G-07

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学習環境の開発

岸本 和理†　　井口 信和†
Kazuri Kishimoto　Nobukazu Iguchi

1. 序論

平成 30 年度に警視庁が行った調査によると不正アクセスの認知件数は 1486 件と前年度より 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 アプリケーションへの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)が挙げられる．XSS とは攻撃者が作成した不正なスクリプトを脆弱性のある 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のことを言う[2]．その 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 Web アプリケーションへの攻撃として用いられている[3]．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[4]．

このように攻撃の手口が複雑になっている事から，机上学習に加えて，実践形式の学習がされている．高度化・複雑化するサイバー攻撃に対して，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[5]．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[6]．

そこで本研究では，XSS に関する安全な Web アプリケーション作成において実践的な学習ができるよう支援する事を目的に，仮想マシンを活用した XSS の実践的学習環境を開発する．この学習環境を用いることで XSS に関する安全な Web アプリケーションの作成方法の学習を支援できることが期待できる．

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[7]．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．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，対策方法の学習を行い 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ため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．

†近畿大学理工学部情報学科，
Department of Informatics,Faculty of Science and Engineering, Kindai University

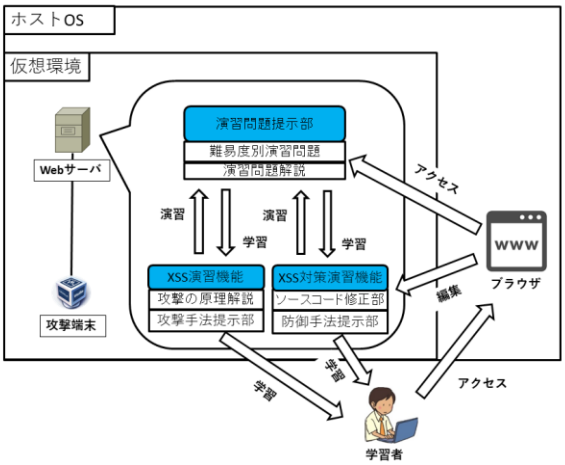

図 1　システム構成図

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の確保を行っている．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の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 に関する対策演習を行うことができるシステムである．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公式より提供され，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 Apache2.4.29，サーバサイド言語には PHP7.2.17，データベースソフトには MySQL8.0.16 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 対策演習部および演習問題提示部が用意されている．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 KaliLinux [8]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 にアクセスしてしまうと，脆弱性のあるサイトに誘導されてしまい XSS の被害を受けてしまう．これが反射型 XSS の流れである．

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(以下，DB)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. 演習の手順

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．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 KaliLinux からローカルプロキシツールを用いた XSS の脆弱性の検出を行う．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[9]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[10]を用いて実際に XSS 攻撃を実施することで被害状況の確認を行う．これらの演習を通して学習者は XSS 攻撃について学んでいく．

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

実験は情報系大学生，大学院生を対象に行う．演習前と演習後に XSS に関する問題を解いてもらい，点数の差からシステムの有用性を明らかにする予定である．

テスト内容は IPA が刊行する参考書をもとに問題を作成する．SP 表分析を行い問題の妥当性を確認し，演習前に解いた問題を公開せず，本システムを使用した後に同じ内容のテストを受けてもらう．演習前に解いた点数と演習後に解いた点数の差によって有用性の証明を予定している．

6. 結論

本研究では仮想マシンを活用した XSS の実践的学習環境の開発を行った．このシステムを使用し，XSS について学習することで安全な Web アプリケーションの作成方法や既存の Web アプリケーションに対する防御策の方法を学習し，不正アクセスを減らすことが期待できる．

このシステムの今後の予定として演習問題の難易度の追加や学習者の進捗度合い，理解度を図るような機能の追加を予定している．難易度の追加に関しては，バグバウンティ報奨金プラットフォームである HackerOne[11]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．

また Web アプリケーションへの主要な攻撃として存在する SQL インジェクションや OS コマンドインジェクションの対策学習ができるような拡張を行うことを検討している．

7. 参考文献

[1] 警視庁：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 2019/07/24)

[2] TrendMicr：クロスサイトスクリプティング(XSS)，入手先<https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/xss.html>(参照 2019/07/20)

[3] 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 2019/07/20)

[4] Secure SketCH：サイバーも「防災訓練」の時代へ！企業が実施すべき演習のやり方，入手先<https://www.secure-sketch.com/blog/security-incident-response-training (参照 2019/07/20)

[5] NRI FinancialSolutions：高まるサイバー演習の重要性と有効活用のための考え方，入手先<http://fis.nri.co.jp/~/media/Files/publication/kinyu-itf/2017/05/itf_201705_4.pdf > (参照 2019/07/20)

[6] 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<https://www.jpcert.or.jp/present/2015/ICS20150212-NITech.pdf> (参照 2019/07/20)

[7] 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，<https://www.ipa.go.jp/security/vuln/appgoat/index.html>(参照 2019/07/20)

[8] Offencive Security：KaliLinux，入手先<https://www.kali.org >(参照 2019/07/20)

[9] OWASP ZED Attack Proxy Project，入手先<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project >(参照 2019/07/20)

[10] THE BROWSER EXPLOITATION FRAMEWORK PROJECT，入手先<https://beefproject.com/> (参照 2019/07/20)

[11] HackerOne:BugBounty-Hacker Powered Security Testhing, 入手先<https://www.hackerone.com/>(参照 2019/07/20)