مجله "پدافند الکترونیکی و سایبری"، سال اول، شماره ۲، تابستان ۱۳۹۲، ص ۵۳-۶۹

تحلیل ساختاری و معنایی پرس‌وجو برای تشخیص حملات تزریق SQL

بهاره تجلی پور*[۱]، علی اصغر صفایی[۲]

۱- گروه مهندسی کامپیوتر، دانشگاه مالک اشتر، تهران، ایران، ۲- گروه انفورماتیک پزشکی، دانشکدهٔ علوم پزشکی، دانشگاه تربیت مدرس، تهران، ایران
(دریافت: ۹۱/۷/۵ ، پذیرش: ۹۱/۱۲/۲۱)

چکیده

یکی از مهمترین حملاتی که امنیت پایگاه داده را به خطر می‌اندازد حملهٔ تزریق SQL است که اغلب در برنامه‌های تحت وب اتفاق می‌افتد. هدف از این مقاله ارائه روشی برای پیشگیری و کشف حملهٔ تزریق SQL است. روش پیشنهادی مبتنی بر رویکرد ترکیبی تحلیل ایستا و پویا و تحلیل معنایی پرس‌وجو است. پرس‌وجوهای تولید شده در زمان اجرا، با لیست ایستا و الگوهای معنایی مطابقت داده شده و میزان وجود فاکتورهای حمله در آن بررسی می‌شود. برای ایجاد الگوهای معنایی نیز از هستان‌شناسی استفاده شده است. نتایج حاصل از آزمایش روی چند پایگاه داده نشان می‌دهد که این روش می‌تواند بسیار مفید عمل کند و قابلیت انعطاف بالایی در کشف حملات جدید را داشته باشد. معماری پیشنهادی وابستگی زیادی به پایگاه داده ندارد و با اندکی تغییر، قابل استفاده برای سایر پایگاه داده‌ها نیز هست. این روش بر خلاف روش‌های پیشین، پرس‌وجوهای پویا را پشتیبانی می‌کند و وابسته به کد منبع برنامه نیست.

واژه‌های کلیدی :

پایگاه داده، تزریق SQL، هستان‌شناسی، تحلیل معنایی، تحلیل ایستا و پویا، پرس‌وجوهای پویا

Syntax and Semantic Analysis for SQL-Injection Attacks

Bahare Tajalli Pour*[1], Ali Asghar Safaei[2]

1- Department of Computer Engineering, Malek ashtar University, Tehran, Iran, 2- Medical Informatics Group,University of Medical Sciences,Tarbiat Modares University,Tehran, Iran

Abstract

One of the most critical attacks, threatening the security of databases is SQL injection attack which is mostly held through web applications. This paper proposes a new new method to detect and prevent SQL injection attacka. The method is based on combination of both static and dynamic approaches and semantic analysis of queries. Run time queries are matched with static list and semantic pattern and as a result the degree of attack factor existence will be checked. Ontology is used on creation of semantic patterns. According to tests which are gathered from different databases, this method acts efficiently and flexibly enough to discover new attacks. The suggested architecture, in contrast with the others, is designed in such a way that it does not have a great database dependency and by some changes it can be used for the other databases.

Keywords: Database, SQL injection, Ontology, Semantic Analysis , Static and Dynamic Analysis, Dynamic Query

* Corresponding Author Email:bahar_tj@yahoo.com