

수 행 프 로 젝 트	항목	주요내용
	프로젝트 명	DB 소프트웨어 어플리케이션 프로젝트
	수행기간	2025.03.01 ~ 2025.03.20
	목표	WordPress 기반 웹·DB 환경에서 보안 설정과 모니터링 체계를 구축해, DB 권한 관리·성능 가시성·WAF 탐지 역량 확보
	내용	<p>통합 모니터링 환경</p> <p>-WordPress+MariaDB(192.168.5.50)↔Percona PMM(Server/Client) 연동</p> <p>-실시간 성능·쿼리·리소스 사용량 대시보드 제공</p> <p>웹 보안 실습 플랫폼</p> <p>-OWASP Juice-Shop을 웹 인터페이스로 활용</p> <p>-XSS, SQLi, Command Injection 등 공격 시나리오 실행 후 탐지 로그 확인</p> <p>계정·권한 관리</p> <p>-test/1234: 192.168.5.50 전용 접속</p> <p>-PMM 계정(본인): 모든 권한</p> <p>-test1/9876·test2/4321: 제한 권한 및 비밀번호 재설정</p> <p>스키마 설계 및 집계 쿼리</p> <p>-ANIMAL_INS/ANIMAL_OUTS 테이블, COST 컬럼 설계</p> <p>-전체 입양비 합계·평균 계산 쿼리 작성 및 권한 제어 실습</p> <p>WAF 적용</p> <p>ModSecurity + OWASP CRS 배포</p> <p>Juice-Shop 공격 트래픽 탐지 여부 검증</p>
	설계/프로세스	<p>1.WordPress/MariaDB 환경 구축 → PMM-Server/Client 연동</p> <p>2.사용자 계정·권한 정책 수립 및 적용</p> <p>3.DB 스키마 변경 및 집계 쿼리 구현</p> <p>4.Juice-Shop 기반 웹 공격 실습 → WAF 탐지 확인</p> <p>5.PMM 대시보드·ModSecurity 로그·쿼리 결과 보고서화</p>
	담당 역할	<p>PMM 모니터링 인프라 설계·구축</p> <p>사용자 계정·권한 정책 설계 및 적용</p> <p>DB 스키마 설계·집계 쿼리 작성</p> <p>ModSecurity WAF 룰 튜닝 및 탐지</p>
	느낀점/성장점	<p>-단순 DB 운영을 넘어서, 모니터링 및 보안 제어까지 통합적으로 고려하는 시야를 기를 수 있었습니다.</p> <p>-실습을 통해 웹과 DB 사이의 공격 경로 및 탐지 메커니즘을 실제로 경험하며 보안 감수성 향상되었습니다.</p> <p>-사용자 권한 분리, WAF 설정 등 실무에 가까운 환경 구성 과정을 통해 보안 정책 설계 능력을 키웠습니다.</p> <p>-Percona PMM을 활용한 성능 시각화 및 지표 분석 경험으로 문제 진단 능력 향상되었습니다.</p>