6ZA-06

仮想マシンを活用した クロスサイトスクリプティングの実践的演習システム

岸本　和理†　　井口　信和†

近畿大学理工学部情報学科†

1.　序 論

平成 30 年度に総務省が行った調査によると不正アクセスの認知件数は 1486 件と平成 29 年度より 20%以上増加している[1]．不正アクセスが発生する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代表的な攻撃の一つにクロスサイトスクリプティング(以下，XSS)がある．XSS とは攻撃者が作成した不正なスクリプトを脆弱性が存在する Web アプリケーションを利用して閲覧者に実行させる攻撃である．XSS は，Web アプリケーションに対する攻撃において，2013 年より 5 年連続検出数が第一位となっており，現在でも常に Web アプリケーションへの攻撃として脅威になっている[2]．加えて XSS は，1990 年代に存在が確認されてから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，XSS の対策方法を学習するために机上学習だけでなく，実践形式の学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際に被害を最小化し，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いる．また攻撃者の思考や心理，技術を勘案した対抗措置を講じる事を可能にするために，実践型のセキュリティ演習がされている[3]．

そこで本研究では，Web アプリケーションに対する XSS 対策の学習を支援することを目的に，仮想マシンを活用した XSS の実践的演習環境を開発した．本システムにより，XSS に関する安全な Web アプリケーションの作成方法を学習できると考えられる．

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 を提供している[4]．このツールはホスト OS 上に脆弱性を含んだ Apache Web Server を用意して，脆弱性の体験学習を行う．学習方法は，まず攻撃の原理を学習してから簡易的な攻撃演習を実施する．攻撃演習完了後にその攻撃の影響や対策方法についてさらに教材で学習する．最後に，対策方法を学習し，Web アプリケーションのソースコードを修正する．しかし，ホスト OS 上に Web サーバを用意して脆弱性の体験学習をするには安全性への懸念から PC をインターネットから切り離す必要がある．

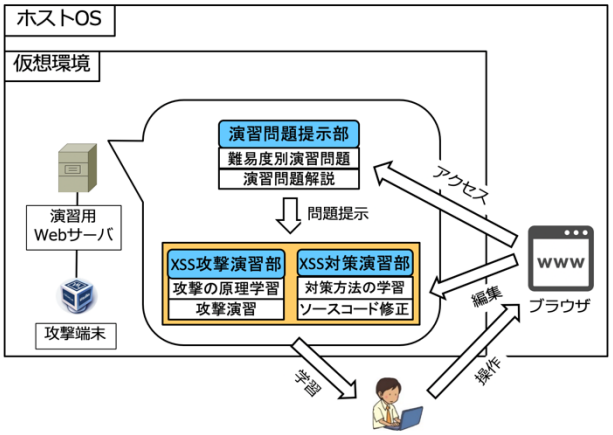

図 1　本システムの構成

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攻撃演習をする上で必要な脆弱性の発見方法の学習を重点的に支援できることを特徴としている．脆弱性の発見にはローカルプロキシツールを用いてサーバとクライアント間の通信を監視する．攻撃には実際に 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．実際に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．これらのことから本システムを使用することにより XSS に関する安全な Web アプリケーションの作成方法を学べるだけでなく，既存の Web アプリケーションへの対策方法を学ぶことができる．

3.　研究内容

本システムの構成を図 1 に示す．本システムは Web エンジニアを対象とした XSS に関する対策演習ができるシステムである．仮想化ソフトウェアには VirtualBox6.0.14 を使用した．演習用 Web サーバの構成として，仮想マシンの OS には安定したパッケージリストやメンテナンスが長期間提供され，サーバ OS としてもシェアを占めていることから Ubuntu18.04LTS を採用した．Web サーバソフトウェアには Apache2.4.41，サーバサイド言語には PHP7.2.24，データベースソフトには MySQL8.0.18 を導入した．また仮想マシン内には XSS の演習を実施するために，XSS 攻撃演習部，XSS 対策演習部お

Practical Exercise System for Cross-Site Scripting using Virtual Machines

†Kazuri Kishimoto, Nobukazu Iguchi, Department of Informatics, Faculty of Science and Engineering, Kindai University

Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.

よび演習問題提示部を用意する．攻撃端末には情報セキュリティ監査やペネトレーションテストで用いられる Kali Linux を使用する．本システムではこの仮想マシン上の Web サーバを起点として XSS の対策学習を行っていく．Web エンジニアが Web アプリケーションを作成する上で対策すべき XSS の種類として反射型 XSS と格納型 XSS がある．本システムでは，この 2 つの XSS に焦点を当てた演習ができる．

反射型 XSS は主に攻撃者が用意した URL を介してスクリプトを実行させる攻撃の手法である．まず攻撃者は XSS の脆弱性がない正常な Web サイト上にスクリプトを含ませた URL を書き込む．被害者が正常な Web サイトにて攻撃者が書き込んだスクリプト入りの URL にアクセスすると，脆弱性のあるサイトに誘導され XSS の被害を受けてしまう攻撃手法である．

格納型 XSS とは攻撃者が Web アプリケーション内のデータベースなどにスクリプトを埋め込み，ユーザがサイトを閲覧しただけでスクリプトが実行される攻撃手法である．一度スクリプトが埋め込まれてしまえばスクリプトが除去されない限り持続的に動作し続ける．また反射型のように脆弱性のあるページへ誘導するといった手順が不要なため，被害も受けやすくなっている．

4. 演習手順

学習者はまず XSS 攻撃演習部において，攻撃が発生する原理を学習する．そして，演習問題提示部に配置されている対象の Web アプリケーションに対して攻撃端末の Kali Linux からローカルプロキシツールを用いて XSS の脆弱性を検出する．ローカルプロキシツールには Web アプリケーションを保護することを目的としているコミュニティである The Open Web Application Security Project（以下，OWASP）が開発した OWASP ZAP を使用する．そして発見した XSS の脆弱性に対してペネトレーションテストツールである BeEF Framework を用いて実際に XSS 攻撃を実施することで被害状況を確認する．これらの演習を通して学習者は XSS 攻撃について学ぶ．

次に学習者は XSS 対策演習部において XSS 攻撃演習部で発見した XSS の脆弱性箇所のソースコードを修正する．ソースコードの修正後，XSS 攻撃演習部にて再度同じ攻撃を行い，攻撃を受けないように適切に修正できているかを確認する．

5. 実 験

実験は本学の情報系の学生 16 名を対象に行った．まず実験対象者を XSS について本システムで学ぶグループ 8 名と座学で学ぶグループ 8 名の 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・事後テスト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．テストは IPA が刊行する参考書をもとに作成を行い，事後テストでは事前テストと同レベルの別のテストを用いた．事前テストで解いた問題の回答は公開せずに事後テストを行った．実験の結果を表 1 に示す．実験の結果から，本システムでの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 点上昇していることが分かる．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．

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

これらの結果からも本システムが XSS 対策の学習を支援できていることを確認した．

6. 結 論

本研究では，Web アプリケーションに対する XSS 対策の学習を支援することを目的に，仮想マシンを活用した XSS の実践的演習環境を開発した．本システムを用いることで XSS に関する安全な Web アプリケーションの作成方法を学習できると考えられる．

今後の予定として OWASP により最も重大なウェブアプリケーションリスクの第一位に選ばれているインジェクションに関する演習の追加を検討している．インジェクションの種類には SQL インジェクション，OS コマンドインジェクションなどが含まれている．これらの対策演習を追加することで Web アプリケーション全体の安全な作成方法を学習できるシステムを作成する．

また XSS の演習に関しても演習問題の難易度の追加を検討している．難易度の追加にはバグバウンティ報償金プラットフォームである HackerOne[5]などの利用を検討している．HackerOne の XSS に関するバグバウンティレポートを参考に，実際にあった脆弱性の事例をもとに脆弱性の発見方法とその対策方法についての実践的な学習を行えるようにしたいと考えている．

参考文献

1) 総務省：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況，入手先〈http://www.soumu.go.jp/main_content/000606259.pdf〉(参照 2020/01/10).
2) 株式会社 LAC：セキュリティ診断レポート 2018 陽春，入手先<https://www.lac.co.jp/lacwatch/report/20180405_001609.html>(参照 2020/01/10).
3) 青山友美：サイバー演習の有効性 レジリエントな組織づくりに向けて 国立大学法人名古屋工業大学，入手先<https://www.jpcert.or.jp/present/2015/ICS20150212-NITech.pdf>(参照 2020/01/10).
4) 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 2020/01/10).
5) HackerOne:BugBounty-Hacker Powered Security Testing，入手先<https://www.hackerone.com>(参照 2020/0/10).

Copyright ©2020 Information Processing Society of Japan.
All Rights Reserved.