

K-Shield Jr.11기 단기_1조

수행계획서



K-Shield Jr.

목 차

1. 수행 일정

2. 절차

3. 수행 배경 및 목적

4. 각 수행원의 담당 업무

1. 수행 일정

10월 25일	보고서 작성 및 수행계획서작성
10월 25일 ~ 26일	프로젝트 자료 조사 및 체크리스트 자료
10월 26일~ 30일	취약점 분석 및 위협 정의, 위협 개선
10월 31일	최종 결과 보고서 작성

1.1)WBS

구분	주요 Task		산출물	10. 25	10. 26	10. 27	10. 28	10. 29
	대분류	소분류						
착수	프로젝트 수행 계획서 수립	프로젝트 수행 계획서 작성	프로젝트 수행 계획서, WBS					
	자료 조사	프로젝트 자료 조사						
구축	체크리스트 작성	인젝션	체크리스트 자료					
		취약한 인증						
		민감한 데이터 노출						
		취약한 접근 통제						
		크로스 사이트 스크립팅						
		잘못된 보안 구성						
		알려진 취약점이 있는 구성요소 사용						
	위협분석	취약점 분석, 위협 정의	취약점					
		위협 정의	위협 정의 보고서					
		위협 개선	위협 개선 보고서					
	위협 조치 방안	위협 조치 방안에 대한 세부 수행절차 제시	위협 조치 계획서					
종료	최종 결과 보고	최종 결과 보고서 작성	최종 결과 보고서					
		최종 결과 발표 자료 작성	최종 결과 발표 자료					
		영역별 수행 결과 보고서 작성	최종 결과 발표 자료					

2. 절차

절차	설명
정보수집단계	점검할 대상에 대해 어떤 서비스인지, 외부에서 파악할 수 있는 정보들을 수집하는 단계
취약점 수집	Burp suite를 사용하여 취약점에 대한 정보를 수집하는 단계
침투 단계	취약점 수집 단계를 통해 획득한 정보를 기반으로 수동점검(Maual)을 통해 내부 시스템까지 침투할 가능성이 있는지 시나리오 기반으로 접근하는 단계
상세 분석	취약점이 발견되었을 경우에 공격에 의해서 보안 위협이 시스템 및 사용자 측면에서 어느정도 영향을 줄 수 있는지 분석하는 단계
보고서 작성	발견된 취약점에 대한 총평 및 상세분석이 포함된 보고서를 작성하는 단계

3. 수행배경 및 목적

3.1) 수행배경

- * 외부 관점 시나리오로 취약점 분석 수행
- * 웹 서비스 공격

3.2) 목적

- * 웹 취약점 진단
 - a. 체크리스트 및 최신 동향을 반영한 취약점 반응을 확인
 - b. 홈페이지의 각 항목별 점검방법(문자열)을 적용하여 반응을 확인 => 동적분석
 - c. 식별된 취약점을 이용한 위험성 확인
 - d. 위험성 확인 후 위험성 개선방안 분석
- * 식별된 취약점을 이용한 위험성 확인
 - a. 확인된 취약한 반응을 응용하여 DB정보를 알아낼 수 있는지 확인

b. DB정보를 이용하여 관리자페이지 접근이 가능한지 확인

* 식별된 위험성에 대한 개선방안

a. 웹 페이지 취약점한 반응이 일어나는 위치의 코드를 분석

b. 취약점이 나타나지 않도록 코드 변경

4. 각 수행원의 담당 업무

이름	담당 업무
장예지	보고서 작성, 취약점 진단 및 개선방안
이송추	보고서 작성 및 취약점 진단
곽민지	취약점 진단 및 개선방안
김성재	보고서작성, 취약점 진단 및 개선방안
진준영	취약점 진단
정찬형	취약점 진단 및 발표