


확장형 강의계획서

(상세 내용은 학기 중 변경 가능. 11/21 저녁에 실습시험 일정이 있으므로 확인할 것)

과목명	해킹및정보보안 (Hacking and Information Security)	학기	2024년 2학기
학점	3	과목코드	CSE4104
수업시간	화/목 12:00~13:15	수강대상	3~4학년 권장

	교수: 최재승	홈페이지: islabsogang.github.io
	이메일: jschoi22@sogang.ac.kr	전화: 02-705-8490
	사무실: AS관 711호 면담 시간(office hour): 강의 첫 시간 오리엔테이션에서 공지	

I. 교과목 개요

1. 수업개요

본 교과목에서는 정보보안 분야의 기초적인 개념을 배우고 실습한다. 특히, 정보보안의 다양한 세부분야 중에 소프트웨어 보안에 집중하여 학습을 진행한다. 구체적으로, 소프트웨어 취약점의 발생 원리를 배우고 이러한 취약점이 어떤 보안 문제를 일으키는지 학습한다. 또한 웹 보안 및 운영체제 보안의 몇몇 주제들을 소프트웨어 보안의 관점에서 간략하게 다루며, 암호학 및 네트워크 보안 관련 주제는 본 과목에서 다루지 않는다.

2. 선수학습내용

본 과목에서는 x86 어셈블리 코드를 자주 다루기 때문에 **컴퓨터시스템개론** 과목을 미리 수강하는 것이 강력하게 권장된다. 수업 초반에 어셈블리 언어를 간단하게 복습하기는 하지만, **컴퓨터시스템개론** 과목을 수강하지 않은 학생이라면 스스로 충분한 시간을 투자하여 공부해야 한다.

또한, **시스템프로그래밍** (또는 **운영체제**) 과목의 지식 또한 어느 정도 요구된다. 예를 들어, *커널*, *프로세스*, *쓰레드* 등의 개념을 처음 들어보는 학생이라면 중간에 생소하게 느껴지는 주제가 있을 것이다.

마지막으로, 리눅스 서버를 과제 환경으로 사용하기 때문에, 리눅스를 익숙하게 다룰 수 있는 능력이 요구된다.

3. 수업방법

강의	토론	실험	현장학습	발표
100%				

4. 평가방법 (조정가능)

중간고사	기말고사	실습과제	실습시험	참여도
35%	25%	25%	15%	

II. 교과 목표

다양한 소프트웨어 취약점이 어떠한 원리로 발생하며, 해커가 이런 취약점을 어떻게 공격할 수 있는지 살펴본다. 또한 취약점에 대한 공격을 방어하기 위한 기법들과, 그러한 방어 기법을 우회하는 고급 공격 기법에 대해서도 공부한다. 본 교과목을 통해, 안전한 소프트웨어를 만들기 위해서는 항상 공격자의 입장에서 생각해 보는 태도가 중요하다는 것을 이해하게 될 것이다.

III. 수업 운영 방식

매주 2회의 강의를 통해 정보보안 분야의 주요 개념을 학습한다. 또한 학기 내내 다양한 실습 과제를 진행하여 개념을 더 깊이 이해할 수 있도록 돕는다. 때때로 수업 시간에 실습 과제에 대한 접근 방향 설명이 이뤄질 것이다.

IV. 평가 기준 및 필수 요건

학점 수료를 위해 필수적으로 만족해야 하는 요건은 없으나, FA 규정은 학교 규정이므로 준수해야 한다. 최상위 20~30% 학생에게 A 학점을 부여하며, 차상위 30~40% 학생들에게 B 학점을 부여한다. 학기 총점 중 20% 이하의 점수를 받을 경우 D를 받게 된다. **과제 비중이 높은 과목의 특성상, 재수강생의 경우 별도의 평가 기준이 적용될 수 있다.**

V. 수업 규정

본 과목은 강의를 중심으로 진행되므로, 수업 시간에 떠드는 등의 강의에 지장을 주는 행동을 엄격히 금지한다. 또한 출석 관련 규정은 서강대학교의 학사 규정을 따른다.

시험에서의 부정행위는 적발 시 즉시 F학점으로 처리된다. 실습과제에서의 부정행위(솔루션 공유 등)가 적발될 경우 해당 과제가 0점 처리되며, 최종 학점을 한 단계 낮춘다(예: A->B).

VI. 교재 및 참고문헌

별도의 교과서는 없으며, 수업에서 제공하는 강의록(슬라이드) 및 실습 자료를 성실하게 학습하는 것으로 충분하다.

Ⅶ. 수업 계획 (학기 진행 상황에 따라 변경 가능)

전 주차에 대해, (1) 수업 방식은 강의 형태로 진행되며, (2) 수업 자료는 Cyber Campus 를 통해 제공되는 강의 슬라이드를 사용한다.

1 주차	학습목표	본 교과목에서 다룰 전반적인 주제들과 학습 목표를 이해한다
	주요학습내용	9.3 오리엔테이션 / 9.5 교과목 주제 소개
	과제	
2 주차	학습목표	소프트웨어 보안의 기초 개념을 학습한다
	주요학습내용	9.10 소프트웨어 취약점 개념 소개 / 9.12 휴강(개강미사)
	과제	실습 환경 소개
3 주차	학습목표	소프트웨어의 low-level 작동 원리를 복습한다
	주요학습내용	9.17 휴강(추석) / 9.19 어셈블리 복습, 과제 소개
	과제	실습 과제 #1
4 주차	학습목표	기본적인 버퍼 오버플로우 공격 원리를 학습한다
	주요학습내용	9.24 함수 호출 작동 원리 / 9.26 버퍼 오버플로우 기초
	과제	
5 주차	학습목표	버퍼 오버플로우 취약점에 대한 고급 공격 기법 및 이에 대한 방어 기법을 학습한다
	주요학습내용	10.1 Shellcode, Stack canary, NX / 10.3 휴강(개천절)
	과제	
6 주차	학습목표	방어 기법을 우회하는 고급 공격 기법을 학습한다
	주요학습내용	10.8 과제 소개, ASLR, ROP 가젯 / 10.10 ROP 공격 기법
	과제	실습 과제 #2
7 주차	학습목표	버퍼 오버플로우 외에도 다양한 종류의 취약점이 있으며, 사용자 입력을 함부로 신뢰해서는 안 된다는 것을 배운다
	주요학습내용	10.15 포맷 스트링 버그 / 10.17 예비 차시
	과제	
8 주차	중간고사 기간 (10.21 - 10.25)	

9 주차	학습목표	동적 메모리 할당과 관련된 취약점을 학습한다
	주요학습내용	10.29 중간고사 풀이, heap 복습 / 10.31 Use-after-free
	과제	
10 주차	학습목표	다양한 보안 취약점에 대한 학습을 계속한다
	주요학습내용	11.5 과제 소개 / 11.7 Type confusion
	과제	실습과제 #3
11 주차	학습목표	메모리 오류 없이 일어날 수 있는 취약점에 대해 학습한다
	주요학습내용	11.12 프로세스 및 스레드 복습 / 11.14 Race condition
	과제	
12 주차	학습목표	운영체제에서 어떤 보안 문제가 발생할 수 있는지 학습한다
	주요학습내용	11.19 커널 취약점 / 11.21 실습 시험 (오후 6:00~9:30)
	과제	
13 주차	학습목표	웹에서 어떤 보안 문제가 발생할 수 있는지 학습한다
	주요학습내용	11/26 웹 시스템 기초 / 11.28 File upload, SQL injection
	과제	
14 주차	학습목표	웹에서 어떤 보안 문제가 발생할 수 있는지 학습한다
	주요학습내용	12.3 Cross-site scripting / 12.5 예비 차시
	과제	
15 주차	학습목표	한 학기동안 배운 내용을 정리하고, 소프트웨어 보안 분야의 최신 연구 동향을 간략히 살펴본다
	주요학습내용	12.10 기말고사 / 12.12 기말고사 풀이, 과목 되돌아보기
	과제	
16 주차	기말고사 기간 (12.16 - 12.20)	

VIII. 참고 사항

수업에 관련된 사항은 사이버 캠퍼스(cyber.sogang.ac.kr)에서 공지하므로 수강생들은 해당 사이트를 수시로 확인하여야 한다.

IX. 장애학생 지원 사항

본 수업에서는 장애학생지원센터를 통해 전달되는 요청에 최대한 응할 것이며, 장애로 인해 수강 시 지원이 필요한 학생들은 개별적인 면담 또한 가능하다. 상담 결과에 따라 좌석 우선배정 등의 편의가 제공된다.