7X-01

Webアプリケーションセキュリティにおける 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† 井口信和‡

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†
近畿大学理工学部情報学科，近畿情報学研究所‡

1. 序論

JPCERT が公開しているインシデント報告対応レポートによると，Web サイト改ざんの報告件数は，2018 年に 1055 件，2019 年には 1013 件となっており，Web サイトの改ざんは常に攻撃の対象となっている[1].

Web サイトが攻撃の対象とされる原因の一つとして，脆弱性を含んだ Web アプリケーションの存在があげられる．Web アプリケーションの脆弱性を悪用した代表的な攻撃にクロスサイトスクリプティング（以下，XSS）と SQL インジェクション（以下，SQLi）がある．XSS とは，ユーザのアクセス時に表示内容が生成される「動的 Web ページ」の脆弱性，もしくはその脆弱性を利用した攻撃方法のことである．SQLi とは，データベースシステムを不正に操作されてしまうことで，個人情報の漏洩や Web サイトが改ざんされてしまう攻撃のことである．XSS は Web アプリケーションに対する攻撃において検出数が 5 年連続で第一位となっている[2]．また SQLi も OWASP Top10 のレポートによると，SQLi 攻撃を含むインジェクション攻撃は 2010 年度版，2013 年度版，および 2017 年度版において常に第一位となっている[3].

前述のように，この 2 つの攻撃は Web アプリケーションを脅かす攻撃として常に脅威になっている．加えて XSS，SQLi は，攻撃の手口が年々複雑になっている．攻撃の手口が複雑になっている事から，これらの対策方法を学習するためには机上学習だけでなく，実践形式の演習が求められている．高度化・複雑化するサイバー攻撃を受けた時の被害を最小化し，他システムなどへの被害拡大を防ぐためには，サイバー演習が有効であるとの認識が国内外で高まっており，実践型のセキュリティ演習システムが開発されている[4].

Hands-on Learning System for Secure Programming in Web Applications
Kazuri Kishimoto†, Nobukazu Iguchi††,
† Department of Electronics and Systems Engineering, Interdisciplinary Graduate School of Science and Engineering Kindai University,
†† Department of Informatics, Faculty of Science and. Engineering, Kindai University, Cyber Infomatics Research Institute, Kindai University

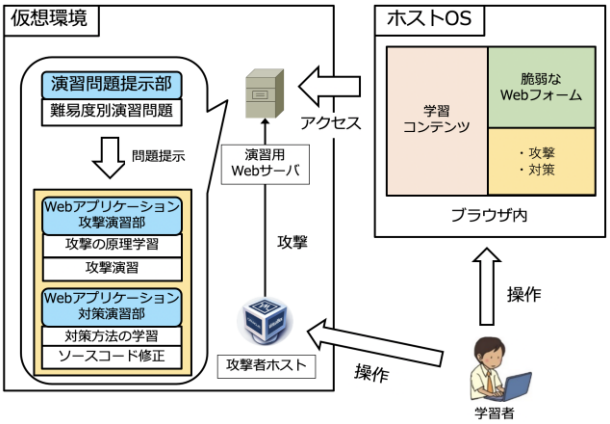

図 1 システム構成図

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学習を支援することを目的に，仮想マシンを用いたセキュアプログラミングについて学習できる実践的演習システムの開発した．仮想マシンを活用することで，実機を用意する必要がないため，低コストで演習が可能である．また，1 台のコンピュータ上に演習用 Web サーバと攻撃者ホストを構築することで，実運用されているネットワークやサーバに影響を与えずに，学習者は Web ブラウザ上で演習が可能である．

2. 関連研究

情報処理推進機構（以下，IPA）は，Web アプリケーションやサーバ・デスクトップアプリケーションの脆弱性について学習できる脆弱性体験学習ツール AppGoat[5]を提供している．このツールはホスト OS 上に脆弱性を含んだ Web サーバを用意して，脆弱性の体験学習を実施するものである．しかし，ホスト OS 上で脆弱性の体験学習を実施するには，安全性への懸念から PC をインターネットと切り離す必要がある．

これに対して本システムでは，仮想マシン上に脆弱な Web サーバを用意することで安全性を確保している．また本システムでは，ローカルプロキシツールを用いた脆弱性の発見方法の演習を重点的に支援することを特徴としている．さらに，攻撃には Web セキュリティの現場で使用されているペネトレーションテストツールを用いる．現実に近い被害を体験することで，実践的な対策学習への応用も可能となる．

3. 研究内容

本システムの構成を図1に示す．本システムでは，学習者の PC で安全に演習を実施するために，VirtualBox 上の仮想ネットワークに演習用 Web サーバと攻撃者ホストを生成する．演習用 Web サーバ内には演習を実施するために，Web アプリケーション攻撃演習部，Web アプリケーション対策演習部および演習問題提示部を配置している．

本システムでは，この演習用 Web サーバに Web ブラウザを使用してアクセスすることで，攻撃演習と対策演習を実施する．攻撃者ホストには，情報セキュリティ監査で用いられる KaliLinux2020.4 を使用する．

3.1. Web アプリケーション攻撃演習

本システムで学習可能な攻撃として XSS と SQLi がある．XSS に関する攻撃演習では，反射型 XSS と格納型 XSS の演習が可能である．SQLi に関する攻撃演習では，認証回避の SQLi，ブラインド SQLi，UNION インジェクションの演習が可能である．

3.2. Web アプリケーション対策演習

本システムで学習可能な XSS と SQLi 攻撃への対策方法としてそれぞれ次のようなものがある．XSS の対策方法としては特殊文字を一般的な文字列に変換するサニタイジングについて演習する．SQLi の対策としては，プレースホルダの実装方法について演習する．

3.3. 演習手順

本システムでは，Web アプリケーション攻撃演習部と Web アプリケーション対策演習部で攻撃と対策の方法について学び，それぞれの実践を繰り返し演習することで，対策方法への理解を深める．

Web アプリケーション攻撃演習部では，XSS と SQLi に対して脆弱な Web アプリケーションに攻撃を実施する．まず初めに，学習者は，演習用 Web サーバ内に格納されている学習コンテンツを利用して，XSS や SQLi の概要や攻撃原理を学習する．実際に入力をして，脆弱な Web アプリケーションの挙動を確認しながら学習を進めていく．

次に，学習者は攻撃者ホストから BurpSuite を使用して，攻撃者ホストと演習用 Web サーバ間のリクエストとレスポンスの解析手法を学習する．最後に演習問題提示部に格納されている問題に対して攻撃演習を実施して，脆弱性の見つけ方を学習する．

Web アプリケーション対策演習部では，学習者が脆弱性箇所のソースコードを修正することで対策演習を実施する．初めに，学習者は学習コンテンツを使用して対策方法について学習する．その後，Web アプリケーション対策演習部内に配置されているコンソール画面を通じて，脆弱な Web アプリケーションのソースコードを修正する．修正後，適切に修正がなされているかを確認するために再度攻撃を実施して，攻撃を受けないように修正できているかを確認する．

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	4.71	1.28	8.71	0.88
座学	5.29	1.98	7.86	0.98

4. 評価実験

実験では，本システムを用いることで XSS 対策学習の支援ができることを確認するために評価実験を実施した．対象者は情報系学部の大学生 10 名，大学院生 6 名の計 16 名である．まず実験対象者を XSS について本システムで学習するグループと座学で学習するグループの 2 つに分割し，それぞれ学習の前後に XSS に関する事前・事後テストを実施した．2 グループの事前テストと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した．テスト内容は IPA による情報処理安全確保支援士試験の過去問と問題集を基に問題を作成し，事後テストでは事前テストと同レベルの別の問題を用意した．問題数はそれぞれ 10 問となっており，1 問 1 点として点数をつける．事前テストで解いた問題の解答は公開せずに，事後テスト実施した．

実験結果が表 1 である．本システムを用いた学習時には平均点が 4.00 点上昇しており，座学での学習時には平均点が 2.57 点上昇している．また事後テストの標準偏差が小さいことから学習後の点数が本システム，座学ともに安定していることが分かる．これらの結果から，本システムが XSS 対策学習の支援ができていることを確認できた．SQLi についても同様の方法で評価実験を実施する予定である．

5. 結論

本研究では，Web アプリケーションセキュリティにおけ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．本システムを使用することで安全な Web アプリケーションの作成方法を学べると期待できる．今後の予定として，NoSQL インジェクションに関する演習項目の追加を検討している．

参考文献

1) JPCERT/CC，インシデント報告対応レポート[2019 年 10 月 1 日~2019 年 12 月 31 日]<https://www.jpcert.or.jp/pr/2020/IR_Report20200121.pdf>(参照 2020-10-13)
2) 株式会社 LAC:セキュリティ診断レポート 2018 陽春<https://www.lac.co.jp/lacwatch/report/20180405_001609.html}>(参照 2020-10-13)
3) OWASP，OWASPTop10-2017<https://www.owasp.org/www-pdf- archive/OWASP_Top_10-2017(ja).pdf>
4) 八代哲，高橋和氏ほか，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，(参照 2017-10-16)
5) 独立行政法人情報処理推進機構 IPA:脆弱性体験学習ツール AppGoat 入手先<https://www.ipa.go.jp/security/vuln/appgoat/index.html>(参照 2020-07-21)