[ポスター発表] 研究報告

データベースへのインジェクション攻撃に対するセキュアプログラミング演習システムにおける評価実験の検討

岸本 和理[1]　井口 信和[2]

A Study of Evaluation Experiments on Hands-on Secure Programming Exersises System against Database Injection Attacks

1. 序論

総務省によると，令和元年の不正アクセスの認知件数は2960 件であり，前年度と比較して 99%増加している [1]．不正アクセスの要因として脆弱性を含んだ Web アプリケーションの存在がある．Web アプリケーションの脆弱性を悪用した攻撃には，データベースへのインジェクション攻撃がある．

データベースへのインジェクション攻撃とは，データベースと連携した Web アプリケーションの脆弱性を利用し，不正にデータベースシステムを操作する攻撃のことである．データベースインジェクションのうち，MySQL などの RDBMS を対象とした攻撃を SQL インジェクション（以下，SQLi），MongoDB などの非 RDBMS を対象とした攻撃を NoSQL インジェクション（以下，NoSQLi）と呼ぶ．どちらの脆弱性も存在してしまうと、能動的にデータベースシステムを操作することができてしまうため，攻撃を受けることで個人情報の漏洩や認証回避などの不正アクセスを可能としてしまう脆弱性である．ソフトウェアセキュリティを取り巻く脅威，課題の解決を目的とした国際的なコミュニティである OWASP が発表している OWASP Top10 というレポートによるとデータベースへのインジェクション攻撃は 2010 年度版，2013 年度版，2017 年度版において常に第 1 位 [2] となっており，常に Web アプリケーションへの脅威となっている．これらの実状から，Web アプリケーション開発者は，データベースへのインジェクション攻撃への対策手法を身に付けることは重要である．

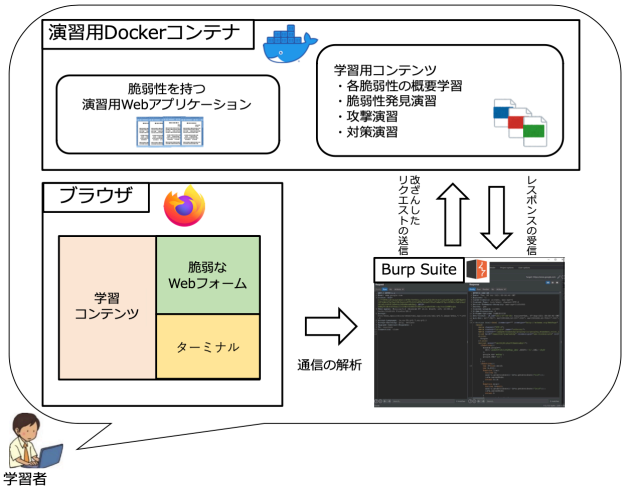

図 1　システム構成図

Web アプリケーション攻撃への根本的な対策手法としてセキュアプログラミングがある．しかし，開発者の知識やスキル不足，外部ライブラリや古くからあるコードを引き継いで利用している等の理由により，対策が行われていない Web アプリケーションが存在する．また，Web アプリケーション攻撃への対策として，クライアントからの入力文字数を制限する，特定のキーワードの使用を不許可とする，Web Application Firewall（以下，WAF）を導入する，などの表面的な対策のみを行っている Web アプリケーションも多くある．これらの Web アプリケーションは根本的な脆弱性の対策が不十分なため，悪用可能な脆弱性を内包している場合がある．

そこで本稿では，Web アプリケーションセキュリティに関する実践的な演習を支援することを目的に，脆弱性を発見するという攻撃者視点を取り入れたデータベースへのインジェクション攻撃に対するセキュアプログラミング演習システム（以下，本システム）を開発する．

[1] 近畿大学大学院総合理工学研究科エレクトロニクス系工学専攻
Graduate School of Science and Engineering Research, Kindai University .
[2] 近畿大学理工学部情報学科
Department of Informatics, Faculty of Science and Engineering, Kindai University.
近畿大学情報学研究所
Cyber Informatics Research Institute, Kindai University.

2. 研究内容

本システムは，Web アプリケーション開発者を目指す初学者や，本システムで扱う SQLi，NoSQLi に関する知識が不足している Web アプリケーション開発者を本システムの利用者（以下，学習者）として想定する．本システムの構成を図 1 に示す．本システムは，学習者の PC 上で本システムの演習用 Web サーバを内包した Docker イメージを展開して，ブラウザから演習用コンテナにアクセスすることで演習を可能とする．

演習用 Docker イメージの構築には Ubuntu18.04 のイメージを基に，演習に必要なソフトウェアを導入することで作成した．それぞれ Web サーバには Apache2.4.29，サーバサイド言語には PHP7.4/Node.js 14.17.5，データベースには MySQL 5.7，MongoDB 3.6.3 を導入した．また，攻撃者視点を取り入れた脆弱性の発見演習を実施するために，演習用 Web サーバとブラウザ間の通信を解析に使用するローカルプロキシツールである Burp Suite Community Edition v2021.8.1 を導入した．

本システムによる演習を実施する場合，学習者はまず，脆弱性概要学習用のコンテンツを利用して各脆弱性の概要を学ぶ．実際に Web ブラウザに表示される脆弱な Web フォーム上に，学習用コンテンツに従いながら入力を実施し，各脆弱性の概要を学習する．

続いて，学習者は，脆弱性発見演習用のコンテンツを利用して，脆弱性発見手法の学習と演習を実施する．この演習では，各脆弱性への対策が不十分な Web アプリケーションを使用する．学習者は学習コンテンツに従い，Burp Suite を使用して，攻撃者ホストと演習用 Web サーバ間の HTTP リクエストと HTTP レスポンスを解析する．Burp Suite を用いて改ざんした HTTP リクエストの送信とそのレスポンスの解析を繰り返すことで，Web アプリケーションの構造把握を進め，各脆弱性を発見する．これらのハンズオンによる演習を通して学習者は，Web アプリケーションに含まれる脆弱性の発見手法を習得する．

最後に学習者は，対策演習用のコンテンツを利用して対策手法の学習と演習を実施する．まず，学習者は対策演習用コンテンツ内のテキストや動画を視聴して防御の理論や対策手法について学習する．学習者は，ブラウザ上の右下に表示されるターミナル画面，もしくは Visual Studio Code を通じて，脆弱な Web アプリケーションのソースコードを閲覧，修正する．学習者は，ソースコードの修正後，再度攻撃を実施して攻撃の影響を受けないように適切に脆弱性が解消されたことを確認する．

3. 実験

本稿では，情報系学科の学生 20 名程度を実験協力者とし，本システムを用いたデータベースへのインジェクション攻撃に関するセキュアプログラミング演習における学習効果の評価実験を実施する予定である．評価実験では，実験協力者を，データベースへのインジェクション攻撃について本システムを使用して学習するグループと，座学で学習するグループの 2 つに分割する．学習時間はいずれのグループとも 30 分間とする．なお，座学で学習するグループの実験協力者には，情報処理安全確保支援士試験の参考書 [3] のデータベースへのインジェクション攻撃に関して記述された箇所（2.8.2 節，pp. 144–158）を使用して自習をしてもらう．それぞれ学習の前後にデータベースへのインジェクション攻撃に関する事前・事後テストを実施する．テスト内容は情報処理安全確保支援士試験の参考書 [3] と IPA 試験の過去問を基に作成する．問題数はそれぞれ 10 問となっており 1 問 1 点とする．事後テストは，事前テストと同レベルの別の問題を使用する．また，事前テストの解答は実験協力者に知らせずに，事後テストを実施する．2 グループの事前・事後テストの点数の差から本システムが対策学習の支援ができているかを確認する予定である．

また，本システムを使用して学習したグループには，攻撃者の視点を取り入れたことによる効果を確かめるために，こちらで用意した複数の脆弱性を含む Web アプリケーションを対象に，脆弱性の列挙を実施してもらう．列挙できた脆弱性の数とその脆弱性を悪用した攻撃内容，セキュアプログラミングよる修正方法について記述してもらい，本システムによる演習の理解度を測る．加えて，本システムを使用して学習したグループには，利用評価アンケートを実施する．利用評価アンケートでは，学習コンテンツ，演習の難易度，演習時間などについて「5. 満足」「4. やや満足」「3. 普通」「2. やや不満」「1. 不満」の 5 段階による回答と，自由記述形式で演習について記述してもらう．

4. おわりに

本稿では，開発したデータベースへのインジェクション攻撃に対するセキュアプログラミングの演習システムについて，有用性を確認するための実験を検討した．今後の予定として，本稿で検討した実験を実施する予定である．

謝辞　本研究は JSPS 科研費 21K12185 の助成を受けたものです．

参考文献

[1] 総務省：不正アクセス行為の発生状況 (2020) <https://www.soumu.go.jp/main_content/000671872.pdf>(参照 2021-10-07)
[2] OWASP Foundation：OWASP Top10 - 2017<https://www.owasp.org/www-pdf-archive/OWASP_Top_10-2017(ja).pdf>(参照 2021-10-07)
[3] 上原孝之，情報処理教科書 情報処理安全確保支援士　2020 年版．翔泳社，2019.