2025학년도 1학기 SW 캡스톤디자인 경진대회

교내 시스템 취약점 점검

팀 명 대방어

팀 원 이진규(IT정보공학과, 4), 조대인(IT정보공학과, 4)

지도교수 김윤경

개발 동기 및 목적

개발동기

- 대학 웹 서비스에 대한 사이버 공격으로 학사정보·개인정보·연구데이터 유출 위험이 심각함
- 교육기관 대상 해킹 시도가 전년 대비 35% 증가하여 보안 강화 필요성이 대두됨
- 학사관리·학습관리(LMS)·도서관·연구행정 시스템이 상호 연계되어 하나의 침해가 전체 서비스로 확산될 수 있음

경기대학교	• 약 1만 명 개인정보 웹사이트 유출
홍익대학교	• 1만 2,367명의 개인정보가 담긴 자료를 메일로 오발송
경북대학교	• 대학원 재학생 전원 5,905명 개인정보 메일 오발송
전북대학교	• 해킹으로 학생 및 졸업생 등 32만 2,425명 개인정보 유출
선문대학교	• SW 업데이트 과정에서 9,700여 명 개인정보 유출
이화여자대학교	• 해킹으로 졸업생 8만 명 개인정보 유출

출처: 캐치 시큐리티

목적

- OWASP Top 10 및 국내 주요정보통신기반시설 취약점 분석 가이드를 기반으로 종합적인 웹 취약점 진단을 수행
- 정적 분석(SAST), 동적 분석(DAST), 모의해킹(Black-/White-box) 등을 병행하여 심층 취약점 평가를 실시
- 인증·인가, 세션 관리, 입력값 검증, 출력 인코딩, API 보안, TLS/SSL 구성 등 핵심 보안 요소를 체계적으로 점검
- 리스크 평가를 통해 취약점 우선순위를 도출하고, 단계별 개선·보완 계획(보안 아키텍처 재설계, Secure Coding 가이드 제공 등)을 수립
- 본 과제 결과물을 바탕으로 대학 정보 시스템의 보안 수준 향상 및 지속가능한 보안 대책 촉구

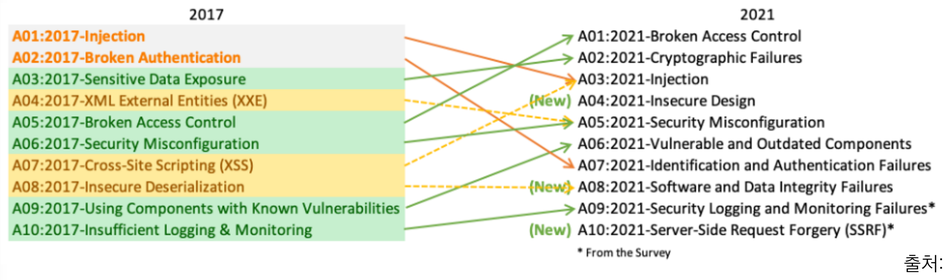
주요 기술

활용 도구

- Shodan과 Censys를 활용하여 공개정보 출처를 통해 웹 애플리케이션의 기본 정보를 파악함.
- OWASP ZAP 및 Burp Suite를 이용해 웹 애플리케이션 동적 분석(DAST)을 수행함.
- OWASP ZAP을 이용한 정적 소스 코드 분석(SAST)을 실행함.

기술

- OWASP TOP 10 활용 분석
- 주요통신기반시설 점검 체크리스트 활용



출처: OWASP

- OWASP는 4년 주기로 갱신, 기술 트렌드의 변화로 위화같이 3가지 주요 공격 기법이 추가되고 공격기법의 중요도가 변화함
- 표와 같이 KISA에서 발행한 주요통신기반시설 점검 가이드 북에는 28가지의 웹 취약점 점검 항목이 기제됨
- 본 가이드 북은 통신 기반시설의 연속성과 가용성을 확보하기 위해 시스템 구성부터 운영 절차까지 전반적인 보안·운영 프레임워크를 제시함.
- 법적·규제적 요구사항을 반영하여 점검 대상별 최소 보안 기준과 개선 권고 사항을 상세히 정의하고 있음.

Web 취약점 분석·평가 항목

점검항목	항목 중요도	항목코드
버퍼 오버플로우	상	BO
포맷스트링	상	FS
LDAP 인젝션	상	LI
운영체제 명령 실행	상	OC
SQL 인젝션	상	SI
SSI 인젝션	상	SS
XPath 인젝션	상	XI
디렉터리 인덱싱	상	DI
정보 누출	상	IL
악성 콘텐츠	상	CS
크로스사이트 스크립팅	상	XS
약한 문자열 강도	상	BF
불충분한 인증	상	IA
취약한 패스워드 복구	상	PR
크로스사이트 리퀘스트 변조(CSRF)	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV
파일 업로드	상	FU
파일 다운로드	상	FD
관리자 페이지 노출	상	AE
경로 추적	상	PT
위치 공개	상	PL
데이터 평문 전송	상	SN
쿠키 변조	상	CC

출처: KISA, 주요정보통신기반시설 점검 가이드 북

개발 내용

〈그림1. XSS로 인해 스크립트가 실행된 모습〉

〈그림2. 파라미터 조작을 통한 다른 강의 파일 다운〉

- 교내 LMS J-Query 버전에 대한 취약점 점검을 수행하여 클라이언트 측 스크립트 필터링 오류를 확인함.
- 전북대학교 스마트학습관리시스템(LMS) 로그인 프로세스를 분석하여 인증 우회 가능성을 검증함.
- 인증 우회 취약점 탐지 방법론을 적용하여 세션 토큰 예측 및 하이재킹 공격 시나리오를 테스트함.
- 세션 관리 취약점 분석 결과, 세션 고정(Session Fixation) 및 세션 탈취 가능성이 존재함을 확인함.
- 수강신청 사이트의 SQL 인젝션 발생 가능성을 점검하여, 강의 조회 및 신청 모듈에서 파라미터 검증 미흡으로 인한 취약점을 발견함.
- 정보 노출 취약점 분석을 통해 학생 개인정보 API가 과도한 사용자 정보를 반환함을 확인함.
- 공지사항 게시판 및 입력폼에 대해 저장형 XSS 취약점 점검을 실시하여 스크립트 삽입 가능성을 발견함.
- 중요 기능 요청에 CSRF 토큰 적용 여부를 확인한 결과, 다수 엔드포인트에서 토큰 미적용을 확인함.
- 진단 결과를 체계적으로 정리할 수 있는 웹 취약점 분석 보고서 템플릿을 개발함.
- OWASP Top 10 및 국내 주요정보통신기반시설 취약점 분석 가이드에 기반하여 우선순위별 개선 방안을 도출함.

결과 및 분석

* 전반적으로 강의 관리자 권한 획득 및 무단 침입 등 핵심 기능 우회 등의 기능은 서버단에서 잘 대응 되었으나 문자열 필터링, 정보노출, 취약한 API 활용 등의 문제점이 있음.

취약점 항목	건수	주요 내용
버퍼 오버플로우	00(다수)	입력값 길이 제한(문자열 길이 검증) 정책이 적용되어 오류 및 오버플로우 미발생
정보 누출	00(다수)	에러 메시지나 서버 구성 정보(DBMS, 서버 정보 등) 노출 방지 정책이 적용되어 정보 누출 없음
크로스사이트 스크립팅 (XSS)	5	사용자 입력값에 대한 필터링·출력 인코딩 미흡 → 세션 탈취, 피싱 등 공격 가능
불충분한 인가	2	중요 페이지 접근 제어 미비 → 파라미터 조작으로 정보 열람·변조 가능
불충분한 인증	1	로그인 시 사용자 신원 확인 절차 부족 → 무단 접근 및 계정 도용 위험
프로세스 검증 누락	1	업무 처리 단계 검증 로직 생략 → 비정상적 흐름으로 시스템 우회 가능
파일 업로드 검증 부족	1	업로드 파일 확장자·크기·내용 검증 부재 → 악성 파일 업로드를 통한 시스템 침해 가능

대응 방안

- 모든 입력값에 대해 서버 사이드 검증 수행 및 파라미터화된 쿼리(Prepared Statement) 사용함
- 파일 경로에 대해 화이트리스트 검증을 적용하고, 사용자 입력을 기반으로 한 파일 접근을 차단함
- 출력 시 HTML 이스케이프 처리를 철저히 하고, CSP(Content Security Policy)를 설정함
- 모든 상태 변경 요청에 CSRF 토큰을 적용하고, Referer 검증을 병행함
- 보안 패치 적용 주기를 단축하고, 제로데이 정보 구독을 통해 신속 대응 태세를 유지함