웹 시큐어 프로그래밍 학습 플랫폼 개발

백승진*, 송인봉*, 이현*, 백다인*, 강지형*

Web Secure Programming Learning Platform Development

Baek Seung Jean*, Song In Bong*, Lee Hyeon*, Back Da In*, Kang Ji Hyeong*

요 약

사이버 보안의 중요성이 부각됨에 따라 국가는 소프트웨어 개발보안 가이드를 배포하여 개발자들이 안전한 소프트웨어를 개발하도록 제시하고 있다. 하지만 이런 조치에도 불구하고 많은 개발자들이 시큐어 프로그래밍을 제대로 수행하지 못하고 있는 것이 현실이다. 본 논문에서 소개하는 시큐어 프로그래밍 학습 플랫폼은 개발자들의 시큐어 프로그래밍 습관화를 목표로, 개발자들이 본인의 개발 과정에서 발생하는 다양한 취약점을 인지하고 이를 개선하도록 하여 시큐어 프로그래밍의 학습을 유도한다.

Abstract

As the importance of cyber-security emerges, the state is encouraging developers to develop safe software by distributing software development security guidelines. However, despite this measures, the reality is that many developers are not properly performing secure programming. The secure programming learning platform introduced in this paper aims to make it a habit of secure programming for developers, and induces learning of secure programming by allowing developers to recognize and improve various vulnerabilities that occur in their own development process.

Key words

security, programming, secure programming, secure software devlopment, learning, platform

Ⅰ. 서 론

하루가 다르게 IT기술이 발전하는 오늘날, 사이버 공격 기술은 더욱 다양해지고 있으며, 이에 관해 해킹 사례는 나날이 증가하고 있다. 국가에서는 ISMS-P 인증심사를 시행함으로써 기업 및 기관의 정보보호 및 개인정보보호 관리체계를 심사하는 동시에, 소프트웨어 개발보안 가이드[1] 등의 자료를 배포하여 개발자들에게 시큐어 프로그래밍 방법을 제시하고 있다. 하지만 가이드라인이 존재함에도 많은 개발자들이 시큐어 프로그래밍을 제대로 수행하고 있지 못하는 것이 현실이다. 해킹·보안 지식의 부족으로 취약점 공격이 어떻게 이뤄지는지 이해하지 못하는 것이 첫 번째 이유이고, 본인의 프로그래밍 스타일에서 어떠한 부분이 취약한 요소가 되는지 알지 못하는 것이 두 번째 이유이다.

이에 본 논문에서는 다음과 같은 방식의 웹 시큐어 프로그래밍 학습 플랫폼을 제안한다. 플랫폼에는 여러 종류의 개발 시나리오가 존재하며, 사용자는 각 시나리오에서 제시된 요구사항에 맞춰 웹 페이지를 개발한다. 본 플랫폼은 사용자가 개발한 웹 페이지를 대상으로 사전에 준비된 POC (Proot Of Concept) 코드를 활용해 블랙박스 테스트를 진행한다. 이 채점 과정에서 사용자의 요구사항 충족 및 취약점 존재 여부를 확인하고 이에 대한 결과와 함께 솔루션을 제시한다. 이를 통해 사용자는 본인의 프로그래밍 스타일에 대한 보안 피드백을 받을 수 있고, 이를 개선함으로써 시큐어 프로그래밍 능력을 향상시킬 수 있다.

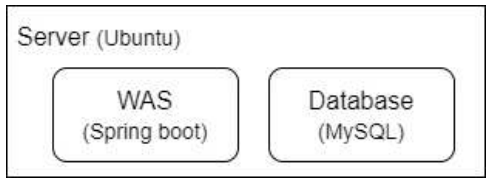
Ⅱ. 관련연구

수준 높은 시큐어 프로그래밍을 진행하고 트렌디한 사이버 공격에 대응하기 위해 많은 보안 및 개발 업체들은 새로운 취약점들을 연구 및 제보 받고, 이에 대한 시큐어 프로그래밍 방안을 제시하고 있다. Acunetix, PortSwigger 등의 해외 보안 업체들은 매번 새로운 공격 POC를 업데이트하여 제품을 발행하고 있고 국내 개발 업체인 에스아이알소프트나 엑스이허브는 제보 받은 취약점들에 대한 패치 코드를 github에 올려 공개하고 있다. 따라서 본 제품에서는 제공된 공격 POC와 패치 코드를 분석하고, 이를 패턴화하여 제공함으로써 최신 공격 트렌드를 반영한 시큐어 프로그래밍 학습을 진행하고자 한다.

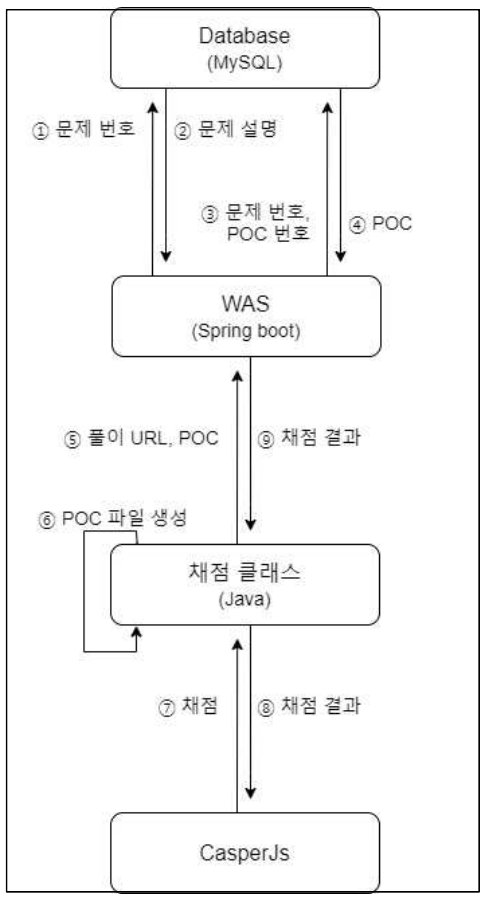
Ⅲ. 제안연구

1. 시스템 구성

본 논문에서 다루는 웹 시큐어 프로그래밍 학습 플랫폼은 [그림1]와 같이 WAS와 Database가 설치된 Ubuntu 서버로 구성되어 있으며, [그림2]의 흐름으로 문제 채점이 동작한다.



[그림1] 소프트웨어 구성도



[그림2] 소프트웨어 흐름도

2. 시나리오

시나리오는 하나의 사이트 개발(커뮤니티 사이트, 쇼핑몰 사이트 등)을 목표로, [그림3]과 같이 기능에 따라 여러 스테이지로 구성된다. 각 스테이지는 [그림4]와 같이 요구사항이 명세되어 있으며, 해당 기능 구현에 필요한 조건과 입력 데이터 파라미터 형식을 제시된다.

[그림3] 시나리오 구성 예시

[그림4] 요구사항 예시

시나리오는 사용자에게 다양한 웹사이트를 제작하도록 하여, 해당 상황에서 발생하는 특정 취약점들을 접할 수 있도록 한다. 가령, 쇼핑몰 사이트에는 결제금액 변조 취약점이 발생할 수 있다. 이는 일반적인 커뮤니티 사이트나 메일함 사이트에서 구현하지 않는 결제 기능에서 발생하는 취약점이다. 사용자는 쇼핑몰 사이트 제작 시나리오를 해결하는 과정에서 해당 취약점을 접하게 되고 이를 방어하는 과정을 수행하게 된다. 이와 같이 시나리오는 다양한 웹사이트를 주제로, 사용자가 다양한 상황을 경험할 수 있도록 제시된다.

3. 기능 검증 및 보안 검증

기능 검증은 사용자가 요구사항을 충족하여 웹 페이지를 구성했는지 확인하는 과정이다. 기능 검증 없이 보안 검증을 시행할 경우, 보안 검증 실패가 기능 미구현으로 발생할 가능성이 있으므로 보안 검증 이전에 기능 검증을 우선 시행하도록 한다. 보안 검증은 사용자가 개발한 웹 사이트에 대해 취약점이 존재하는지 판별하는 과정이다. 보안 검증에서 점검하는 취약점은 KISA의 소프트웨어 개발보안 가이드, 안전행정부의 행정·공공 웹사이트 구축 및 운영 가이드[2], 금융보안원의 전자금융기반시설 보안 취약점 분석·평가항목 취약점 판단기준[3]의 자료를 참고하여 선정한다.

데이터베이스에는 문제 번호, 문제 설명, 기능 및 보안 POC 등의 문제 채점 관련 정보가 저장되어 있다. 기능 및 보안 POC는 CasperJs로 작성된 검증 스크립트로, 이를 실행하여 채점을 시행한다.

Ⅳ. 실험결과 및 분석

사용자는 각 스테이지에 마련된 요구사항에 맞춰 웹 사이트를 개발한다. 개발한 웹 사이트를 제출하면, 기능 및 보안 검증 절차를 거쳐 스테이지 통과 여부를 판별한다. [그림5]는 사용자가 제출한 웹 사이트에 대해 본 플랫폼의 “게시글 작성”에 관한 기능 및 보안 검증 POC를 실행한 결과 중 일부이다.

```
# Open Document Test
PASS 문서 열람 결과 유무
PASS 문서 열람 결과 확인
PASS Open Document Test
# Write Document Test
PASS 회원가입 결과 유무
PASS 회원가입 결과 확인
PASS 로그인 결과 유무
PASS 로그인 결과 확인
PASS 문서 번호 유무
PASS 문서 작성 결과 확인
PASS 문서 번호 유무
PASS 문서 번호 일치 여부 확인
PASS Write Document Test
# Write Document Test
PASS 회원가입 결과 유무
PASS 회원가입 결과 확인
PASS 로그인 결과 유무
PASS 로그인 결과 확인
PASS 문서 번호 유무
PASS 문서 작성 결과 확인
PASS 문서 번호 유무
PASS 문서 번호 일치 여부 확인
PASS Write Document Test
```

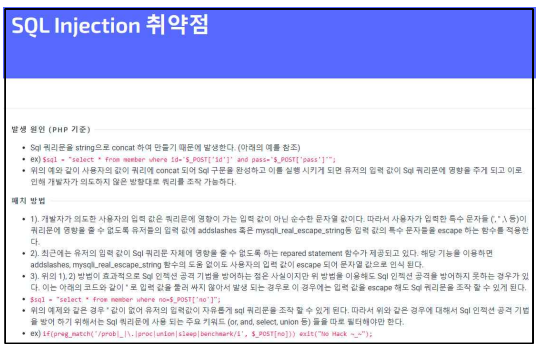
[그림5] 채점 결과 (CLI 화면 - 기능 검증)

CaspserJs로 작성된 POC가 동작하면 실행 여부에 따라 PASS / FAIL 의 값이 반환되며, 이러한 POC들을 종합적으로 검사하여 사용자의 스테이지 통과 여부를 판별한다. 사용자는 채점 결과를 [그림6]과 [그림7]과 같이 웹사이트 상으로 확인하게 된

다. 이후 스테이지 통과를 위해 본인의 웹사이트를 지속적으로 수정하게 되며, 필요에 따라 [그림8]과 같이 POC의 발생 원인과 보안 패치 방법 등을 확인하고 이를 적용할 수 있다. 이러한 일련의 과정 속에서 사용자는 능동적으로 시큐어 프로그래밍 능력을 습득한다.

[그림6] 채점 결과 (채점 페이지 - 기능 검증)

[그림7] 채점 결과 (채점 페이지 - 보안 검증)



V. 결 론

본 논문은 웹 시큐어 프로그래밍을 습관화하는 학습 플랫폼 개발을 제안하였다. 시나리오 형식의 문제 풀이 형식으로 진행된다는 점과, 개발자가 본인의 프로그래밍 스타일을 중점으로 문제점을 파악하여 시큐어 프로그래밍을 학습하는 점에서 본 플랫폼은 타 시큐어 프로그래밍 학습 플랫폼과 차별성을 가진다. KISA에서 제시한 소프트웨어 개발 보안 가이드, 안전행정부에서 지정한 행정·공공 웹사이트 구축 및 운영 가이드 등을 기준으로 제시된 취약점 점검 항목들을 선정하여 보안 검증 과정에서 신빙성을 갖추었고, 취약점별 POC들을 DB로 관리함으로써 멀티 프로세서와 관리자의 관리 효율성을 높였다.

사용자는 기능 및 보안 검증의 피드백을 통해 본인의 프로그래밍 스타일에 대해 문제점을 파악하고 개선해나갈 수 있다. 이 과정을 통해 시큐어 프로그래밍 스킬을 자연스레 함양할 수 있으며, 개발 이전의 설계 단계에서부터 취약점을 고려하며 사이트를 개발하는 습관을 지닐 수 있다. 궁극적으로 시큐어 프로그래밍이 체화된 사용자가 증가한다면, 현대 사회에서 필요로 하는 개발자들이 양성되어 안전한 소프트웨어 개발에 기여할 수 있다.

Acknowledgement

본 논문은 대학혁신지원사업비의 지원으로 작성되었음.

참 고 문 헌

[1] 행정안전부&한국인터넷진흥원(2019),
소프트웨어 개발보안 가이드
[2] 행정안전부(2019),
행정·공공 웹사이트 구축·운영 가이드
[3] 금융보안원(2019),
전자금융기반시설 보안 취약점 분석·평가항목
취약점 판단기준