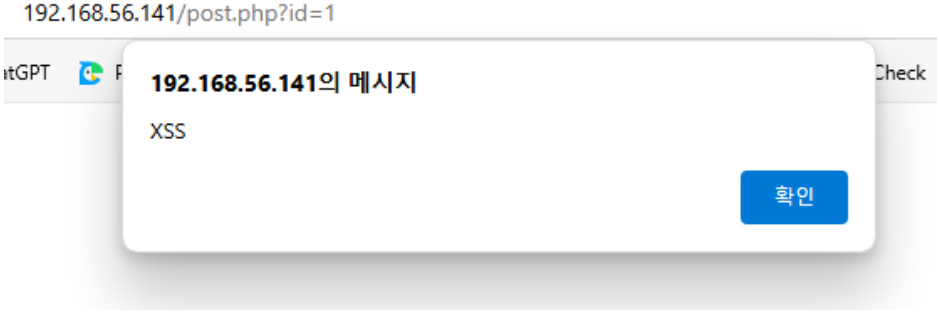
- 모든 직원 및 협력업체와 비밀 유지 서약서를 체결하여 기밀 정보 유출을 방지

4. 침해사고 시연

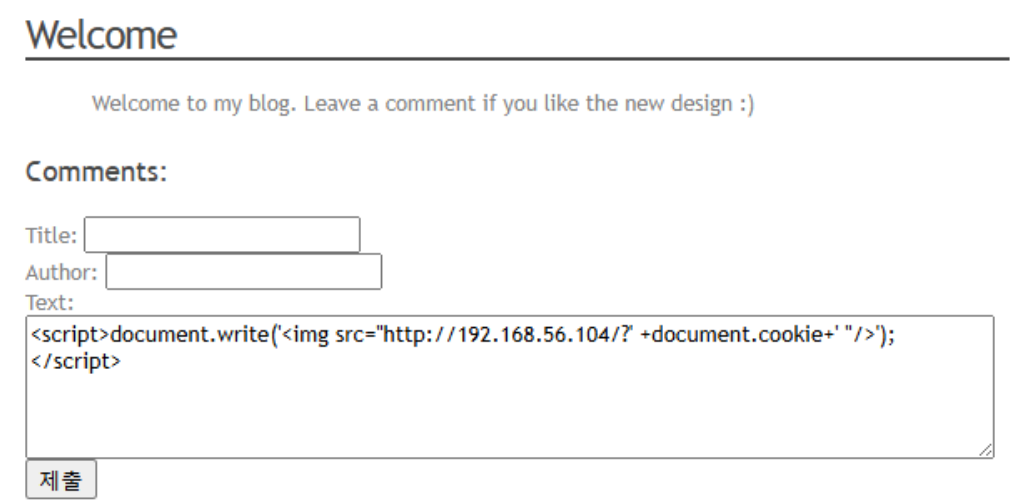
1. 웹 사이트로 접속해 텍스트 필드에 명령어를 제출하여 XSS 취약점이 있는지 확인

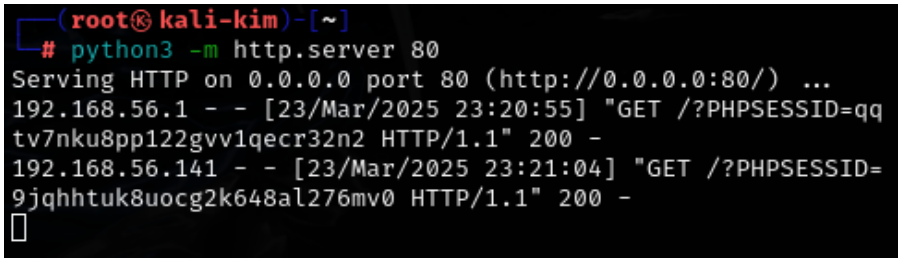


2. 실제로 명령어가 실행되어 취약점이 있다는 것을 확인

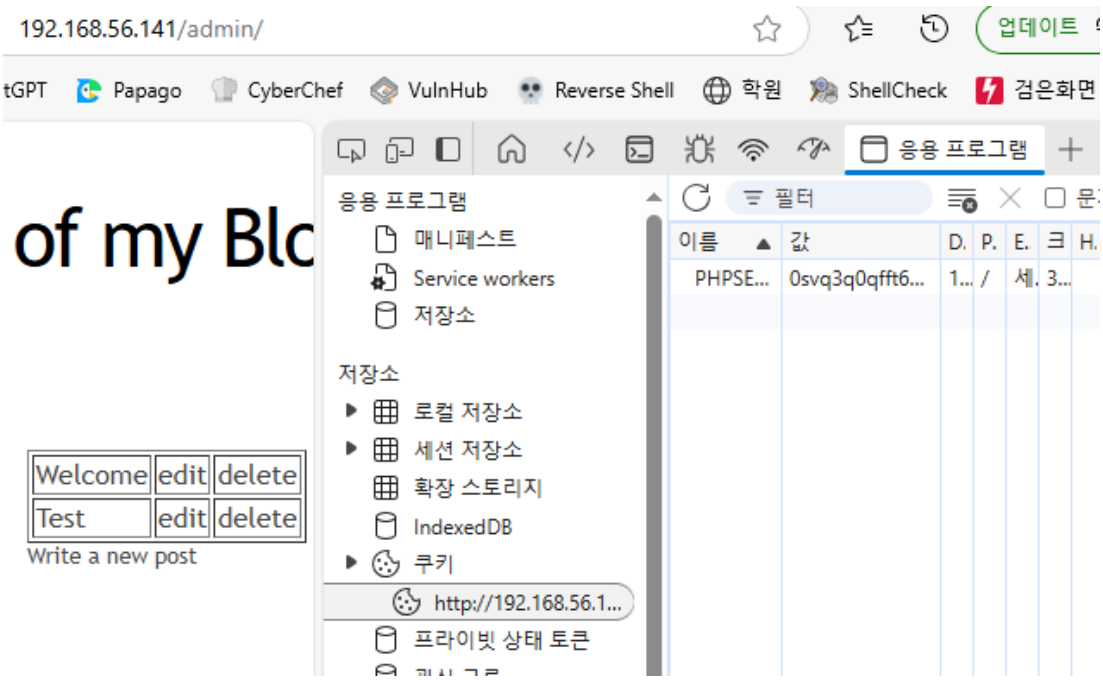


3. 관리자 쿠키값을 얻기 위해 명령어를 입력해 칼리에서 받아온다





4. 알아낸 쿠키값을 웹 페이지에 할당하여 아이디 비밀번호가 필요했던 로그인 페이지에 접속이 되었음. 치명적인 취약점 확인



2. 직무분리에 대한 내용 간단히 서술(10 점)

직무 분리란 업무의 발생, 승인, 변경, 확인, 배포 등이 모두 한 사람에 의해 처음부터 끝까지 처리될 수 없도록 하는 강제적인 보안정책으로 양립할 수 없는 직무를 분리시키는 개념이다. 이는 부주의 및 고의에 의한 시스템 오용이나 권한의 악용의 위험을 감소시키며 업무 수행 시 과정, 분야별 독립적인 판단에 의한 실수를 예방하고 부정, 사기를 차단한다.

특히 금융, 정보보안, 개발 및 운영 등 다양한 분야에서 적용되며, 업무의 투명성과 책임성을 높이는 데 기여한다. 또한, 직무 분리는 법규 및 규정 준수를 위한 중요한 요소이며, 효과적인 감사 및 내부 감사를 가능하게 한다.

3. 최소 권한 원칙에 서술(10 점)

최소 권한 원칙이란 특정 업무를 수행함에 있어 필요한 권한만 보유하고 불필요한 권한은 보유하지 않게 하는 원칙으로 내부, 외부로부터의 악용의 소지를 차단하기 위한 개념이다. 특정 업무를 수행하는 동안 필요했던 권한을 해당 업무 종료 후에도 보유하면 권한 오용, 악용으로 업무 손실이 발생할 가능성이 높기에 필요하다.

이를 방지하려면 권한을 주기적으로 점검하고, 필요 없어진 권한은 회수해야 한다. 또한, 업무 역할에 따라 권한을 부여하는 시스템(RBAC)이나, 상황에 따라 권한을 조정하는 시스템(ABAC)을 활용하면 효율적으로 관리할 수 있다. 최소 권한 원칙을 잘 지키면 보안 사고를 줄이고 안전한 시스템 운영이 가능해진다.