

Secure Coding

유효곤

ugonfor@gmail.com

시작하며,

강사 소개.

유효곤(ugonfor)

-

카이스트 AI대학원 석사과정(현재)

고려대학교 사이버국방학과 졸업(2023년)

네이버 인턴(2022년)

네이버 클로바 AI RUSH 입상(2021년)

사이버국방학과 해킹동아리 CyKor 부회장(2021년)

Best of the Best 취약점분석 9기 수료(2021년)

DEFCON CTF Finalist (2020년)

CODEGATE CTF Univ. Finalist (2020, 2022년)

그 외 CTF 다수 참여, 리버스 엔지니어링 위주

-

시작하며,

목차

- 시큐어 코딩이란,

- 의미
- 다른 강의들을 살펴보면,

- 소프트웨어 개발 실습

- 이전 내용 요약
 - 시큐어 소프트웨어 공학
 - 시큐어 코딩과 소프트웨어 공학
- 실습
 - 목표
 - 요구사항 도출

- 시스템 설계
- 시스템 구현
- 체크리스트 작성 및 테스트
- 유지보수

- 마무리

- 과제
- 프로젝트 관련
- 레퍼런스

시큐어 코딩이란,

- 의미
- 다른 강의들을 살펴보면,

시큐어 코딩이란,

의미

소프트웨어 프로그래밍 과정에서 안전한 코드를 만드는 것.

: 소프트웨어 개발자가 선제적으로 보안 약점을 제거하는 것.

: 정보보호에서 블루 팀의 역할.

상위개념: 시큐어 소프트웨어 공학

: 소프트웨어 개발 전 과정에 걸쳐 보안을 고려하여 안전한 소프트웨어를 만드는 것.

시큐어 코딩이란,

다른 강의들을 살펴보면,

KISA 가이드라인

Python: <https://www.kisa.or.kr/2060204/form?postSeq=13&page=1>

Java: <https://www.kisa.or.kr/2060204/form?postSeq=14&page=1>

C, C++ 시큐어 코딩 원서:

<https://github.com/DarkCodeOrg/welcome-to-cybersecurity/blob/master/secure%20coding%20in%20c%20and%20c%2B%2B.pdf>


대표적인 시큐어 코딩 점검 툴:

Polyspace Bug finder


...

시큐어 코딩이란,


다른 강의들을 살펴보면,



Secure Coding - Secure application development
Methodologies and tools to develop **secure** applications
G.L. Golinelli
4.0 ★★★★★ (2,720)
총 2.5시간 · 41개의 강의 · 중급자









Principles of Secure Coding
Mastering **Secure Coding** Practices for Robust Applications
Chris B Behrens
4.4 ★★★★★ (6,607)
총 3.5시간 · 55개의 강의 · 중급자
베스트셀러




Cyber Secure Coder (CSC-110)
Certificate Exam Preparatory Course
Stone River eLearning
4.4 ★★★★★ (6)
총 10시간 · 49개의 강의 · 모든 수준

최고의 기업들이 수요가 많고 경력에 도움이 되는 능력 개발을 위해 **Udemy Business**를 신뢰합니다.






Secure Coding & Design Best Practices in Python
Secure Coding Best Practices, **Secure Coding** Principles, **Secure Coding** in Python
Basics Strong
4.3 ★★★★★ (293)
총 3시간 · 51개의 강의 · 초급자



Secure Coding - Ensuring Safe Deployment of Code
Understanding the Significance of **Secure Coding** in DevOps Processes



secure coding

전체 이미지 동영상 쇼핑 뉴스 더보기

Tool 가이드 이란 예제 Java PHP 점검 툴 교육 솔루션

검색결과 약 406,000,000개 (0.26초)

요즘IT
<https://yozm.wishket.com> > 개발 > **시큐어 코딩의 의미와 실천 방안: ①시큐어 코딩이란? | 요즘IT**
2022. 12. 12. — 시큐어 코딩은 무엇인가? 시큐어 코딩은 사이버 공격에 대한 방어뿐만 아니라, 개발자의 실수나 코드상의 논리적 오류로 인해 발생할 수 있는 문제점을 ...

TISTORY
<https://codelib.tistory.com> > ... > **01 시큐어코딩(secure coding) 이란? - CODELIB - 티스토리**
2018. 8. 11. — 1. 시큐어코딩(**secure coding**) 이란? 소프트웨어(SW)를 개발함에 있어 개발자의 실수, 논리적 오류 등으로 인해 SW에 내포될 수 있는.

KISA 한국인터넷진흥원
<https://www.kisa.or.kr> > form > **JavaScript 시큐어코딩 가이드**
보안취약점 및 침해사고 대응. 인쇄하기 공유하기. 달기. 트위터. 페이스북. JavaScript 시큐어코딩 가이드. 담당자: 디지털정보보호팀 이수원. 전화: 061-820-1429.

관련 질문 :

What is the meaning of secure code? ▾

What is a secure coding technique? ▾

What are the principles of secure coding? ▾

Why is secure coding important? ▾

시큐어 코딩이란,

다른 강의들을 살펴보면,

- <https://github.com/basicsstrong/secure-coding-practices-python>
- <https://github.com/OWASP/SecureCodingDojo>
- <https://github.com/OWASP/Go-SCP>
- ...

➔ 예제 위주의 시큐어 코딩 강의 및 강의자료들

➔ 입력값 검증, 보안 기능 활성화, 시간 및 상태 처리, 에러 처리, 코드 오류 처리, 캡슐화, API 오용 방지 등

➔ 개발을 할 때는 기능 구현에 집중하다 보니, 보안 기능에 대해서 미처 생각하지 못한 경우가 많음

시큐어 코딩이란,

다른 강의들을 살펴보면,

시큐어 코딩은 주어진 예제에 적용하는 것은 쉽지만,

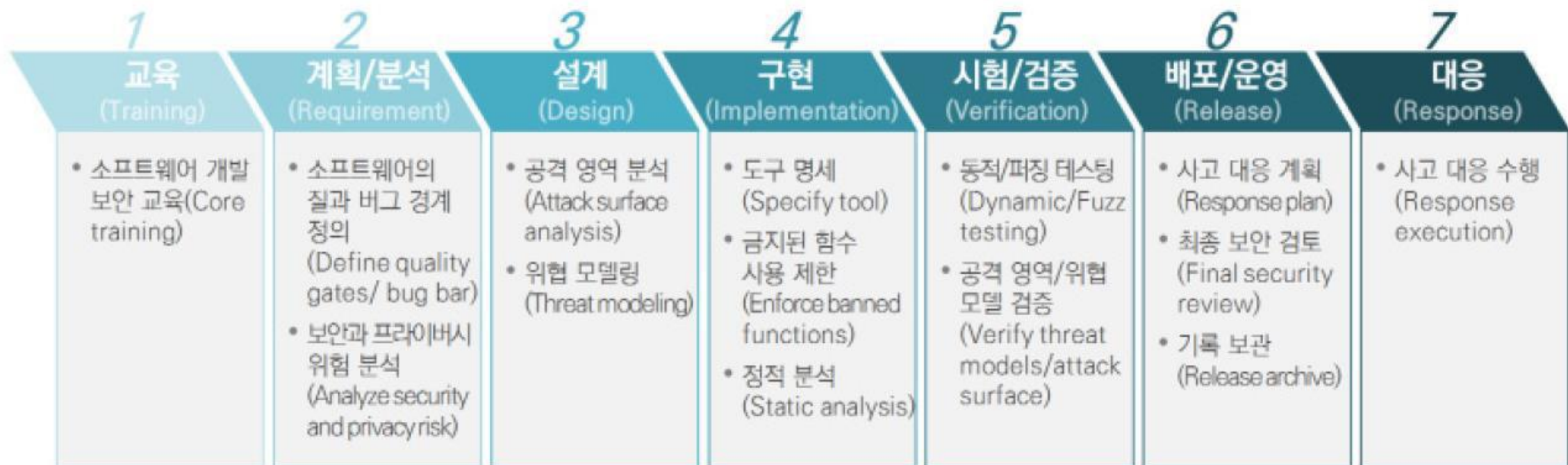
실제로 개발을 하면서 시큐어 코딩을 신경 쓰는 것은 어렵습니다.

소프트웨어 개발 실습

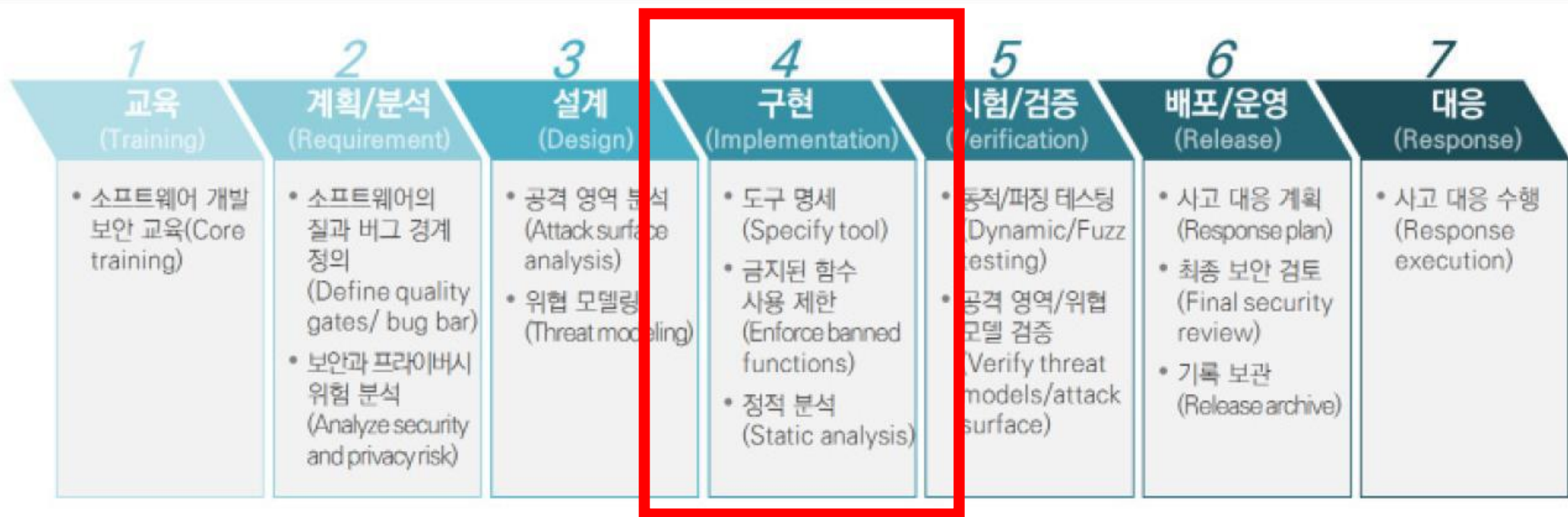
실제로 소프트웨어를 개발해보며, 시큐어코딩을 적용해보자.

- 이전 내용 요약
- 실습

시큐어 소프트웨어 공학



시큐어 코딩



목표

- 요구사항 도출
- 시스템 설계
- 시스템 구현
- 체크리스트 작성 및 테스트
- 유지 보수

목표

간단한 쇼핑몰 사이트 구현

Simple Shopping Mall Website.

목표

실습 환경 구성: 아래 github의 README를 참고하세요.

<https://github.com/ugonfor/secure-coding>

목표

streamlit: 대표적인 프로토타이핑 도구 (간단한 웹 프론트 제공)

FastAPI: 대표적인 백엔드 도구 (API구현을 위함)

SQLite3: 데이터베이스 관리 시스템

요구사항 도출

온라인 쇼핑몰이 있어야 하는 기능

- 사람들이 웹에서 상품을 볼 수 있어야 함.
- 상품을 구매할 수 있어야 함.
- 다른 사람의 구매내역은 볼 수 있으면 안 됨.
- 관리자가 관리할 수 있어야함.

시스템 설계

도식으로 그리는 것이 더욱 일반적임.

그러나, 없는 것보다는 어떤 형태든 있는 것이 나음.

시큐어 소프트웨어공학 기법을 활용하는 경우에는 정형 명세를 활용함.

시스템 설계

기능 도출:

- 사람들이 웹에서 상품을 볼 수 있어야 함.
 - : 기본 페이지에서 상품 목록을 볼 수 있게 하자.
 - : 각 상품은 상품 명, 가격, 사진을 보여주어야 함.
- 상품을 구매할 수 있어야 함.
 - : 주문 페이지를 만들어야 함.
 - : 결제할 수 있는 기능을 넣자.
 - : 집주소 및 결제 정보 입력이 필요함.
- 다른 사람의 구매내역은 볼 수 있으면 안 됨.
 - : 회원으로 관리하여, 각 회원마다 본인만의 정보만 볼 수 있게 하자.
 - : 본인의 구매내역을 확인할 수 있는 마이페이지를 만들자.
- 관리자가 관리할 수 있어야 함.
 - : 관리자 페이지를 만들자.

시스템 설계

기능 도출:

- 사람들이 웹에서 상품을 볼 수 있어야 함.
 - : 기본 페이지에서 상품 목록을 볼 수 있게 하자.
 - : 각 상품은 상품 명, 가격, 사진을 보여주어야 함.
- 상품을 구매할 수 있어야 함.
 - : 주문 페이지를 만들어야 함.
 - : 결제할 수 있는 기능을 넣자.
 - : 집주소 및 결제 정보 입력이 필요함.
- 다른 사람의 구매내역은 볼 수 있으면 안 됨.
 - : 회원으로 관리하여, 각 회원마다 본인만의 정보만 볼 수 있게 하자.
 - : 본인의 구매내역을 확인할 수 있는 마이페이지를 만들자.
- 관리자가 관리할 수 있어야 함.
 - : 관리자 페이지를 만들자.

기능 도출:

- 상품 표시 기능
- 상품 구매 기능(상품 정보 및 결제정보 입력)
- 외부 온라인 결제 API 연결 기능
- 회원 가입 기능
- 회원 정보 확인 기능, 변경 기능
- 구매기록 확인 기능
- 로그인 기능
- 관리자 권한 분리 기능
- 상품 구매기록
- 상품 업로드 기능

시스템 설계

기능 도출:

- 사람들이 웹에서 상품을 볼 수 있어야 함.
 - : 기본 페이지에서 상품 목록을 볼 수 있게 하자.
 - : 각 상품은 상품 명, 가격, 사진을 보여주어야 함.
- 상품을 구매할 수 있어야 함.
 - : 주문 페이지를 만들어야 함.
 - : 결제할 수 있는 기능을 넣자.
 - : 집주소 및 결제 정보 입력이 필요함.
- 다른 사람의 구매내역은 볼 수 있으면 안 됨.
 - : 회원으로 관리하여, 각 회원마다 본인만의 정보만 볼 수 있게 하자.
 - : 본인의 구매내역을 확인할 수 있는 마이페이지를 만들자.
- 관리자가 관리할 수 있어야 함.
 - : 관리자 페이지를 만들자.

기능 도출:

- 상품 표시 기능
- 상품 구매 기능(상품 정보 및 결제정보 입력)
- 외부 온라인 결제 API 연결 기능
- 회원 가입 기능
- 회원 정보 확인 기능, 변경 기능
- 구매기록 확인 기능
- 로그인 기능
- 관리자 권한 분리 기능
- 상품 구매기록 관리 기능
- 상품 업로드 기능

시스템 설계

웹 페이지 설계:

일반 사용자:

1. 로그인 / 회원가입 페이지
2. 상품 목록 페이지
3. 상품 구매 페이지
4. 마이 페이지

관리자:

1. 상품 등록 페이지
2. 구매내역 확인 페이지
3. 회원정보 확인 페이지

소프트웨어 개발 실습 - 실습

시스템 설계

데이터베이스 설계:

사용자 정보 (아이디, 비밀번호, 이름, 주소, 결제정보)

상품 정보 (아이디, 상품명, 카테고리, 가격, 이미지 주소)

구매내역 정보 (구매자 아이디, 구매 상품 아이디, 구매 시간, 결제완료 여부, 구매자 주소)

시스템 구현

<코드 참고>

상품 표시 기능

상품 구매 기능(상품 정보 및 결제정보 입력)

외부 온라인 결제 API 연결 기능

회원 가입 기능

회원 정보 확인 기능, 변경 기능

구매기록 확인 기능

로그인 기능

관리자 권한 분리 기능

상품 구매기록 관리 기능

상품 업로드 기능

체크리스트 작성 및 테스트

- 1) 기능 구현 여부 확인.
- 2) 정상작동 여부 확인.
- 3) 보안 요소 확인
 - 1) 각각의 기능에 대해서, 점검이 필요한 내역을 추리고,
 - 2) 점검이 필요한 내역에 대해서 조건을 만족하고 있는 지 확인.

체크리스트 작성 및 테스트

함수명	코드 영역	기능	구현 여부
streamlit_app.py (root)	streamlit_app.py 1~2, 137~138	프로그램 실행	o

		점검 필요 여부	만족 여부
입력데이터검증및표현	SQL injection	x	
	Code injection	x	
	Path traversal	x	
	XSS	x	
	Command Injection	x	
	File upload	x	
	CSRF	x	
	SSRF	x	
	HTTP	x	
	Integer Overflow	x	
	Format String Injection	x	
보안기능	암호화알고리즘	x	
	하드코딩	x	
	안전하지않은난수생성기	x	
	쿠키유효기간설정	x	
	무결성검증	x	
	반복된인증시도제한	x	
시간및상태	Race Condition	x	
	Recursive / infinite loop	x	
에러처리	오류메시지노출	x	
	오류상황처리	x	
코드오류	Nullpointer역참조	x	
	Filedescriptor	x	
	신뢰할수없는역직렬화	x	
API 오용	DNS Lookup에 의존한 보안 결정	x	
	취약한API 사용	o	x

유지 보수

사용해보며, 부족한 기능, 잘못된 보안 기능 등이 존재하면 확인 후 적절한 단계로 돌아가서 다시 수행.

마무리

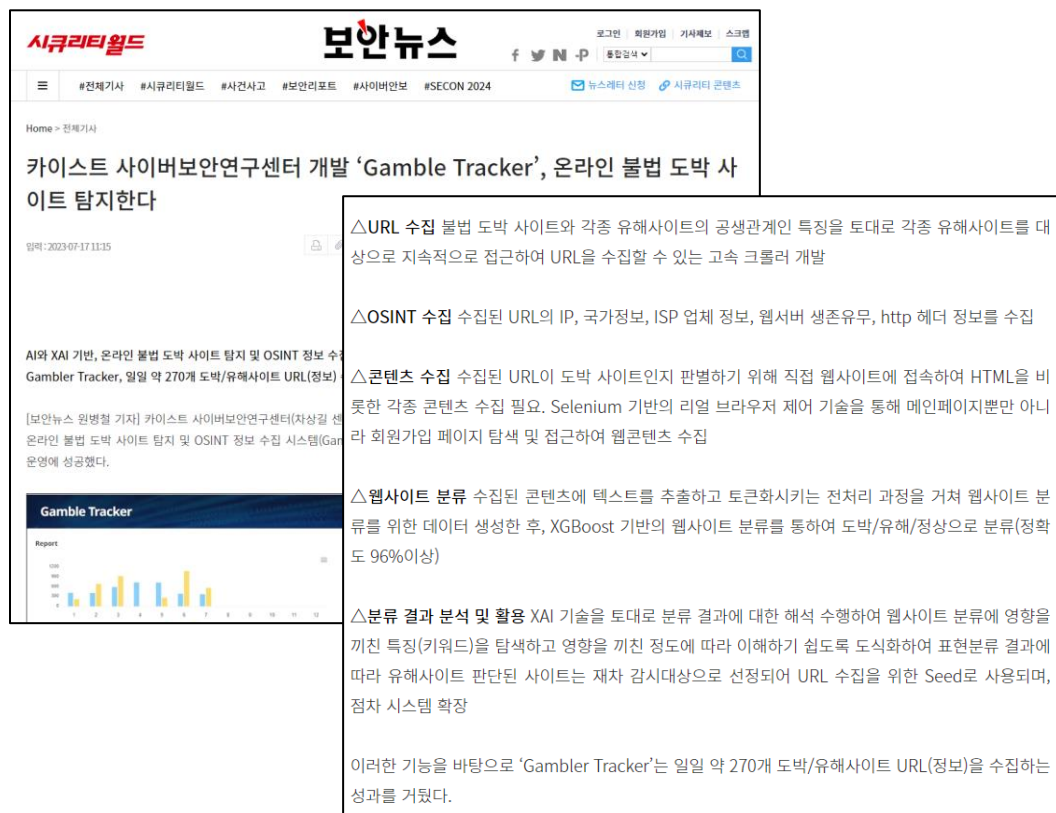
과제

- Simple Shopping Mall Website
 - 쇼핑몰 사이트의 요구사항을 만족하도록 구현되지 않은 부분을 완성
 - 쇼핑몰 사이트의 개발 전 과정(요구사항 분석, 설계, 구현, 체크리스트 작성 및 테스트, 유지보수 과정)에 대한 보고서 작성
 - 개발 과정에서 확인한 보안 약점들이 무엇이고, 어떻게 변경하였는지 작성
 - 완성한 프로그램은 github에 public으로 올리고, README.md에 환경 설정 및 실행방법 명시
 - 본 강의에서 언급한 최소 기능(24page)를 모두 구현한다면, 이외 어떤 기능이든 추가 가능하며, 다른 모든 것이 자유.
 - 단, 최대한 보안 약점이 없도록 할 것.
- 제출 기한: 2024년 4월 28일(일) 23:59:59
- 제출 내용: 보고서(개발 전 과정에 대한 설명이 포함된 보고서), github 링크
- 제출: LMS에 제출
- 질문: Discord DM(이름 유효곤, 혹은 ugonfor일 수 있음.)

마무리

그외, 프로젝트 설명

1. 악성 웹사이트 모니터링



시큐리티월드 **보안뉴스** 로그인 회원가입 기사제보 스크랩

#현재기사 #시큐리티월드 #사건사고 #보안리포트 #사이버보안 #SECON 2024 뉴스레터 신청 시큐리티 콘텐츠

Home > 전체기사

카이스트 사이버보안연구센터 개발 'Gamble Tracker', 온라인 불법 도박 사이트 탐지한다

입력: 2023-07-17 11:15

△URL 수집 불법 도박 사이트와 각종 유해사이트의 공생관계인 특징을 토대로 각종 유해사이트를 대상으로 지속적으로 접근하여 URL을 수집할 수 있는 고속 크롤러 개발

△OSINT 수집 수집된 URL의 IP, 국가정보, ISP 업체 정보, 웹서버 생존유무, http 헤더 정보를 수집

△콘텐츠 수집 수집된 URL이 도박 사이트인지 판별하기 위해 직접 웹사이트에 접속하여 HTML을 비롯한 각종 콘텐츠 수집 필요. Selenium 기반의 리얼 브라우저 제어 기술을 통해 메인페이지뿐만 아니라 회원가입 페이지 탐색 및 접근하여 웹콘텐츠 수집

△웹사이트 분류 수집된 콘텐츠에 텍스트를 추출하고 토큰화시키는 전처리 과정을 거쳐 웹사이트 분류를 위한 데이터 생성한 후, XGBoost 기반의 웹사이트 분류를 통하여 도박/유해/정상으로 분류(정확도 96%이상)

△분류 결과 분석 및 활용 XAI 기술을 토대로 분류 결과에 대한 해석 수행하여 웹사이트 분류에 영향을 끼친 특징(키워드)을 탐색하고 영향을 끼친 정도에 따라 이해하기 쉽도록 도식화하여 표현분류 결과에 따라 유해사이트 판단된 사이트는 재차 감시대상으로 선정되어 URL 수집을 위한 Seed로 사용되며, 점차 시스템 확장

이러한 기능을 바탕으로 'Gamble Tracker'는 일일 약 270개 도박/유해사이트 URL(정보)을 수집하는 성과를 거뒀다.

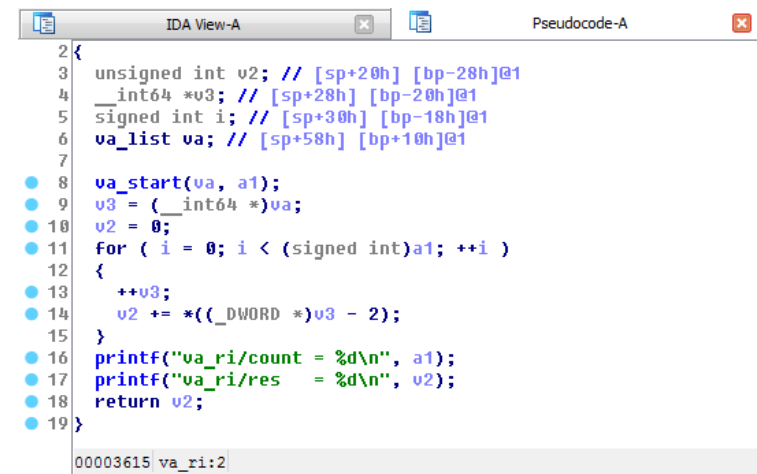
AI와 XAI 기반, 온라인 불법 도박 사이트 탐지 및 OSINT 정보 수집 Gambler Tracker, 일일 약 270개 도박/유해사이트 URL(정보)

[보안뉴스 원병철 기자] 카이스트 사이버보안연구센터(차상길 센터장)는 온라인 불법 도박 사이트 탐지 및 OSINT 정보 수집 시스템(Gamble Tracker)을 개발하여 성공했다.

Gamble Tracker

Report

2. Tiny-C Compiler



```
2 {
3   unsigned int v2; // [sp+20h] [bp-28h]@1
4   __int64 *v3; // [sp+28h] [bp-20h]@1
5   signed int i; // [sp+30h] [bp-18h]@1
6   va_list va; // [sp+58h] [bp+10h]@1
7
8   va_start(va, a1);
9   v3 = (__int64 *)va;
10  v2 = 0;
11  for ( i = 0; i < (signed int)a1; ++i )
12  {
13    ++v3;
14    v2 += *((_DWORD *)v3 - 2);
15  }
16  printf("va_ri/count = %d\n", a1);
17  printf("va_ri/res = %d\n", v2);
18  return v2;
19 }
```

00003615 va_ri:2

마무리

그외, 프로젝트 설명

그 외에도, 멘티 제안 프로젝트를 하고 싶으시다면 아래와 같은 주제에 대해서는 조언을 드릴 수 있습니다.

1. AI 관련,
2. 리버스 엔지니어링, 악성코드
3. 컴퓨터 시스템,
4. 네트워크 관련,
5. 안드로이드 어플리케이션

(위 내용에 한정되지는 않음.)

다음과 같은 내용은 다른 더 우수한 멘토분들께서 더 잘 조언을 주실 것 같습니다.

1. 정책
2. 컨설팅
3. IoT 펌웨어 분석
4. 하드웨어 포렌식
5. 클라우드