要 旨

SQL インジェクション攻撃に含まれる記号の出現頻度とその関連性による攻撃検出手法の提案

合路 健人

Web アプリケーションを標的とするサイバー攻撃は，Web アプリケーションを運営管理する者だけでなく，その利用者にとっても大きな脅威となっている．中でも SQL インジェクション攻撃の脆弱性を狙った攻撃が多く，以前から知られている脆弱性であるにもかかわらず，対策が追いついていないことが指摘されている．SQL インジェクション攻撃には多くの記号が含まれる傾向がある．そこで，既存手法として SQL インジェクション攻撃に含まれる記号に着目した攻撃検出手法が提案されている．しかし，既存手法は，正常データの検出においては高い検出率を示した一方，攻撃データの検出率は他の検出手法と比較して高くない．SQL インジェクション攻撃による被害を防ぐために，正常データに対するパフォーマンスを下げずに攻撃検出率を向上させる必要がある．

SQL インジェクション攻撃には以下のような特徴があることが示されている．SQL インジェクション攻撃に挿入される SQL 文は攻撃者の目的に応じて異なる．また，SQL インジェクション攻撃を成立させ，目的の情報を得るには，データベースに関連する情報が必要であり，ブラインド SQL インジェクションという手法が使われる．そこで本論文では，攻撃者の目的とブラインド SQL インジェクション攻撃に含まれる記号の出現頻度の関連性を利用した攻撃検出手法を提案する．提案手法は，攻撃者の目的と攻撃データに含まれる記号の情報の関連性を利用することで正常データの検出率を下げずに，攻撃検出率を向上させる．また，攻撃データにブラインド SQL インジェクション攻撃のデータを用いることによってデータベース関連する情報を収集するリクエストを遮断することが可能となり，実際

の SQL インジェクション攻撃においても有用な攻撃検出であると考えられる．

キーワード　攻撃検出，SQL インジェクション，機械学習

Abstract

Proposal of attack detection method based on appearance frequency of symbols included in SQL injection attack and its relevance

Cyber attacks targeting Web applications are a great threat to not only those who operate and manage Web applications but also their users. Among them, there are many attacks aimed at vulnerability of SQL injection attack, and it is pointed out that countermeasures have not kept up despite being a previously known vulnerability. SQL injection attack tends to include many symbols. Therefore, as an existing method, attack detection method focusing on symbols included in SQL injection attack has been proposed. However, while the existing method shows a high detection rate in detection of normal data, the detection rate of attack data is not higher than other detection methods. In order to prevent damage caused by SQL injection attack, it is necessary to improve attack detection rate without lowering performance against normal data.

It is shown that the SQL injection attack has the following features. SQL statements inserted into SQL injection attacks differ according to the purpose of the attacker. In addition, in order to establish an SQL injection attack and obtain target information, information related to the database is required, and a method called blind SQL injection is used. In this paper, we propose an attack detection method that exploits the relationship between the attacker's purpose and the occurrence frequency of symbols included in blind SQL injection attack. The proposed method improves the attack detection rate

without lowering the detection rate of normal data by using the relationship between the purpose of the attacker and the information of the symbol included in the attack data. Moreover, by using blind SQL injection attack data for attack data, it is possible to block requests to collect database related information, which is considered to be a useful attack detection even in actual SQL injection attack.

key words attack detection, SQL injection, machine learning