G-07

仮想マシンを活用した SQL インジェクションの実践的学習環境の開発

Virtual Machine Based SQL Injection Developing a Practical Learning Environment

岸本 和理† 井口 信和‡
Kazuri Kishimoto Nobukazu Iguchi

1. 序論

JPCERT によって行われたインシデント報告対応レポートによると、2019 年における Web サイト改ざんの報告件数は 1013 件となっている[1]. 2018 年における報告件数は 1055 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.

Web サイトが攻撃の対象とされる原因として，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の一つに SQL インジェクションがある．SQL インジェクションとはデータベースシステムを不正に操作する攻撃のことで、個人情報の漏洩や Web サイトの改ざんなどが行われてしまう攻撃である．ソフトウェアセキュリティを取り巻く脅威、課題の解決を目的とした国際的なコミュニティである OWASP が発表している OWASP Top10 というレポートによると、インジェクション攻撃は 2010・2013・2017 年度版において常に第一位となっており、その被害影響度も甚大なものとなっている[2]. 加えて SQL インジェクションは，現代のシステム環境に合わせた攻撃も増え、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，SQL インジェクション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いる[3]. 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システムが開発されている[4].

そこで本研究では，Web アプリケーションに対する SQL インジェクション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 SQL インジェクションの実践的学習環境の開発を行う．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，低コストで学習が可能である．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及ぼさずに，学習者は Web ブラウザ上で SQL インジェクション攻撃と SQL インジェクション対策の両方の演習を行うことが可能である.

1 近畿大学大学院総合理工学研究科
Graduate School of Science and Engineering Research, Kindai University .Higashiosaka，Osaka 577-8502，Japan
2 近畿大学理工学部情報学科
Department of Informatics, Faculty of Science and Engineering, Kindai University .Higashiosaka，Osaka 577-8502，Japan

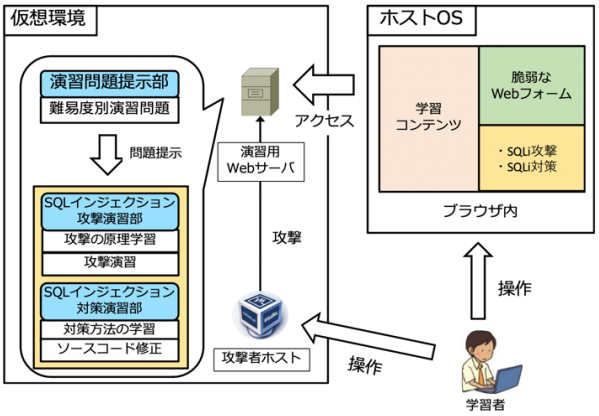

図 1　システム構成図

2. 関連研究

情報処理推進機構は，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行う．しかし，ホスト OS 上で脆弱性の体験学習を行うには，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学習を重点的に支援できることを特徴としている．加えて，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

3.1 システム構成

本システムの構成を図 1 に示す．本システムは，Web エンジニアを対象に，SQL インジェクションに対して対策演習が実施できるシステムである．このシステムでは，学習者の PC で安全に演習を行うために，2 つの仮想マシンを演習用 Web サーバと攻撃者ホストとして使用する．これらを構築するために仮想化ソフトウェアに VirtualBox6.1.4 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 Ubuntu18.04LTS，Web サーバソフトウェア Apache2.4.41，サーバサイド言語には PHP7.2.24，データベースには MySQL8.0.18 を導入した．また演習用 Web サーバ内には SQL インジェクションの演習を実施するために，SQL インジェクション攻撃演習部，SQL インジェクション

対策演習部および演習問題提示部を用意する．

本システムでは，この演習用 Web サーバに対して Web ブラウザを使用してアクセスすることで SQL インジェクションの対策学習を実施する．攻撃者ホストには，情報セキュリティ監査で用いられる KaliLinux2020.1 を使用する．KaliLinux のツールの中で，主に使用するツールは BurpSuite，OWASP ZAP，SQLMap である．

3.2 使用ツール

■ BurpSuite

BurpSuite は PortSwigger 社が提供しているローカルプロキシツールである．ローカルプロキシツールとは Web サーバとブラウザ間の通信の監視などが行えるツールである．本研究では、BurpSuite を用いて通信の解析を行い SQL インジェクションの脆弱性を検出するために用いる．

■ OWASP ZAP

OWASP ZAP(Zed Attack Proxy)は，オープンソースの Web アプリケーション脆弱性診断ツールである．こちらもローカルプロキシツールであるが、本研究では SQL インジェクションの自動検出に用いる．OWASP ZAP で検査可能な主な脆弱性として，以下のものがある．

・XSS（クロスサイトスクリプティング）
・SQL インジェクション
・ディレクトリトラバーサル

■ SQLMap

SQLMap は SQL インジェクションの脆弱性の検出を自動化するオープンソースのペネトレーションテストツールである．特徴として MySQL をはじめ Oracle，Microsoft SQL Server，PostgreSQL など多くのデータベース管理システムに対応している．

3.3 演習手順

演習手順は SQL インジェクション攻撃演習部と SQL インジェク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行うことで，理解を深める．

SQL インジェクション攻撃演習部では，SQL インジェクションに対して脆弱な Web アプリケーションに SQL インジェクション攻撃を行う．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，SQL インジェクションの概要や攻撃原理を学ぶ．実際に入力を行い，Web ページ上に埋め込まれた脆弱な 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，学習コンテンツ内の Web アプリケーション上で，ローカルプロキシツールの使い方を学習する．最後に演習問題提示部に格納されている難易度別演習問題に対して SQL インジェクション攻撃演習を行う．

学習者は手動の SQL インジェクション攻撃に加えて，攻撃者ホストからローカルプロキシツールである 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を解析する．また OWASP ZAP や SQLMap などの自動検出ツールを用いて SQL インジェクションの検出方法についても学習をする．

SQL インジェクション対策演習部では，脆弱性箇所のソースコードを修正して SQL インジェクション対策を行う．まず初めに，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， SQL インジェクション 対策演習ページ内に配置されている演習用 Web サーバのコンソール画面を通じて，演習用 Web サーバ内の脆弱な Web アプリケーションのソースコードを編集する．

ソースコードの編集では，プレースホルダによる SQL 文の組み立て方法について学習する．プレースホルダを用いた SQL 文の組み立てを行うことで SQL インジェクションの脆弱性を解消することが可能である．ソースコードの修正後，修正が適切になされているかを確認するために再度 SQL インジェクション攻撃を行い，攻撃を受けないように修正できているかを確認する．

4. 実験

実験は情報系学部の大学生，大学院生を対象に行う．実験対象者を SQL インジェクションについて本システムで学ぶグループと座学で学ぶグループ 2 つに分割し，それぞれ学習の前後に SQL インジェクションに関する事前・事後テストを実施する予定である．2 グループの事前・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する予定である．

テスト内容は情報処理推進機構による情報処理安全確保支援士試験の参考書[6]と過去問を基に問題を作成する．事後テストでは事前テストと同レベルの別の問題を用いる．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，事後テストを行う予定である．

5. 結論

本研究では，Web アプリケーションに対する SQL インジェクション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 SQL インジェクションの実践的演習環境を開発した．本システムを使用することで SQL インジェクションに対して安全な 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，現在のシステム環境では SQL と NoSQL を併用して構築が行われていることが多いことから、学習環境に NoSQL インジェクションについて学習することができるシステムの追加を検討している．

謝辞

本研究は JSPS 科研費 18K11592 の助成を受けたものである．

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]入手先 <https://www.jpcert.or.jp/pr/2020/IR_Report20200121.pdf > (参照 2020-07-21)

[2] OWASP:OWASP Top10 -2017 入手先 <https://www.owasp.org/www-pdf-archive/OWASP_Top_10-2017(ja).pdf > (参照 2020-07-21)

[3] 八代哲，高橋和氏，渡辺亮平ほか．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，2017(2), (2017-10-16)

[4] 立岩佑一郎，岩崎智弘，安田孝美．仮想マシンネットワークによる継続的なクラッキング防衛演習システム．電子情報通信学会論文誌，Vol. J96-D, No. 7, pp. 1585–1594 (2013).

[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).

[6] 上原孝之，情報処理教科書 情報処理安全確保支援士 2020 年版．翔泳社，2019.