강의계획서

[1] 기본 정보

■ 수업 정보

개설년도/학기	2025/1	교과목명	시큐어코딩
학수번호	012744	분반	01
강의실/강의시간	융합과학관(24호관)-24408:화(6,7,8)	학점	3학점
수업유형	과목구분(일반과목), 이론(3), 실습(0)	교과목인증	-
이수구분	전공선택	교수참여유형	단독
성적 평가 구분	상대평가	독서인증	No
		ESG 관련성	-

■ 교수자 정보 (1)

교수명	에런스노버거	소속	정보보안학과
연락처		이메일	
연구실		교과목 상담 가능 시간 (Office Hours)	

▽ 학칙 제 58조의 2에 의거하여 장애학생은 학기 초에 교과목 담당자의 면담을 통해 강의,과제,시험등에 관한 학습지원을 요청할 수 있으며, 요청된 사항은 담당교수 혹은 장애학생 지원센터를 통해 지원받을 수 있습니다. 자세한 사항은 아래 '■ 참고사항'을 확인하기 바랍니다.

[2] 학습목표 / 학습성과

■ 강의개요

『웹 애플리케이션 보안 완벽 가이드』는 취약점을 최소화하기 위한 다양한 방법을 소개한다. 이 책에서는 PHP를 사용하지만 웹의 기본을 다루고 있어 다른 언어에서도 충분히 적용할 수 있는 내용을 다룬다.

■ 선수과목(강좌이수 필수사항)

이 책은 웹 개발자뿐 아니라 보안 업계에 종사하는 웹 취약점 진단자에게도 유용한 내용이 수록돼 있어 진단 실무자에게도 유용할 것이다.

■ 강의목표

4장까지는 PHP를 바탕으로 취약점을 소개하고, 취약점으로 발생할 수 있는 위협, 취약점을 없애기 위해 어떻게 개발해야 할지 예제 코드와 함께 상세하게 설명한다. 책에서 다루는 소스코드는 책과 함께 제공하는 가상 머신에도 포함돼 있으므로 책을 보면서 곧바로 실습을 진행할 수 있다.
5장 이후로는 개발 전 기획 단계에서 고려해야 할 기본적인 보안 기능과 직접 보안 진단을 하기 위한 방법들을 심도 있게 설명한다.

■ 핵심역량 연계성

구분	핵심역량	비율	주역량과 교과목 간 연계성
주역량 (1순위)	과학적사고역량	80%	(전공 교과목은 제시되지 않음)
부역량 (2순위)	자기주도역량	20%	

■ 역량 기반 학습성과

역량 구분		하위역량	구성요소	행동지표
핵심역량	과학적사고	분석적 사고	관찰력	나는 주변 사물이나 현상들을 다른 사람에 비해 주의깊게 살펴보는 편이며, 세세한 부분까지 다양하게 구체적으로 관찰한 내용들을 묘사한다.
			분석력	나는 문제나 상황들을 부분적으로 세분화하고, 부분별로 해결해야 할 과제가 무엇인지 명확히 파악하며, 부분들 간의 관계성까지 분석한다.
			논리력	나는 구체적인 근거를 제시하며 주어진 문제의 원인들을 파악하고, 원인에 따른 결과가 무엇인지 연계하여 분석한다.
		종합적 사고	추리력	나는 수집된 여러 지식과 정보들을 서로 연관시키며 조합하여 중요하게 해결될 문제가 무엇인지와 향후 예상되는 결과들을 다양하게 추리한다.
			통찰력	나는 외면적으로 드러난 정보와 숨어있는 정보 뿐만 아니라 여러 정보들 간의 의미있는 패턴, 관계성까지 찾아내고, 그 정보들을 연결하여 유용한 아이디어로 활용한다.
			판단력	나는 적절한 선정기준을 만들어 여러 해결안들을 서로 비교하고, 예상되는 결과까지 고려하여 최종 해결안을 판단한다.
		창의적 사고	호기심	나는 어떤 내용이든 호기심이 생기면 바로 질문을 하거나 궁금한 내용이 해소될 때까지 계속 찾아본다.
			독창성	나는 항상 친구들이 생각하지 못하는 새로운 아이디어를 많이 제시하고, 제시한 아이디어들이 다수로부터 인정을 받는다.
			실용성	나는 새로운 아이디어가 실제 현장에서 적용 가능한가를 함께 파악하고, 실용성 있게 구체적으로 정교화하여 아이디어로 제안한다.

[3] 수업 진행 정보

■ 교수학습방법

강의식 수업	PBL/ 프로젝트	발표·토의	협동학습	Co-ACT	실험/실습 /실기	현장실습	플립러닝	블렌디드/ MOOC	사이버	기타
	0				0					

교수학습방법	세부 설명
PBL/프로젝트	-
실험/실습/실기	-

■ 수업자료 및 기타자료

주교재	교재명	웹 애플리케이션 보안 완벽 가이드: 체계적으로 배우는 안전한 웹 애플리케이션 제작 기법
	저자	토쿠마루 히로시 저/양현, 김민호, 연구흠 역
	출판사	위키북스
	발행년	2019년 10월 04일

부교재	교재명	C & C++ 시큐어 코딩
	저자	로버트 시코드 저 / 이승준 역
	출판사	에이콘출판사
	발행년	2015년 01월 09일
기타 자료		-
온라인 자료		https://hacksplaining.com/lessons

[4] 학습 평가 방법

출석	중간고사	기말고사	핵심역량평가	퀴즈	과제	팀 프로젝트
10%	25%	30%	5%		30%	
발표 · 토의	수업활동 결과물	수업 참여/태도	실기평가	기타1 ()	기타2 ()	기타3 ()

학습 평가 방법	세부 설명	평가준거
출석		
중간고사		
기말고사		
핵심역량평가		
과제		

[5] 주별 세부 수업계획

1주차	수업 주제	01장: 웹 응용 프로그램 취약점이란?
	수업 목표	01장: 웹 응용 프로그램 취약점이란?
	수업 내용	01장: 웹 응용 프로그램 취약점이란? 01. 취약점이란 '악용 가능한 버그' 02. 왜 취약점이 존재하면 안 되는가? ____경제적 손실 ____법적 규제 ____사용자가 회복 불가능한 손실을 받을 수 있다 ____웹 사이트 사용자에게 신뢰도 하락 ____의도하지 않게 공격자가 될 수 있다 03. 취약점이 발생하는 이유 04. 보안 버그와 보안 기능 05. 이 책의 구성 06. 보안 지침과 대응 ____소프트웨어 개발 보안 가이드 ____OWASP Top10
	수업 방법 및 평가 활동	강의 (PPT) + 실습

[5] 주별 세부 수업계획		
2주차	수업 주제	02장: 실습 환경 설정
	수업 목표	02장: 실습 환경 설정 (Virtual Machine)
	수업 내용	02장: 실습 환경 설정 01. 실습 환경 개요 ____실습용 가상 시스템 다운로드 ____예제 프로그램 라이선스 02. 파이어폭스 설치 03. 버추얼박스 설치 ____버추얼박스란? ____버추얼박스 다운로드 04. 가상머신 가져오기 및 동작 확인 ____가상 시스템 동작 확인 ____가상 시스템 종료 방법 ____리눅스 운영 05. OWASP ZAP 설치 ____OWASP ZAP이란? ____JRE 설치 ____OWASP ZAP 설치 ____OWASP ZAP 설정 06. 파이어폭스 확장 기능 FoxyProxy-Standard 설치 07. OWASP ZAP 사용하기 08. 웹 메일 확인 ____참고 / 가상머신 데이터 목록
	수업 방법 및 평가 활동	강의 (PPT) + 실습
3주차	수업 주제	03장: 웹 보안 기초 - HTTP, 세션 관리, 동일 출처 정책, CORS
	수업 목표	03장: 웹 보안 기초 - HTTP, 세션 관리, 동일 출처 정책, CORS
	수업 내용	03장: 웹 보안 기초 - HTTP, 세션 관리, 동일 출처 정책, CORS 01. HTTP와 세션 관리 ____왜 HTTP를 공부하는가? ____가장 간단한 HTTP ____입력-확인-등록 형식 ____상태 비보존 HTTP 인증 ____쿠키 및 세션 관리 ____정리 02. 수동적 공격과 동일 출처 정책(Same Origin Policy) ____능동적 공격과 수동적 공격 ____브라우저는 어떻게 수동 공격을 막을까 ____자바스크립트 이외의 크로스 도메인 접근 ____CSS ____정리 03. CORS(Cross-Origin Resource Sharing) ____간단한 요청 ____사전 점검 요청 ____인증 정보를 포함한 요청
	수업 방법 및 평가 활동	강의 (PPT) + 실습
4주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #1-4
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #1-4
	수업 내용	04장: 웹 응용 프로그램 기능별 보안 버그 01. 웹 응용 프로그램의 기능과 취약점 대응 ____취약점은 어디서 발생하는가?
	수업 방법 및 평가 활동	강의 (PPT) + 실습

[5] 주별 세부 수업계획		
4주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #1-4
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #1-4
	수업 내용	____인젝션 관련 취약점이란? ____정리 02. 입력 처리와 보안 ____웹 응용 프로그램에서 '입력'은 무슨 역할인가? ____문자 인코딩 검증 ____문자 인코딩 변환 ____문자 인코딩 검사 및 변환의 예 ____입력값 검증 ____예제 ____정리 ____참고: '제어 문자 이외'를 표현하는 정규 표현식 03. 표시 처리에 따른 문제 __4.3.1 크로스 사이트 스크립팅(기본편) ____개요 ____공격 방법과 영향 ____취약점이 발생하는 원인 ____대책 ____참고: Perl을 이용한 대책 예 __4.3.2 크로스 사이트 스크립팅(응용편) ____href 속성과 src 속성을 사용한 XSS ____자바스크립트 동적 생성 ____HTML 태그와 CSS 입력을 허용하는 경우의 대책 __4.3.3 에러 메시지로부터의 정보 유출 ____정리 _
	수업 방법 및 평가 활동	강의 (PPT) + 실습
5주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #5-8
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #5-8
	수업 내용	05. '중요한 처리'시에 삽입되는 취약점 __4.5.1 크로스 사이트 요청 변조(CSRF) ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 __4.5.2 클릭재킹 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____정리 06. 세션 관리 미비 __4.6.1 세션 하이재킹의 원인과 영향 __4.6.2 추측 가능한 세션 ID ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____참고: 자체 세션 관리 메커니즘과 관련된 다른 취약점 __4.6.3 URL에 삽입된 세션 ID ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 __4.6.4 세션 ID 고정화 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____정리 07. 리다이렉트 처리와 관련된 취약점
	수업 방법 및 평가 활동	강의 (PPT) + 실습

[5] 주별 세부 수업계획		
5주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #5-8
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #5-8
	수업 내용	__4.7.1 오픈 리다이렉트 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대
	수업 방법 및 평가 활동	강의 (PPT) + 실습
6주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #9-12
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #9-12
	수업 내용	09. 메일 전송 문제 __4.9.1 메일 전송 문제 개요 __4.9.2 메일 헤더 인젝션 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____정리 ____더 높은 단계로 나아가기 위해 10. 파일 접근과 관련된 문제 __4.10.1 디렉터리 탐색 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____정리 __4.10.2 의도하지 않은 파일 노출 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____참고: Apache 웹 서버에서 특정 파일을 숨기는 방법 11 OS 명령 호출 시 발생하는 취약점 __4.11.1 OS 명령어 인젝션 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____참고: 내부 셸을 호출하는 함수 12. 파일 업로드와 관련된 문제 __4.12.1 파일 업로드 문제 개요 __4.12.2 업로드된 파일을 통한 스크립트 실행 ____개요 ____공격 방법 및 영향 ___
	수업 방법 및 평가 활동	강의 (PPT) + 실습
7주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #13-15
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #13-15
	수업 내용	13. 포함 기능과 관련된 문제 __4.13.1 파일 포함 공격 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인
	수업 방법 및 평가 활동	강의 (PPT) + 실습

[5] 주별 세부 수업계획		
7주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #13-15
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #13-15
	수업 내용	____대책 ____정리 14. 구조화된 데이터 읽기 관련 문제 __4.14.1 eval 인젝션 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____정리 ____더 높은 단계로 나아가기 위해 __4.14.2 안전하지 않은 역직렬화 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 __4.14.3 XML 외부 개체 참조(XXE) ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____정리 15. 공유 자원 및 캐시와 관련된 문제 __4.15.1 경쟁 상태 취약점 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 ____정리 ____참고: 자바 서블릿의 기타 주의 사항 __4.15.2 캐시로부터의 정보 유출 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원
	수업 방법 및 평가 활동	강의 (PPT) + 실습
8주차	수업 주제	중간고사
	수업 목표	중간고사
	수업 내용	중간고사
	수업 방법 및 평가 활동	중간고사
9주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #16-17
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #16-17
	수업 내용	16. 웹 API 구현에서 발생할 수 있는 취약점 __4.16.1 JSON과 JSONP 개요 ____JSON이란? ____JSONP이란? __4.16.2 JSON 이스케이프 미흡 ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책
	수업 방법 및 평가 활동	강의 (PPT) + 실습

[5] 주별 세부 수업계획		
9주차	수업 주제	04장: 웹 응용 프로그램 기능별 보안 버그, #16-17
	수업 목표	04장: 웹 응용 프로그램 기능별 보안 버그, #16-17
	수업 내용	__4.16.3 JSON 직접 열람에 의한 XSS ____개요 ____공격 방법 및 영향 ____취약점이 발생하는 원인 ____대책 __4.16.4 JSONP의 콜백 함수 이름을 통한 XSS ____개요 ____공격 방법 및 영향 ____취약점이 발생한 원인 ____대책 __4.16.5 웹 API의 CSRF ____웹 API에 대한 CSRF 공격 경로 ____대책 __4.16.6 JSON 하이재킹 ____개요 ____공격 방법 및 영향 ____대책 __4.16.7 JSONP의 부적절한 사용 ____JSONP에 의한 비밀 정보 제공 ____신뢰할 수 없는 JSONP API 사용 ____정리 __4.16.8 CORS 검증 미흡 __4.16.9 보안을 강화하는 응답 헤더 ____정리 17. 자바스크립트 문제 __4.17.1 DOM Based XSS ____개요 ____취약점이 발생한 원인 ____대책 __4.17.
	수업 방법 및 평가 활동	강의 (PPT) + 실습
10주차	수업 주제	05장: 대표적인 보안 기능
	수업 목표	05장: 대표적인 보안 기능 (Representative Security)
	수업 내용	05장: 대표적인 보안 기능 01. 인증 __5.1.1 로그인 기능 ____로그인 기능에 대한 공격 ____로그인 기능이 파손됐을 때의 영향 ____부정 로그인을 막기 위해서는 __5.1.2 패스워드 인증을 노리는 공격에 대한 대책 ____기본적인 계정 잠금 ____패스워드 인증에 대한 공격 종류와 대책 __5.1.3 패스워드 저장 방법 ____패스워드 보호의 필요성 ____암호화를 통한 패스워드 보호와 해결 과제 ____메시지 다이제스트를 통한 패스워드 보호와 과제 __5.1.4 자동 로그인 ____안전하지 않은 구현 예 ____안전한 자동 로그인 구현 방법 ____자동 로그인의 위험을 낮추기 위해 __5.1.5 로그인 폼 __5.1.6 오류 메시지 요건 ____ID와 패스워드 어느 쪽이 틀렸는지를 표시하면 안 되는 이유 ____ID와 패스워드를 2단계로 나눠 입력하는 사이트 증가 __5.1.7 로그아웃 기능 __5.1.8 인증 기능 정리 02. 계정 관
	수업 방법 및 평가 활동	강의 (PPT) + 실습

[5] 주별 세부 수업계획		
11주차	수업 주제	06장: 문자 코드와 보안
	수업 목표	06장: 문자 코드와 보안 (Character Code and Safety)
	수업 내용	06장: 문자 코드와 보안 01. 문자 코드와 보안 개요 02. 문자 집합 03. 문자 인코딩 04. 문자 코드로 인한 취약점 발생 요인 정리 05. 문자 코드를 올바르게 취급하는 방법 06. 정리
	수업 방법 및 평가 활동	강의 (PPT) + 실습
12주차	수업 주제	07장: 취약점 진단 입문
	수업 목표	07장: 취약점 진단 입문 (Vulnerability Checking)
	수업 내용	07장: 취약점 진단 입문 01. 취약점 진단 개요 02. 취약한 응용 프로그램 Bad Todo ____Nmap 03. 진단 도구 다운로드 및 설치 ____OpenVAS ____RIPS 04. Nmap을 이용한 포트 스캔 ____Nmap 사용해보기 ____Nmap 결과를 보는 방법 ____OpenVAS 사용해보기 05. OpenVAS을 통한 플랫폼 취약점 진단 ____OpenVAS 결과 확인 방법 ____OWASP ZAP 설정 06. OWASP ZAP을 이용한 자동 취약점 스캔 ____세션 정보 설정 ____크롤링 ____자동 진단 ____진단 결과 확인 ____진단 보고서 작성 ____진단 후처리 07. OWASP ZAP을 이용한 수동 취약점 진단 ____URL 목록표 작성 ____진단 작업 ____보고서 작성 ____진단 후처리 ____RIPS 사용해보기 08. RIPS를 사용한 소스코드 진단 09. 취약점 진단 실시를 할 때 주의할 점 10. 정리 11. 취약점 진단 보고서 예제 __7.11.1 XML 외부 엔티티 참조(XXE) __7.11.2 크로스 사이트 스크립팅(XSS)
	수업 방법 및 평가 활동	강의 (PPT) + 실습
13주차	수업 주제	08장: 웹 사이트의 안전성을 높이기 위해
	수업 목표	08장: 웹 사이트의 안전성을 높이기 위해
	수업 내용	08장: 웹 사이트의 안전성을 높이기 위해 01. 웹 서버에 대한 공격 경로 및 대책
	수업 방법 및 평가 활동	강의 (PPT) + 실습

[5] 주별 세부 수업계획		
13주차	수업 주제	08장: 웹 사이트의 안전성을 높이기 위해
	수업 목표	08장: 웹 사이트의 안전성을 높이기 위해
	수업 내용	__8.1.1 기반 소프트웨어 취약점을 노린 공격 __8.1.2 무단 로그인 __8.1.3 대책 ____적절한 서버 기반을 선정 ____불필요한 소프트웨어는 사용하지 않음 ____취약점 대처는 실시간으로 수행 ____공개할 필요가 없는 포트나 서비스는 접근을 제한 ____인증 강도를 높임 02. 피싱 사이트 대책 __8.2.1 네트워크를 통한 피싱 사이트 수법 ____DNS에 대한 공격 ____ARP 스푸핑 __8.2.2 피싱 __8.2.3 가짜 웹 사이트 대책 ____네트워크적인 대책 ____TLS 도입 ____확인하기 쉬운 도메인명 사용 03. 도청, 변조 대책 __8.3.1 도청, 변조 경로 __8.3.2 중간자 공격 ____OWASP ZAP을 이용한 중간자 공격 실습 ____OWASP ZAP 루트 인증서 설치 __8.3.3 대책 ____TLS 이용 시 주의할 점 04. 악성코드 대책 __8.4.1 웹 사이트 악성코드 대책이란?
	수업 방법 및 평가 활동	강의 (PPT) + 실습
14주차	수업 주제	09장: 안전한 웹 응용 프로그램을 위한 개발 관리
	수업 목표	09장: 안전한 웹 응용 프로그램을 위한 개발 관리
	수업 내용	09장: 안전한 웹 응용 프로그램을 위한 개발 관리 01. 개발 관리에 따른 보안 대책의 전체 모습 02. 개발 체제 03. 개발 프로세스 __9.3.1 기획 단계에서의 유의점 __9.3.2 발주할 때의 유의점 __9.3.3 요건 정의를 할 때 유의할 점 __9.3.4 기본 설계 진행 방식 __9.3.5 상세 설계, 프로그래밍시 유의점 __9.3.6 보안 테스트의 중요성 및 방법 __9.3.7 수주자측 테스트 __9.3.8 개발자 쪽에서의 테스트(검수) __9.3.9 운영 단계에서의 유의점 __9.3.10 애자일 개발 프로세스에 적용 04. 정리
	수업 방법 및 평가 활동	강의 (PPT) + 실습

15주(보충/보강주)		
16주차	수업 주제	기말고사
	수업 목표	기말고사
	수업 내용	기말고사
	수업 방법 및 평가 활동	기말고사

■ 참고사항

장애학생의 학습권을 보장하기 위한 강의, 과제, 시험 및 평가와 관련된 지원 유형의 예는 아래와 같으며, 구체적인 학습지원은 개별학생의 장애특성과 요구에 맞게 적절하고 합리적인 수준에서 제공되며, 강의 특성에 따라 달라질 수 있습니다.

분류	지원유형
강의관련	· 시각장애 : 점자, 확대자료 제공, 교재 제작, 수업보조 도우미 허용 등 · 청각장애 : 대필 도우미 배치 등 · 지체장애 : 대필 도우미 배치, 휠체어 접근이 가능한 강의실 제공 등
과제관련	· 제출일 연장, 대체과제 제공 등
시험 및 평가관련	· 확대 시험지 제공, 시험시간 연장 및 평가 방법 변경 등