https://doi.org/10.5392/JKCA.2022.22.02.125

웹취약점 자동진단 개선방안

Improvement Mechanism for Automatic Web Vulnerability Diagnosis

김태섭, 조인준
배재대학교대학원 사이버보안학과

Tae-Seop Kim(ktsdrive9@naver.com), In-June Jo(injune@pcu.ac.kr)

요약

스마트폰 기술의 발전으로 인하여 2020년 기준 전 국민의 91.9%가 인터넷 이용[1]하여 수시로 홈페이지와 모바일 앱을 통해 정보를 습득하고 있다. 정보제공을 담당하는 홈페이지의 수가 점점 늘어남에 따라 홈페이지의 안전성을 진단하는 웹취약점 진단 신청수도 매년마다 증가하고 있는 상황이다. 기존 웹취약점 점검은 진단원이 수작업으로 홈페이지를 모의 해킹하여 취약점을 진단했기 때문에 진단대상 홈페이지 수에 비례하여 진단인력이 늘어나야한다. 하지만 현실적으로 웹취약점 진단인력 확보에 한계가 있고, 진단인력을 늘렸을 경우 많은 비용이 발생한다. 이러한 문제점 해결을 위해 자동진단 도구를 사용하여 수동진단의 일부를 대체하고 있다. 본 논문에서는 현재의 자동진단 범위를 확대하기 위한 방안을 새롭게 제안하였다. 즉, 웹취약점 진단항목의 영향도를 분석하여 자동진단 가능 항목을 도출하고, 실제 운영 중인 홈페이지에 수동 및 자동진단을 수행하여 진단결과에 대한 비교 분석을 통해 자동진단 가능항목을 파악하였다. 또한 자동진단 개선방안을 제시하여 자동진단 도구 개선을 통해 모든 취약점 항목은 아니지만 가능한 항목에 대해서 수동진단을 대체할 수 있다. 이를 통해서 진단 및 정밀진단이 필요한 부분에 집중하여 안전한 홈페이지 운영환경 조성에 기여할 수 있을 것이다.

■ 중심어 : | 웹취약점 | 웹취약점 점검항목 | 자동진단 | 개선방안 |

Abstract

Due to the development of smartphone technology, as of 2020, 91.9% of people use the Internet[1] to frequently acquire information through websites and mobile apps. As the number of homepages in charge of providing information is increasing every year, the number of applications for web vulnerability diagnosis, which diagnoses the safety of homepages, is also increasing. In the existing web vulnerability check, the number of diagnostic personnel should increase in proportion to the number of homepages that need diagnosis because the diagnosticians manually test the homepages for vulnerabilities. In reality, however, there is a limit to securing a web vulnerability diagnosis manpower, and if the number of diagnosis manpower is increased, a lot of costs are incurred. To solve these problems, an automatic diagnosis tool is used to replace a part of the manual diagnosis. This paper explores a new method to expand the current automatic diagnosis range. In other words, automatic diagnosis possible items were derived by analyzing the impact of web vulnerability diagnosis items. Furthermore, automatic diagnosis identified possible items through comparative analysis of diagnosis results by performing manual and automatic diagnosis on the website in operation. In addition, it is possible to replace manual diagnosis for possible items, but not all vulnerability items, through the improvement of automatic diagnosis tools. This paper will explore some suggestions that can help improve plans to support and implement automatic diagnosis. Through this, it will be possible to contribute to the creation of a safe website operating environment by focusing on the parts that require precise diagnosis.

■ keyword : | Web Vulnerability | Web Vulnerability Check Items | Automatic Diagnosis | Improvement |

접수일자 : 2021년 10월 27일
수정일자 : 2021년 11월 09일
심사완료일 : 2021년 11월 09일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

최근 스마트폰 기술의 발전으로 인하여 우리는 수시로 홈페이지와 모바일 앱을 통해 정보를 습득하고 있다. 정보제공을 담당하는 홈페이지의 수와 침해사고 신고접수[2]가 지속적으로 증가함에 따라 홈페이지의 안전성을 진단하는 웹취약점 진단 신청수도 매년마다 증가하고 있는 상황이다.

다만 진단원의 수가 한정적이기 때문에 모든 홈페이지를 진단원이 모의해킹으로 안전성 진단을 수행하기에는 한계점이 존재한다. 따라서 웹취약점 자동진단을 통해 수동진단에 소요되는 시간을 감소시킬 필요성이 있다. 하지만 자동진단이 만능은 아니다. 자동진단의 경우 진단 시 프로그램에 설정된 점검항목을 홈페이지에 전송하여 취약여부를 파악하므로 홈페이지 구성항목 및 게시물이 많은 경우 홈페이지 서비스에 지장을 초래하여 서버를 다운시키는 경우도 발생한다. 이 문제 때문에 실제 운영 중인 홈페이지에 웹취약점 진단을 수행하는 경우 수동진단을 선호한다. 수동진단의 경우 전문적인 지식을 가진 진단원이 홈페이지의 구성을 먼저 파악한 후 점검항목별 취약점이 존재하는지 진단하기 때문이다. 다만 진단원이 수동으로 모든 항목을 점검해야 하기 때문에 자동진단에 비해 취약점 발견 정확도는 향상되나 시간이 많이 필요하다. 자동진단 방식을 개선하여 수동진단 만큼 정확도를 향상시키고 홈페이지 서비스에 영향을 완화한다면 보다 많은 홈페이지에 대한 웹취약점 진단이 가능할 것이다. 웹취약점 진단항목 중 영향도를 분석하고 실제 홈페이지에 수동 및 자동진단을 수행한 후 결과를 분석하여 수동진단 대체가 가능한 자동진단 항목을 파악하고 진단에 활용하는데 목적이 있다.

II. 웹취약점 진단방법 연구

1. 웹취약점 자동진단 방식

웹취약점 자동진단 방식은 오픈소스 프로그램을 이용하거나 상용 솔루션을 이용하는 방식이 있다. 다만 웹 취약점 진단 정확도나 홈페이지 서비스에 영향을 미치지 않도록 진단항목별 옵션을 적용하려면 상용소프트웨어를 이용하여 진단하는 것이 좋다.

또한 웹취약점 진단을 의뢰하여 수행하는 기관은 대다수 공공기관으로 해당기관에 웹취약점 자동진단을 하기 위해서는 CC(Common Criteri) 및 GS(Good Software) 인증을 받은 소프트웨어를 사용해야한다.

2. 웹취약점 수동진단 방식

웹취약점 수동진단은 우선 홈페이지에를 구성하는 기능(회원가입, 로그인, 게시판 등) 및 디렉토리 구조를 파악한 후 오픈소스 자동진단 도구(Nikto, Skipfish 등)를 통해 숨겨진 경로 및 정보를 분석한다. 외부에 노출되는 정보를 수집하여 디렉토리 구조, 관리자페이지 존재여부, 웹서버 정보 노출여부, 게시물 내용 및 첨부파일에 중요정보 노출여부를 파악한다.

수집된 정보를 바탕으로 진단영역의 우선순위를 부여[3]한 후 웹취약점 진단항목을 기준으로 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드[4]의 진단방법을 참고하여 웹프록시 도구를 이용 수동진단을 수행 취약점 존재여부를 파악한다.

3. 웹취약점 진단항목

웹취약점 진단 기준은 OWASP(The Open Web Application Security Project)에서 발표하는 OWASP TOP 10[5], CWE/SANS TOP 25[6], 국정원 8대 취약점, 행정안전부의 웹취약점 점검 항목 21개가 있다. 여러 개의 진단기준 중 행정안전부의 웹취약점 점검항목 21개[표 1]를 기준으로 웹취약점 진단방법을 KISA에서 발행하는 소프트웨어 개발보안가이드[7]를 참조 및 분석하여 진단 시 홈페이지 서비스에 미치는 영향도를 파악할 것이다. [표 1]은 행정안전부 웹취약점 점검항목 21개 항목 목록이다.

표 1. 행정안전부 웹취약점 점검항목(21개)[8]

순	점검항목	설명
1	운영체제 명령 실행	- 웹 서버에 존재하는 명령어 실행 가능 함수 인자를 조작하여 특정 명령어 실행이 가능한 취약점
2	SQL 인젝션	- 입력 폼에 악의적인 쿼리문을 삽입하여 DB 정보, 타 사용자 권한 획득이 가능한 취약점
3	XPath 인젝션	- XPath 쿼리문 구조를 임의로 변경하여 DB 정보 열람, 타 사용자 권한 획득이 가능한 취약점

순	점검항목	설명
4	디렉토리 인덱싱	- 본 페이지의 파일이 존재하지 않을 때 자동적으로 디렉토리 리스트를 출력하는 취약점
5	정보누출	- 개발자의 부주의, 디폴트로 설정된 에러 페이지 등 웹 어플리케이션에서 민감한 정보가 노출되는 취약점
6	악성콘텐츠	- 정상적인 컨텐츠 대신에 악성 컨텐츠를 주입하여 사용자에게 악의적인 영향을 미치는 취약점
7	크로스사이트 스크립트	- 웹 사이트를 통해 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점
8	약한 문자열 강도	- 비밀번호 조합규칙(영문, 숫자, 특수문자 등)이 충분하지 않아 추측 가능한 취약점
9	불충분한 인증 및 인가	- 웹 어플리케이션에서 사용자 인증 및 접근제한 미흡으로 불법 접근 및 조작이 가능한 취약점
10	취약한 패스워드 복구	- 취약한 패스워드 복구로직을 통해 다른 사용자의 패스워드를 획득, 변경할 수 있는 취약점
11	불충분한 세션 관리	- 단순 숫자 증가 방법 등의 취약한 특정 세션의 ID를 예측하여 세션을 가로채거나 중복 접속을 허용하는 경우 타 사용자의 세션을 획득하여 권한 획득 할 수 있는 취약점
12	크로스사이트 리퀘스트 변조 (CSRF)	- 로그온 한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹 어플리케이션에 전송하는 취약점
13	자동화공격	- 정해진 프로세스에 자동화된 공격을 수행함으로써 수많은 프로세스가 진행되는 취약점
14	파일업로드	- 파일 업로드 기능을 이용하여 시스템 명령어를 실행할 수 있는 파일을 업로드 하는 취약점
15	경로추적 및 파일다운로드	- 다운로드 함수 인자를 조작하여 서버에 존재하는 파일 다운로드 가능한 취약점
16	관리자페이지 노출	- 단순한 관리자 페이지 이름, 설정, 설계상 오류 등 관리자 메뉴에 직접 접근할 수 있는 취약점
17	위치공개	- 임시파일, 백업파일등에 접근이 가능하여 핵심정보가 노출될 수 있는 취약점
18	데이터 평문전송	- 서버와 클라이언트 간 통신 시 암호화 하여 전송을 하지 않아 중요 정보 등이 노출되는 취약점
19	쿠키 변조	- 보호되지 않는 쿠키를 사용하여 값 변조를 통한 사용자 위장 및 권한 상승 등이 가능한 취약점
20	웹 서비스 메소드 설정 공격	- PUT, DELETE 등의 메소드를 악용하여 악성 파일(웹쉘) 업로드가 가능한 취약점
21	URL/파라미터 변조	- URL, 파라미터의 값을 검증하지 않아 특정 사용자의 권한 획득이 가능한 취약점

4. 영향도에 따른 자동진단 가능성 웹취약점 항목

웹취약점 진단방법을 분석하여 홈페이지 서비스에 영향을 최소화하여 취약점 자동진단이 가능한 항목을 분류하여 가능항목 12개[표 2]와 불가능 항목 9개[표 3]로 정리하였다.

표 2. 영향도에 따른 자동진단 가능항목

순	자동진단 가능항목	순	자동진단 가능항목
1	운영체제 명령 실행	7	불충분한 세션 관리
2	디렉토리 인덱싱	8	경로추적 및 파일다운로드
3	정보누출	9	관리자페이지 노출
4	크로스사이트 스크립트	10	위치공개
5	약한 문자열 강도	11	데이터 평문전송
6	취약한 패스워드 복구	12	웹 서비스 메소드 설정 공격

표 3. 영향도에 따른 자동진단 불가능 항목

순	자동진단 불가능 항목	비고(영향도)
1	SQL 인젝션	취약점이 존재하는 경우 운영 중인 데이터베이스에 영향을 줄 가능성 존재
2	XPath 인젝션	SQL 인젝션과 동일
3	악성콘텐츠	악성코드가 삽입 되어있는 경우 시스템에 영향을 줄 가능성 존재
4	불충분한 인증 및 인가	다량의 게시글 삽입 또는 데이터 변조 가능성이 있으며, 입력된 데이터 삭제가 필요함
5	크로스사이트 리퀘스트 변조	다량의 게시글 삽입 가능성이 있으며, 생성된 게시글 삭제가 필요함
6	자동화공격	다량의 데이터 삽입 가능성이 있음
7	파일업로드	악성코드가 삽입된 파일이 업로드 되어 실행되는 경우 시스템에 영향을 줄 가능성 존재
8	쿠키 변조	쿠키 값에 인젝션 코드를 삽입하는 경우 시스템에 영향을 줄 가능성 존재
9	URL/파라미터 변조	다량의 게시글 삽입 또는 데이터 변조 가능성이 있으며, 입력된 데이터 삭제가 필요함

Ⅲ. 웹취약점 수동 및 자동진단 결과비교(1차)

1. 진단결과 비교를 위한 시나리오 및 체크리스트

웹취약점 자동진단 수행결과를 수동진단과 비교하여 취약점 발견유무에 대한 비교를 위해 운영 중인 홈페이지 3개를 선정하여 진단을 진행하였다. 자동진단의 경우 홈페이지 취약점 자동진단 상용제품 3개를 이용하여 진단을 수행하고, 수동진단의 경우 웹 프록시 툴을 이용하여 모의해킹을 진행하였다.

수동 및 자동진단 결과비교를 위한 수행절차를 [그림 1]과 같이 정리하였다.

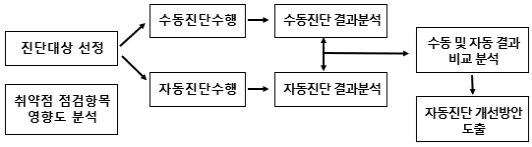

그림 1. 수동 및 자동진단 결과비교 수행절차

또한 수동진단과 자동진단을 비교하기 위한 진단 시나리오를 구상하였으며 [표 4]와 같이 정리하였다.

표 4. 수동 및 자동진단 결과 비교 시나리오

진단방법	시나리오
수동진단	1. 홈페이지 기능 및 디렉토리 구조파악 - 게시판 개수, 글쓰기 기능, 에디터 사용여부, 회원가입여부, 숨겨진 디렉터리 경로 및 기능 확인 등 2. 자동진단 도구(Burp Suite, Nikto, Skipfish 등) 진단 - 수동으로 찾기 어려운 숨겨진 경로 확인 - 진단 결과에 대한 취약점 정보 분석 및 오탐 또는 실제 취약점 확인 3. 외부에 노출된 취약점 정보 수집 - 디렉터리 구조, 관리자페이지, 웹서버 정보, 대외비 등 중요 정보 및 문서에 대한 정보 수집 4. 관리자페이지 및 개인정보 노출 여부 확인 - 관리자 또는 작업자가 접근한 알려지지 않은 페이지 확인 - 개인정보 노출 여부 확인 등 5. 웹 취약점 21개 항목 점검 - SQL 인젝션, 파일 업/다운로드, 인증우회, 권한 탈취 등 수동 진단 수행 6. 웹 취약점 결과 파악 - 진단완료된 취약점 결과 집계
자동진단	1. 취약점 자동화 진단 솔루션 S/W 설치 2. 진단 대상 사전 조사 3. 취약점 자동화 진단 수행 4. 진단 완료 취약점 결과 집계

수동진단에 발견된 취약점을 자동진단 시 동일하게 진단이 가능하거나 더 많은 취약점을 찾을 수 있는지 비교하고, 상용 자동도구를 사용하여 수동진단을 대체할 수 있는지 판단하기 위해 기능성, 사용성, 확장성, 정확성, 효율성과 같이 5개 분야 34개 체크리스트 항목 [표 5]을 작성하여 상용 자동도구에 대해 평가하였다.

다만 상용 자동화도구 명칭에 대해서는 A, B, C로 명칭 하여 자세한 제품명은 생략하였다.

표 5. 웹 취약점 자동진단 수행 체크리스트

항목	내 용
기능성(40)	1. 자동진단 기능구현완전성 ▣ 웹취약점 진단 항목(21개)을 지원하는가? ▣ 웹취약점 자동진단 시 제품/버전별 진단이 가능한가? - WEB : Apache, IIS, WebTOB 등 - WAS : Tomcat, Weblogic, Jeus, jBoss 등 - DBMS : Oracle, MS-SQL, MySQL, Tibero, Cubrid 등 ▣ 웹취약점 자동 진단 중 웹 서비스 부하 발생 시 부하 조정 기능이 있는가? ▣ 자동진단 정지 후 정지 시점부터 재실행 기능이 있는가? ▣ 웹취약점 진단항목별 진단결과 정 · 오탐 분류 기능이 있는가? ▣ 웹취약점 자동진단 중 장애 발생 시 진단 중지 및 알람 메시지 출력이 가능한가? ▣ 일일, 주간, 월간 등 반복적인 점검을 자동으로 수행 할 수 있는 스케줄러 기능을 제공하는가? ▣ 자동진단 종료시간 지정이 가능한가? ▣ 자동진단 시 특정 게시물 등록 후 자동 삭제 기능이 있는가? ▣ 전자정부프레임워크, 스트럿츠, 스프링 등 알려진 프레임워
	크가 아닌 기타 웹구조에 대한 디폴트페이지, 서버정보 등 진단이 가능한가?
	2. 상호 운용성 ▣ 특정 프로그램 또는 취약점 종합(이력)관리시스템과 연동이 가능한가?
	3. 수동진단 가능성 ▣ 전자정부 웹취약점 진단 항목(21개)별 수동 진단 (웹프록시 기능 활용) 기능을 지원하는가? ▣ 전제 진단방식이 아닌 특정 점검항목에 대한 선택적 검증 기능이 있는가?
정확성(30)	1. 진단(점검) 결과 확인 ▣ 웹취약점 진단항목별 진단결과 확인이 가능한가? ▣ 웹취약점 정탐/오탐/미탐을 구분하여 탐지에 대한 정확성을 보장하는가? ▣ 취약점 진단대상 페이지의 스크린샷 및 주석 추가 기능을 제공하는가?
	2. 보고서 품질 ▣ 웹취약점 진단결과를 연계하여 조치항목에 대한 조치방법 및 상세가이드를 제공하는가? ▣ 웹취약점 진단기준을 이용한 레포팅 작성이 가능한가? ▣ 웹취약점 진단 보고서 양식 제공 기능이 가능한가?
사용성(10)	1. 진행상태 파악 용이성 ▣ 점검자가 수행하는 작업의 진행상태를 쉽게 파악할 수 있는 화면 제공이 가능한가?
	2. 운영환경 적합성 ▣ 사용자가 요구하는 사용 환경에 설치가 용이한가?
확장성(10)	1. 환경설정 및 기능 변경 가능성 ▣ 취약점 진단 기준 변경 시 커스터마이징 지원이 가능한가? ▣ 취약점 진단 정책별 라이브러리 업데이트 기능이 있는가? ▣ 취약점 진단 패턴추가, 수정, 삭제 등 사용자 정의 기능이 있는가? ▣ 요구사항별 커스터마이징 지원이 가능한가? ▣ 사용자별 진단 정책 설정 및 환경 설정 기능을 지원하는가? ▣ 결과 보고서 양식이 요구 사항에 맞게 커스터마이징이 가능한가? ▣ 발견된 취약점에 대한 화면캡쳐(스크린샷 기능)가 포함된 레포팅 기능을 지원 하는가? ▣ 벤더사 자동화 도구 진단 패턴 공개 및 커스터마이징이 가능한가?
	2. 로그관리 및 분석 ▣ 자동진단 내역의 로그 저장 관리 기능을 제공하는가? ▣ 자동진단 중 장애발생을 대비한 로그분석 기능을 제공하는가?
효율성(10)	1. 운용안전성 ▣ 웹취약점 자동진단 도구 운용 시 점검 대상 웹서비스 과부하 유발 및 장애발생 가능성이 있는가?
	2. 자원 사용률 ▣ 다수의 웹취약점 자동 진단 시 시스템 자원(CPU, 메모리, 저장공간 등) 사용이 적정하게 유지 되는가?
	3. 처리율 ▣ 웹취약점 자동진단 시 평균점검(1개 도메인 기준) 완료시간은?

2. 취약점 발견 결과 비교

홈페이지 3개 대상에 대한 수동 및 자동진단을 수행한 결과 수동진단에 발견된 취약점 중 자동진단을 통해 2개 제품에서는 크로스사이트 스크립트가 발견되었으

며, 한 개 제품에서는 취약점을 발견하지 못하였다.

수동 및 자동진단 결과를 [표 6]과 같이 정리하였다.

표 6. 수동 및 자동진단 결과 비교표 1차

구분		발견 취약점		
		Home	Home2	Home3
수동		5	4	3
자동	A	지연	1	미완료
	B	0	1	미완료
	C	0	0	미완료

수동진단에서 발견한 웹취약점을 자동진단 수행 시 발견하지 못한 사유를 상용 자동진단 제품의 진단패턴을 분석하여 [표 7]과 같이 정리할 수 있었다.

표 7. 수동진단 발견취약점 자동진단 시 미발견 사유

대상	취약점	미발견 사유
Home 1	디렉토리 인덱싱	디렉토리 인덱싱 진단 시 인젝션에 문제되는 구문까지 점검하므로 패턴을 제외하고 점검하여 검출되지 않음
	크로스사이트 스크립트	게시물 열람 시 파라미터에 크로스사이트 스크립트 구문 실행 부분은 진단이 되었으나, 게시물 및 작성 영역의 진단은 발견되지 않음
	자동화공격	게시물의 댓글 작성에 대한 자동진단 시 서비스에 영향을 주므로 제외하고 점검 이미지 업로드 샘플 주소에 대한 패턴 부재로 발견되지 않음
	파일업로드	이미지 업로드 샘플 주소에 대한 패턴 부재로 발견되지 않음
	위치공개	샘플페이지에 대한 패턴 부재로 발견되지 않음
Home 2	정보누출	로그인 실패 시 메시지를 통해 계정 존재여부 파악에 대한 패턴 부재로 발견되지 않음
	관리자페이지 노출	관리자페이지 주소에 admin단어가 포함되지 않아 (/oz70/server) 발견되지 않음
	위치공개	에디터 샘플페이지에 대한 패턴이 존재하지 않아 발견되지 않음
	데이터 평문전송	관리자페이지 진단 패턴 미흡으로 인한 페이지 미발견과 로그인 영역이 규격화 되지 않아 자동진단으로 발견하지 못함
Home 3	진단미완료로 비교 불가	

자동진단 특이사항으로 3번 홈페이지에 대해서는 3개 제품모두 수집 및 진단단계가 마무리 되지 않아 결과 산출이 되지 않았으며, A제품의 경우 1번 홈페이지 진단 시 일부 접속 장애가 발생하였다.

진단 시 스레드 값이 서버 환경에 맞지 않아 서버부하가 발생하여 지연 및 장애가 발생하는 것으로, 진단 도중 스레드 값을 변경하고 싶었지만 기능이 존재하지 않아 변경할 수 없었다. 자동진단 사용도구에서 지연 및 장애 발생 시 대처하는 부분에 대해 [표 8]과 같이 정리해보았다.

표 8. 응답지연 및 장애발생 대처

제품	구 분		
	응답지연 파악	장애발생 알림	진단 자동중지
A	점검로그	팝업알림	고급설정을 통한 자동중지 가능
B	점검로그	기능없음	불가능
C	점검로그	기능없음	불가능

3. 웹취약점 자동진단 도구 종합 평가

웹취약점 자동도구 검증 체크리스트를 바탕으로 자동진단 결과에 대해 기능성, 정확성, 사용성, 확장성, 효율성 5개 기준으로 상용제품에 대해 [표 9]와 같이 평가하였다.

표 9. 상용 자동진단도구 종합 평가표

평가부문	평가항목	상용 소프트웨어 제품		
		A	B	C
기능성(40)	자동진단 기능구현 완전성	25.3	12.3	14
	상호 운용성	3	3	3
	수동 진단 가능성	5	2.7	5
	소계	33.3	18	22
정확성(30)	자동진단 결과 확인	14.7	10.7	7.3
	보고서 품질	5	9	9
	소계	19.7	19.7	16.3
사용성(10)	실시간 진단 진행상태 파악 용이성	5	5	5
	운용환경 적합성	5	5	5
	소계	10	10	10
확장성(10)	환경설정 및 기능 변경 가능성	5	4.7	6
	로그관리 및 분석	1.7	1	0.3
	소계	6.7	5.7	6.3
효율성(10)	운용 안전성	4	4	1.3
	자원사용률	3	3	3
	처리율	3	3	3
	소계	10	10	7.3
합 계		79.7	63.4	61.9

A제품의 평가점수가 높은 이유는 자동진단 도구에 점검패턴에 대한 추가기능이 존재하여 해당 기능을 이

용하여 웹취약점에 대한 발견 정확도를 향상시킬 수 있었기 때문이다. 상용 자동진단 제품별 우수한점과 미흡한 점을 평가하여 [표 10]과 같이 정리해 보았다.

표 10. 자동진단 도구 제품별 종합평가 의견

제품	구분	내 용
A	우수한점	- 국내 및 해외에서 많이 사용되어 많은 기능 및 패턴정책을 포함하고 있으며 제품별로 진단패턴을 간단히 선택하여 진단이 가능함. - 로그화면을 통해 전반적인 점검내역 파악이 가능하며 장애발생 시 팝업창을 통한 장애 알림이 가능함
	미흡한점	- 많은 진단패턴을 내포한 만큼 진단결과 정오탐에 대한 분석시간이 많이 필요함. - 자동진단 도구 커스터마이징의 경우 제약적으로 벤더사에서 공통으로 승인한 부분만 가능함 - 진단패턴 추가는 가능하나 다량의 정책을 한꺼번에 입력할 수 없음
B	우수한점	- 21개 취약점에 대한 진단패턴을 지원함 - 자동진단 완료 시간이 타 진단도구에 비해 다소 빠름 진단패턴 및 보고서에 대한 커스터마이징이 가능함
	미흡한점	- 자동진단 시 일시정지가 불가능하여 부하 시 점검 취소 후 재 점검해야함 - 진단로그를 실시간으로 모니터링이 불가능하여 장애관련 파악이 어려움 - 다수 대상을 진단 및 관리하기 위한 환경이 부족함
C	우수한점	- 21개 취약점에 대한 진단패턴을 지원함 - 자동화진단 시 사용되는 진단패턴 확인 및 분석이 가능함 - 진단패턴 및 보고서에 대한 커스터마이징이 가능함
	미흡한점	- 다수 홈페이지 진단 시 일부 홈페이지만 일시정지 및 재실행이 불가능함 - 로그에 포함되는 항목이 적어 장애 및 진단내역 파악이 불가능 - 타 제품에 비해 취약점 검출 효율이 낮음

Ⅳ. 웹취약점 수동 및 자동진단 결과비교(2차)

1. 수동 및 자동진단 비교 2차 필요성 및 준비사항

수동 및 자동진단 결과비교 1차의 경우 자동진단 도구를 통해 수동진단으로 찾은 웹취약점의 발견이 가능한지 파악하고 대체 가능여부를 확인하려 하였으나, 표본이 적고 진단이 미완료된 상황이 발생하였다.

영향도에 따른 진단가능 웹취약점 항목 12개에 대한 대체 가능성을 추가적으로 비교하기 위해 사전에 자동진단도구에 해당항목에 대한 진단패턴을 검토한 후 자동진단을 수행하였다.

홈페이지별 자동진단 시 소요되는 시간과 서버부하 정도를 파악하여 진단수행에 문제점이 없는지 확인하고 수동진단 대비 취약점 발견 정확도를 비교하였다.

1차의 경우 3개 홈페이지 대상을 통해 비교하였으나, 2차에서는 진단 가능성 및 발견 정확도의 정확한 비교를 위해 8개 대상에 대해 진단을 수행하였다.

2. 수동 및 자동진단 2차 결과

1차와 같은 방법으로 취약점 자동 및 수동진단을 수행하였으며, 결과는 아래와 같이 정보대상, 제품, 소요시간, 발견취약점, 수동결과, 비고로 [표 11]과 같이 정리하였다.

서버부하는 모든 대상에서 발생하지 않아 제외하였다.

표 11. 수동 및 자동진단 2차 결과

대상	제품	소요시간	발견취약점	수동(8개)	수동(전체)	비고
Home 1	A	9시간 37분	2개	2개	6개	- 크로스사이트 스크립트 정탐 - 데이터 평문전송 정탐
	B	18분	1개			-데이터 평문전송 정탐
	C	1시간 42분	1개			-데이터 평문전송 정탐
Home 2	A	20시간 42분	1개	3개	3개	-크로스사이트 스크립트 정탐
	B	4시간 6분	0개			
	C	3시간 16분	0개			
Home 3	A	7시간 59분	1개	1개	3개	-크로스사이트 스크립트 정탐
	B	3시간 8분	1개			-크로스사이트 스크립트 정탐
	C	5분	0개			
Home 4	A	3시간 20분	1개	4개	5개	-크로스사이트 스크립트 정탐
	B	3시간 32분	2개			-크로스사이트 스크립트 정탐 -데이터 평문전송 정탐
	C	3분	0개			
Home 5	A	5시간 3분	1개	2개	3개	-크로스사이트 스크립트 정탐
	B	1시간 56분	1개			-크로스사이트 스크립트 정탐
	C	미완료	미완료			-SSL 관련 문제점 으로 진단 미완료
Home 6	A	26분	0개	2개	2개	
	B	5분	1개			-데이터 평문전송 정탐
	C	33분	0개			
Home 7	A	23시간 41분	1개	4개	5개	-자체 정체현상 발생 -크로스사이트 스크립트 정탐
	B	8시간 이상 (분석6%진행)	미완료			-정체현상은 없으나 조치기반 탐색 및 분석에 대한 패턴이 많아 미완료됨
	C	2시간 21분	1개			-크로스사이트 스크립트 정탐

대상	제품	소요 시간	발견 취약점	수동 (8개)	수동 (전체)	비고
Home 8	A	2시간 20분	1개	3개	5개	-데이터 평문전송 정탐
	B	8시간 3분	1개			-데이터 평문전송 정탐
	C	18분	0개			

home7에 대한 자동진단 시 A제품에서 자체적으로 정체현상이 발생하였다. 정체현상 발생 사유는 전자정부표준프레임워크로 홈페이지를 개발한 경우 파라미터 인자값에 취약점 패턴을 입력하면 에러페이지로 리다이렉션 되는데 있다. 이 현상을 A제품이 통신오류로 감지하여 취약점 진단패턴마다 일정시간 정지하였다가 전송하는데 문제점이 있다.

홈페이지를 구성하는 메뉴 및 배치된 컨텐츠의 양이 많거나, 상용 자동진단 제품의 진단패턴의 많고 적음에 따라 전체 진단소요시간의 차이가 발생하였다.

또한 에러페이지나 SSL 관련 문제점으로 자동진단 수행 시 지연되거나 미완료되는 경우도 발생하였다.

해당 결과를 통해 크로스사이트 스크립트나 데이터 평문전송 취약점에 대해서는 대체적으로 자동진단이 가능한 것으로 판단되며, 관리자페이지 노출, 위치공개 취약점은 발견하지 못하였다.

운영체제 명령어 실행과 웹 서비스 메소드 설정 공격 취약점의 경우 취약점이 발견되지 않아 자동진단 여부에 대한 검증이 이루어지지 못했다.

V. 효율적인 자동진단을 위한 개선방안

1. 자동진단 가능 항목에 대한 문제점 및 개선사항

영향도를 분석하여 웹취약점 진단항목 21개중 자동진단 가능항목 12개를 제안하였으며, 수동 및 자동진단 비교 1,2차를 통해 자동진단의 수동진단 대체 가능여부를 분석해 보았다.

웹취약점 자동진단 결과와 상용 자동진단 도구의 진단패턴 등을 분석하여 취약점 항목별 자동진단 시 문제점 및 가능성, 개선필요사항에 대해 [표 12]와 같이 정리해 보았다.

표 12. 점검항목별 자동진단 가능성 및 개선필요사항

취약점	내 용
크로스사이트 스크립트	▣ 문제점 - 규격화된 검색부분은 취약점을 발견하였으나 규격화되지 않은 파라미터를 통한 취약점은 발견하지 못함 ▣ 자동진단 가능성(O) - 규격화된 스크립트 영역이 대다수이므로 자동진단 가능함 ▣ 개선필요사항 - 규격화되지 않는 코드의 경우 일부 커스터마이징하여 개선이 필요
데이터 평문전송	▣ 문제점 - URL에 login.jsp, login.do와 같이 규격화되고 단순한 로그인 페이지에서만 SSL 적용 여부를 파악 - A제품의 경우 로그인이 가능한 경우에만 SSL적용 여부 판단 - 수동진단결과 규격화되지 로그인 영역에서 취약점이 발생하여 자동진단으로 발견하지 못함 ▣ 자동진단 가능성(O) - 규격화된 일반적인 로그인페이지에서는 자동진단이 가능함 ▣ 개선필요사항 - A제품의 경우 로그인이 성공하지 않더라도 진단되도록 방식에 대한 수정이 필요함 - 비규격화된 영역에서도 진단이 가능하도록 커스터마이징이 필요 - 로그인 주소가 login으로 시작하지 않는 경우에 대한 진단패턴 추가가 필요함
운영체제 명령 실행	▣ 문제점 - 자동진단이 가능하나 진단대상 모두 취약점이 없는 상태로 검증이 필요함 ▣ 자동진단 가능성(O) - 모든 제품에서 진단을 위한 기능을 지원하므로 바로 자동진단 가능 ▣ 개선필요사항 - 진단 시 일부항목의 경우 서버에 영향을 줄 수 있으므로 진단패턴을 세부적으로 선택하여 진단을 수행이 가능하도록 해야함
웹 서비스 메소드 설정공격	▣ 문제점 - 자동진단이 가능하나 진단대상 모두 취약점이 없는 상태로 검증이 필요함 ▣ 자동진단 가능성(O) - 모든 제품에서 진단을 위한 기능을 지원하므로 진단 가능
디렉토리 인덱싱	▣ 문제점 - 취약점 존재 폴더가 진단패턴에 없을 경우 취약점이 발견되지 않음 - C제품의 경우 서버에 영향도를 줄 수 있어 점검패턴을 제외하고 점검 ▣ 자동진단 가능성(△) - 진단패턴 추가 시 자동진단 가능 ▣ 개선필요사항 - 진단패턴 추가기능 필요 - C제품의 진단패턴을 세분화하여 영향도를 주지않도록 커스터마이징이 필요
약한 문자열 강도	▣ 문제점 - admin, guest, test 정도의 단순 계정에 대한 취약점 존재여부 파악 가능 ▣ 자동진단 가능성(△) - 진단패턴 추가 시 자동진단 가능 ▣ 개선필요사항 - 취약한 아이디, 비밀번호에 대한 진단패턴 추가 기능 필요 - 일부 제품에 경우 로그인 영역을 지정하여 진단할 수 있도록 개선이 필요함

취약점	내 용
관리자페이지 노출	▣ 문제점 - URL에 admin.jsp, admin.do처럼 단순한 패턴만 취약점 존재여부를 파악하므로 다양한 제품의 관리자페이지를 발견하지 못함 ▣ 자동진단 가능성(△) - 진단패턴 추가 시 자동진단 가능 ▣ 개선필요사항 - 서비스 중인 관리자페이지 URL 등을 진단패턴에 추가할 수 있는 기능 필요 - 많이 사용하는 제품들의 관리자페이지 URL에 대한 주소를 업데이트 시 제공 필요
위치공개	▣ 문제점 - 백업파일(.bak, .old)정도의 단순한 패턴만 취약점 존재여부를 파악하므로 다양한 제품의 디폴트 페이지 및 불필요한 페이지 진단이 어려움 - 수동진단 대비 에디터 샘플페이지 진단패턴이 존재하지 않아 취약점을 발견하지 못함 ▣ 자동진단 가능성(△) - 진단패턴 추가 시 자동진단 가능 ▣ 개선필요사항 - 전자정부프레임워크 및 에디터 샘플페이지에 대한 URL을 진단패턴에 추가할 수 있는 기능 필요
정보누출	▣ 문제점 - 서버정보 노출 관련 취약점 진단만 가능하므로 사용자 주요정보 노출, 로그인 시 문구 동일 여부 등 취약점 영역은 진단이 불가능함 ▣ 자동진단 가능성(X) - 서버정보 노출에 대해서는 자동진단 가능 - 로그인 실패 시 발생 문구를 인식기능을 도입 시 계정 존재 취약한 진단가능 - 사용자정보 및 문구의 경우 자동진단이 어려우므로 수동진단 병행 필요 ▣ 개선필요사항 - 로그인 실패 시 문구인식 기능 추가필요
불충분한 세션 관리	▣ 문제점 - 모든제품 동일 일정시간 동안 홈페이지를 사용하지 않을 경우 자동로그 아웃여부 파악기능 없음 - A제품의 경우 로그아웃 후 인증정보 유지여부만 취약점 점검 ▣ 자동진단 가능성(X) - 자동진단도구의 엔진자체를 수정해야하므로 커스터마이징이 어려움 - 자동진단 불가능 ▣ 개선필요사항 - 진단 전 로그인 정보 입력 시 일정시간 사용하지 않을 경우 자동로그아웃 여부를 파악하도록 엔진 수정 필요 - 일부 제품의 경우 로그아웃 후 인증정보 유지여부 파악 기능 추가 필요
경로추적 및 파일다운로드	▣ 문제점 - 파일다운로드 취약점의 경우 시도 시 서버에 영향을 줄 수 있으므로 제외하고 수행 ▣ 자동점검 가능성(X) - 홈페이지 현상을 모니터링 하면서 진단해야하므로 자동진단 불가능 ▣ 개선필요사항 - 알려진 다운로드 모듈에 존재 시 시스템 파일 다운로드 가능여부만 진단하도록 기능 추가 필요 - 다운로드 모듈에 대한 존재여부를 파악하여 진단원에게 목록을 제공하고 시도할 시스템 파일을 지정하게 하여 영향도 최소화
취약한 패스워드 복구	▣ 문제점 - 모든제품에서 해당 점검 기능 없음 ▣ 자동점검 가능성(X) - 아이디/비밀번호 찾기를 수행하여 취약한 패스워드를 복구해야하는 취약점이므로 자동진단 수행이 어려움 - 자동진단 불가능

위에서 분석하여 제시한 개선사항을 반영할 경우 자동진단 가능항목을 개선사항과 함께 [표 13]과 같이 요약하여 정리하였다.

표 13. 자동진단 가능항목과 개선필요사항

순	자동진단 가능 취약점	개선사항(비고)
1	크로스사이트 스크립트	비규격화 진단 개선
2	데이터 평문전송	비규격화 진단 개선
3	운영체제 명령 실행	세부 진단패턴 선택
4	웹 서비스 메소드 설정공격	-
5	디렉토리 인덱싱	점검패턴 추가기능 개선
6	약한 문자열 강도	점검패턴 추가기능 개선
7	관리자페이지 노출	점검패턴 추가기능 개선
8	위치공개	점검패턴 추가기능 개선
9	정보누출	로그인 실패 문구 인식
10	불충분한 세션 관리	자동로그아웃 및 인증정보유지 여부 파악 기능 개선
11	경로 추적 및 파일다운로드	알려진 다운로드 모듈에 대한 시스템 파일 다운로드

2. 자동진단 소요시간 관련 개선

웹취약점 자동진단 결과 홈페이지 메뉴 및 컨텐츠 양에 따라 적게는 2분에서 많게는 20시간 이상 소요되었으며, 상황에 따라 미완료된 홈페이지도 존재하였다.

메뉴 및 컨텐츠 양이 적어 1시간 이내로 진단이 가능한 홈페이지는 바로 자동진단이 가능하겠지만 20시간 이상 소요되는 상황인 경우 모니터링을 통한 진단의 이상유무(장애)파악에 한계가 있다.

따라서 자동진단에 대한 스케쥴링 기능을 추가하여 일정시간 진단을 수행하였으나, 완료되지 않은 경우 진단을 일시정지하고 차후에 이어서 진단을 이어서 수행할 수 있도록 중간에 정지하는 기능이 존재해야한다.

일부 상용제품의 경우 진단을 시도하면 중간에 정지가 불가능하고, 현재 진단상황을 저장하는 기능이 존재하지 않아 진단시간이 오래 걸리는 홈페이지의 경우 시도조차 불가능한 부분이 있다. 그러므로 진단을 일시중지하고 진단 수행 내용을 저장하는 기능이 제공되어야 한다.

또한 진단패턴을 세분화하여 진단원이 진단패턴을 선택함으로써 필요한 부분만 진단한다면 진단 소요시간을 단축시킬 수 있다.

3. 기타 개선사항

홈페이지 취약점 자동진단 시 장애 및 지연상황에 대비하기 위해서는 로그 기록 및 분석이 중요하다고 생각된다.

자동진단 시 현재 수행중인 진단내용을 로그을 통해 기록해야하며, 만약 진단패턴을 전송했을 때 지연현상이 발생한다면 알림을 통해 바로 안내하여 현재 홈페이지에 장애가 발생하였는지 판단해야한다.

물론 자동진단 도구에 홈페이지를 접속하여 지연현상 및 장애의 발생유무를 자동으로 판단해 준다면 더할 나위가 없다고 생각된다.

자동진단 상용도구 제품들은 로그는 저장하지만 분석도구를 제공하지 않고 저장된 로그를 메모장 및 문서편집 프로그램을 통해 열람한 후 일일이 분석해야하므로 불편함이 존재한다. 로그를 저장하는 기능과 더불어 분석도구가 같이 탑재된다면 문제점 사후 분석에 도움이 될 것이다.

Ⅵ. 결론

본 논문에서는 점점 증가하는 홈페이지로 인하여 웹취약점 진단대상이 증가하는 상황에서 수동진단만으로 모든 홈페이지를 진단하려면 진단인력이 계속적으로 증원되어야 한다. 웹취약점 진단항목 중 자동진단 가능항목 12개를 우선 제시하고, 1, 2차에 걸친 수동 및 자동진단 결과비교를 통해 수동진단을 자동진단으로 대체 가능한 웹취약점 항목을 파악하였다.

본 논문에서 제안하는 방법을 활용하여 웹취약점 자동진단 도구가 개선된다면 현재 수동진단 중인 취약점 중 11개 항목을 자동진단으로 대체할 수 있으며, 기존에 웹취약점 자동진단을 위해 판매되는 상용솔루션의 성능을 향상시킬 수 있다.

이에 따라 상용 솔루션의 웹취약점 자동진단 결과에 대한 신뢰를 증가시켜 상용솔루션을 구매하여 자동진단을 수행하는 기관 및 업체가 증가할 것이다.

자동도구를 사용한 모든 취약점 항목에 대한 취약점 진단은 현재 불가능하나 영역을 분리하여 수동진단과 자동진단을 병행한다면 조금 더 많은 대상에 대한 진단수행이 가능해지며, 수동진단을 통해 정밀진단이 필요한 영역에 더 많은 시간을 할애하여 안전한 홈페이지 운영환경 조성에 기여할 수 있을 것이다.

다만 운영중인 홈페이지를 대상으로 연구가 이루어진 상황으로, 서비스에 대한 영향도를 고려하여 12개 항목에 대한 수동 및 자동 진단결과를 비교한 것으로 9개 항목에 대한 부분은 제외되었다. 차후 전체 21개 항목에 대한 수동진단을 대체할 수 있도록 개선방안을 도출하기 위한 추가 연구가 필요하다.

참 고 문 헌

[1] 과학기술정보통신부, *2020년 인터넷 이용 실태조사 발표,* 2021.03.

[2] https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1363, 2021.10.13.

[3] 이재호, “웹 페이지 수행기능분석과 점검 우선순위를 활용한 모델기반 웹 취약점 점검,” 예술인문사회 융합멀티미디어 논문지, 제9권, 제3호, pp.727-736, 2019.

[4] 한국인터넷진흥원, *주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드,* 2021.03.

[5] https://owasp.org/Top10/, 2021.

[6] https://www.sans.org/top25-software-errors/, 2021.10.14.

[7] 한국인터넷진흥원, *(전자정부 SW 개발·운영자를 위한) 소프트웨어 개발보안 가이드,* 2019.11.

[8] 행정안전부, *웹취약점 점검 항목,* 2020.09.

[9] 최은정, 정휘찬, 김승엽, “크로스 사이트 스크립팅(XSS) 취약점에 대한 공격과 방어,” 디지털융복합연구, 제13권, 제2호, pp.177-183, 2015.

[10] 김광현, “웹 취약점 분석을 위한 프락시 시스템의 설계 및 구현,” 한국전자통신학회 논문지, 제9권, 제9호, pp.1011-1018, 2014.

[11] 장희선, “Web Vulnerability Scanner를 이용한 취약성 분석,” 융합보안논문지, 제12권, 제4호, pp.71-76, 2012.

[12] 이택진, 손수엘, “오픈 소스 웹 취약점 스캐너의 성능 분석,” 정보과학회지, 제36권, 제3호, pp.42-49, 2018.03.

저 자 소 개

김 태 섭(Tae-Seop Kim) 정회원

- 2016년 2월 : 국가평생교육진흥원 멀티미디어과 졸업
- 2014년 12월 ~ 현재 : 이글루시큐리티
- 2020년 3월 ~ 현재 : 배재대학교 사이버보안학과(석사과정)

〈관심분야〉 : 웹취약점, 정보보안, 소스코드 보안약점 진단

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 졸업
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 정보처리기술사