Egyptian Informatics Journal 23 (2022) 145–162

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Provably throttling SQLI using an enciphering query and secure matching

Mohammed Abdulridha Hussain [a,b], Zaid Alaa Hussien [c], Zaid Ameen Abduljabbar [a,b,d], Junchao Ma [e,*], Mustafa A. Al Sibahee [e,f], Sarah Abdulridha Hussain [g], Vincent Omollo Nyangaresi [h], Xianlong Jiao [i]

[a] *Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq*
[b] *Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq*
[c] *Information Technology Department, Management Technical College, Southern Technical University, Basrah 61005, Iraq*
[d] *Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen 430074, China*
[e] *College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China*
[f] *Computer Technology Engineering Department, Iraq University College, Basrah 61004, Iraq*
[g] *National Center for Management Development and Information Technology, Basrah 61004, Iraq*
[h] *Faculty of Biological & Physical Sciences, Tom Mboya University, Homabay 40300, Kenya*
[i] *College of Computer Science, Chongqing University, Chongqing 400044, China*

ARTICLE INFO

Article history:
Received 7 March 2022
Revised 12 September 2022
Accepted 13 October 2022
Available online 16 November 2022

Keywords:
SQL injection
Cryptography
Searchable encryption
Web application
Internet Security

ABSTRACT

Web applications, which dominate the internet, act as communication media between customers and service providers. Web applications are an internet innovation that provide customer services such as e-banking, e-commerce and e-booking. Developing web applications has become increasingly complicated because of security threats and service issues that involve valuable information. Attack methods such as structured query language (SQL) injection insert malicious code within user input data requests to gain unauthorised access, and then the attacker targets a database to manipulate information. In this paper, we propose a prevention method against SQL injection attacks through cryptography and searchable encryption. The proposed method uses a cryptography technique to encrypt all database information, where each piece of user information is encrypted with a separate key. The rest of the database information is ciphered with secret keys, and a searchable encryption technique is used for other database operations to preserve privacy. The login process compares the ciphered username from the database and user entry to authenticate the user. The proposed method is implemented on the PHP and MySQL databases, which are open-source applications. The results show efficient prevention of SQL injection attacks, and the database remains protected against SQL injection attacks

1. Introduction

The industry is moving toward web applications to support remote services with ubiquity and cost efficiency [1]. Organisation and companies rely on web applications to deliver services to customers while reducing the cost to a minimum because the infrastructure is based on the internet. Services such as e-banking, shopping, e-governance and reservations increase productivity in daily life due to speed and utility flexibility [2].

Web applications are built upon a number of program layers in tier architecture to handle complexity and specific functions. The basic internet technology architecture is client–server, whereas a web application adds a third level (i.e., database tier) to manage information [3]. The database contains records for managing the web application and authenticating users. However, any breach in web application authorisation leads to the disclosure of all database records and information [4]. Access to the database is controlled by access control policies, but other data operations are not controlled or limited. In other words, access policies define how to access but not how to use data [5].

[*] Corresponding author.
E-mail address: majunchao@sztu.edu.cn (J. Ma).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2022.10.001