様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ４ 月 ２２ 日現在

機関番号：３４４１９
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１２１８５

研究課題名（和文）仮想マシンを活用したSQL・NoSQLインジェクション対策演習支援システム

研究課題名（英文）SQL/NoSQL Injection Countermeasure Exercise Support System Using Virtual Machines

研究代表者
井口　信和（Iguchi, Nobukazu）

近畿大学・情報学部・教授

研究者番号：５０３５１５６５

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：Webアプリケーションに対するSQLおよびNoSQLインジェクション対策の学習を支援する、仮想マシンを活用した実践的な演習システムの開発研究を目的とし研究を遂行した。本システムによって、学習者は安全かつ手軽にセキュリティ対策の実践的な演習が実施できる。さらに学習者は一人で対策演習と攻撃演習を実施することが可能である。
本課題では，予定どおりSQLインジェクションとNoSQLインジェクションの対策演習機能と攻撃演習機能を実装した。さらに，これまでに開発したDoS攻撃、ARP Spoofing攻撃等の演習機能を統合化した。本システムにより，実践的なセキュリティ演習の実施が可能となる。

研究成果の学術的意義や社会的意義
サイバー攻撃が増加し、手口も巧妙化することで対策の難易度が上昇している。こうした現状を改善するために、防御側視点だけでなく、攻撃側視点からも攻撃の性質やプロセスを学習し、対策に活かすことが重要である。
本課題で開発した仮想マシンを活用したSQL・NoSQLインジェクション対策演習支援システムは、一般に広く使われているWebアプリケーションに対するセキュリティ攻撃への実践的な対策演習を可能とするものである。本課題の成果によって、ソフトウェアによるセキュリティ対策の実践的演習システムが実現できる事、ネットワークセキュリティ技術者の早期の養成を目的とした学習環境の構築が可能である事を明らかにした。

研究成果の概要（英文）：I conducted a research project to develop a practical exercise system using a virtual machine to support the learning of SQL and NoSQL injection countermeasures for Web applications. This system enables learners to practice practical security countermeasures safely and easily. Furthermore, the learner can perform both countermeasure exercises and attack exercises by himself/herself.
In this project, I implemented the countermeasure and attack practice functions for SQL injection and NoSQL injection as planned. In addition, I have integrated the previously developed exercise functions for DoS attacks, ARP Spoofing attacks, and others. This system enables the implementation of practical security exercises.

研究分野：情報ネットワーク

キーワード：攻防戦型セキュリティ演習機能　SQLインジェクション攻撃演習　仮想マシン

１．研究開始当初の背景

情報システムに対する不正アクセスや情報漏えいの事故は社会問題の一つになっている。その一方で、組織における脆弱性診断などの実施は十分にされていない現状がある。その原因の一つとして、セキュリティ対策に精通したネットワーク技術者の慢性的な不足があげられる。さらに、年々サイバー攻撃が増加し、手口も巧妙化することで対策の難易度が上昇している。こうした現状を改善するために、サイバー攻撃に対して防御視点だけでなく、攻撃視点からも攻撃の性質やプロセスを学習し、対策に活かすことが重要である。

そこで本研究では、SQL インジェクション対策と NoSQL インジェクション対策を対象に、攻撃側と防御側の両視点からセキュリティ演習が実施可能な環境の提供を目的に、攻防戦型演習を可能とするセキュリティ演習システム（以下、本システム）を開発した。

２．研究の目的

本研究課題の目的は、仮想マシン環境を活用した SQL インジェクション対策演習システムおよび、NoSQL インジェクション対策演習システムを用いて、Web アプリケーションに対するインジェクション対策演習を実現する各機能と演習システムの開発である。本システムによって、学習者は安全かつ手軽にセキュリティ対策の実践的な演習が実施できる。さらに本システムを用いることで、学習者は一人で対策演習と攻撃演習を実施することが可能となるため、身近に他の学習者がいない環境、たとえば対面による実習・演習が困難な場合や学習者が自宅で自己学習として演習を行う場合でも、対策側と攻撃側の双方の演習が可能となる。

３．研究の方法

本研究課題では、申請者がこれまでに開発した IP ネットワーク構築演習支援システムを基盤技術として活用した。また、仮想マシンを活用したネットワークセキュリティ学習支援システムを発展させ、インジェクション攻撃対策演習機能を開発した。さらに、攻防戦型ネットワークセキュリティ学習支援システムで実装した攻撃用仮想サーバや仮想マシンによるネットワーク機器のログ確認機能等を活用した。本課題では以下の新規機能を既存システムに組み込むことで確実に動作するシステムとして開発した。

本研究課題で新規に開発した項目は次の通りである。図１にシステム構成案を示す。

1. 演習課題提示部と学習者操作側 GUI
2. SQL インジェクション攻撃演習部・対策演習部
3. NoSQL インジェクション攻撃演習部・対策演習部

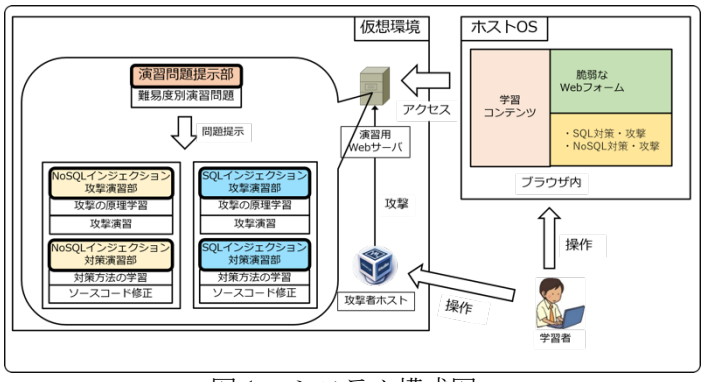

図１：システム構成図

SQL インジェクション攻撃演習部・対策演習部と NoSQL インジェクション攻撃演習部・対策演習部には、Web アプリケーション脆弱性診断ツールである Burp Suite を組み込むことで、脆弱性の発見方法の学習を可能とした。脆弱性と発見と OWASO ZAP、SQLmap 等を使ったインジェクション攻撃の体験が可能である。さらに、対策演習部によって、対策手法の解説ページを参照しながら、Web アプリケーションのソースコードの編集が可能である。演習課題提示部と学習者操作側 GUI はブラウザで表示可能とした。

さらに攻防戦型セキュリティ対策演習の体験機能を追加で実装した。これは、学習者が 2 人 1 組で攻撃側と防御側に分かれ、リアルタイムで DoS 攻撃、ARP Spoofing 攻撃、不正侵入攻撃及び SQL インジェクション攻撃の実施を可能とするものである。本機能は、Firewall、WebServer 及び攻撃用ホストを新規に実装することで実現した。学習者は、演習実施前に、事前学習ページで本システムの利用方法と攻撃方法及び防御方法を学習する。その後、防御側が仮想ネットワークを構築する。利用可能な機器は Host、Hub、Router、Firewall 及び WebServer である。次に攻撃側は、演習時間を設定し、制限時間内で攻撃用ホストを用いて攻撃を実施する。攻撃は、サービスの妨害や個人情報の閲覧、DB の閲覧と改ざんを目的として行う。防御側は、攻撃内容を調

査し、攻撃の対策を施す。演習中に攻撃方法や対策方法が分からない場合は、ヒント機能を活用し、円滑に演習に取り組める。演習終了後、勝敗判定機能により、対応できなかった攻撃に関するフィードバックを提示する。2 人 1 組のセキュリティ演習は、防御側はランダムに実施される攻撃の種類を特定して対策するため、実践的なセキュリティ演習が可能である。また攻撃側は、実際に攻撃を体験することで攻撃の性質やプロセスを学習できる。図 2 に攻防戦型セキュリティ演習の画面を示す。

図 2:攻防戦型セキュリティ演習の表示例

４．研究成果

本システムが想定する演習のネットワークの規模に対応可能であることを確認するために、性能評価実験を実施した。実験内容は、想定する最大規模のネットワークを用いて、本システム利用時に最も負荷がかかる DoS 攻撃実施時の最大 CPU 使用率とメモリ使用量を計測した。また、同時に何組まで演習可能かを計測した。測定はそれぞれの場合で 10 回ずつ計測した。想定する最大規模は、Host、Router、Firewall をそれぞれ 5 台、Hub を 2 台、WebServer、攻撃用ホストをそれぞれ 1 台とした。サーバは VirtualBox 上で起動し、割り当てたスペックは CPU：AMD Ryzen5 4600G with Radeon Graphics 3、70GHz、Mem：10G、OS：Ubuntu 20.04 LTS である。計測結果を表 1 に示す。また、演習は同時に 5 組まで、円滑に利用できることを確認した。この結果から、本システムは想定する演習のネットワークの規模に対応可能であることを確認した。

表 1 ：性能評価実験

計測項目	平均	標準偏差
最大CPU使用率	40.1%	2.8%
メモリ使用量	1.78GB	0.06GB

続いて、本システムを用いた場合の学習効果を確認するために利用評価実験を実施した。実験対象者は学部生 2 名、大学院生 8 名の合計 10 名である。実験内容は、まず、事前テストを実施し、次に学習者を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に分け、学習に取り組んでもらった。学習終了後、事後テストを実施した。テスト内容は基本情報技術者試験と応用情報技術者試験を基に作成した。事前・事後テストはそれぞれ 15 点満点とし、両テストは同レベルの別問題とした。実験の結果を表 2 に示す。事前・事後テストの点数差から本システムの方が学習効果が高いことを確認した。

表 2 ：利用評価実験

計測項目	平均	標準偏差
最大CPU使用率	40.1%	2.8%
メモリ使用量	1.78GB	0.06GB

本研究課題では、SQL インジェクション対策と NoSQL インジェクション対策の演習機能などを実装する，攻防戦型の SQL・NoSQL インジェクション対策演習システムを開発した。本システムの利用により、攻撃側と防御側の両視点からネットワークセキュリティ演習の実施が可能な環境が提供でき、本研究の成果から、ソフトウェアによって実装するセキュリティ対策演習システムが、セキュリティ対策学習に有用であることを明らかにした。本研究成果は、今後ますます必要となるネットワークセキュリティ技術者の養成の一助になることが期待できる。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 寺西 弘登, 井口 信和
２．発表標題 攻防戦型演習を可能とするネットワークセキュリティ学習システムにおけるSQL インジェクション攻撃演習機能の追加
３．学会等名 情報処理学会第85 回全国大会
４．発表年 2023年

１．発表者名 岸本和理、　井口信和
２．発表標題 仮想マシンを活用したNoSQLインジェクションの実践的演習環境の開発
３．学会等名 2021年度情報処理学会関西支部支部大会
４．発表年 2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関