한국항행학회 논문지 제15권 제3호 2011년 6월

OWASP 및 WASC 중심의 웹 애플리케이션 보안에 관한 고찰

Study on the OWASP and WASC-oriented Web Application Security

이재현*

Jae-Hyun Lee*

요 약

지금까지의 웹 애플리케이션의 보안 취약성 분석과 관련하여 현재 국외에서 진행되고 있는 각종 프로젝트들에 대한 조사와 국내 연구 자료가 미비한 실정이다. 이는 국내 웹 서비스의 질적 향상 및 향후 발전된 서비스의 제안을 위한 선행 연구의 부족이 주요 원인이라 할 수 있다. 본 논문에서는 현재까지 발표되어 악용되어온 웹 애플리케이션의 취약성 유형들을 체계있게 살펴보고 향후 방안에 대해 살펴보고자 한다.

Abstract

Until now, the study and research on the projects which have internationally conducted are in poor condition with regard to the security vulnerability analysis of web application. This is due to a lack of precedent study for improving the quality of the web services in order to provide better services for the future. In this paper, I analyze the types of the web application vulnerabilities which have been studied and mapped out a plan for protecting them.

Key words : Web Application, Security, OWASP, WASC

I. 서 론

그 동안의 해킹 기법들은 운영체제나 프로토콜 설계상의 버그나 개발자들의 본래 의도와는 다르게 보안상 심각한 결과가 초래될 수 있는 취약성을 이용한 기법들이 대부분이었다.

전문 해커들에 의해 해킹 코드가 발표될 때까지는 해킹 지식이 적은 스크립트 키디들에 의해 무분별하게 악용될 가능성은 적었지만 일단 발표가 되고나면 쉽게 악용되어 취약한 시스템은 운영하는 기업이나 기관에 많은 악영향을 미친다. 그러나 이러한 취약성들은 패치를 적용하고 구성설정을 변경하거나 외부로부터의 접근을 적절히 통제할 수 있는 보안 솔루션들(예: 라우터, 방화벽 등)에 의해 비교적 쉽게 해결이 가능했다.

현재 대부분의 기관이나 기업들은 시스템의 패치나 구성설정이 미흡하더라도 접근 통제 솔루션을 적어도 하나이상 갖추고 있어 외부로부터 유입되는 부적절한 접근으로부터 내부의 시스템을 보호할 수 있는 장치를 마련하고 있다. 그러나 이러한 솔루션이 갖추어져 있다 하더라도 반드시 서비스해야하는 것이 바로 웹 서비스이다.

* 강릉원주대학교 과학기술대학(College of Science and Technology)
· 제1저자 (First Author) : 이재현
· 투고일자 : 2011년 4월 27일
· 심사(수정)일자 : 2011년 4월 28일 (수정일자 : 2011년 6월 23일)
· 게재일자 : 2011년 6월 30일

접근 통제 솔루션은 웹 서비스로 접근하는 패킷을 통제하지 않고 내부로 유입시키기 때문에 만약 통과되는 패킷에 악의적으로 패킷을 조작해서 보낸다면 정상 패킷으로 간주하여 적절한 통제를 하지 못하게 되었다. 이는 과거 웹 서비스의 보안 취약성 분석과 관련하여 국외에서 진행되고 있는 각종 프로젝트들에 대한 조사와 국내 연구 자료가 미비한 것이 그 주요 원인이며 또한, 국내 웹 서비스의 질적 향상 및 향후 발전된 서비스의 제안을 위한 선행 연구의 부족이 주요 원인이다.

결론적으로 현재까지 발표되어 악용되어온 웹 애플리케이션의 취약성 유형들을 체계 있게 살펴보고 이를 예방할 수 있는 방안을 모색할 필요가 절실하다.

또한 이들에 대한 동향과 새로운 방안 제시는 향후 웹 취약점을 노출에 적극 예방과 대응에 기초 자료로서 충분한 가치가 있을 것으로 사료된다.

국내의 경우 주로 OWASP top 10 [1]에서 제시하고 있는 취약점들을 근거로 하여 이들에 대응할 수 있는 새로운 기법들을 제안하고 있다. 특히 OWASP Top 10 취약점을 바탕으로 공격패턴을 분석, 실시간 공격탐지 및 차단이 가능한 시스템을 설계 [2]한다거나 웹 해킹에 대한 탐지 능력 향상을 위해 기존 통합보안관리시스템에 OWASP Top 10에서 제시한 웹 응용 공격탐지기능을 추가한 모델을 제안 [3]하고 있는 실정이다.

국외의 경우 OWASP Top 10에서 제시하고 있는 보안 취약점들에 대한 분류 기준을 근거로 특정 웹서비스에 응용될 수 있는 새로운 방법론을 제시 [4,5,6]하거나 취약점을 감지하는 새로운 분석 기법을 제시하는 경향이 두드러졌으며 한편으로 OWASP 에서 제시한 각종 보안 가이드라인에 대해 이를 개발자나 학생들을 위한 교육 교재 활용을 제안한 논문 [7]도 있었다.

그러나 이러한 기법들은 모두 전체 웹 서비스 취약점 가운데 극히 일부분을 다룬 것으로 전반적인 관점에서 최근의 동향을 바탕으로 이를 분석하고 이에 따른 향후 발전방향을 제시하지는 못하고 있는 실정이다.

OWASP(Open Web Application Security Project) [8]와 WASC(Web Application Security Consortium) [9]는 모두 웹 애플리케이션 보안에 비전을 갖고 있는 기업과 개인들이 자발적으로 참여하고 있는 오픈 프로젝트로 웹 애플리케이션 취약점에 대한 방대한 연구와 그 결과를 제공하는 세계적으로 권위 있는 오픈 프로젝트이다. 앞서 언급한 OWASP Top 10 또한 OWASP에서 수행하고 있는 여러 프로젝트 가운데 하나에 지나지 않는다.

본 연구에서는 연구 범위를 OWASP와 WASC에서 수행하고 있는 프로젝트들로 한정하고 이들에 대한 개괄적인 소개와 현재 진행되고 있는 각 프로젝트들의 동향에 대해 분석하고 그 대응방안에 대해 제시하고자 한다.

Ⅱ. OWASP [8]

OWASP(Open Web Application Security Project)는 보안 관련 전문가나 각 기업들이 제품을 개발 또는 믿고 구매, 유지 보수할 수 있도록 도와주는 전문화된 오픈 커뮤니티이다. 현재 OWASP의 모든 도구, 문서, 포럼 및 모든 자료들은 무료이며, 애플리케이션 보안 향상에 관심이 있는 사람이면 누구에게나 공개되어 있다.

OWASP는 새로운 형태의 조직으로서 상업적인 이용을 배제하고 애플리케이션 보안에 관한 공평하고, 실용적이며, 비용-효율적인 정보를 제공한다. OWASP는 영리적인 보안 기술들에 대한 유익한 사용법을 제공하지만 어떠한 회사에도 제휴되어 있지 않으며 많은 오픈 소스 소프트웨어 프로젝트와 마찬가지로, OWASP는 많은 종류의 자료들을 공개하고 있다. [그림 1]은 OWASP의 멤버국을 나타낸 것이다.

OWASP의 프로젝트는 다양한 관점에서 애플리케이션 보안을 다루며, 조직들이 안전한 코드를 생산하기 위한 능력 향상을 목적으로 문서, 도구, 교육 환경, 가이드, 체크 리스트 및 다른 자료들을 배포하고 있다. OWASP 프로젝트는 정의된 로드맵과 팀 회원들을 보유한 수집물이다. OWASP 프로젝트 리더는 프로젝트에 대한 비전, 로드맵 및 업무를 정의하는 책임이 있다. 프로젝트 리더는 프로젝트를 활성화 시키

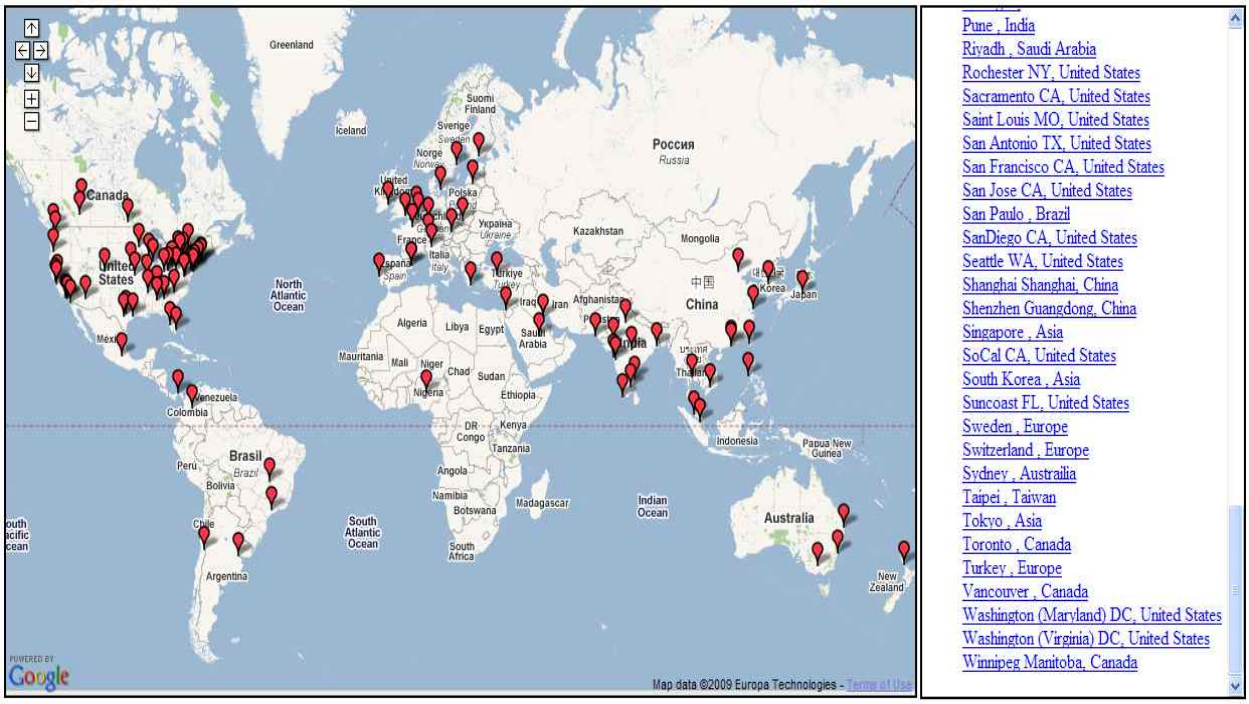

그림 1. OWASP 멤버국 현황
Fig. 1. OWASP national members

며, 팀을 꾸린다. 도구 및 문서들은 다음 항목에 맞춰서 체계화 되어 있다.

PROTECT - 보안에 관련된 설계 및 실행 오류를 방어하기 위한 도구 및 문서들

DETECT - 보안에 관련된 설계 및 실행 오류를 발견하기 위한 도구 및 문서들

LIFE CYCLE - 보안에 관련된 활동들을 소프트웨어 개발 생명 주기에 추가하기 위한 도구 및 문서들

또한 프로젝트의 진행 상태에 따라 아래와 같은 5가지로 분류된다.

• Release 품질 프로젝트

Release 품질 프로젝트는 일반적으로 전문적인 도구 또는 문서 수준의 품질을 보유하고 있다. 보호, 감지 및 두 가지 주요 기준으로 분리된 라이프 사이클로 구성되어 있다.

•Beta 품질 프로젝트

Beta 품질 프로젝트는 완료되었으며, 설명서를 사용할 준비가 된 것들이다. 릴리스 품질 프로젝트와 마찬가지로, 보호, 감지 및 두 가지 주요 기준으로 분리된 라이프 사이클로 구성되어 있다.

• Alpha 품질 프로젝트

Alpha 품질 프로젝트는 일반적으로 사용할 수 있으나 문서 또는 품질에 대한 검토한 미비한 수준이다. 보호, 감지 및 두 가지 주요 기준으로 분리된 라이프 사이클로 구성되어 있다.

• 비활성 프로젝트

비활성 프로젝트 (Alpha, Beta 또는 Release 상태 중 하나에 도달하지 않은 프로젝트) 평가가 되지 않은 버려진 프로젝트이다.

한편 프로젝트 평가는 OWASP 프로젝트 매니저가 배정하는 검토자에 의해서 실행되며, 각각의 항목은 충족 되어져야 하는 요구사항 및 기준을 포함하고 있다. Beta 품질은 Beta 프로젝트 요구사항 및 기준과 Alpha 품질 요구사항들을 충족 시켰다는 것을 의미하며, Release 품질이란 Release 프로젝트 요구사항 및 기준과 더불어 Alpha 및 Beta 프로젝트의 요구사항을 모두 충족 시켰다는 것을 의미한다. 비활성 프로젝트는 각각의 프로젝트 품질 요구사항 및 기준을 충족시키지 못한 경우이다.

현재까지 조사한 바에 의하면 Alpha 품질의 경우

툴과 관련하여 14종, 도큐먼트와 관련 25종의 프로젝트가 진행 중이고, Beta 품질의 경우 툴과 관련하여 17종, 도큐먼트와 관련 8종의 프로젝트가 진행 중이며 그 외 현재 진향 중인 프로젝트는 31종이 있다. 해당 프로젝트에 대한 자세한 사항들은 [8]의 홈페이지를 참조하기 바란다.

Ⅲ. WASC [9]

WASC(Web Application Security Consortium)는 전문가, 산업체실무자, 기관의 대표자들로 이루어진 국제적인 모임으로 공개자료와 World Wide Web에 널리 인정되는 가장 실제적인 보안기준을 만들어 내고 있다.

WASC는 활발하게 활동하는 조직체로서 의견들을 교환하는 일을 촉진하고 몇몇 산업체 과제들을 구성하는 일을 하고 있다. WASC는 지속적으로 기술적인 정보, 기고된 논문, 보안가이드라인과 다른 유용한 자료들을 내놓는 일을 하고 있다. 사업체, 교육기관, 정부, 응용 개발자, 보안전문가, 세계각지에 흩어져 있는 소프트웨어 벤더들은 웹 응용 보안에 의해 제시된 여러 도전들을 보조하기위해서 위에서 언급된 자료들을 활용한다. 참고로 WASC와 관련한 여러활동에 참여하기위한 자원은 무료이며 모든 사람들에게 열려있다.

현재 진행되고 있는 주요 프로젝트는 모두 9가지이며 그 내용은 웹 응용 보안 스캐너 평가 기준 (Web Application Security Scanner Evaluation Criteria), 보안 기사(Security Articles), 웹해킹 사고 DB(Web Hacking Incidents Database), 스크립트 매핑 프로젝트(Script Mapping Project), 보안 용어(Security Glossary), 오픈 프락시 허니팟(Open Proxy Honeypots), 보안 위협 분류(Security Threat Classification), 응용 방화벽 평가 기준(Application Firewall Evaluation Criteria), 응용 보안 통계(Application Security Statistics)이다. 각 프로젝트들에 대한 자세한 사항은 [9]의 홈페이지를 참조하기 바란다.

Ⅳ. OWASP vs WASC

WASC는 다른 그룹들과는 달리 공개된 리소스를 이용하여 산업체에 가이드라인과 문서화된 표준들을 제공하고 있다. WASC는 산업체에서 실질적으로 활용될 수 있는 웹 응용 보안 표준들을 제정함으로써 산업체에 도움이 되도록 하는데 그 목적을 두고 있다.

반면에 OWASP의 경우 목적 지향적이며 표준화된 XML 포맷을 이용함으로써 정보 교환을 용이하게 하고 있으며 현재 프로젝트 단위의 활발한 활동을 통해 오픈 소스 웹 보안 소프트웨어 개발과 문서화, 그리고 관련 라이드라인을 제공하는데 초점을 맞추고 있다.

OWASP의 경우 문제를 해결하는 데 있어 사회적 이유가 되는 일명 ‘folksonomy’ 태깅이라는 접근 방식을 취하는 반면 WASC의 경우 각각의 카테고리를 프로젝트 형식으로 분류하여 진행하고 있다. 각 카테고리 내 항목들은 각기 서브 카테고리로 나뉘어지며 (없는 경우도 있음) 참가자들의 필요에 따라 이들을 프로젝트 형태로 일부 진행하고 있다.

한편 웹 취약점 가운데 하나인 "Cross site scripting"의 경우를 예를 들어 소개하면 아래와 같다. WASC에서는 “웹 응용 보안 스캐너 평가 기준”의 프로젝트 내에 한 부분으로 기술적인 측면에 있어 공격기법과 대응방안을 레퍼런스로 소개하고 이들에 대한 평가기준을 전반적으로 제시하고 있는 반면, OWASP의 경우 위 부분과 관련하여 “OWASP TOP 10 Project [1]”에서 전반적인 소개와 대응방안에 대해 기술하고 있으며, “OWASP Testing Project”에서는 “OWASP Testing Guide V3”에서 모의 해킹(Penetration testing)을 할 수 있는 방법에 대해 소개하고 있고 “OWASP Code Review Project”에서는 각 프로그래밍 언어별로 간단한 예시와 더불어 그 대응방안에 대해 보다 자세하게 소개하고 있다.

WASC의 경우 웹 어플리케이션 보안 부분에 있어 거의 대부분의 사항들(예: 논문, 통계, 해킹 사례 등)을 다루고 있다면 OWASP의 경우 웹 서비스 취약점과 관련한 보안부분 가운데 특히, 소프트웨어분야의 개발 부분에 보다 중점을 두고 있다. 일례로 WASC

에서 다루고 있는 “The Web Hacking Incidents Database”, “Distributed Open Proxy Honeypots”, “Web Application Security Statistics” 프로젝트들에 대해 OWASP에서는 다루고 있지 않다.

결론적으로 볼 때, 서로 다루고 있는 영역의 차이가 있으나 양측이 모두 현재까지 웹 응용 보안 부분에 있어 가장 활발한 활동을 벌이고 있고, 다루고 있는 영역 중 일부는 서로 관련이 있는 바 상호협력을 통해 효과를 극대화할 필요가 있을 것이다. 본 연구에서는 이러한 유사성과 차이점을 살펴보고 향후 양측이 상호 협력할 수 있는 기반을 모색해본다는 점에서 의미가 있을 것으로 사료된다.

Ⅴ. 향후 대응방안

한국인터넷진흥원에서는 해킹에 많이 이용되고 있는 웹 어플리케이션의 취약점에 대한 최신 동향과 해킹기법, 보안대책을 다룬 “웹 보안 4종 가이드” [10]를 발간하여 배포하고 있다. 주된 내용은 OWASP Top 10에서 제시하고 있는 취약점들과 그 대응방안들에 대해 홈페이지 개발 시 필요한 보안 고려사항, 웹서버 구축 시 취약점 및 안전한 웹 프로그래밍 기법들, 그리고 서버 및 네트워크, Database와 application의 점검 방법, 끝으로 가이드 CD로 구성되어 있다.

그러나 현재 OWASP에서는 앞서 언급한 바 웹 어플리케이션 보안 소프트웨어 분야에 있어 코드 리뷰, 테스팅 가이드 등에 대해 보다 폭넓고 다양한 최신의 정보들이 업데이트되고 있음을 알 수 있다. 따라서 우리나라에서도 한국인터넷진흥원을 포함한 업계와 학계 등의 전문가들이 지속적으로 OWASP 뿐만 아니라 WASC의 프로젝트들과 관련한 최신 동향들을 분석하고 이를 보안 개발자나 관리자들이 적극 활용할 수 있도록 연구할 필요가 있다. 이는 현재도 국가나 관련 기업들에서 많은 관심과 투자가 진행되고 있는 바, 향후 실질적인 대처 방안이 마련될 것으로 사료된다.

Ⅵ. 결 론

지금까지 OWASP와 WASC에 대한 개괄적인 소개와 현재 진행되고 있는 각종 프로젝트들의 동향들에 대해 살펴보았다. 또한 양측의 비교를 통해 유사성과 차이점을 살펴보고 향후 양측이 상호협력을 통해 얻을 수 있는 시너지 효과에 대해 모색해 보았다.

이러한 조사를 바탕으로 특히 OWASP의 프로젝트들을 분석하여 향후 웹 애플리케이션의 취약성 유형들을 예방할 수 있는 방안을 제시하였다. 이는 향후 한국인터넷진흥원을 비롯한 보안관련 기관에서 향후 정책을 반영하는데 있어 가치있는 기초자료로 활용될 수 있을 것이다.

감사의 글

본 논문은 2009년도 강릉원주대학교 학술연구조성비지원에 의하여 수행되었음.

참 고 문 헌

[1] http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[2] 김성락, "A Study of Web Application Attack Detection extended ESM Agent," *한국컴퓨터정보학회논문지*, 제 12권, 제 1호, pp. 161-168, 2008.

[3] 장문수, 오창석, “Web Application Attack Prevention by Traffic Analysis,” *한국컴퓨터정보학회논문지*, 제 13권, 제 3호, pp. 139-146, 2008.

[4] V. Benjamin-Livshits, S. Monica, “Finding Security Vulnerabilities in Java Applications with Static Analysis,” *Technical Report, Dept. Computer Science*, Stanford University, 2005.

[5] F. Jacobs and B. Joosen, "Software Security: Experiments on the .NET Common Language Run-time and the Shared Source Common Language Infrastructure," *Software : IEE Proceedings,* vol. 150, issue 5, pp. 303-307, 2003.

[6] J. Bau, E. Bursztein, D. Gupta, and J. Mitchell, " State of the Art: Automated Black-Box Web Application Vulnerability Testing," *2010 IEEE Symposium on Security and Privacy*, pp. 332-345, 2010.

[7] C. Vanden-Berghe, F. Piessens, and J. Riordan, "A Vulnerability Taxonomy Methodology applied to the Web Services," *Proc. the 10th Nordic Workshop on Secure IT Systems*, 2005

[8] OWASP(Open Web Application Security Project), http://www.owasp.org

[9] WASC(Web Application Security Consortium), http://webappsec.org

[10] http://www.kisa.or.kr/notice/noticeView.jsp? mode =view&b_No=4&d_No=189

이 재 현 (李在鉉)

1989년 2월 : 중앙대학교 컴퓨터공학과 (공학사)
1991년 2월 : 중앙대학교 컴퓨터공학과 (공학석사)
2001년 2월 : 연세대학교 인지과학전공 (공학박사)
1991년 9월~현재 : 강릉원주대학교 과학기술대학 정보기술 공학과 교수
관심분야 : 정보보안, 정보윤리, 인지과학