セキュアコーディング学習支援システムの開発

Developing a Learning Support System of Secure Coding

森田 浩平[*1], 松本 慎平[*1]
Kohei MORITA[*1], Shimpei MATSUMOTO[*1]
[*1] 広島工業大学情報学部
[*1]Faculty of Applied Information Science, Hiroshima Institute of Technology.
Email: {b214205, s.matsumoto.gk}@cc.it-hiroshima.ac.jp

あらまし：本稿では，セキュアコーディング学習支援と脆弱性を自動的に発見するプラットフォーム CureVuln[1]を開発したので，その詳細を示すことを目的とする．著者らはこれまで，デバッガ機能，コーディング過程の自動記録機能，オンラインジャッジメント機能を備えた Web ベースのプログラミング開発環境を開発してきた．CureVuln は，これを拡張した仕組みである．CureVuln は Web アプリケーションにおける脆弱性の対策を学習できるシステムである．Web アプリケーションとして動作するため，ユーザはブラウザのみで利用ができ，脆弱性の生じる原理や対策を脆弱なコードを修正することで学べる．学習効果や効率を高めるために CureVuln では以下の特徴を持たせている：１．学習コンテンツを容易に管理・追加が可能，２．学習コンテンツである脆弱なアプリケーションは特定の言語やフレームワークに依存しない，３．ユニットテストとファジングによる自動採点．
キーワード：プログラミング，Web サービス，セキュアコーディング，学習支援

1. はじめに

近年，ウェブに対するクロスサイト・スクリプティング（以後 XSS と称す）や SQL インジェクションなどの脆弱性を利用した攻撃が増加している．独立行政法人情報処理推進機構（以後 IPA と称す）の「ソフトウェア等の脆弱性関連情報に関する届出状況」[2]によると，IPA に報告された脆弱性届出件数は 2016 年には 12,916 件あり，ウェブサイトに関する届出が 9,483 件で全体の約 7 割を占めている．Web アプリケーション開発現場では Web アプリケーションフレームワークを用いることが主流である．このような Web アプリケーションフレームワークは基本的なセキュリティ機構が標準で備わっているため，開発者はセキュリティを意識せずとも堅牢なアプリケーションを作れるようになった．しかし，フレームワークやライブラリによって全ての脆弱性が保護されるわけではなく，これらを適切に使用しなければ脆弱性を作り込んでしまう．

安全なアプリケーションを開発するための根本的な解決方針としては，セキュアコーディングの指針に従うことである．OWASP によりセキュアコーディングガイド[3]が公開されるなど，開発者によってアプリケーションの脆弱性を防止する動きがある．ただし，ガイドラインに従った設計や開発を行うには開発者に相応の知識が要求される．よって，開発終了後の運営段階で，ガイドラインに準拠していないアプリケーションをガイドラインに準拠したアプリケーションへ変更する手法が取られることが多い．しかし，Web アプリケーションの脆弱性の検出は限定的であることから，セキュアなアプリケーションを開発できる技能の養成が必要であると考えられる．そこで本研究では，既存基盤(1)を土台とし，セキュアコーディング学習支援と脆弱性を自動的に発見するプラットフォーム CureVuln を開発した．本稿では，その概要と評価結果を示す．

2. 関連研究

Web アプリケーションの脆弱性を検出するための手法として様々な解析手法が提案されている．本研究に近いところでは，ソースコードの静的解析であるが，テイント解析などの手法で潜在的に危険なコードを発見する方法も進められている．Zhang らは ASP ベースのアプリケーションにおける XSS や SQL インジェクションをテイント解析で発見する手法を提示したが(2)，動的解析や静的解析の問題点として，実行速度や誤検出の多さなどの問題がある．鈴木らは Self-Protecting 技術を用いて Web アプリケーションにおける DOM based XSS を防止するためのガイドラインに沿った実装へ変更することで有用性を示したが(3)，この手法ではビルドインメソッドに変更を加えるため，アプリケーションが正常に動作する保証がない．

本研究と同様に，セキュアなアプリケーションを開発できる技能を養成することを目的とした取り組みもある．菱田らは，Java のセキュアコーディングを対象とし，インスタンスの状態を変更できないという特徴をもつ不変クラスのセキュアコーディングを利用した学習支援システム及びコードのチェッカ

[1] https://curevuln.com/
[2] https://www.ipa.go.jp/security/vuln/report/vuln2016q4.html
[3] https://www.owasp.org/images/0/08/OWASP SCP Quick Reference Guide v2.pdf

を設計・実装した(4). 不変クラスを用いたアプリケーション開発は有用であるが，Web アプリケーションの脆弱性は多岐に渡るため，不変クラスの利用だけで防げる脆弱性は少ない．竹下らは，WebGoat という攻撃方法理解用のツールと組み合わせたウェブサイト製作者向け脆弱性対策 e ラーニングシステム VulCES を開発した(5)．現在，セキュアコーディングを学べる環境は少なく，IPA からは脆弱性体験学習ツールとして AppGoat[4]が，OWASP からは OWASP Broken Web Application が提供されているが，脆弱性の発見手法に重みを置いたものである．

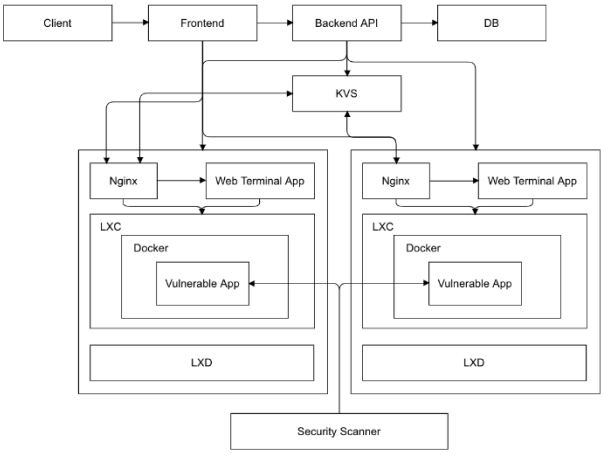

図 1 CureVuln のシステム構成図

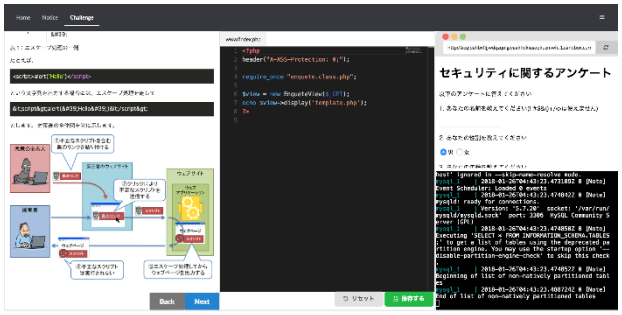

図 2 CureVuln の学習画面

3. CureVuln の提案と実装

CureVuln は Web アプリケーションにおける脆弱性の対策を学習できるシステムである．Web アプリケーションとして動作するため，ユーザはブラウザのみで利用ができ，脆弱性の生じる原理や対策を脆弱なコードを修正することで学べる．

CureVuln のシステム構成図を図 1 に示す．クライアントが学習コンテンツにアクセスすると，LXC コンテナが生成される．学習コンテンツである脆弱なアプリケーションは LXC 上で docker-compose が実行され，Docker コンテナ内で動作する．そのため，特定の言語やフレームワーク，アプリケーション構成に依存しない柔軟な環境の提供ができ，セキュアな環境で実行される．クライアントが問題の正誤判定を行うと，対応したユニットテストとファジングが実行され，自動採点が行われる．ユニットテストが失敗(Failure)した場合や，ファジングによって異常が発見された場合は不正解となる．CureVuln の学習画面を図 2 に示す．左ペインに学習用テキストを表示している．テキストは Markdown で記述したものを HTML としてレンダリングを行っている．中央ペインにはエディタを表示し，シンタックスハイライトや補完機能などのプログラミングにおける必須な機能を搭載している．右ペインには学習用アプリケーションの Web ページと動作しているコンテナのターミナルを表示している．エディタで編集した内容は即時学習用アプリケーションに反映され，一画面で学習を行える構成になっている．これら学習コンテンツはそれぞれ，Docker 利用時のディレクトリ構成に加えて，たった 1 つの YAML で管理されている．このように学習コンテンツは平文で管理が可能な状態であり，GitHub 上で公開することでユーザによる自由なコンテンツの追加や修正を実現している．

4. おわりに

本稿では，Web アプリケーションにおける脆弱性の対策を学習するためのサービス CureVuln を開発した．評価結果は当日発表で明らかにする．

謝辞

本研究は，本研究は独立行政法人 情報処理推進機構未踏 IT 人材発掘・育成事業[5]，独立行政法人日本学術振興会科学研究費助成事業(基盤研究(C)16K01147，17K01164)の助成を受けて実施した成果の一部である．ここに記して謝意を表します．

参考文献

(1) K. Morita, S Matsumoto, Developing a Cloud-Based Programming Learning Support Tool - Aiming to the Most Accessible Development Environment for University Students -, Proc. of AROB 2017, GS6-2, pp.143-146 (2017).
(2) Xin-Hua Zhang, Zhi-jian Wang, A Static Analysis Tool for Detecting Web Application Injection Vulnerabilities for ASP Program, 2nd International Conference on e-Business and Information System Security (EBISS), pp.22-23 (2010)
(3) 鈴木富明，白井丈晴，小林真也，川端秀明，西垣正勝，セキュリティガイドラインに準拠したアプリケーション作成支援に関する一提案，研究報告コンピュータセキュリティ，Vol. 2015, No. 8, pp.1-8 (2015).
(4) 菱田昂宏，早川智一，疋田輝雄，Java セキュアコーディングを促進する不変クラスチェッカの提案と実装，情報処理学会第 76 回全国大会講演論文集，pp.537-539 (2014).
(5) 竹下数明，小林偉昭，佐々木良一，脆弱性対策教育のための e ラーニングシステムの開発と評価，日本セキュリティ・マネジメント学会誌，24(1), pp.17-26 (2010).

[4] https://www.ipa.go.jp/security/vuln/appgoat/

[5]https://www.ipa.go.jp/jinzai/mitou/2017/gaiyou_t-1.html