S/W 개발 보안의 필요성과 기대효과

신성윤*, 김도관**, 이현창**, 박기홍*

*군산대학교 컴퓨터정보통신공학부

**원광대학교 정보전자상거래학부

Identification of Vehicle Using Edge Detection

S-Y Shin*, D-K Kim**, C-W Lee*, H-C Lee**, T-W Lee***, K-H Park*

*School of Comp. Info. & Comm. Eng., Kunsan National University

**School of Info. & Elec. Comm., Wonkwang University

E-mail : {s3397220, spacepark}@kunsan.ac.kr, {kimdg, hclglory}wku.ac.kr

요 약

시큐어 코딩이란 개발 단계에서 해킹 등의 공격을 유발할 가능성이 있는 잠재적인 보안 취약점을 미리에 제거하여, 외부 공격으로부터 안전한 소프트웨어를 개발하는 기법을 말한다. 본 논문에서는 이러한 소프트웨어 개발 보안의 필요성 및 기대효과에 대하여 알아보도록 한다. 이로 인하여, 안전한 소프트웨어 개발을 위해 위협에 대비하고 프로젝트 품질 향상에 효과가 있다.

ABSTRACT

Secure Coding is in the development phase, removing a potential security vulnerability that could lead to attacks such as hacking in advance, says the technique to develop secure software from external attacks. In this paper, we'll learn about the needs and expectations of the effectiveness of these security software development. Due to this, the threat to the safe software development project, and there is an effect to improve quality.

키워드

잠재적인 보안 취약점(potential security vulnerability), 해킹(hacking)

Ⅰ. 서 론

소프트웨어 개발 보안 또는 시큐어 코딩(Secure Coding)이란 안전한 소프트웨어 개발을 위해 소스 코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 일련의 보안 활동을 말한다[1].

S/W 설계단계에서 제품 출시까지의 보안 취약점 등 결함을 없애는 시점에서 비용을 분석한 결과로서 설계부터 제품출시 등 각 단계에서 보안 취약점 제거 비용이 크게는 서른 배까지 차이가 날수 있으며, 이를 위해서 반드시 결함을 수정해야 한다.

Ⅱ. 필요성

그동안 발생했던 다수의 보안 사고를 살펴보면, 이들 대부분인 응용 소프트웨어에서 발생하였으며 이를 개선할 필요가 있는 것으로 나타났다.

또한 안전행정부의 소프트웨어 개발 단계부터 보안 약점 제거의 의무화를 들 수 있다. 2012년 12월부터 행정기관 등에서 추진하는 사업 중 연구 개발비가 40억 이상인 정보화 사업에 시쿠어 코딩 적용을 의무화하고 단계별로 2015년에는 감리대상 정보화 사업에 시큐어 코딩을 적용하였다.

안전행정부는 소스 코드의 분석을 통하여 매우 다양한 어플리케이션에 대한 초기 개발 단계부터의 조기 보안 약점의 탐지 및 조치를 위한 소프

(안전행정부고시 제2013-36호)

유형	내용
입력데이터 검증 및 표현	• 15개 (SQL 삽입, 경로 조작 및 자원 삽입 등)
보안기능	• 16개 (적절한 인증 없는 중요 기능 허용, 부적절한 인가 등)
시간 및 상태	• 2건 (경쟁조건, 종료되지 않는 반복문 또는 재귀함수)
에러처리	• 3개 (오류 메시지 통한 정보 노출, 오류상황 대응 부재 등)
코드오류	• 4개 (널(Null)포인터 역참조, 부적절한 자원 해제 등)
캡슐화	• 5개 (잘못된 세션에 의한 데이터 정보 노출 등)
API 오용	• 2개 (DNS lookup에 의존한 보안결정, 취약한 API 사용)

01_컨설팅팀 Template____PT_02_본문.png

대상 언어
- JAVA, C, 안드로이드

조건
- 47개 보안 약점 제거해야 함

그림 1. S/W 보안 약점

트웨어 개발 보안을 점차적으로 의무화 적용하여 왔다. 그림 1은 소프트웨어 보안 약점의 예이다.

III. 기대효과

시큐어 코딩 솔루션을 도입하여 안전한 소프트웨어의 개발을 위하여 소스코드 등에 방치되었거나 존재할 수 있는 잠재적인 보안 약점을 없애서 사이버 테너의 위험에 대비하고 프로젝트 품질 향상에 효과를 가져 올 수 있다. 우리는 크게 4가지로 기대효과를 분석할 수 있다.

첫째, 사이버 테러 위협 대비이다. 소프트웨어 개발 단계부터 소스코드를 관리하여 소프트웨어를 위변조 하는 보안 약점을 최소하 한다. 안전한 소프트웨어 개발 및 보안전략 수립으로 날로 증가하고 있는 보안 사고를 대처라며 원초적으로 막을 수 있다.

둘째, 시큐어 코딩 의무화에 완벽한 대응이다. 행정안전부 고사에 따라 정보시스템 구축 운영 지침에 따라 총 47개 항복에 대한 소프트웨어 보안약점 기준과 개발보안 적용 의무화의 단계적 추진을 들 수 있다.

셋째, 방대한 비용 절감이다. 소프트웨어 개발 단계에 보안 약점에 대한 진단으로 에러 검출 및 수정에 드는 비용을 절감할 수 있다. 또한 보안 약점도 거의 반을 줄여 기업의 이미지를 되살리고 사고에 따른 후속조치에 따른 비용도 절감할 수 있다.

넷째, 프로젝트 품질의 향상에 기여한다는 것이다. 보안 코딩 점검하는 습관의 마련으로 프로젝트 품질 향상에 어느 정도 기여할 수 있다.

IV. 결 론

소프트웨어 개발 보안의 필요성 및 기대효과에 대하여 알아보았다. 안전한 소프트웨어 개발을 위해 위협에 대비하고 프로젝트 품질 향상에 효과가 있는 것으로 나타났다. 다수의 보안 사고를 살펴보면, 이들 대부분인 응용 소프트웨어에서 발생하였으며 이를 개선할 필요가 있는 것으로 나타났다.

시큐어 코딩 솔루션을 도입하여 안전한 소프트웨어의 개발을 위하여 소스코드 등에 방치되었거나 존재할 수 있는 잠재적인 보안 약점을 없애서 사이버 테너의 위험에 대비하고 프로젝트 품질 향상에 효과를 가져 왔다.

우리는 크게 4가지로 기대효과를 분석할 수 있다. 사이버 테러 위협 대비, 시큐어 코딩 의무화에 완벽한 대응, 방대한 비용 절감, 프로젝트 품질의 향상에 기여의 4 가지이다.

참고문헌

[1] https://ko.wikipedia.org/wiki/소프트웨어_개발_보안