인공지능을 활용한 웹 취약점 자동화 진단 프레임워크 제안

최정원, 정건우, 최영경, 허준원, 장재영, 최하호, 조용권, 김주원*

KITRI 화이트햇 스쿨 1기(멘티), *KITRI 화이트햇 스쿨 1기(멘토)

{ally01choi, geoun395, va1ue.cyk, jwcs1768, jjy200812, imhaho, fish4240, *arresterloyal}@gmail.com

Proposal of a Web Vulnerability Automated Assessment Framework Using AI

Jeongwon Choi, Gunwoo Jeong, Youngkyung Choi, Junwon Heo, Jaeyoung Jang, Haho Choi,

Yongkwon Jo, Joowon Kim*

KITRI Whitehat School 1st (Mentee), *KITRI Whitehat School 1st (Mentor)

요 약

초연결 사회에서 인터넷상에서의 정보가 증가함에 따라 IT 자산의 보안 중요도가 함께 증가하였다. 이에 따라 외부와의 접점이 존재하는 웹 어플리케이션의 취약점을 진단하는 다양한 연구가 진행되고 있다. 기존의 웹 취약점 자동화 진단 도구는 주로 단일화된 취약점을 대상으로 설계되며, 도구의 스캐닝 옵션이 방대하여 적절하지 않게 사용하는 경우 진단 대상의 가용성을 침해하는 위험성이 있다. 따라서 오픈소스로 공개 되어있는 다양한 웹 취약점 진단 도구를 비교, 분석하고, 분석 결과를 활용하여 가용성 침해를 유발할 수 있는 스캐닝 옵션을 파악하는 것이 중요하다. 본 논문에서는 인공지능을 활용한 취약점 진단 및 추가적인 정밀 진단을 수행하여 취약점 진단 결과의 정확도가 기존 대비 높음을 보였다. 또한, 취약점 진단이 완료된 후 인공지능을 활용한 취약점 진단 보고서를 제공함으로써 사용자에게 상세한 진단 결과를 제공하는 프레임워크를 제안하였다.

Ⅰ. 서 론

오늘날 초연결 사회로 접어들면서 인터넷상에서의 정보가 방대해짐에 따라 IT 자산에 대한 보안의 중요성이 대두되고 있다[1]. 외부와 접점이 발생하는 웹 어플리케이션의 보안성이 취약한 경우 기업과 개인의 정보가 외부자에게 유출되는 등 위험성이 존재한다. 이러한 보안 위험성을 낮추기 위한 방법으로 사전 관리와 사후 관리가 있다. 사전 관리란 취약점 진단 스캐너를 사용하여 웹 어플리케이션에서 취약성이 존재하는지 점검하는 방법과 웹 방화벽(WAF, Web Application Firewall)을 사용하여 공격이 발생한 것을 예상한 즉시 이를 차단하는 방법을 말한다. 사후 관리란 공격이 발생한 후, 정보 유출 정황을 파악하고, 유출의 원인이 되는 기술적 취약점을 개선하는 것을 말한다.[2]

본 논문에서는 사전 관리에 해당하는 웹 취약점 진단 스캐너를 이용하여 웹 어플리케이션에서 발생할 수 있는 취약성을 사전에 대응하고 보안성을 높이는 것에 주목하였다. 웹 취약점 진단 스캐너는 주로 단일 취약점을 대상으로 제작되고, 도구에서 제공하는 스캐닝 옵션을 선택, 수치를 지정한다. 이는 사용자의 전문적인 지식과 입력이 필요하므로 보안 전문가가 아닌 경우 사용하기에 어려움이 있다. 따라서 전문적인 지식이 없는 사용자라도 취약점 진단을 원활하게 수행하며 이를 통해 보안성을 높이는 도구의 필요성이 존재한다. 하지만 취약점 진단이 자동으로 수행되더라도 대상의 데이터베이스에서 데이터가 무단으로 수정, 삭제되거나 의도하지 않은 게시글이 생성되는 등 가용성을 침해할 위험성이 존재한다. 따라서 기존 자동화 도구의 한계점을 개선하기 위해 인공지능을 활용한 웹 취약점 자동화 진단 프레임워크를 제안한다.

Ⅱ. 관련 연구

2.1. 웹 취약점 자동화 도구 분석

본 논문에서는 오픈소스 소프트웨어로 공개된 웹 취약점 진단 도구를 분석하고 성능을 비교하였다.

웹 취약점 진단 도구란 특정 URL을 대상으로 사전에 정의된 공격 벡터를 이용하여 발생할 수 있는 다방면의 취약점을 탐지하는 도구를 말한다. 웹 취약점 진단 도구를 분석하기 위해 사용할 도구 분석 환경으로 Bwapp[3], WackoPicko[4], Acunetix WVS[5] 를 선정하였다. 도구 분석 환경에서의 비교, 분석 결과는 [표 1]과 같다. 이때 동일한 취약점을 탐지하는 도구들은 같은 환경에서 진단하였다.

웹 취약점 진단 도구의 선정은 클라이언트, 서버 측 취약점 5가지를 기준으로 하였다. 또한, 정상적으로 취약점 진단이 가능하면서 수행 속도, 정확도, 위험 페이로드 사용 여부, 분석의 깊이를 비교 항목으로 사용하였다.

표 1. 도구별 비교

Category		Speed (s)	Accuracy	Risk Payload	Deep Analysis
SQL Injection	SQLmap	14	High	O	High
	Ghauri	9	High	X	Medium
	OWASP ZAP	20	High	X	Low
SSRF	SSRFmap	6	High	X	High
	ssrfuzz	16	High	X	Medium
XSS	Dalofx	44	High	X	High
	XSStrike	70	Medium	X	Medium
	Xspear	10	Low	X	Low
CSRF	XSRFProbe	19	Medium	X	High
	OWASP ZAP	10	Medium	X	Low
Open Redirect	Openredirex	15	High	X	High
	Injectus	2	Medium	X	Medium

도구 간 비교 결과 SQL Injection 취약점의 경우 속도 측면에서 Ghauri 도구가, 분석의 깊이, 정확도 측면에서는 SQLmap 도구가 우수함을 보였다. SSRF(Server-Side Request Forgery) 취약점의 경우 속도, 정확도, 깊은 분석 측면에서 SSRFmap 도구가 가장 우수하였다. XSS(Cross-Site Scripting) 취약점의 경우 속도 측면에서는 Xspear 도구가 우수함을 보였다. 하지만 탐지 정확도가 낮으면서 깊은 분석을 수행하지 못하는 단점이 존재한다. 정확도, 깊은 분석 측면에서 Dalfox 도구가 가장 우수함을 보였다. CSRF(Client-Side Request Forgery) 취약점의 경우 두 도구 모두 정확도

는 같으며 XSRFProbe 도구가 깊은 분석이 가능함을 확인하였다. Open Redirect 취약점의 경우 정확도, 깊은 분석 측면에서 Open Redirex 도구가 우수함을 보였다.

비교 결과를 기반으로 우수한 성능을 보인 도구를 [그림 1]과 같이 첫 번째, 두 번째 진단에서 각각 사용하도록 설계하였다.

2.2. 인공지능 기반의 자동화 도구 연구

2018년 윈도우 환경에서 사용할 수 있는 GUI 기반의 블랙박스 테스트 자동화 프로그램 도구[6]가 논의되었다. 2020년 알려지지 않은 패턴의 웹 공격을 WAF로 탐지하기 위해 웹 공격 패턴을 분류할 때 인공지능을 활용하는 연구[7]와 진단 대상의 웹 어플리케이션 취약 여부를 확인하기 위해 정보 수집과 취약점 탐지를 통합한 웹 취약점 자동 진단 스캐너[8]가 논의되었다. 이와 같이, 웹 어플리케이션에 대한 보안도 향상을 위하여 다양한 분야에서 인공지능을 도입하고 있고, 웹 어플리케이션 취약점 진단 프레임워크에 대한 지속적인 관심과 연구가 진행되고 있다.

Ⅲ. 제안 방안

본 논문에서 제안하는 프레임워크는 클라이언트 측 취약점(XSS, CSRF, Open Redirect)과 서버 측 취약점(SQL Injection, SSRF) 그리고 CSP(Content-Security Policy)에 대한 보안 진단을 수행하도록 설계하였다. 프레임워크의 흐름도는 [그림 1]과 같다.

사용자는 Client Interface에 진단할 대상의 URL을 입력한다. 이후 분석 깊이, 자바스크립트 분석, 엔드포인트 분석 등 설정값을 차례대로 입력 후 서버로 전달한다.

서버는 전달된 URL, 설정값을 기반으로 포트 스캐닝을 통해 네트워크 정보를 수집한다. 이후 엔드포인트와 파라미터를 수집하여 Client Interface에서 보여주는 과정을 수행한다.

취약점 진단은 모두 2회 수행한다. 첫 번째 진단은 속도, 정확도 측면에서 우수한 도구를 사용하며 분석을 통해 선정한 스캐닝 옵션을 사용한다. 스캐닝 옵션을 선정하는 경우 진단할 대상의 가용성을 침해하는 옵션은 사용하지 않는다. 첫 번째 진단 이후 인공지능을 활용하여 발생 가능성이 낮은 취약점을 검증하는 과정을 수행한다. 검증 결과 발생 가능성이 높은 취약점 데이터를 기반으로 두 번째 진단을 진행한다. 두 번째 진단은 정확도, 분석 깊이 측면에서 우수한 도구를 사용하고, 가용성 침해에 대한 위험성이 존재하는 스캐닝 옵션은 사용하지 않는다. 최종 진단 결과를 바탕으로 인공지능을 활용하여 취약점 분석 보고서를 사용자에게 제공한다.

본 논문에서 제안하는 프레임워크는 취약점 진단을 2회 수행하기 때문에 단일 도구를 사용하는 것보다 높은 정확도를 보일 수 있다. 또한 자동화 도구 분석을 통해 비교한 결과를 바탕으로 대상 웹 서비스의 가용성을 침해하지 않는 도구와 스캐닝 옵션을 사용하므로 가용성 침해 가능성이 낮으며, 기존 도구보다 효과적인 취약점 진단이 가능하다.

Ⅳ. 결론

기존의 웹 어플리케이션 자동화 진단 도구들은 단일 취약점만 진단하거나 진단 대상의 가용성을 침해할 수 있는 스캐닝 옵션이 포함되어 있다. 따라서, 전문적인 지식이 없는 경우 상세한 옵션을 작성하거나 정확한 수치를 지정하기에 한계가 존재한다. 본 논문에서는 기존 자동화 진단 도구의 한계점을 해결하기 위해 높은 정확성과 가용성을 침해하지 않는 인공지능을 활용한 웹 어플리케이션 취약점 자동화 진단 프레임워크를 제안하였다. 제안하는 프레임워크는 사용자 중심의 접근 방식을 도입하여 사용자의 조작을 최소화하고, 인공지능을 통한 취약점 진단 보고서를 제공한다. 또한, 취약점 별 잘 알려진 자동화 도구를 분석하여 효과적으로 진단이 가능한 도구와 가용성을 침해하지 않는 스캐닝 옵션을 선정하였다. 이를 기반으로 인공지능을 활용한 취약점 진단 및 추가적인 정밀 진단을 수행하여 정확도 측면에서 우수함을 보였다.

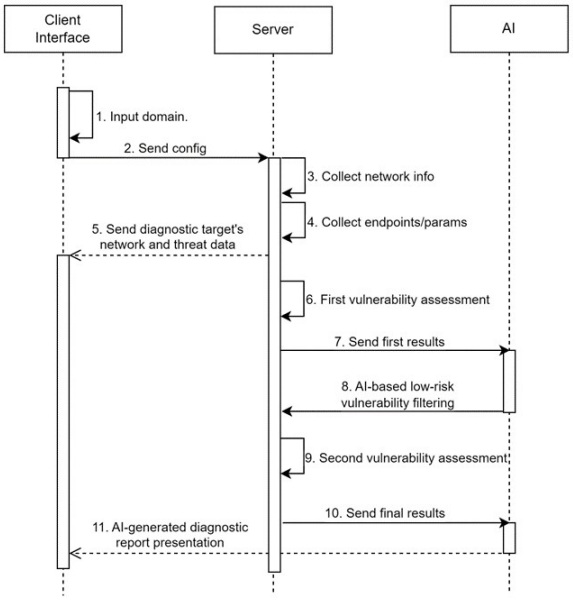

그림 1. 인공지능 기반 웹 취약점 진단 프레임워크 흐름도

참 고 문 헌

[1] Xiaowei, and Yuan Xue, “A Survey on Web Application Security”. Technical report, Vanderbilt University, 2011.

[2] National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61 Rev. 2). Retrieved Jan., 02, 2024, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[3] Malik Mesellem, *BWAPP*, Retrieved Dec., 29, 2023, from http://www.itsecgames.com/

[4] Adam Dupe, *WackoPicko*, Retrieved Dec., 30, 2023, from https://github.com/adamdoupe/WackoPicko

[5] Acunetix, *Acunetix Web Vulnerability*, Retrieved Jan., 01, 2024, from http://testphp.vulnweb.com/

[6] Jeong, Beomjin, Lee, Jungwoo, Hong, Changwan, and An, Beongku, "GUI-based Black Box Test Automation Program Tool in Windows Environment," JIIBC, vol. 18, no. 2, pp. 163-168, 2018.

[7] Yeonsu Kim, Younghun Ko, Ieckchae Euom, and Kyungbaek Kim, "Web Attack Classification Model Based on Payload Embedding Pre-Training," Journal of the Korea Institute of Information Security & Cryptology, vol. 30, no. 4, pp. 669-677, 2020.

[8] H. Chen, J. Chen, J. Chen, S. Yin, Y. Wu and J. Xu, "An Automatic Vulnerability Scanner for Web Applications," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1519-1524, 2020.