仮想 Linux 環境を利用したネットワーク構築演習システムへの SQL インジェクション対策学習機能の実装

上田 拓実† 谷村 真一郎‡ 井口 信和‡

近畿大学大学院総合理工学研究科† 近畿大学理工学部情報学科‡

1. はじめに

近年，Web サイトを対象とした SQL インジェクションによる攻撃の被害が急増している(1)．図 1は，SQL インジェクションによる攻撃の被害数の急増を示すグラフである．2008 年 2 月以降，被害数が急増していることが分かる．

情報セキュリティの学習では，攻撃手法を知ることがセキュリティ対策の学習につながる．また，攻撃を受けた際にどのようなログが出力されるかを学ぶことで，ログから攻撃手法やシステムの脆弱性を推測するスキルを習得できる．

しかし，学習のために運用中のシステムを利用することは，システムの動作に影響を及ぼす可能性があるため困難である．そこで，本研究では，SQL インジェクションによる攻撃の手法と対策の学習を目的として，仮想 Linux 環境を用いたネットワーク構築演習システム(2)（以下，本システム）に SQL インジェクション対策学習機能を実装した．本システムでは，仮想化技術を用いて構築した Web サーバを対象に，SQL インジェクションによる攻撃を実践する．また，ログを効率的に確認する機能も実装しており，サーバが出力するログを攻撃手法と対応付けて確認できる．

2. 研究内容

2.1. システム概要

本システムは，仮想 Linux 環境を用いたネットワーク構築演習システムである．仮想 Linux 環境である User Mode Linux（以下，UML）による仮想マシンを改変し，仮想的なネットワーク機器として利用することで，1 台の PC 上でネットワーク構築演習が可能なシステムである．

SQL インジェクション対策学習機能は，攻撃実践機能，個人情報抽出機能，ログ表示機能から構成される．SQL インジェクション対策学習機能の実装にあたり，UML による仮想マシンを改変した仮想的なサーバを実現した．本稿では，この仮想的なサーバを仮想サーバと呼ぶ．

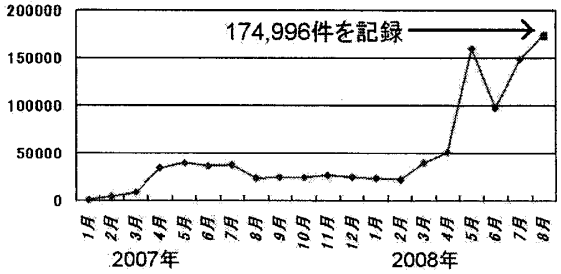

図 1：SQL インジェクションによる攻撃の被害

仮想サーバでは，Web サーバソフトウェアである Apache が動作している．SQL インジェクションによる攻撃の対象となるデータベースは，PostgreSQL を用いて構築した．データベースには，筆者らが作成した個人情報が登録されている．個人情報には，氏名・電話番号・住所などが含まれる．また，ユーザ登録用の Web ページから任意の個人情報をデータベースに登録することも可能である．

2.2. 攻撃実践機能

攻撃実践機能は，仮想サーバに対して SQL インジェクションによる攻撃を実践する機能である．実践可能な攻撃の種類は，個人情報の取得，テーブル名またはカラム名の取得，登録されているデータの改ざん，テーブルの破壊である．

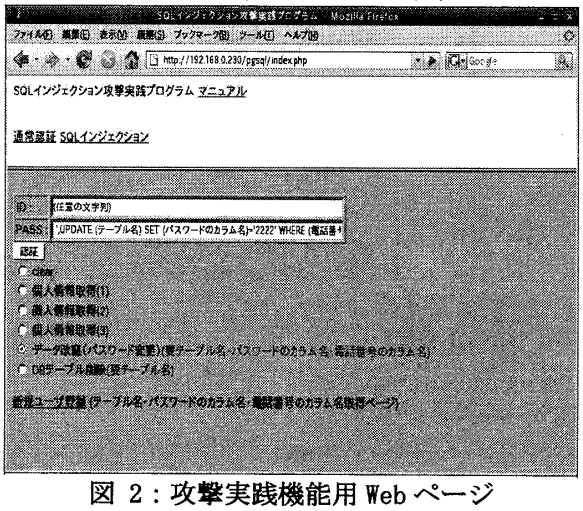

図 2：攻撃実践機能用 Web ページ

Implementation of Learning Function for Measure to SQL Injection on the Network Construction Training System using Virtual Linux Environment

Takumi UEDA†, Shinichirou TANIMURA‡, Nobukazu IGUCHI‡

†Interdisciplinary Graduate School of Science and Technology, Kinki University

‡Department of Informatics, School of Science and Engineering, Kinki University

図 3：個人情報抽出機能用 GUI

SQL インジェクションによる攻撃は，攻撃実践機能用 Web ページを用いて行う．図 2に攻撃実践機能用 Web ページを示す．この Web ページでは，攻撃に用いる SQL 文をラジオボタンによって選択し実行できる．また，登録されている ID とパスワードを用いて個人情報を参照することも可能である．

2.3. 個人情報抽出機能

個人情報抽出機能は，仮想サーバに対して自動的に複数回の SQL インジェクションによる攻撃を実行し，データベースに含まれるすべての個人情報を抽出する機能である．攻撃実践機能では，SQL 文で指定した 1 件の個人情報のみを不正に抽出する．個人情報抽出機能では，データベースに含まれるすべての個人情報を抽出でき，SQL インジェクションによる攻撃の被害を確認することができる．図 3に個人情報抽出機能用 GUI を示す．この GUI では，抽出した個人情報と攻撃に用いた SQL 文を一覧表示する．

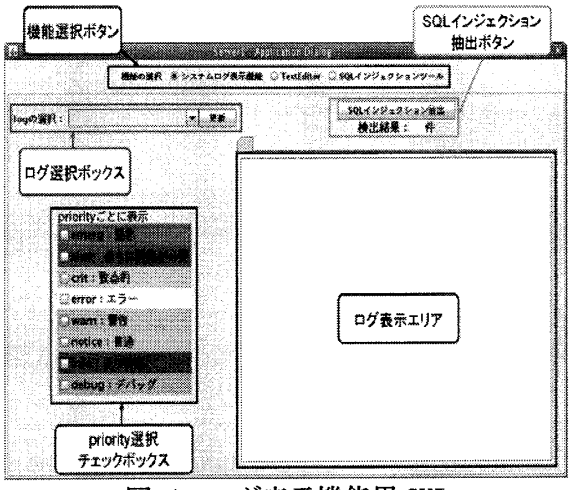

図 4：ログ表示機能用 GUI

2.4. ログ表示機能

ログ表示機能は，仮想サーバが出力したログを確認するための機能である．表示可能なログは，Linux が出力した Syslog によるログと Apache が出力したログである．ログの確認は，ログ表示機能用 GUI を用いて行う．図 4にログ表示機能用 GUI を示す．ログ表示機能用 GUI では，SQL インジェクションによる攻撃に該当する部分を色づけし，ログの件数を表示する．また，ログを重要度（Priority）ごとにタブ表示することも可能である．

3. 評価実験と結果

本学の情報学科の学生 8 名を対象に，評価実験を実施した．実験の手順は下記の通りである．

1　ユーザ登録後，ログインの成功を確認
2　攻撃実践機能の使用
　①不正ログインによる個人情報の取得
　②テーブル名，カラム名の取得
　③登録データの改ざん
3　個人情報抽出機能の使用
4　ログ表示機能の使用
　①Apache のログを確認
　②攻撃時のログをハイライト表示

実装した機能の有効性やシステムの操作性についてアンケートを実施した結果，SQL インジェクションの攻撃手法やログの理解に役立つという評価が得られた．しかし，今回の被験者は情報セキュリティに関する知識と経験が十分にあるとは言えない．したがって，情報セキュリティに精通したエンジニアを対象とした評価実験の実施が今後の課題として挙げられる．また，ログの内容から攻撃手法を推測するスキルの習得を支援する機能の実装も必要である．

4. おわりに

本研究では，SQL インジェクションによる攻撃の手法と被害を学習する機能を本システムに実装した．攻撃を受けた際にどのようなログが出力されるかを確認する機能も合わせて実装した．これらの機能により，実機による学習環境の実現が困難であった SQL インジェクション対策学習が容易に可能となった．今後，ログと攻撃手法を関連付ける学習のための機能を実装し，評価実験の実施する予定である．

参考文献

(1) JSOC：侵入傾向分析レポート vol. 11(2008).
(2) 上田拓実，井口信和，島村博：仮想 Linux 環境を用いたネットワーク教育システムにおける通信の可視化機能の実装，情報処理学会第 70 回全国大会