웹(WEB)애플리케이션 보안관리 통합플랫폼 개발 연구

김기환[O], 이동일**,이현빈*** 신용태***
[O*]한국전자통신연구원
[**](주)코드원
[***]숭실대학교 컴퓨터공학과
e-mail: itconsult@hanmail.net[O], {jason, hyunbin23}@code1.co.kr[**], shin@ssu.ac.kr[***]

Web application security management integrated platform development study

Kihwan Kim[O], Dongil Lee[**], Hyunbin Lee[***],Yongtae Shin[***]
[O*]ETRI
[**]Codeone Corp
[***]Dept. of Computer Science, Sungsil University

● 요 약 ●

본 논문에서는 사이버공격의 주요 대상인 웹 애플리케이션의 보안을 위하여 취약점진단 및 제거, 이행점검의 웹 통합보안관리 플랫폼을 제안한다. 이 플랫폼은 동적진단엔진, 취약점제거보안모듈, UI를 제공하는 통합관리시스템, 진단 결과를 저장하는 결과 및 통계 DB, 와 진단을 위한 관련 정보를 저장하는 진단 및 보안정보 DB로 구성되며, 동적진단결과에 대한 상관관계분석 기능과 취약점 개선 활동 시 스마트 보안모듈을 통해 빠르고 손쉬운 취약점 제거수정, 완화할 수 있는 통합플랫폼 연구를 통하여 웹 애플리케이션보안을 효율적으로 할 수 있다.

키워드: 웹보안(Web Security), 통합플랫폼(Integrated Platform), 동적진단(Dynamic diagnosis)

I. Introduction

국정원에서 발표한 2016년 국가정보보호백서에 따르면 2016년 취약점 분석 시스템의 시장 규모는 496억 정도의 규모를 형성한 것으로 조사되며, 해마다 40%이상의 증가율을 보이고 있으며,나날이 증가하고 있는 사이버 위협에 대응하기 위해 사전에 위험요소를 발견 및 식별을 위하여 필수적으로 사용하는 시스템(SYSTEM)이 취약점 분석 시스템이다.

취약점 분석 시스템의 종류는 다양하지만, 현재 시장에서 가장 많은 고객이 사용하고 있으며, 가장 많이 접해본 시스템은 단연 웹 취약점 분석 시스템이다. 이러한 이유는 웹사이트는 서비스 특성상 대부분 누구나 자유로이 접근이 가능하도록 설계되어 있기 때문에 보안에 취약하여 사이버 공격 대상의 80% 이상을 차지하고 있기 때문이다.

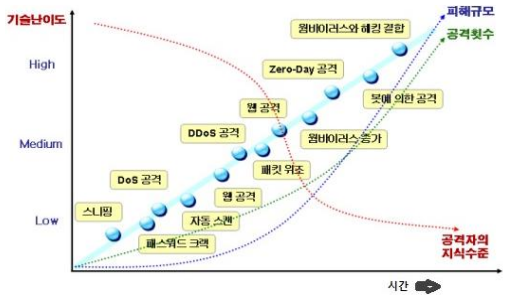

Fig. 1. web site attack specific dimension

이러한 이유로 행정안전부는 사이버 공격의 주요 원인인 소프트웨어 보안 취약점을 개발단계에서 제거하기 위하여 2014년 7월부터 감리대상 전 정보화 사업에 소프트웨어 개발 보안을 의무적으로 적용하고 있으며, 이러한 분위기는 공공기관 및 금융계를 시작으로 전 산업계로 확산되어 가고 있는 상황이다.

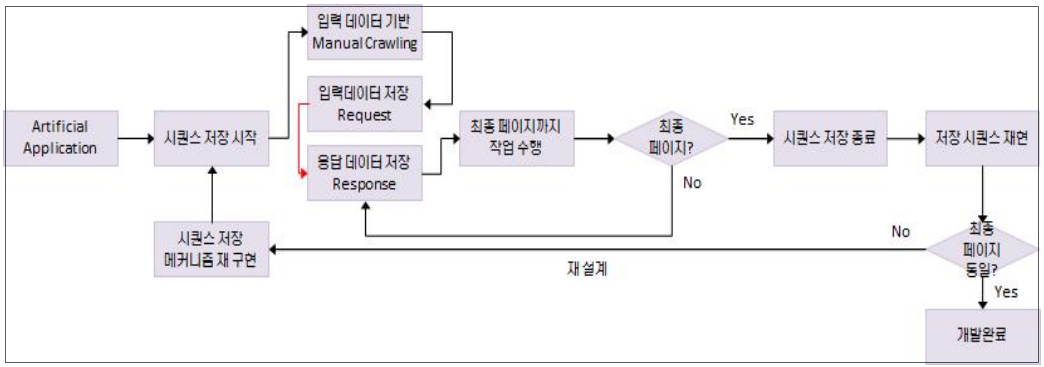

Fig. 3. login sequence record and multi step operation record function

II. Web Application Integrated Security Management

1. 기존 기술의 문제점

기존 웹 취약점진단 시스템들은 대부분 취약점을 발견하고 보여주는 화면만 제공하는 형태여서 발견된 취약점의 사후관리가 어려우며 배포된 취약점에 대한 관리 및 모니터링 기능이 없으므로 취약점의 조치 여부와 웹(Web) 애플리케이션의 보안 취약성의 관리가 어렵다. 또한 취약점 제거 시 전체 코딩부문을 수정해야 하므로 시간 및 경비 소요가 많으며 지속적인 통합관리가 안 되고 있는 실정이다.

2. 새로운 웹 보안 기술의 필요성

현재 웹 취약점진단, 웹 취약점 제거, 웹 이행 점검 및 관리의 웹 보안 통합관리 기술은 없으며, 단순 취약점 진단 도구 제품이 외산제품과 국산제품이 있는 관계로 순수 기술로 국내시장 뿐 아니라 세계시장을 대상으로 기술을 개발하며 사용자가 쉽게 사용하며 웹 보안을 통합하여 대처할 수 있는 제품 신뢰성을 확보한 웹 보안 통합관리 기술이 필요하다.

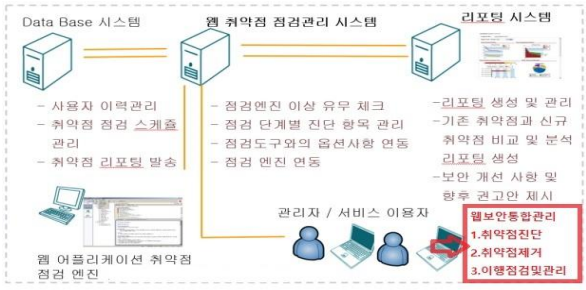

Fig. 2. Technical Overview

Fig 2.에서 나오는 것처럼 관리자 및 서비스 이용자는 한 대의 pc에서 웹 보안 통합관리가 가능해야하며 그 안의 기능으로는 취약점 진단과 제거 이행점건 및 관리 기술이 필요하다.

동적 진단 기술에서 필수 항목은 탐색 및 진단 커버리지를 높이기 위한 중요 기능으로 복잡한 로그인 시퀀스 기록 및 멀티스텝 오퍼레이션 기능을 구현, 동적 진단결과에 대한 상관관계분석 기능의 제공을 위한 동적진단결과 분류기능 구현, 발견 취약점에 대한 손쉬운 수정 적용을 지원하며 취약점 개선 활동 시 보안 기능과 비즈니스 로직을 구분하는 스마트 보안 모듈의 적용이 필요하다.

III. Conclusions

웹 애플리케이션의 보안을 위하여 통합적인 관리 기술을 제안한다.

웹 보안 통합관리 기술은 웹 애플리케이션의 보안 취약점을 진단하기 위해서 필요한 동적진단을 통한 분석 및 제거관리를 지원하는 기술로 다양한 개발환경과 언어에서 만들어지는 다양한 웹 애플리케이션에 대한 동적진단 및 취약점제거를 제공하고 스마트산업화 사회를 이끌어가는 웹 애플리케이션 개발 및 운영으로 진행되는 산업현장에서 지속적으로 사용할 수 있도록 기술적 선도 능력과 확장성과 범용성을 제공하는 기술이다.

REFERENCES

[1] "A Study on Malicious Code Hiding Web Site Detection Using WhiteList-Based Malicious Code Behavior Analysis".2011

[2] "A Study on Detection of Malicious Code Diffusion Site", Korea Information Processing Society, 2008.11

[3] “Vulnerability Detection and Mitigation of Web Application based on SW Security Testing”, 2012.2

[4] “(A) Remote System to Diagnose Security Vulnerabilityes of Systems on Based Web,” 2000