Aziz Almeqrin

InfoTc 2910

Final Project Report

Introduction

This web application is about Encryption and Decryption of the information that are being stored in the database. Databases are one of the most targets that attract hackers to attack and steel, sometimes when the information gets in the wrong hands will cause a big issue. Therefore, in this web application project I will encrypt the input data that get stored in the database which will show meaningless characters and digits, and Decrypt them in the queries.

Application components

Host: Localhost using XAMPP 5.5.30.

Programming: HTML, CSS, PHP, JavaScript, and JQuery.

Database: MySQL.

Technical Overview

MySQL: For this web application I created 2 tables (first one "Card" is optional, it is created for explanation) while second one "encrypted" is the important, where the data will be saved at. These tables will save Credit Cards information.

HTML: The form is built with HTML and made up some constraints.

PHP: Where most of the work have done here with the encryption and decryption functions.

First of all, this encryption method is encode and decode the information using a key, which is as its name imply, will be the key for encoding and decoding the data. I made the key as a string that is encrypted with MD5() function.

1) For extra protection, "function protect" is created. This function is using mysql_real_escape_string() to prepends backslashes to certain characters. Moreover, "trim", "strip_tags", and "addslashes" are used.
2) "encrypt" function. This function takes 2 values, the input data and the encrypting/decrypting key, then returns an encrypted string. In this function, "mcrypt_encrypt" is taking 4 values and returns a string ("MCRYPT_RIJNDAEL_256" as the mcrypt cipher, "encryption key", "data"

that is wanted to be encrypted, “MCRYPT_MODE_ECB” as a mcrypt mode). Then, the returned string will be assigned into “base64_encode” function that will encode the data with base64. Then, the encoded value will go to “rtrim” function to strip whitespaces. At the end, the function will return an encrypted data.

3) “decrypt” function. Basically this function is doing reversible operation of the “encrypt” function. This function takes 2 values, the encrypted data and the encrypting/decrypting key, then returns a decrypted version of the encrypted string. In this function, “mcrypt_decrypt” is taking 4 values and returns string “MCRYPT_RIJNDAEL_256” as the mcrypt cipher, “encryption/decryption key”, “data” with using base64_decode due to using base64 in encoding, “MCRYPT_MODE_ECB” as a mcrypt mode). Then, the decoded value will go to “rtrim” function to strip whitespaces. At the end, the function will return a decrypted data.

JQuery: it used to implement a nice shape of tables to show output.

Cyber Security Concerns:

Securing the databases information is a very critical and fatal thing. For example, let’s think about an online store that sells goods, and accept credit cards for purchases. Usually the credit card information will be stored in the database. However, what about if the stored credit cards information was not secured, and the database got leaked? There will be a big problems are about to come because who got these information will be able to use the credit card.

Therefore, there are many methods for securing data in the databases. For this project, the database will store encrypted data that make no sense without decrypting them. In other word, if the database got leaked, it mostly will not cause problems because it is already encrypted.

Application in Cyber Security:

There many application could be implemented with the idea of this project.

1) As the project shows, credit cards security.
2) Out of the box implementations, it could be a web site to store passwords for people whom usually using different passwords and usually forget them. ^^

Important Note: the “Key” is supposed to be highly, as well as the database connection. However I made them within the index file just to clarify the idea.

In conclusion

The idea of this application is to encrypt the data the will be stored in the database using a key. This encryption and decryption process will be based on that key, so it must be very well secured. there are 3 main function were created to make this process in this application which are “protect”, “encrypt”, and “decrypt”. These function used a built in methods to provide security. HTML and CSS are used to make the interface, and MySql is used for database. PHP is used to make the encryption/decryption operation and taking the values and managing the database. JavaScript and jQuery are used to implement the nice sortable table.