修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　　情報システム　　学研究科 情報ネットワークシステム学位専攻　博士前期課程		
氏　　名	八木　達哉	学籍番号	0952027
論 文 題 目	未知の SQL インジェクション検知システム構築・実装と実運用での評価		

要　　旨

WEB ブラウザ上で動作するアプリケーションは高い利便性により、多くの人に使われている。しかしその発展と共に、WEB アプリケーションから他人の個人情報への不正アクセスなどが社会問題となっている。
中でも、データベースの情報を不正に閲覧、削除、改ざんが行える SQL インジェクションは脅威となっている。

データベースを扱っている WEB アプリケーションに一つでも SQL インジェクション攻撃に対する脆弱性の穴が存在すると、データベース全体に情報漏洩の危険性がでてくる。
WEB アプリケーションに脆弱性の穴を作らないため、脆弱性の検知を行う必要がある。その方法の一つがデータベースログからの脆弱性検知である。

データベースログを用いた脆弱性検知の先行研究で、Elisa らは SQL クエリログを学習することで検知基準を設け SQL インジェクション検知する手法を提案した。
彼女らの提案手法は汎用性が高く、利便性の高かったが、学習の自由度が非常に大きいが故に検知ミスが発生するような場合があった。

本論文では先行研究の手法よりも厳密にアクセスログ、または SQL クエリログから SQL インジェクション攻撃を攻撃検知 できるシステムの構築を提案し、実装・評価を行った。その後、攻撃を含んだ SQL クエリログを 解析させる実験を行った。この実験でログに攻撃の可能性があった場合に警告として出力される ことを示し、さらに SQL インジェクション攻撃の可能性がある攻撃者の IP アドレスをアクセス ログから絞り込み表示した
結果、SQL インジェクション攻撃を含んだアクセスログと SQL クエリのログをデータマイニング技術を用いた解析で、攻撃の検知に洩れがないことを確認した。