7ZH-02

攻撃者視点を取り入れた Web アプリケーションセキュリティに関する セキュアプログラミングの実践的演習システム

岸本　和理† 谷口　義明‡§ 井口　信和‡§

近畿大学大学院総合理工学研究科† 近畿大学理工学部情報学科‡ 近畿大学情報学研究所‡§

1. 序論

警察庁，総務省及び経済産業省が公表した不正アクセス行為の発生状況によると，令和 2 年における不正アクセス行為の認知件数は 2806 件である[1]．不正アクセスの原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，クロスサイトスクリプティング（以下，XSS）やデータベースへのインジェクション攻撃がある．

不正アクセスの原因となるこれらの脆弱性を減らすためには，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により，脆弱性対策が十分でない Web アプリケーションがある．また，WAF などのセキュリティ機構を利用した表面的な対策により，脆弱性が内在したまま運用されている Web アプリケーションがある．前述の場合，脆弱性が悪用されてしまう危険性があり，不正アクセスの原因となってしまう．

この問題を解決するためには，セキュアプログラミングによる実装方法を学ぶことに加えて，攻撃者視点で Web アプリケーションを解析して，内在する脆弱性を顕在化する必要がある．セキュリティ人材の育成において，座学よりも体験型の学習の方が高い学習効果が得られるとされていることから，体験型のサイバーセキュリティ学習システムが開発されている[2]．

そこで本研究では，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，脆弱性を特定するという攻撃者視点を取り入れた Web アプリケーションセキュリティに関するセキュアプログラミングの実践的演習システム（以下，本システム）を開発する．本システムは，Docker を利用して構築しているため，実運用されているネットワークや PC 環境に影響を与えずに，演習可能である．

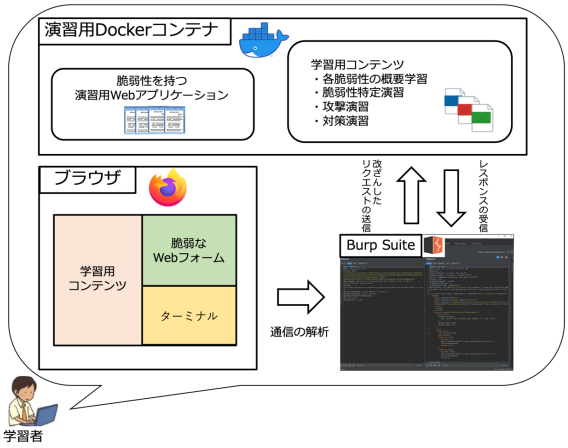

図 1 システム構成

2. 開発システム

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，XSS，データベースへのインジェクション攻撃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 上で演習用 Docker コンテナを稼働させて，Web ブラウザから演習用 Web サーバにアクセスすることで演習を実施する．本システムで演習可能な脆弱性は，XSS とデータベースへのインジェクション攻撃に分類される SQL インジェクション，NoSQL インジェクションの 3 つである．

各脆弱性に関する演習を実施するため，本システムでは，攻撃原理や対策手法について学ぶための学習用コンテンツと，これらの演習を実施するための脆弱性を内包した演習用 Web アプリケーションを開発した．

学習者は，学習用コンテンツに表示される解説や動画を参考にしながら，演習を進める．また，脆弱性を特定する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す

Hands-on System for Secure programming on Web application security with an Attacker's perspective
Kazuri KISHIMOTO †, Yoshiaki TANIGUCHI‡§, Nobukazu IGUCHI‡§
†Graduate School of Science and Engineering Research, Kindai University
‡Department of Informatics, Faculty of Science and Engineering, Kindai University
§Cyber Informatics Research Institute, Kindai University

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.

るためのローカルプロキシツールである Burp Suite Community Edition を導入した．学習者は，攻撃者視点で Burp Suite を使用した HTTP 通信の解析演習を実施することで，Web アプリケーションに内在する脆弱性を特定するためのスキルと脆弱性を修正するためのセキュアプログラミングスキルを習得可能である．

3. セキュアプログラミング演習の流れ

学習者はまず，学習用コンテンツを利用して脆弱性の概要について学習する．続いて，学習者は，本システムに配置されている演習用 Web アプリケーションに対してハンズオン形式で攻撃を体験する．サーバサイドで動作しているソースコードと攻撃スクリプトを照らし合わせて，攻撃の原理について学習する．

次に学習者は学習用コンテンツに従い，Burp Suite を使用して，改ざんした HTTP リクエストを送信する．演習用 Web サーバから返ってきた HTTP ステータスコード，HTTP レスポンスの内容，HTTP レスポンスのデータサイズの変化などに着目して，脆弱性箇所を特定する．

最後に学習者は，セキュアプログラミングによって演習用 Web アプリケーション内の脆弱性箇所を修正する．セキュアプログラミング演習として，各脆弱性に対応したエスケープ処理やプレースホルダによる実装方法などを学ぶ．ソースコードの修正には，Web ブラウザ上に表示されるターミナル画面もしくは Visual Studio Code を使用する．ソースコードの修正後，再度演習用 Web アプリケーションに攻撃を実施して，攻撃の影響を受けないように脆弱性が解消されたことを確認する．

XSS，SQL インジェクション，NoSQL インジェクションの各脆弱性に対して，これらの演習を繰り返すことで，内在する脆弱性の特定方法や脆弱性を修正するためのセキュアプログラミングスキルを習得する．

4. 実 験

実験では，データベースへのインジェクション攻撃に関する演習について，座学と比較した本システムによる演習の有用性を検証した．実験対象者は，情報系学科の学生と情報系学科を卒業した大学院生（3 年生：3 名，4 年生：9 名，修士 1 年生：8 名）20 名を実験協力者とした．

実験の手順はまず，実験協力者 20 名に対して事前テストを実施した．次に，事前テストの平均点が均等になるように 2 グループに分割した．その後，それぞれのグループには本システムを利用した学習と座学による学習を実施してもらった．学習終了後に実験協力者 20 名に事後テストを実施した．なお，座学用の資料と事前テスト・事後テストの作成には，情報処理安全確保支援士試験の参考書と OWASP Foundation の資料を基に作成した．事前テストと事後テストは 10 点満点として，事後テストでは事前テストと同レベルの別の問題を使用した．また，事前テストの解答は実験協力者に公開せずに，事後テストを実施した．

表 1　実験結果

	事前テスト		事後テスト	
	平均	標準偏差	平均	標準偏差
本システム	3.5	1.12	8.4	1.36
座学	3.5	1.43	5.9	1.04

実験結果を表 1 に示す．表 1 に示されるように，事後テストの点数の標準偏差は小さいため，実験協力者は本システムを利用した学習と座学による学習ともに，一定の水準の学習レベルに到達したと考えられる．また，座学で学習したグループは平均点が 2.4 点上昇しているのに対して，本システムを利用して学習したグループは平均点が 4.9 点上昇している．以上の結果から，座学で学習したグループと比較して本システムを利用したグループの方がより有意に点数が高いことが確認できた．

5. 結 論

本研究では，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，脆弱性を特定するという攻撃者視点を取り入れた Web アプリケーションセキュリティに関するセキュアプログラミングの実践的演習システムを開発した．実験の結果，座学で学習したグループと比較して本システムを利用したグループの方がより有意に点数が高いことが確認できた．

謝辞

本研究は JSPS 科研費 21K12185 の助成を受けたものである．

参考文献

1) 総務省：不正アクセス行為の発生状況(2021), <https://www.npa.go.jp/cyber/pdf/R030304_access.pdf>, (参照 2021-12-21)
2) 八代哲，高橋和氏，渡辺亮平，角田裕太，田邉一寿，横山雅展，齋藤祐太，齋藤孝道: 体験型サイバーセキュリティ学習システムの提案と構築，コンピュータセキュリティシンポジウム 2017 論文集，Vol. 2017, No. 4, pp. 180–183 (2017).

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.