

프로젝트 수행계획서

노래하는 하리보팀



K-Shield Jr.

최종 작성일 : 2024년 6월 5일

< 변경 기록표 >

버전	변경일자	변경 내용	변경자
0.1.0	24.06.03.	최초 작성	박현규
0.1.1	24.06.05	수행계획서 작성 완료	김서현

목 차

제 1 장 프로젝트 개요	4
프로젝트 명 및 기간	4
프로젝트 배경	4
관련 사례 및 의의	4
프로젝트 목표	5
프로젝트 범위	5
제 2 장 프로젝트 조직	6
프로젝트 조직도	6
책임 및 역할	6
프로젝트 환경	6
제 3 장 프로젝트 수행 일정	7
프로젝트 추진 일정	7
단계별 세부 일정	7

제 1 장 프로젝트 개요

프로젝트 명 및 기간

- ▷ 프로젝트 명: 웹 취약점 분석 연습 플랫폼 구축
- ▷ 프로젝트 기간: 2020.06.03. ~ 2020.07.05 (5주)

프로젝트 배경

인터넷과 웹 애플리케이션의 급속한 확산으로 인해 비즈니스와 개인 생활에서 웹 기술의 중요성이 높아지고 있다. 이러한 확산은 편리함을 제공하는 동시에 다양한 보안 위협에 노출되는 문제를 야기하고 있다. 최근 몇 년 동안 웹 애플리케이션은 해커들의 주요 공격 대상이 되었으며, 이는 데이터 유출, 금전적 손실, 회사 평판 손상 등 심각한 피해를 초래하고 있다.

보안 솔루션 회사 'Barracuda'의 2024년 2월 보안 보고서¹에 따르면, 2023년에 웹 애플리케이션 공격 시도는 약 180억 번 이루어졌으며, 그 중 SQL Injection, XSS(Cross-Site Scripting), CSRF(Cross-Site Request Forgery) 등의 취약점이 가장 많이 악용되고 있다. 또한, 2022년에는 글로벌 기업 중 60% 이상이 웹 취약점을 통해 데이터 유출 피해를 입었다는 통계도 있다. 이러한 피해는 단순한 금전적 손실을 넘어 기업의 신뢰도와 평판에까지 악영향을 미치고 있다.

이와 같은 상황에서 웹 보안 전문가에 대한 수요는 지속적으로 증가하고 있지만, 숙련된 인력은 여전히 부족한 실정이다. 웹 보안 전문가 양성을 위한 교육 프로그램과 훈련 플랫폼이 절실히 요구되는 이유다. 실제로 많은 기업들이 웹 보안 인력을 채용하는 데 어려움을 겪고 있으며, 이는 곧 웹 애플리케이션 보안 수준의 저하로 이어질 수 있다.

따라서, 본 프로젝트는 웹 보안에 대한 체계적이고 실질적인 교육을 제공하기 위해 온라인 훈련 플랫폼을 개발하는 것을 목표로 한다. 이 플랫폼은 사용자가 실제 웹 애플리케이션에서 발생할 수 있는 취약점들의 코드를 진단하고 대응할 수 있는 시큐어코딩 능력을 배양하도록 설계될 것이다. 이를 통해 웹 보안 인력의 부족 문제를 해결하고, 기업과 개인의 웹 애플리케이션 보안을 강화하는 데 기여하고자 한다.

관련 사례 및 의의

현재 많은 기업들이 웹 보안 훈련 프로그램과 모의 해킹(펜테스팅) 도구를 도입하여 직원들의 보안 역량을 강화하고 있다. 이러한 훈련 프로그램은 실제 공격 시나리오를 기반으로 하여 실습을 통해 취약점을 진단하고 대응하는 능력을 배양할 수 있게 도와준다. 대표적인 예로, HackerOne과 같은 플랫폼이 있다. HackerOne은 전 세계 보안 연구원들과 협력하여 기업의 보안 취약점을 찾아내고 이를 해결하도록 돕는 플랫폼으로, 실제로 많은 기업들이 이 플랫폼을 통해 보안 수준을 크게 향상시키고 있다.

이와 같은 사례들은 웹 취약점 분석과 대응 훈련의 중요성을 강조하며, 본 프로젝트가 제안하는 온라인 훈련 플랫폼 개발의 필요성을 뒷받침한다. 그러나 이러한 플랫폼들은 주로 해외에서 개발되고 제공되기 때문에 한국 사용자들에게는 언어적인 장벽과 높은 가격 부담이 존재한다.

따라서, 우리 프로젝트는 가격 부담 없이 한국어로 지원되는 웹 취약점 분석 연습 플랫폼을 제공하여 이러한 문제를 해결하고자 한다. 이 플랫폼은 한국어로 제공되기 때문에 사용자들이 언어의 장벽 없이 편리하게 이용할 수 있으며, 무료 또는 저렴한 비용으로 제공되어 더 많은 사람들이 접근할 수 있게 할 예정이다. 이를 통해 한국의 웹 보안 전문가 양성에 기여하고, 국내 웹 애플리케이션의 보안 수준을 향상시키는 데 중점을 두고 있다.

¹ 출처:

<https://blog.barracuda.com/2024/02/07/threat-spotlight-attackers-targeting-web-applications-right-now>

프로젝트 목표

- Django 및 Python 웹 개발 학습
- OpenAI API 사용법 학습
- 웹 해킹 취약점 훈련 문제 선별 및 취약점 포함 웹페이지 구현
- 취약점에 대한 시큐어코딩 방법 및 관련 CVE 조회를 위한 프롬프트 추가

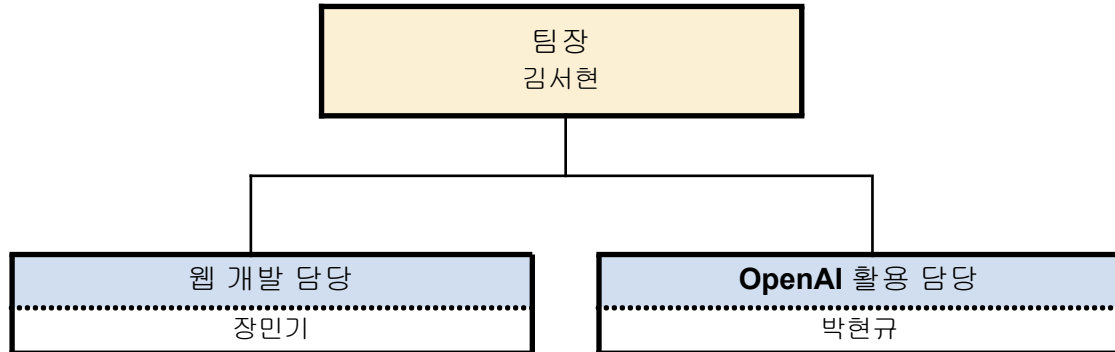
프로젝트 범위

주요 기능	사용 기술
취약점 분석 훈련장을 위한 웹페이지 작성	Django OpenAI GitHub Action
OpenAI API 활용 시큐어코딩 프롬프트 작성 및 기능 구현	

[표 1-1] 프로젝트 범위

제 2 장 프로젝트 조직

프로젝트 조직도



<그림 2-1> 프로젝트 조직도

책임 및 역할

책임	역할	담당자명
팀장	- 프로젝트 총괄 책임 - 웹 페이지 기능 통합 및 테스트를 통한 보완	김서현
웹 개발 담당	취약점 분석 플랫폼을 위한 웹 페이지 구현 담당	장민기
OpenAI 활용 담당	OpenAI API 활용 프롬프트 작성 및 구현	박현규

[표 2-1] 책임 및 역할

프로젝트 환경

웹 개발	구분	항목
	개발 언어	Python
	프레임워크	Django

[표 2-3] 웹 개발 환경

협업	구분	사용 목적
	카카오톡	회의 진행 및 소통
	Google Drive	관련 문서 및 산출물 관리
	GitHub	웹 구현 코드 공유 및 병합

[표 2-4] 협업 환경

제 3 장 프로젝트 수행 일정

프로젝트 추진 일정

프로젝트 일정		2020.06.03.~2020.07.05 (5주)																			
단계		1주					2주					3주					4주				
분석	요구사항 분석																				
설계	시스템 설계																				
	DB 설계																				
	웹 페이지 설계																				
	코드 설계																				
구현	와이어프레임 제작																				
	openai api 기능 구현																				
	웹 페이지 구현																				
	기능 병합 및 추가 구현																				
테스트	테스트 및 문제점 보완																				
완료	프로젝트 보고 및 종료																				

[표 4-1] 프로젝트 추진 일정

단계별 세부 일정

일정	단계	작업
2024.06.03 ~ 2024.06.07	요구사항 분석	- 요구사항 분석 및 정의 - 프로젝트 주제 및 범위 확정 - 프로젝트 일정 확정 - 프로젝트 진행 방향 확정
2024.06.10 ~ 2024.06.14	프로젝트 설계	- 기능 설계 및 와이어프레임 작성 - 개발환경 구축 및 반영 - 웹 페이지 개발 업무 분배 - OpenAI 개발 업무 분배
2024.06.17 ~ 2024.06.21	프로젝트 구현	- OpenAI 기능 구현 및 웹 페이지에 적용 - 웹 페이지 구현 및 취약점 반영
2024.06.24 ~ 2024.06.28	테스트	- 기능 단위 테스트 진행 - 보완 사항에 대한 추가 구현 진행
2024.07.01 ~ 2024.07.05	완료	- 프로젝트 완료 및 검수

[표 4-2] 단계별 세부 일정