효율적인 웹 취약점 점검을 위한 점검항목의 위험도 분석

이현아
고려대학교 정보통신대학원 소프트웨어보안학과
e-mail : hyunaaa13@naver.com

Risk analysis of checklist for efficient web vulnerability inspection

Hyun-A Lee
Dept. of Software Security, Korea University Graduate School of Computer & Information Technology

요 약

웹 해킹 사고 건수와 피해규모가 매년 증가하고 있다. 해킹사고의 대부분이 웹을 통해 발생하고 있으며 웹 취약점 점검을 통해 사전에 예방할 수 있지만 인력과 예산 부족으로 주기적인 점검이 어려운 것이 현실이다.
본 연구에서는 효율적인 웹 점검을 위해 공격가능성을 바탕으로 점검 항목의 위험도를 분석하고 향후 지속되어야 할 연구 방향을 제시한다.

1. 서론

해킹 사고가 매년 증가하고 있고 그 피해 규모도 지속적으로 커지고 있다. 2017 년 사드 배치에 따른 중국 발 사이버 공격으로 여러 기관의 웹사이트들이 사드 배치 반대 문구로 위·변조 된 사건과 여기어때 사용자의 이용정보 323 만건 유출 사고, 인터넷 나야나 랜섬웨어 감염사태 등 피해 규모와 파급 효과가 큰 사건들이 다수 발생했었다.

이를 사전에 방지하기 위해 정기적인 취약점 점검이 필요하다. 그러나 이러한 업무를 수행할 수 있는 정보보안 담당자는 한 기관에 평균 1~2 명 정도로 업무량에 비해 인원이 턱없이 부족한 편이다. 인력 충원은 많은 예산과 시간이 투자되어야 하므로 문제를 즉각적으로 해결하기에 어려움이 크다.

해킹 사고의 80%는 웹을 통해 발생한다. 앞으로의 해킹 사고 발생 가능성을 줄이기 위해 효율적인 웹 취약점 점검을 위한 방법이 필요하다. 현재 웹 취약점 점검 방법의 문제점을 파악한 후 해결방안을 제시하겠다.

2 장에서 보안실태를 알아보고 3 장에서 해결방안 제시 후 4 장에서 결론을 정리한다..

2. 보안실태

2.1 사고 사례 분석

2017 년 사드 배치 보복에 따른 중국 발 해킹 공격으로 공공기관, 기업들의 디페이스 공격이 발생했고, 국내 웹사이트를 타깃으로 한 동남아 해커들의 디페이스 공격이 있었다. 아시아나항공 홈페이지 해킹과 웹 호스팅 업체 서버가 디페이스 공격을 수차례 받았다. 또한 중국 추정 해커가 국내 2 개 인트라넷 페이지를 디페이스 해킹한 사고도 있었다.

이러한 디페이스 공격은 자신의 실력을 과시하고 재미 삼아 해킹하는 스크립트 키드 수준의 해커들이라는 게 보안전문가들의 공통된 분석이다.

또한 북한 배후 해커 조직이 지난해 5 월부터 6 개월간 국내 기업을 타깃으로 한 해킹 공격을 지속해왔다. 142 개의 기업을 공격해 실제 15 개 기업에 침해사고가 발생했다.

초급 수준의 해킹 공격에도 취약한 사이트가 많은 것을 위의 사례를 통해 알 수 있었고, 최근 우리나라는 중국, 북한을 비롯한 여러 국가들의 해킹 표적이 되고 있다.

특정 대상을 목표로 한 공격이 아닌 무차별적인 공격으로 인해 취약한 서버들은 손쉽게 해킹 당해 기업과 국가 이미지를 실추시키고 있다.

현실에 맞게 보안성을 향상 시킬 방안을 찾아 단순한 공격에 의한 피해를 줄이고, 스크립트 키드들의 표적이 되지 않도록 해야한다.

2.2 문제점 도출

국가정보보안기본지침(국정원) 제 28 조(서버 보안관리)에 따르면 사이버 공격 대비 정보시스템 홈페이지와 모바일 앱의 취약점 진단 및 제거를 해야 한다. 또한 행정기관 및 공공기관 정보시스템 구축·운영 지침(행정자치부고시 제 2017-7 호)에 따르면 '행정기관, 공공기관은 정보화사업을 추진하고자 하는 경우 행정기관등의 장은 정보화사업 감리를 수행하는 경우, 감리법인으로 하여금 사업자가 소프트웨어 보안약점을 제거하였는지 진단하도록 해야 한다.

그러나 이러한 점검은 점검 비용과 시간이 많이 들고 전문 점검 인력이 필요하므로 1 회성 점검에 그치는 경우가 대부분이다. 웹 어플리케이션의 경우 지속적인 업데이트로 인해 소스코드 업데이트가 수시로 일어나는 경우도 있는데 그 당시의 점검에는 문제점이 없었다 할지라도 점검 이후 수정되어 발생하는 문

제점은 파악하기 어렵다.

보안 컨설팅의 경우 전문인력이 보통 한달 간 점검을 하는데 기관 보안담당자가 수시로 점검하는 것은 현실적으로 불가능하다.

2.3 현재 점검 방식

현재 국내에서 웹 어플리케이션 취약점 점검항목은 주요정보통신기반시설의 웹 점검항목과, KISA 홈페이지 취약점 진단 제거 가이드의 항목을 주로 사용하고 있다. 이 점검 항목의 개수는 주요기반시설 점검항목의 경우 28 개 항목, KISA 의 경우 21 개 항목으로 수시로 점검하기에는 점검항목이 많은 편이다.

시중에 웹 취약점 점검을 위한 자동화 도구도 많지만 가격이 비싸서 규모가 작은 기관들의 경우 사용하기에 어렵다. 보안장비와 보안 솔루션의 경우에도 구축 비용이 많이 들어서 현실적인 해결방안으로는 부적합하다.

3. 해결방안

3.1 위험도 분석의 필요성

최소한의 보안을 위해서라도 분기별 웹 취약점 점검이 필요하다 보여지고, 이를 위해서는 보안담당자가 자체적으로 점검할 수 있을 정도의 점검항목으로 항목 수를 줄여야 한다고 판단했다.

국내 점검항목의 경우 위험도 분석이 세분화 되어 있지 않다. 주요정보통신기반시설 웹 점검항목의 경우 항목중요도가 전체 '상'으로 되어있고 KISA 점검 항목의 경우 중요도 분석이 되어있지 않다.

OWASP Top 10 의 경우 위험도 분석을 위해 위험요인을 공격가능성, 확산 정도, 탐지가능성, 기술로 세분화 하여 점수화 하여 Top 10 을 선정하고 있다.

3.2 위험도 분석 방법

이번 연구에서는 스크립트 키드들의 단순한 해킹 공격을 막기 위해 국내 웹 취약점 점검항목의 위험도 분석을 통해 위험도가 높은 순으로 점검 항목을 선별하여 효율적인 웹 취약점 점검 방안을 제시하고자 한다.

OWASP 위험도 분석을 참고해서 공격가능성만을 위험 요인으로 두고 KISA 점검 항목으로 위험도 분석을 하겠다. KISA 점검 항목은 '주요정보통신기반시설 취약점 분석 평가 기준' 항목을 기반으로 통폐합 및 신규 항목이 추가되어 있으므로 점검항목의 위험도 분석을 위해 KISA 점검 항목을 사용했다.

공격이 쉬울수록 높은 점수를 부여하고 공격 가능성이 높은 것으로 보고, 공격 가능성이 높을수록 위험도가 높은 것으로 판단한다. 공격 가능성의 점수는 OWSAP 위험도 분석을 참고하여 작성하였다.

OWASP Top 10 2017 에서는 공격 가능성을 판단하기 위한 위협 요소 요인으로 기술수준, 동기, 기회, 위협을 가하는 그룹의 크기를 0~9 등급으로 나누어 점수화 하였다. 그리고 아래와 같이 공격 가능성을 아래와 같이 점수화 하였다. 공격가능성이 쉬움인 경우 3 점, 평균인 경우 2 점, 어려움일 경우 1 점이다.

<표 1> OWASP Top 10 (2017) 공격 가능성

OWASP 2017	공격 가능성
인젝션	3
인증	3
민감 정보 노출	2
XXE	2
취약한 접근 제어	2
보안 설정 오류	3
XSS	3
안전하지 않은 역직렬화	1
취약한 컴포넌트	2
불충분한 로깅 및 모니터링	2

이를 참고하여 KISA 점검항목으로 공격 가능성을 분석한 표는 아래와 같다.

<표 2> KISA 점검항목 공격 가능성

KISA 점검항목	공격 가능성	OWASP
운영체제 명령 실행	3	인젝션
SQL 인젝션	3	인젝션
XPath 인젝션	3	인젝션
정보누출	2	민감 정보 노출
악성콘텐츠	2	XXE
크로스 사이트 스크립트(XSS)	3	XSS
약한 문자열 강도	3	취약한 인증
불충분한 인증 및 인가	3	취약한 인증
취약한 패스워드 복구	3	취약한 인증
불충분한 세션 관리	3	취약한 인증
크로스 사이트 리퀘스트 변조(CSRF)	2	CSRF
자동화 공격	3	취약한 인증
파일 업로드	2	XXE
경로추적 및 파일 다운로드	3	보안 설정 오류
데이터 평문전송	2	민감 정보 노출
쿠키 변조	2	취약한 접근 제어
URL/파라미터 변조	2	취약한 접근 제어
디렉터리 인덱싱	3	보안 설정 오류
관리자페이지 노출	3	보안 설정 오류
위치공개	3	보안 설정 오류
웹 서비스 메소드 설정 공격	2	취약한 접근 제어

CSFR 는 2017 년에 제거된 항목으로 2013 년 기준으로 공격가능성을 작성하였다.

3.3 위험도 분석 결과

위험도 분석 결과 공격 가능성이 3 점인 항목이 13 개, 2 점인 항목이 8 개, 1 점인 항목이 0 개로 총 21 개 항목을 분석하였다.

공격가능성이 높고 OWASP 항목의 위험도 순위가 높은 순으로 정렬하면 아래 표와 같은 결과가 도출된다.

<표 3> KISA 점검항목 공격가능성 순위

순위	KISA		OWASP	
	점검항목	공격 가능성 (점수)	항목	위험도 순위
1	운영체제 명령 실행	3	인젝션	1
2	SQL 인젝션	3	인젝션	1
3	XPath 인젝션	3	인젝션	1
4	약한 문자열 강도	3	취약한 인증	2
5	불충분한 인증 및 인가	3	취약한 인증	2
6	취약한 패스워드 복구	3	취약한 인증	2
7	불충분한 세션 관리	3	취약한 인증	2
8	자동화 공격	3	취약한 인증	2
9	경로추적 및 파일 다운로드	3	보안 설정 오류	6
10	디렉터리 인덱싱	3	보안 설정 오류	6
11	관리자페이지 노출	3	보안 설정 오류	6
12	위치공개	3	보안 설정 오류	6
13	크로스 사이트 스크립트(XSS)	3	XSS	7
14	정보누출	2	민감 정보 노출	3
15	데이터 평문전송	2	민감 정보 노출	3
16	악성콘텐츠	2	XXE	4
17	파일 업로드	2	XXE	4
18	쿠키 변조	2	취약한 접근 제어	5
19	URL/파라미터 변조	2	취약한 접근 제어	5
20	웹 서비스 메소드 설정 공격	2	취약한 접근 제어	5
21	크로스 사이트 리퀘스트 변조(CSRF)	2	CSRF	11

CSRF 는 2017 년 제거된 항목이므로 가장 낮은 순위로 계산하였다.

4. 결론

4.1 연구결과

본 연구는 초급 해커들에 의한 무차별적 해킹 피해를 줄이기 위해 공격가능성을 바탕으로 웹 취약점 점검항목 위험도 분석을 하였다.

KISA 점검항목 21 개에 대해 점검 항목의 공격가능성 순위를 작성하였고, OWASP 위험도를 기반으로 공격가능성이 같은 점수인 항목에 대해서도 우선순위를 도출하였다.

4.2 향후 연구 방향

점검 대상과 점검 목적에 따른 다양한 위험도 분석이 추가로 연구되고, 위험도가 높은 순으로 점검항목을 선정하여 국가기관에서 취약점 테스트 툴을 만들어 배포한다며 더 효율적인 점검이 될 수 있을 것이라 예상된다.

또한 점검 항목의 주기적 업데이트도 필요하다. 현재 OWASP Top 10 은 3 년에 한번 발표가 되고, 주요정보통신기반시설과 KISA 점검 항목은 4 년전에 만들어졌다.

신규 취약점이 발견되는 속도에 빠르게 대응하기 위해서는 점검 항목과 점검 자동화 툴의 주기적인 업데이트가 필요하고 지속적으로 점검 자동화 툴 개발에 대한 연구와 점검 항목 선정을 위한 연구가 필요하다.

참고문헌

[1] OWASP Top 10 - 2017
[2] OWASP Top 10 - 2013
[3] OWASP Risk Rating Methodology https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
[4] 주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세 가이드, 안전행정부
[5] 홈페이지 취약점 진단 제거 가이드, KISA
[6] 보안뉴스, 국내 웹호스팅 업체 노린 해외 해커들, 130 여곳 대량 해킹 사태, http://www.boannews.com/media/view.asp?idx=54187
[7] 보안뉴스, 중국발 해킹 공격 이미 진행형! 두려움보다 철저함 필요하다, http://www.boannews.com/media/view.asp?idx=53981
[8] 보안뉴스, 정보보호 산업에 정작 보안인력이 부족한 이유 3 가지, http://www.boannews.com/media/view.asp?idx=54300
[9] 보안뉴스, 북한 배후 해커조직, 국내 142 개 기업 타깃 공격...15 곳 뚫려, http://www.boannews.com/media/view.asp?idx=67802