

General Introduction

Web applications are everywhere on the Internet. Almost everything you do online is done through a web application whether you know it or not. They come in the form of web-based email, forums..., it is important to understand that these types of websites are all database driven.

Databases are a principal element of web applications because they are able to store user's preferences, personal identifiable information, and other sensitive user information. Web applications interact with databases to dynamically build customized content for each user, the web application communicates with the database using structured query language (SQL).

SQL is a programming language for managing databases that allows you to read and manipulate data in MySQL, SQL Server, Access, Oracle, and other database systems, the relationship between the web application and the database is commonly abused by attackers through SQL injection.

The SQL injection is a type of injection attack in which SQL commands are supplied (provided) in the user-input variables, such as a web form entry field, in a try to trick the web application into executing the attacker's code on the database.

The results of SQLI (SQL injection) can be disastrous because the successful SQL injection can read sensitive data from the database, modify database data (insert/update/delete), execute administrative operations on the DB, recover the contents on the DBMS file system.

There is a lot of approach that assistance to protect web and preventing SQL injection, but not all this technique offer the same levels of security, so had better to select best technique which help us to protect personal information against hackers, we think the approach that rely on cryptography system gives more security compared to other strategies.

In our project, we present the implementation of a novel idea to prevent SQL injection, which relies on a cryptography system, where we use effective cryptography system (public key cryptography) to build a strong digital signature, hence access to a novel mechanism that helps to offer more a secure web application, we also explain the Random encryption algorithm and use it in our application.

The goals of this work

The objective of the work entitled «**implementation of a cryptography system to prevent a SQL injection** » is to give a maximum security to protect the web application against SQL injections, we can summarize our work in the following steps:

- ✓ Explain the SQL injection vulnerability
- ✓ Study and analyse some public-key cryptosystems and digital signatures
- ✓ Discuss about existing solutions that are based on a cryptography system.
- ✓ Implement digital signature on the web application to prevent a SQL injection.

Research paper outline

Our research paper is divided into four chapters:

- ✓ The first chapter presents the definition of the SQL injection and the SQLI mechanism and different kinds of SQLI which are used by the hackers to avoid security of web application. We also explain some strategies to prevent and detect a SQL injection.
- ✓ The second chapter studies some public-key cryptography systems like (RSA, Elgamal, NTRU, ECC...). We also attempt to clarify the principal roles of digital signatures and the hashing secure technique.
- ✓ The third chapter deals with the existing techniques to prevent a SQL injection, which uses a cryptography system.
- ✓ The fourth chapter discusses the implementation of some public-key cryptosystems to prevent a SQL injection, the implementation of a digital signature to make authentication.