JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 29 No. 11, pp. 197-207, November 2024
https://doi.org/10.9708/jksci.2024.29.11.197

Research on Efficient Automated Web Vulnerability Inspection Methods

Tae-Seop Kim*, Ah Reum Kang**

*Student, Dept. of Cyber Security, Pai Chai University, Daejeon, Korea
**Professor, Dept. of Cyber Security, Pai Chai University, Daejeon, Korea

[Abstract]

In the modern Internet environment where web applications can be easily produced, this study aims to check how much manual inspection can be replaced through automatic inspection to solve the problem that it is difficult to secure sufficient stability of web application services only with manual inspection, identify improvements to the shortcomings, and reflect them in the automatic inspection solution. To this end, automatic inspection and manual inspection were compared and analyzed for 175 homepages using a commercial solution. As a result of the analysis, it was confirmed that automatic inspection is possible in 10 items out of 21 web vulnerability inspection items of the Ministry of Public Administration and Security. In particular, the top five items found the most accounted for about 80% of the total vulnerabilities, so the effectiveness of automatic inspection has been proven. However, items with complex structures are difficult to automatically check, so when manual inspection and automatic inspection are used complementarily, the efficiency of web vulnerability inspection can be maximized.

▸ **Key words**: Web vulnerabilities, automatic inspection of web vulnerabilities, automatic inspection, improvement measures, efficient automatic inspection

[요 약]

본 연구는 웹 애플리케이션을 손쉽게 제작할 수 있는 현대의 인터넷 환경에서, 수동점검만으로는 웹 애플리케이션 서비스의 안정성을 충분히 확보하기 어렵다는 문제를 해결하고자 자동점검을 통해 수동점검을 얼마나 대체할 수 있는지를 확인하고, 부족한 부분에 대한 개선사항을 파악한 후 이를 자동점검 솔루션에 반영하는 것을 목표로 한다. 이를 위해 상용 솔루션을 사용하여 175개의 홈페이지를 대상으로 자동점검과 수동점검을 비교 분석하였다. 분석 결과, 행정안전부의 웹 취약점 점검항목 21개 중 10개 항목에서 자동점검이 가능하다는 것이 확인되었다. 특히, 가장 많이 발견된 상위 5개 항목이 전체 취약점의 약 80%를 차지하여 자동점검의 실효성이 입증되었다고 볼 수 있다. 그러나 구조가 복잡한 항목은 자동점검이 어려워, 수동점검과 자동점검을 서로 보완하여 사용할 때 웹 취약점 점검의 효율성을 극대화할 수 있다.

▸ **주제어**: 웹취약점, 웹취약점 자동점검, 자동점검, 개선방안, 효율적인 자동점검

• First Author: Tae-Seop Kim, Corresponding Author: Ah Reum Kang
*Tae-Seop Kim (ktsdrive9@naver.com), Dept. of Cyber Security, Pai Chai University
**Ah Reum Kang (armk@pcu.ac.kr), Dept. of Cyber Security, Pai Chai University
• Received: 2024. 10. 14, Revised: 2024. 11. 04, Accepted: 2024. 11. 14.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

인공지능(AI)의 급속한 발전과 이용자 증가[1]로 인해 우리는 AI를 활용하여 이미지 생성, 언어 번역, 지식 검색 등을 쉽게 수행할 수 있는 사회에 살고 있다. 인공지능을 이용하여 과거에는 개발자를 통해서만 만들 수 있던 프로그램도 직접 만들 수 있으며, 클릭 몇 번만으로 손쉽게 홈페이지나 애플리케이션을 제작할 수 있는 시대가 되었다. 이러한 AI 기반의 홈페이지 제작이 가속화됨에 따라, 인터넷상에는 수많은 홈페이지가 운영되고 있으며, 이 때문에 대량의 데이터가 서로 전송됨에 따라 웹 애플리케이션에 대한 취약점 점검 수요도 함께 증가하고 있다. 클라우드 컴퓨팅 플랫폼 기업 Akamai에서 발간한 인터넷 현황 보고서[2]를 보면 2022년과 2023년에는 일일 300만~400만 건에 달하는 웹 애플리케이션 및 API 공격이 발생하고 있다고 한다. 또한, Verizon의 데이터 유출 조사 보고서[3]에 의하면 웹 애플리케이션 취약점을 악용한 공격이 이전보다 3배 이상 증가했으며, 이는 웹 애플리케이션의 무단 사용 및 취약점 악용에 대한 심각한 경고를 주고 있다. 급증하는 홈페이지와 웹 애플리케이션에 대해 수동으로 취약점을 점검하는 모의 해킹 방식은 시간과 비용이 많이 소요되기 때문에, 자동화된 웹 취약점 점검 도구의 필요성이 대두하고 있다. 이에 따라 다양한 오픈 소스 및 상용도구들이 개발되어 웹 취약점 자동점검이 활발히 이루어지고 있다. 본 논문에서는 기존에 연구된 웹 취약점 자동 진단의 개선방안[4]을 보완하여, 효율적인 웹 취약점 자동점검 방안을 연구하고자 한다. 자동점검을 통해 수동점검을 대체할 수 있도록 자동점검의 현황을 분석하고, 개선점을 반영하여 웹 취약점 자동점검의 가능성과 효과성을 검증하고 효율적인 웹 취약점 점검방안에 대해 제시하고자 한다.

II. Web Vulnerability inspection Method and inspection Items

2.1 Manual inspection of web vulnerabilities

웹 취약점 수동점검은 점검자가 로그인, 회원가입, 패스워드 복구, 게시판 등 홈페이지를 구성하고 있는 기능 등과 디레토리 구조 등을 먼저 크롤링하여 파악한 후 스캐너와 같이 자동점검 도구를 사용하지 않고, 웹 프록시 도구[5]를 사용하여 수동으로 홈페이지 구성요소에 점검패턴을 입력하여 웹 취약점이 홈페이지에 존재하는지 파악하는 점검이다. 수동점검은 자동점검보다 구조가 복잡하고 다양한 영역에 대해 심층적으로 취약점 분석이 가능하다는 장점이 있다. 다만, 수동점검은 점검자의 경험과 숙련도에 따라 홈페이지를 점검하는 방식이 달라지고[6], 점검자가 점검패턴을 일일이 입력해야 하므로 메뉴가 많거나, 파라미터가 많은 구조의 홈페이지는 모든 영역에 취약점을 찾지 못하고 빠뜨릴 수 있는 위험성도 존재한다.

2.2 Automatic inspection of web vulnerabilities

웹 취약점 자동점검은 자동점검 솔루션이나 스캐너 도구와 같이 도구를 사용하여 점검하는 방식[7]이다. 자동점검은 웹 취약점 점검자가 일일이 점검패턴을 입력하는 수동점검 방식과는 달리 프로그램에 고정된 알고리즘과 점검패턴을 차례대로 전송하여 되돌아오는 반응을 보고 취약점 존재 여부를 판별한다. 자동점검은 수동점검과 비교하여 점검이 빠르므로 많은 메뉴와 파라미터를 가진 홈페이지를 점검하는데 이점을 가진다. 다만, 복잡한 구조를 가진 기능에 자동점검을 하면 인식하지 못해 취약점 점검이 불가능할 수 있고, 오탐이 존재하여 해당 부분에 대한 분석에 시간이 소요되는 단점이 존재한다. 웹 취약점 자동점검 도구로는 OWASP ZAP[8], Burp Suite[9], Acunetix[10], Sparrow Dast[11], Web Security Checker[12], HCL AppScan[13], SecureGuard WSE[14] 등이 있다.

2.3 Web Vulnerability inspection Criteria

웹 취약점 점검기준으로는 대표적으로 OWASP에서 선정한 OWASP TOP 10[15], CWE/SANS TOP 25[16], 국정원 8대 취약점, 행정안전부 모바일 서비스 서버(웹·앱) 대상 보안취약점 점검기준(전자정부 서비스 점검기준) 21개[16], 주요통신 기반시설 기술적 취약점 분석·평가 방법 상세가이드 기준 웹 28개 항목[17]이 존재한다. 여러 개의 점검기준 중 본 논문에서는 행정안전부 점검방법 기준을 적용하였다.

III. Understand the status of automatic inspection of web vulnerabilities

3.1 Prepare to understand the status of automatic inspection in advance

웹 취약점 점검은 웹 취약점 점검업무에 어느 정도 숙련된 점검자가 웹 프록시 툴을 이용하여 홈페이지 구조를 분석한 후 각 홈페이지 구성요소(로그인, 회원가입, 게시판 등)에 취약점 점검패턴을 수동으로 입력하여 점검한다. 각 구성요소에 웹 취약점이 존재할 경우 점검패턴에 따른 반응이 점검

자에게 전송되며 점검자는 해당 반응을 보고 취약점 존재 여부를 파악하게 된다. 웹 취약점 자동점검으로 점검자들이 수동으로 수행하는 수동점검을 대체할 수 있는지와 대체가 바로 어렵다면 개선점을 파악하기 위해 웹 취약점 자동점검 솔루션을 분석해 보기로 하였다. 웹 취약점 자동점검에 대해 검증을 하기 위해 검증절차를 아래와 같이 검증대상 제품선정, 사전준비, 검증실시, 결과분석 평가의 4단계로 검증절차를 설정하였다. 해당 내용을 Table 1로 정리하였다.

Table 1. Automatic inspection verification procedure

구분	검증내용
검증대상 제품선정	·검증대상 업체 및 솔루션 확정 ·제품업체와 사전협의
사전준비	·기능·성능 검증 항목선정 ·검증 테스트 환경 구축 ·검증 세부 시나리오설정
검증실시	·점검결과 비교분석을 위한 수동점검 수행 ·수동점검 후 웹 취약점 자동화 점검 실시 ·웹 서비스 부하 및 장애여부 모니터링
결과분석	·제품별 웹 취약점 점검결과 산출물 분석 (수동점검 비교분석) ·산출물 분석을 통한 적용 적합 여부 작성

웹 취약점 수동점검을 바로 자동점검으로 대체하기 위해서는 현황을 파악하고 개선점을 파악한 후 바로 개선해야 하므로 무료로 배포된 솔루션보다는 상용으로 현재 판매되고 있는 상용 솔루션을 분석하는 게 좋을 것 같다는 판단을 먼저 하게 되었다. 웹 취약점 자동점검 상용 솔루션 중 비교검증에 참여 의사를 파악하여 3개 업체가 참여하기로 하였으며, 편의상 A,B,C 솔루션으로 부르기로 하였다. 웹 취약점 자동점검 솔루션 3개에 대한 비교분석을 위해 기능·성능 검증항목 선정, 검증 테스트 환경 구축. 검증 세부 시나리오를 설정하기로 하였다. 웹 취약점에 대한 기능 및 성능을 검증하기 위한 항목이므로 공통, 기능성, 정확성, 사용성, 확정성, 효율성의 총 6개 단계의 검증항목을 수립하였으며, 검증항목별로 세부내용을 Table 2와 같이 정리하였다.

Table 2. Automatic Inspection Verification Item

Category (points)	content
Common (5)	·CC인증 및 조달청 등록여부 ·점검기준 충족여부
functionality (30)	·사용자 요구 기능구현 여부 ·취약점 정·오탐 분류 가능여부 ·점검패턴 추가 가능여부 ·특정 프로그램 또는 이력관리 시스템과 연동 여부 ·특정 점검항목에 대한 선택적 검증 기능 여부
accuracy (30)	·점검항목별 점검결과 확인 여부 ·존재하는 취약점 발견 여부 ·점검결과를 연계하여 조치항목에 대한 조치방법 및 상세가이드 제공 여부
Usability (15)	·점검자가 점검 진행상태를 쉽게 파악할 수 있는 화면 제공 여부 ·사용자가 요구하는 사용 환경에 설치 용이 여부 ·대시보드를 통한 관리시스템 접근성, 직관성, 편의성, 효율성을 제공
Scalability (10)	·기능요구 커스터마이징 가능 여부 ·웹 취약점 수행내역 로그 저장 관리 기능 제공 여부
fficiency (10)	·자동점검 완료 시간의 적정성 ·운영 웹서비스 과부하 발생 및 장애 발생 여부

자동점검 3개 솔루션에 대한 동등한 검증환경을 구축하기 위해 동일한 사양과 환경을 설정한 서버를 할당하였으며, 각 서버에 솔루션을 설치하여 자동점검을 시행하기로 하였다. 웹 취약점 수동점검을 통해 점검하는 대상은 신규로 구축하는 홈페이지만 존재하지 않고 기존에 구축되어 운영 중인 홈페이지도 존재하기 때문에 두 케이스에 존재하는 홈페이지를 대상으로 수동점검과 자동점검을 진행하여 비교 분석하기로 하였다. 자동점검과 수동점검을 비교·분석하기 위한 세부 시나리오를 Fig. 1과 같이 정리하였다.

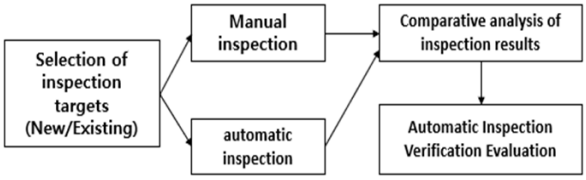

Fig. 1. Detailed scenarios for manual and automatic inspections

3.2 Preparing to understand the status of automated checks

신규구축 홈페이지 9개 대상과 기준운영 홈페이지 5개 대상에 대해 홈페이지 운영담당자와 협의하여 점검을 허락받아 점검을 진행하였으며, 자동점검 3개 솔루션을 웹 취약점 점검기준인 전자정부 서비스 웹 취약점 표준 점검항목과 주요정보통신기반 취약점 분석·평가 점검항목에 맞춰서 진행하여 결과를 Table 3으로 정리하였다.

Table 3. Results of new construction and existing operation inspection

Category	Manual inspection Vulnerability	Automatic inspection vulnerability		
		A	B	C
New(9)	20	0	2	0
Existing(5)	18	4	2	0
Total	38	4	4	0
Vulnerability Detection Rate (Automatic inspection vulnerability / Manual inspection vulnerability)		10.5%	10.5%	0%

전체적으로 수동점검 대비 자동점검 시 발견된 취약점 개수가 현저하게 낮았으며, 취약점 개수가 아닌 발견한 취약점 기준으로 Table 4로 정리하였다.

Table 4. Found vulnerability items

구분	발견취약점
A(2)	정보누출, 크로스사이트 스크립트
B(2)	웹 서비스 메소드 공격, 크로스사이트 스크립트
C(0)	-
수동점검 (12)	정보누출, 악성콘텐츠, 크로스사이트 스크립트, 약한 문자열 강도, 불충분한 인증 및 인가, 취약한 패스워드 복구, 자동화공격, 경로추적 및 파일다운로드, 관리자페이지 노출, 위치공개, 데이터 평문전송, 웹 서비스 메소드 설정 공격

자동점검 솔루션 A는 외산제품이다 보니 CC 인증이나 조달청에 등록되지 않았다. 또한, 자동점검 보고서에 대한 커스터마이징이 불가능하고, 별도의 추가적인 이력 관리 프로그램을 추가설치 하지 않는 이상 대시보드 기능이 존재하지 않아 통계확인 및 업무를 파악하는데 효율성이 낮았다. 다만, 기능완성도에서는 3개 솔루션 중 제일 높았다.

자동점검 솔루션 B는 국산제품으로 평가 당시 개발된 지 얼마 되지 않은 제품이라 CC 인증이 미완료되고 일부 기능이 미비된 상태였으나, 타제품과 비교하여 최신 트랜드에 맞는 대시보드 디자인과 사용성이 편리하게 개발되었다. 또한, 국산제품으로 일부 커스터마이징이 가능한 장점이 있었다. 자동점검 솔루션 C 제품은 국산제품으로 CC 인증 및 조달청 등록이 되어있고, 점검패턴을 추가하는 기능은 있으나, UI로 구현되지 않아 점검패턴을 일일이 입력해야 하는 번거로움이 존재하였다. 다만, 공정한 평가를 위해 점검패턴을 추가하지 않았다. 국산제품으로 일부 커스터마이징을 지원하는 것이 장점이나, 자동점검 결과 취약점을 발견하지 못해 정확성이 떨어졌다. 웹 취약점 자동점검 솔루션 3개에 대한 자동점검과 수동점검 비교결과에 대한 검증항목별 의견을 종합하여 평가점수를 Table 5로 정리하였다.

Table 5. Evaluation score by automatic inspection solution

Category	Evaluation score(100)		
	A	B	C
Common	4	4.5	5
functionality	20.5	20.5	19
accuracy	12	14	10
Usability	7	12	6
Scalability	5	5	3
fficiency	3	4	3
Total	51.5	60	46
Ranking	2	1	3

자동점검 솔루션 중 B제품이 사용성 부분의 높은 점수로 평가점수가 가장 높았으나, 3개 제품 모두 취약점 발견이 현저히 낮아 바로 도입하여 수동점검을 대체하기는 어렵다고 판단할 수밖에 없었다. 다만, 낮은 취약점 발견율을 개선한다면 자동점검이 수동점검을 대체할 수 있지 않을까 생각하여 개선사항 파악의 위해 자동점검 미발견 사유를 Table 6과 같이 정리하였다.

Table 6. Reasons for not detecting automatic inspection by vulnerability item

Vulnerabilities	Reason for non-discovery
Information leakage	·다양한 에러페이지에 대한 정보누출 점검 미비 ·정보누출 관련된 사전 파일경로 부족 ·응답 헤더에 버전 정보누출에 대한 점검 미비
Malicious content	·리다이렉션 테스트 구현 미비
Cross-Site Scripting	·"Change request method", "Change body encoding"를 통한 XSS 검증 미비 ·게시물 작성 시 입력한 패턴에 대한 점검 미비 ·일부 파라미터만 확인하고, 그 외 모든 파라미터값 XSS 검증 미비
Weak Strings Strength	·유추하기 쉬운 ID/PW 계정 정보 부족
Insufficient authen tication and authorization	·URL 변조에 대한 점검 관련 사전 정보가 부족 ·다양한 파라미터 값 변조 후 프로그램에서 취약점 여부 검증 불가 ·소스 코드상의 주석문 검증 미비 ·다른 사용자가 작성한 게시물이나 권한이 없는 게시판의 INDEX 값을 확인하여 별도의 테스트 미진행
weak password recovery	·변수값에 대한 다양한 자료 수집이 불가 ·본인인증 서비스에 대한 자동점검이 불가
Automated Attacks	·회원가입 시 자동공격 미진행
Trace paths and download files	·이미지 로드 모듈은 테스트 취약점 점검 미진행
Exposing the admin page	·프로그램에서 보유한 사전 경로 부족 ·일반적인 경로인 관리자페이지 판별 불가
Location disclosure	·프로그램에서 보유한 사전 경로 부족
Data plaintext transfer	·점검 URL 입력 시 443포트로 진행하여 80포트 취약점 점검 미진행
web service method configuration attacks	·불필요한 메소드 점검기준 요구한 기준과 다름

IV. Prepare for automatic inspection possibilities and improvements in advance

4.1 Possible improvements per autocheck item

제3장을 통해 웹 취약점 자동점검 솔루션을 이용하여 자동점검이 수동점검을 대체 가능한지 현황을 파악해 보았으나, 취약점 발견확률이 낮아 많은 개선이 필요한 것으

로 파악되었다. 자동점검의 취약점 발견확률을 올리기 위해서는 솔루션에서 점검 시 사용하는 점검패턴을 추가 및 개선하고 기능적인 부분도 수정이 필요하다고 생각되었다. 이에 따라, 자동점검 솔루션 업체들에 솔루션 개선작업 진행 여부를 협의하였으며 3개 업체 중 C 업체에서 개선작업에 참가 여부를 밝혀 해당 업체와 개선 관련 사전준비를 하게 되었다. 우선 점검항목별로 난이도와 개선 가능 여부를 인터뷰하여 Table 7로 정리하였다.

Table 7. Possibility of automatic inspection by inspection item

No	Inspection item	Level	Improvement
1	Run operating system commands	2	O
2	SQL Injection	3	O
3	XPath Injection	3	O
4	Directory indexing	1	O
5	Information leakage	2	X
6	Malicious content	3	X
7	Cross-site scripts	2	X
8	Weak string strength	2	O
9	Insufficient authentication and authorization	5	X
10	Recover weak passwords	5	X
11	Insufficient session management	3	X
12	Cross Site Request Forgery	5	X
13	Automated Attacks	5	X
14	Uploading file	4	O
15	Trace paths and download files	3	X
16	Exposing the admin page	2	O
17	location disclosure,	2	O
18	Data plaintext transfer	1	X
19	Cookie tampering	4	X
20	Web service method configuration attacks	1	O
21	URL/Parameter Modulation	5	X

4.2 Check Patterns feature added and check results

자동점검에 대해 개선점을 찾기 위해 홈페이지에 대한 웹 취약점 점검을 수동점검과 자동점검 둘 다 수행하여 자동점검으로 취약점을 미발견할 시 해당 내용을 정리 및 개선점을 파악한 후 자동점검 솔루션에 반영하여 지속적인 개선작업을 진행하기로 하였다. 개선점 파악을 위한 점검에 앞서 현황파악 시 제일 개선이 필요한 부분으로 점검항목별로 점검패턴이 솔루션에 미비한 것이 원인이었기 때문에 점검패턴을 추가할 수 있는 기능을 자동점검 솔루션에 Fig 2와 같이 배치하여 개선하였다.

Fig. 2. Additional screen of automatic inspection solution inspection pattern

웹 취약점 자동점검 솔루션에 점검패턴을 추가할 수 있는 기능을 배치한 후 신규 구축 중인 14개 홈페이지 대상으로 자동/수동 점검을 수행하고 결과를 Table 8로 정리하였다.

Table 8. Comparison of results before and after addition of inspection pattern

Category	an understanding of the current situation			Prepare in advance
	A	B	C	
Number of homepages	14			14
Manual inspection(A)	38			27
Automatic inspection(B)	4	4	0	7
Vulnerabilities Detection Rate(B/A)*100	10.5%	10.5%	0.0%	25.9%

웹 취약점 자동 점검 사전 준비를 총 14개 홈페이지에 진행한 결과, 수동 점검에서 27건의 취약점을 발견하였고, 자동 점검에서는 7건의 취약점을 발견하여 25.9%의 취약점 검출률을 기록하였다. 이는 3장에서 파악한 자동 점검 취약점 검출률과 비교했을 때, 개선 작업에 참여한 C 업체의 검출률이 0%에서 25.9%로 증가한 것으로 분석되었다. 그러나 25.9%의 검출률로는 자동 점검이 수동 점검을 대체하기에는 매우 낮은 수준이므로, 추가로 취약점 검출률을 개선하기 위한 연구를 계속 진행하기로 하였다.

V. A Study on the Improvement Direction of Automatic Inspection

5.1 Automated Web Vulnerability inspection First Round of Improvement Research

웹 취약점 자동점검 개선 사전작업을 통해 점검패턴 기능을 추가한 후 라이브러리를 추가하고, 일부 점검항목에 대한 점검패턴을 추가하여 일부 항목에 대해 점검이 가능하도록 설정하였다. 하지만 자동점검이 아직 되지 않는 항목에 많고, 자동점검에 대한 정확성을 검증하기에는 대상이 아직 부족하다고 판단하여 신규 및 기존운영 중인 홈페이지에 대해 자동점검과 수동점검을 수행하여 비교분석을 통해 자동점검 패턴을 개선하여 자동점검에 대한 정확도를 높이고자 하였다. 우선 사전준비 시 미발견된 항목인 웹 서비스 메소드 설정 공격과 위치공개의 진단패턴을 개선하고, 크로스사이트 스크립트 중 Multipart/form-data에 대한 진단이 가능하도록 수정하였다. 자동점검 기능을 개선한 버전으로 54개 홈페이지 대상에 대해 자동점검을 진행하여 수동점검과 비교·분석한 내용을 Table 9로 정리하였다.

Table 9. Analysis of the Results of the First Improvement Study for Automatic Inspection

Vulnerabilities	Manual	Automatic	Frequency	detection rate
Web service method configuration attacks	28	25	20%	89%
Cross-site scripts	23	6	16%	26%
location disclosure,	21	19	15%	90%
Information leakage	20	8	14%	40%
Exposing the admin page	14	13	10%	93%
Data plaintext transfer	8	0	6%	0%
Weak string strength	3	1	2%	33%
Malicious content	1	0	1%	0%
Trace paths and download files	2	0	1%	0%
Other (remaining items)	21	0	15%	0%
Total	141	72	100%	51%

자동점검으로 수동점검을 비교·분석한 결과 수동점검으로 발견한 취약점은 141건이었으며, 자동점검으로는 72건의 취약점을 탐지하여 총 51%의 진단율을 기록하였다. 사전준비 점검 시 기록한 25.9%보다는 개선되었다고 판단되나 많은 개선이 필요해 보였다. 세부항목으로 보면 웹 서비스 메소드 설정 공격은 28건 중 25건을 위치공개는 21건 중 19건을 탐지하였고, 관리자페이지 노출은 14건 중 13건을 탐지하여 각각 89%, 90%, 93%의 점검률을 기록하여 자동점검으로 충분히 점검이 가능한 것으로 분석되었지만, 크로스사이트 스크립트는 23건 중 6건만 발견되었고, 정보누출은 20건 중 8건, 데이터 평문전송은 8건 중 0건을 발견하여 해당 항목에 대해서는 개선이 많이 필요한 것으로 분석되었다. 수동점검 및 자동점검 비교분석을 하다 보니 상위 5개 항목인 '웹서비스 메소드 설정 공격, 크로스사이트 스크립트, 위치공개, 관리자페이지 노출'의 취약점 개수가 전체 21개 항목 중 75%를 차지하는 것으로 나타났으며, 데이터 평문전송 까지 포함한다면 전체 취약점 중 80%에 달하는 취약점에 대해 자동점검이 가능한 것으로 판단되었다. 이 부분을 검증하기 위해 최근 3년간 진행된 수동점검 결과를 분석하여 5개 항목이 차지하는 비율을 조사해 보기로 하였다. 최근 3년간 수동점검하여 발견된 취약점 현황을 Table 10으로 정리하였다.

Table 10. Results of manual inspection conducted over the past three years

Vulnerabilities	`21	`22	`23	Total
Cross-site scripts	398	237	219	854
location disclosure,	213	269	282	764
Information leakage	139	178	219	536
Web service method configuration attacks	6	242	283	531
Exposing the admin page	87	136	170	393
Insufficient authentication and authorization	106	125	138	369
Automated Attacks	108	59	38	205
Trace paths and download files	47	37	25	109
Data plaintext transfer	32	27	25	84
Uploading file	30	30	19	79
Other (remaining items)	59	52	28	139
Total	1,225	1,392	1,446	4,063

해당 결과를 분석해 보니 상위 5개 취약점의 개수가 전체 취약점 대비 각각 68.8%, 76.3%, 81.1%의 비율을 보여 자동점검으로 5개 항목이 가능하다면 어느 정도 수동점검을 대체할 수 있다고 판단되었다. 따라서 개선이 많이 필요한 크로스사이트 스크립트와 정보누출에 대해 중점적으로 개선하기로 하였고, 90%가량 진단한 3개 항목(웹 서비스 메소드 설정 공격, 위치공개, 관리자페이지 노출)도 추가적인 개선을 해보기로 하였다.

5.2 Automated Web Vulnerability inspection Secondary Improvement Research

웹 취약점 자동점검 1차 개선연구에 이어 2차로 개선연구를 진행하면서 정보누출과 크로스사이트 스크립트 2개 항목에 대해 집중적으로 개선하기로 목표를 설정하였다.

그리고 각각 점검항목별로 홈페이지에 취약점이 여러 개 유형이 존재할 수 있으므로 취약점 별로 세분화하여 점검된 유형을 나누어 기록하고 개선해 보기로 하였다. 웹 취약점 자동점검 2차 개선연구에 들어가기에 앞서 1차 개선연구 시 개선이 필요한 내용을 자동점검에 반영하였으며, 개선내용을 Table 11로 정리하였다.

Table 11. Organizing the 1st improvement of automatic inspection

Inspection	Details of improvement
Information leakage	·웹 서버 버전 정보 제공 취약점 ·에러 메시지에 포함된 PHP 버전 정보 유출 ·취약한 Javascript Library 버전 사용
Malicious content	·URL Redirection 조작 가능
Cross-site scripts	·multipart/form 변경 시 실행되는 취약점 ·크로스사이트 스크립트 점검패턴 추가 2건
location disclosure,	·사전 페이지 점검 모듈 수정 ·추측 가능한 파일 이름으로 인한 사용 ·Tomcat status 페이지 노출 취약점 ·위치공개 점검패턴(URL) 추가
Data plaintext transfer	·데이터 평문전송 취약점 패턴 추가 ·관리자 콘솔 로그인 평문전송 추가

개선 부분에 대해 검증하기 위해 48개 홈페이지에 대해 자동점검을 수행하고 1차 개선연구와 비교·분석하여 결과를 Table 12로 정리하였다.

Table 12. Results of 2nd improvement inspection

Category	1st improvement	2nd improvement
Number of homepages	54	48
Manual inspection(A)	141	152
Automatic inspection(B)	72	81
Vulnerabilities Detection Rate(B/A)*100	51.06%	53.29%

웹 취약점 전체항목을 기준으로 2차 개선연구 결과가 1차 개선 연구결과보다 2%가량 개선되었으나 의미 있는 개선이 진행되었다고 판단하기 어려웠다. 또한, 전체 취약점 검출률이 53.29%로 자동점검이 수동점검을 대체하기에는 취약점 검출률이 매우 낮은 상태로 많은 개선이 필요한 것으로 분석되었다. 웹 취약점 자동점검 개선연구 2차를 통해 자동점검 개선 여부를 확인하기 위해 취약점 점검항목별 취약점 검출률을 계산하였으며 결과를 Table 13으로 정리하였다.

Table 13. Analysis of the results of secondary improvement research on automatic inspection

Vulnerabilities	Manual	Automatic	detection rate	1st improvement
Web service method configuration attacks	35	29	82.9%	89%
Cross-site scripts	29	10	34.5%	26%
location disclosure,	22	16	72.7%	90%
Information leakage	26	7	26.9%	40%
Exposing the admin page	19	13	68.4%	93%
Data plaintext transfer	9	6	66.7%	0%
Other (remaining items)	12	0	0.0%	0%
Total	152	81	53.3%	51%

1, 2차 개선연구 결과를 점검항목별로 비교했을 때 크로스사이트 스크립트는 26%에서 34.5%로 취약점 검출률이 증가하였고, 데이터 평문전송 취약점은 0%에서 66.7%로 증가한 것을 확인할 수 있었다. 다만, 다른 항목에 대한 취약점 검출률이 하락하여 개선에 대해 많은 고민이 필요한 상태로 보였다. 취약점 검출률이 하락한 원인을 파악해 본 결과 웹 취약점 자동점검 시 URL이 미수집되어 취약점이 존재하는 영역을 점검하지 못해 취약점을 미발견한 것이 제일 큰 것으로 분석되었다. 따라서 차후 개선연구에서는 URL 수집 엔진을 개선하여 취약점이 존재하는 URL을 전부 수집할 수 있도록 수정이 필요해 보였다. 따라서 웹 취약점 자동점검 솔루션 업체에 URL 수집 엔진에 대한 개선을 요청하였고, 해당 개선점이 반영된 후 웹 취약점 자동점검 3차 개선연구를 진행하기로 하였다.

5.3 Automated Web Vulnerability inspection 3rd Improvement Research

웹 취약점 자동점검 2차 개선연구를 진행하여 발견된 개선 필요 사항을 자동점검에 반영하였다. 개선내용을 Table 14로 정리하였다.

Table 14. Organizing the 2nd improvement of automatic inspection

Inspection	Details of improvement
Information leakage	·개인정보(주민번호, 이메일 등) 유출 취약점 ·MySql, Jsp 데이터베이스 에러메시지 ·개인정보(핸드폰번호) 정보누출 ·Fragment 식별자(#) 에러로 버전정보 노출
Cross-site scripts	·오버플로우로 인한 XSS 취약점 패턴 개선 ·multipart/form-data 파서 수정 ·크로스사이트 스크립트 점검패턴 추가
Exposing the admin page	·표준프레임워크에서 제공파일 노출 취약점 ·HTTP 메소드로 인한 관리자페이지 노출 ·LogonSpnge 패턴 추가
location disclosure,	·점검패턴 추가
Data plaintext transfer	·취약한 ID/PW 설정 취약점 ·점검패턴(기본경로) 추가
Web service method configuration attacks	·취약한 HTTP 메소드(TRACE-upper) 허용

적용된 개선사항의 검증을 위해 45개 홈페이지에 대해 점검결과를 분석하였으며, 결과를 1~2차 점검결과와 비교하여 Table 15로 정리하였다.

Table 15. Results of 3rd improvement inspection

Category	1st improvement	2nd improvement	3rd improvement
Number of homepages	54	48	45
Manual inspection(A)	141	152	130
Automatic inspection(B)	72	81	87
Vulnerabilities Detection Rate (B/A)*100	51.06%	53.29%	66.92%

자동점검 3차 개선연구를 통해 취약점 검출률은 2차 결과보다 13.6% 정도 상승한 66.92% 기록하였다. 취약점별로 자동점검 및 수동점검에 대한 취약점 검출률을 Table 16으로 정리하였다.

Table 16. Analysis of the results of the 3rd improvement research on automatic inspection

Vulnerabilities	Manual	Automatic	detection rate	2nd
Web service method configuration attacks	23	24	104.3%	83%
Cross-site scripts	17	19	111.8%	34%
location disclosure,	19	13	68.4%	73%
Information leakage	25	13	52.0%	27%
Exposing the admin page	15	10	66.7%	68%
Data plaintext transfer	12	7	58.3%	67%
Other (remaining items)	19	1	5.3%	0%
Total	130	87	66.9%	53%

자동점검과 수동점검을 취약점별로 검출률을 비교·분석한 결과 웹 서비스 메소드 설정 공격은 수동점검으로 23건, 자동점검으로 24건을 발견하여 기존에 수동점검으로 발견된 취약점을 전부 발견하고 다른 유형의 취약점 1건을 발견하여 104.3%의 검출률을 기록하였다.

크로스사이트 스크립트 취약점은 수동점검으로 발견된 17건 중 8건을 발견하였으나, 다른 유형의 취약점을 11건 추가 발견하여 111.8%의 취약점 검출률이 도출되었다. 또한, 미발견된 취약점 자체가 게시물 작성 및 특정 페이지 접속 시에만 발견되는 취약점이 다수여서 해당 영역은 자동점검으로 점검하기 어려운바 자동점검이 수행 가능한 영역에 대해서는 자동점검이 가능한 것으로 분석되었다.

위치공개는 수동점검 발견취약점 19건 중 자동점검으로 13건이 발견되어 68.4%가 발견되어, 취약점 점검패턴에 대해 지속해서 업데이트하여 미발견을 줄이는 쪽으로 지속적인 개선이 필요한 것으로 분석되었다.

정보누출 취약점은 수동점검 발견 25건 중 자동점검으로 13건이 발견되어 2차 개선보다 25% 정도 개선되었다. 정보누출 취약점에 대한 자동점검이 개선되려면 자동점검 솔루션의 URL 인식기능이 더 개선되어 미수집되는 URL이 없도록 개선되어야 하나, 많은 URL을 점검할 경우 자동점검 시간이 늘어나고 운영 중인 서버는 부하를 줄 확률이 증가하기 때문에 조심스럽게 접근할 수밖에 없는 문제로 보였다.

관리자페이지 노출 취약점은 취약점 검출률이 2차와 크게 다르게 않았으며, 데이터 평문전송은 8% 하락하여 차후 개선이 필요해 보였다. 하지만 점검패턴이 존재하면 취약점을 발견할 수 있으므로 자동점검 가능 항목으로 설정하고 지속적인 업데이트를 통해 취약점 검출률을 상승시키는 게 나을 것으로 판단되었다.

웹 취약점 자동점검 1차 개선연구에서 파악한 바와 같이 수동점검으로 발견하는 21개 취약점 중 5개 취약점(크로스사이트 스크립트, 위치공개, 정보누출, 웹 서비스 메소드 설정 공격, 관리자페이지 노출)이 전체 발견취약점의 80%가량을 차지하는바 해당 취약점을 위주로 개선작업을 하였으며, 사전준비 점검 시 기록한 취약점 검출률을 25.9%에서 66.92%까지 개선할 수 있었다.

5.4 Possibility of utilizing automatic inspection by inspection item

웹 취약점 자동 점검을 통해 수동 점검을 대체할 수 있는 항목과 대체를 할 수 없는 항목을 구분하여 활용 가능성을 파악하고자 했다. 웹 취약점 개선연구를 통해 개선사항을 반영한 6개 항목과 취약점은 발견되지 않았으나, 업

체의견으로 자동점검이 가능한 4개 항목을 종합하여 총 10개 항목이 자동점검을 활용하여 점검이 가능한 것으로 판단되어 그 항목들을 Table 17로 정리하였다.

Table 17. Inspection items available for automatic inspectio

No	Inspection item	Remarks
1	Run operating system commands	
2	SQL Injection	
3	XPath Injection	
4	Directory indexing	
5	Information leakage	Some areas are not automatically scanned ex) ID, password
6	Cross-site scripts	Some areas are not automatically scanned ex) Writing
7	Exposing the admin page	
8	location disclosure,	
9	Data plaintext transfer	
10	Web service method configuration attacks	

자동점검이 불가능한 11개 항목의 경우 글쓰기, 파라미터 변조, 불분명한 입력값 등 때문에 자동점검 진행이 불가능하였으며, 취약점 항목별로 자동점검이 어려운 사유를 Table 18로 정리하였다.

Table 18. Vulnerability items and reasons for automatic inspection

No	Inspection item	Difficult reason
1	Insufficient authentication and authorization	글쓰기 영역 점검불가, 구조의 복잡성
2	Recover weak passwords	패스워드 복구 시 요구정보 다양화
3	Cross Site Request Forgery	글쓰기 영역 점검불가
4	Automated Attacks	
5	Uploading file	
6	Cookie tampering	구조의 복잡성
7	URL/Parameter Modulation	글쓰기 영역 점검불가, 파라미터 변조 후 비교 분석 불가
8	Insufficient session management	자동점검 항목 추가 발굴 검토 추진 (수시점검으로 진행)
9	Malicious content	
10	Weak string strength	
11	Trace paths and download files	

5.5 Utilization for Efficient Automatic Inspection

웹 취약점 자동점검으로 수동점검을 전부 대체하면 좋겠지만, 현실적으로 불가능하며, 자동점검이 가능한 10개 항목의 경우 취약점 유형에 따라 발견하지 못할 수 있으므로 점검자가 수작업으로 진행하는 수동점검(모의 해킹)을 병행하여 진행할 수밖에 없다고 판단된다. 다만, 수동점검은 1개 홈페이지를 연 1회를 초과하여 점검이 어려우므로 한번 점검하고 다음 점검 시점이 오기까지는 메뉴 추가나 부분리뉴얼을 통해 발생할 수 있는 취약점에 대해 점검 및 조치를 할 수 없다. 자동점검을 통해 연 1회 점검이 아닌 홈페이지 운영자가 필요할 때마다 점검을 진행하여 발견빈도가 높은 취약점을 발견하고 조치하는 데 활용할 수 있을 것이다. 또한, 자동점검을 통해 발견된 취약점을 종합하여 수동점검 시 해당 취약점을 조치하였는지 확인하고 조치가 안 됐을 때 조치할 수 있도록 피드백한다면 홈페이지 운영에 안전성을 충분히 확보할 수 있을 것이다. 기존 수동점검 방식과 자동점검을 혼합하여 점검하는 방식에 대해 Table 19로 정리하였다.

Table 19. Manual and Automatic Inspection Mixing Inspection Method

Inspection	1	2~3	4~5	6~7	8~9	10~12
Manual inspection	Demand survey, schedule establishment	A	C	E	G	Verifying vulnerability actions and notifying results
		B	D	F	H	
Automatic inspection		E	G	A	C	
		F	H	B	D	
	Issue occurrence and inspection if necessary					

현재 취약점 점검을 수행하는 방식은 1월에 점검계획을 수립한 바탕으로 2~9월에 취약점 점검을 수행한 후 발견된 취약점을 10~12월에 조치하고 있다.

점검대상 A~H가 있을 때 A에 2~3월 수동점검을 수행하고 나면 다음 웹취약점 점검은 다음연도에 수행하게된다. 이 공백을 최소화하기 위해 점검대상 A~H 점검 시 자동점검과 수동점검 일정을 교차로 배치하고 점검결과를 공유하여 미발견 취약점을 최소화할 수 있다. 또한, 자동점검은 이슈가 발생하거나, 필요한 경우 언제든지 점검을 추가로 진행할 수 있으므로 매년 증가하는 사이버 공격 대응에 도움이 될 것이다.

VI. Conclusions

6.1 Research Results and Implications

본 연구에서는 웹 취약점 자동점검의 개선사항을 파악하고, 사전준비와 1~3차에 걸친 개선연구를 통해 취약점

검출률을 초기 0%에서 66.92%로 개선할 수 있었다. 또한, 3년간 수동점검으로 발견된 취약점 현황을 분석한 결과, 상위 5개 취약점(크로스사이트 스크립트, 위치공개, 정보 누출, 웹 서비스 메소드 설정 오류, 관리자 페이지 노출)이 전자정부 서비스의 21개 항목 중 약 80%를 차지하는 것으로 나타났다. 이 5개 취약점의 검출률만 개선해도 자동점검이 수동점검을 상당 부분 대체할 수 있다는 가능성을 확인할 수 있었다. 그러나 게시물 작성 부분에서 발생하거나 구조가 복잡한 경우에는 자동점검이 한계가 있어, 수동점검이 병행되어야만 안정성을 확보할 수 있다. 수동점검인 모의 해킹은 많은 시간이 소요되기 때문에 1개의 홈페이지에 대해 빈번한 점검이 어렵다. 따라서 자동점검을 통해 주요 취약점 유형을 여러 차례 점검함으로써, 수동점검 사이의 공백기에 발생할 수 있는 위험성을 예방할 수 있을 것이다. 웹 취약점 점검항목별로 새로운 점검패턴이 계속해서 발생하기 때문에, 지속적인 수동점검과 자동점검의 비교·분석을 통해 자동점검을 업데이트한다면, 검출률을 더 개선하고 자동점검으로 대체 가능한 영역을 확장할 수 있을 것이다.

6.2 Research limitations and future research tasks

웹 취약점 자동점검을 운영 중인 홈페이지에 적용할 경우, 게시물과 같이 작성된 데이터가 많은 경우 점검 시간이 길어지며, 이 때문에 서버 부하가 발생해 홈페이지가 느려지거나 접속 장애가 발생할 가능성이 있다. 이를 방지하기 위해, 본 연구에서는 접속자가 적은 야간 시간대(19시 이후)에 자동점검을 진행하여 부하를 최소화하였다. 그러나 야간에만 자동점검을 수행할 경우 한정된 시간 내에 점검을 완료해야 하고, 모니터링 인력이 야간에 업무를 수행해야 하는 부담이 발생한다. 따라서 자동점검을 24시간 동안 원활하게 수행하는 방법을 모색할 필요가 있다.

또한, 자동점검 시 발생하는 부하를 최소화할 수 있는 기술적 방법을 연구하고 적용하는 것이 향후 과제로 남아 있다. 현재 전자정부 서비스의 21개 항목 중 10개 항목만 자동점검이 가능하므로, 나머지 11개 항목에 대해서도 자동점검을 적용할 수 있도록 연구가 필요하다.

ACKNOWLEDGEMENT

This work was supported by the research grant of Pai Chai University in 2024.

REFERENCES

[1] National Statistical Portal, Artificial Intelligence (AI) technology and services used, 2024.02.
[2] Akamai, SOTI Report, 2023.11.
[3] Verizon business, 2024 Data Breach Investigagions Report, 2024
[4] Tae-Seop Kim, In-June Jo, “Improvement Mechanism for Automatic Web Vulnerability Diagnosis”, The Journal of the Korea Contents Association, v.22 no.2, pp 125-134, 2022
[5] Kim, Gwang-Hyun, "Implementation and Design of Proxy System for Web vulnerability Analysis", The Journal of The Korea Institute of Electronic Communication Sciences, ,Vol.9, No.9, pp.1011-1018, 2014
[6] Jae-Ho Lee, “Model-based Web Vulnerability Inspection Using Web Page's Function Analysis and Inspection Priority”, The Convergent Research Society Among Humanities, Sociology, Science, and Technology, Vol.9, No.3, pp.727-736. 2019
[7] Jang Hee-Seo, "WVulnerability Analysis using the Web Vulnerability Scanner", Convergence security journal, v.12, no.4, pp.71-76, 2012
[8] OWASP ZAP, https://www.zaproxy.org/
[9] Burp Suite, https://portswigger.net/burp
[10] Acunetix, https://www.acunetix.com/
[11] Sparrow Dast, https://sparrow.im/kr/product/dast/
[12] Web Security Checker, https://www.ncloud.com/product/security/webSecurityChecker
[13] HCL AppScan, https://www.hcl-software.com/appscan
[14] SecureGuard WSE, http://www.nilesoft.co.kr/
[15] https://owasp.org/Top10/
[16] https://www.sans.org/top25-software-errors/
[17] The Ministry of Public Administration and Security's criteria for checking security vulnerabilities for mobile service servers (webs and apps). 2014.11
[18] Korea Internet & Security Agency, Detailed Guide to Analysis and Evaluation of Technological Vulnerabilities in Major Information and Communication Infrastructure, 2021.03
[19] YeongSik Pak, “An Empirical Study on the Web Vulnerabilities Analysis Model of Homepages”, TDepartment of IT Policy Management Graduate School of Soongsil University. 2021
[20] Jeongwon Choi, Gunwoo Jeong, Youngkyung Choi, Junwon Heo, Jaeyoung Jang, Haho Choi, Yongkwon Jo, & Joowon Kim (2024-01-31). Proposal of a Web Vulnerability Automated Assessment Framework Using AI. Proceedings of Symposium of the Korean Institute of communications and Information Sciences, Gangwon. 2024
[21] Young-Bok Cho. Secure Coding for SQL Injection Prevention Using Generative AI. Journal of the Korea Society of Computer and Information , 29(9), 61-68. 2024

Authors

Tae-Seop Kim received the M.S. degrees in Computer Science and Engineering from Pai Chai University, Korea, in 2022. he is currently pursuing Ph.D. degree in the Department of Cyber Security at Pai Chai University. His research interests are web vulnerabilities, source code security weakness diagnosis, system security, and artificial intelligence.

Ah Reum Kang received the M.S. and Ph.D. degrees in information security from Korea University, South Korea, in 2012 and 2016. She is a professor in the Department of Information Security at Pai Chai University in Daejeon, South Korea. Her current research interests include security, artificial intelligence, malware, medical data analysis, and online game security.