XSS 취약점 스캔 도구 분석을 통한 효과적인 탐지 프레임워크 제안

서홍준, 이정우, 윤성민, 이승환, 박연준, 배민준, 김주원*
KITRI 화이트햇 스쿨 1 기 (멘티), *KITRI 화이트햇 스쿨 1 기(멘토)

{hjthink2, 2jw2534, potatochip0413, brains8821, jme07136, gguggu6256,
*arresterloyal}@gmail.com

Proposal of an Effective Detection Framework through Analysis of XSS Vulnerability Scanning Tools

Hongjun Seo, Jungwoo Lee, Seongmin Yoon, Seunghwan Lee,
Yeonjun Park, Minjun Bae, Joowon Kim*
KITRI Whitehat School 1st (Mentee), *KITRI Whitehat School 1st (Mentor)

요 약

본 논문에서는 대표적인 XSS 취약점 스캔 도구를 비교 분석하여 각 도구의 성능과 특징을 평가하였다. 평가 결과 XSpear 도구가 효율성, 정확성 측면에서 가장 뛰어난 성능을 보였다. 또한, XSpear 도구를 중심으로 자산 수집 도구를 함께 사용하여 XSS 취약점의 탐지율을 높이고, 제안하는 프레임워크를 통해 얻을 수 있는 이점을 확인하였다. 본 논문에서는 XSS 취약점에 대한 높은 탐지 성능을 제공하는 프레임워크를 제안하였다.

Ⅰ. 서 론

보편적으로 정보보안 담당자는 기업의 IT 자산에 존재하는 취약성을 찾고, 이를 패치하여 자산의 보안도를 높이는 역할을 수행한다. 이때 취약점 탐지를 위해 웹 애플리케이션을 수동으로 분석하여 공격벡터를 찾는다. 그러나 IT 인프라의 자산 규모가 클수록 수동 분석에 대한 한계가 존재한다.[1] 수동 분석의 한계를 극복하기 위한 대안으로 자동화된 취약점 스캔 도구가 존재한다. 이러한 도구는 정보보안 담당자의 작업 효율을 극대화할 수 있다.[2] 하지만 도구의 스캔 옵션을 필요에 따라 적절하게 설정하지 않고 사용하는 경우 불필요한 기능을 사용하게 되어 서버의 가용성이 침해될 수 있고, 오용 탐지(False Negative)로 인해 자동화 도구의 효율성을 극대화할 수 없다.

본 논문에서는 대표적인 XSS(Cross-Site Scripting) 취약점 스캔 도구(Dalfox, XSSer, Xspear, XSStrike)를 비교, 분석하여 가용성 침해에 대한 위험성을 낮추면서 취약점 탐지율이 높은 스캔 옵션을 발견하였다. 또한, 취약점 스캔 도구의 자산 수집 기능의 한계점을 해결하기 위해 자산 수집 도구(Subfinder, Httpx, Katana)를 연계하여 취약점 탐지 범위를 늘릴 수 있는 취약점 탐지 프레임워크를 제안한다.

Ⅱ. 관련 연구

2.1. XSS 취약점 스캔 도구 분석

본 절은 대표적인 XSS 취약점 스캔 도구를 분석한 결과를 보인다. 도구의 취약점 탐지 성능을 판단하기 위해 Acunetix 사에서 지원하는 취약한 웹 애플리케이션 Vulnweb(Vulnerable test website)을 대상으로 취약점 탐지 테스트를 수행하였다.

[표 1]은 대표적인 XSS 취약점 스캔 도구를 대상으로 취약점 탐지율과 Vulnweb 에 전송하는 평균 Payload 개수를 비교한 결과와 특징을 정리한 내용이다. 탐지율을 비교하기 위해 수동 분석으로 Vulnweb 에 존재하는 XSS 취약점을 식별한 후, XSS 취약점 스캔 도구가 탐지하는 개수를 비교하였다.

해당 웹 애플리케이션에서 식별된 XSS 취약점의 개수는 총 5 개이다. 수집된 5 개의 표본으로부터 XSStrike 도구를 제외한 나머지 XSS 취약점 스캔 도구는 5 개의 취약점을 모두 탐지하였다. 평균 Payload 개수는 주어진 XSS 취약점을 대상으로 스캔 도구가 서버에 전송하는 Payload 수를 측정한 평균 수치이다. 평균 수치가 적을수록 대상 서버에 대한 가용성을 침해하지 않는다.

본 논문에서 대표적인 XSS 취약점 스캔 도구의 분석 결과는 다음과 같다.

WAF 탐지 및 우회 기능은 XSStrike, Dalfox 도구가 우수한 탐지 성능을 보였다. DOM-Based 기능의 경우 XSpear 도구를 제외한 세 도구가 모두 지원한다. 하지만 XSpear 도구가 서버에 전송하는 Payload 의 수가 상대적으로 적으면서도 모든 표본에서 취약점을 성공적으로 탐지하였다. 이는 XSpear 도구가 효율성과 정확성 측면에서 우수하다는 것을 의미한다. 따라서 이 논문에서 제안하는 프레임워크에서는 XSpear 도구를 주요 XSS 취약점 스캔 도구로 선정하였다. 이를 통해 웹 애플리케이션에서 발생할 수 있는 XSS 취약점을 효과적으로 탐지할 수 있다.

[표 1] XSS 취약점 스캔 도구 비교

	XSStrike	XSSer	XSpear	Dalfox
Detection Rate	3/5	5/5	5/5	5/5
Average Number of Requests	3103	1293	262	1504
WAF Detection and Bypass	Detection and Bypass	Bypass	Detection	Detection and Bypass
DOM-Based Support	Supported	Supported	X	Supported
Parameter Detection	Crawling Method	Crawling Method	X	Word List Method

[표 2]는 분석하고자 하는 대상의 웹 애플리케이션에서 사용하는 파라미터를 알고 있는 경우 사용할 수 있는 스캔 옵션이다. 해당 옵션은 대상 URL 과 파라미터를 함께 입력한 후 해당 파라미터에 대해 분석을 진행하므로 불필요한 작업을 줄일 수 있으며 가용성 침해의 가능성을 낮추고, 취약점 탐지율을 높일 수 있다.

XSStrike 도구와 Dalfox 도구의 경우 '--skip-dom' 옵션과 '--skip-mining-all' 옵션을 함께 사용하여 불필요한 작업을 줄일 수 있다. XSSer 도구의 경우 분석하고자 하는 파라미터의 값에 'XSS'를 입력해 주어야 해당 파라미터에 대해 XSS 취약점 분석을 수행한다. XSpear 도구는 '-d' 옵션으로 분석하고자 하는 파라미터를 지정할 수 있다.

[표 2] XSS 취약점 스캔 도구의 스캔 옵션

Tool	Options
XSStrike	**-u** [url?param=value] **--skip-dom**
XSSer	**-u** [url] **-g** [endpoint?param=**XSS**]
XSpear	**-u** [url?param=value] **-d** [param]
Dalfox	**url** [url?param=value] **--skip-mining-all**

2.2. 자동화 스캔 도구의 한계점

현재 XSS 취약점 스캔 도구들은 주로 서브도메인이나 파라미터 수집 기능이 제한적이거나 불편함을 갖고 있다.

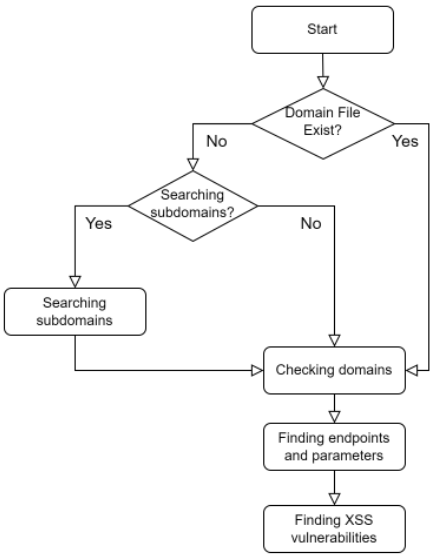
Dalfox 도구의 경우 Wordlist 방식으로 파라미터를 수집하여 대상 웹 페이지의 파라미터가 Wordlist 에 존재하지 않을 경우 효과적이지 않고, 직접 엔드포인트를 수집하는 기능이 존재하지 않는다. XSSer 와 XSStrike 도구는 엔드포인트 수집을 지원하지만, 상위 URL 에 종속된 범위 내에서만 수집한다. 따라서 와일드 카드 형태의 도메인에 대해서는 서브도메인의 수집이 불가능하다. 또한 XSpear 도구는 엔드포인트와 파라미터 수집 기능이 존재하지 않는다.

이처럼 잘 알려진 XSS 취약점 스캔 도구들은 취약점 탐지에 단편적으로 집중하여 자산 정보 수집의 한계점이 존재한다. 그러나 취약점 탐지를 위해 신뢰성 있는 자산 정보를 최대한 수집하는 것이 XSS 취약점 스캔 도구의 효용성과 직결된다. 본 논문에서는 이러한 한계점을 보완한 효과적인 XSS 취약점 탐지 프레임워크를 제안한다.

Ⅲ. 프레임워크 제안 방안

본 논문에서 제안하는 프레임워크는 자산 수집 도구를 사용하여 와일드 카드 형태의 도메인으로부터 모든 서브도메인을 추출하고, 수집된 도메인의 유효성을 판단한다. 유효성이 검증된 도메인에서 파라미터가 포함된 엔드포인트를 수집하고, 이를 XSS 취약점 스캔 도구에 전달하여 공격 벡터를 분석한다. 제안하는 프레임워크는 다수의 단계로 이루어져 있으며, 각 단계별 절차는 다음과 같다.

1. Subfinder 도구를 사용하여 지정된 와일드 카드 형태의 도메인으로부터 서브도메인을 추출한다. 해당 과정은 도메인의 수가 큰 경우 효율적으로 서브도메인을 식별하는데 중요한 역할을 한다.
2. Httpx 도구를 통해 수집된 서브도메인에서 동작하는 웹 서버의 활성화 여부를 통해 유효성을 검증한다. 해당 과정은 존재하지 않거나 비활성화된 도메인을 판별하는 과정으로 효과적인 자원 사용과 분석의 정확도를 높일 수 있다.
3. Katana 도구를 사용하여 추출된 서브도메인으로부터 파라미터가 포함된 엔드포인트를 수집한다. 해당 과정을 통해 XSS 취약점 탐지에 필수적인 정보를 제공한다.
4. 3 번 절차를 통해 생성된 데이터를 XSpear 도구에 전달하여 XSS 취약점을 분석한다. 취약점 탐지율을 높이면서도 시스템 가용성에 미치는 영향을 최소화하는 스캔 옵션을 사용함으로써 XSS 취약점 스캔 도구의 한계점을 해결하고, 효과적인 XSS 취약점 탐지가 가능하다.



[그림 1] 제안하는 프레임워크 흐름도

Ⅳ. 결론

XSS 취약점 스캔 도구의 사용은 보안 담당자가 겪는 수동 분석의 한계를 해결할 수 있는 대표적인 대안 중 하나이다. 하지만 도구의 특징과 성능이 서로 다르며 도구의 정확한 이해가 없는 경우 자동화 도구의 효율성을 극대화할 수 없고, 가용성 침해의 위험성이 높다. 이에 본 논문에서는 대표적인 XSS 취약점 스캔 도구를 비교, 분석하여 각 도구의 성능과 특징을 평가하였다. 평가 결과 가장 우수한 XSpear 도구를 중심으로 자산 수집 도구와 연계하여 XSS 취약점 스캔의 효율성을 극대화하는 효과적인 탐지 프레임워크를 제안하였다. 제안하는 프레임워크를 통해 기존 취약점 스캔 도구의 자산 수집에 대한 한계점을 자산 수집 도구와 연계함으로써 해결하였다. 또한, 각 도구 별 스캔 옵션을 분석하여 가용성 침해를 낮추고, 높은 취약점 탐지율을 보이는 옵션을 사용하여 효율성을 높일 수 있는 이점을 갖는다.

참 고 문 헌

[1] N. Singh, V. Meherhomji and B. R. Chandavarkar, "Automated versus Manual Approach of Web Application Penetration Testing," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225385.

[2] S. Alazmi and D. C. De Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," in IEEE Access, vol. 10, pp. 33200-33219, 2022, doi: 10.1109/ACCESS.2022.3161522.