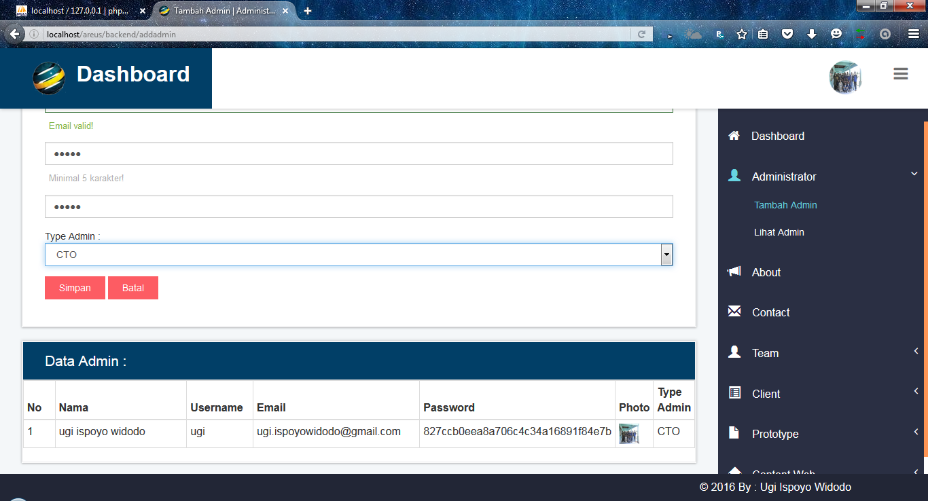
**CHAPTER III  
PROBLEM ANALYSIS**

MD5 algorithm provides a security string for data in database specialized corporate and applications. People need time to get used to the latest technology and started to get used to them. The public is curious about used of MD5 algorithm when it has done designed. Therefore, to avoid mistakes then we should know the details of the MD5 algorithm in terms of its use and applicability.

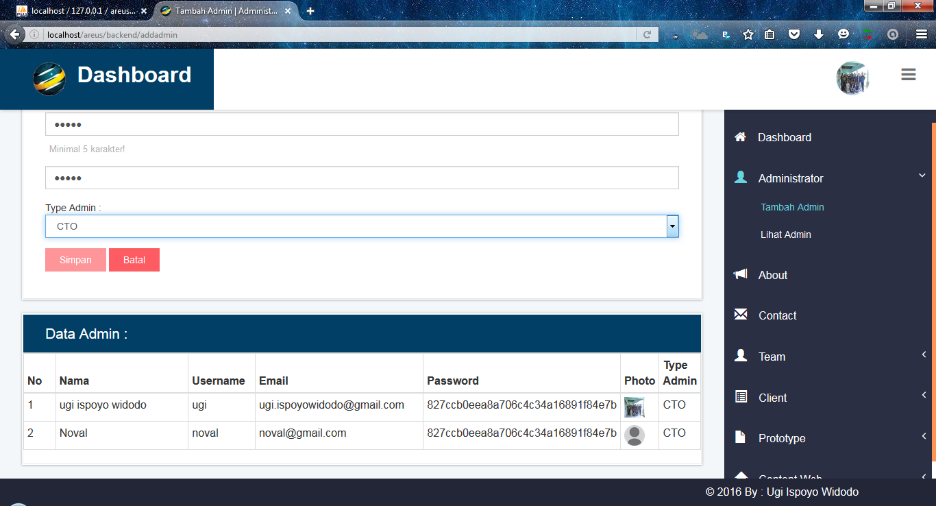
1. **Implementation of MD5 Algorithm**

There is an example of MD5, in this picture the password of admin data already encrypted with MD5 hash. In this back-end web of administartor data the admin can add, delete, or modify admin data. The data initiated as Name, Username, Email, Password, Photo, and Type of Admin. The MD5 hash function initiated for the password of Admin data. It will useful for the credential of user and prevent loose data from database.



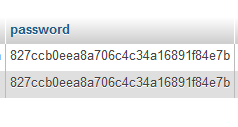
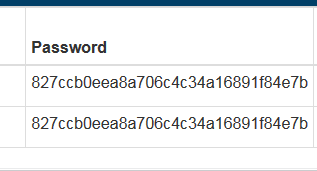
**Figure 3.1 MD5 Example of encrypted data 1**

When the new admin data added, it will automaticallly encrypted to MD5 hash, so the programmed wouldn’t repeat a same code for each data. The data of back-end has a same value from the database. For the password that initiated MD5 hash it will only appear the result of the password after proccessed with MD5 algorithm.



**Figure 3.2 MD5 Example of encrypted data 2**

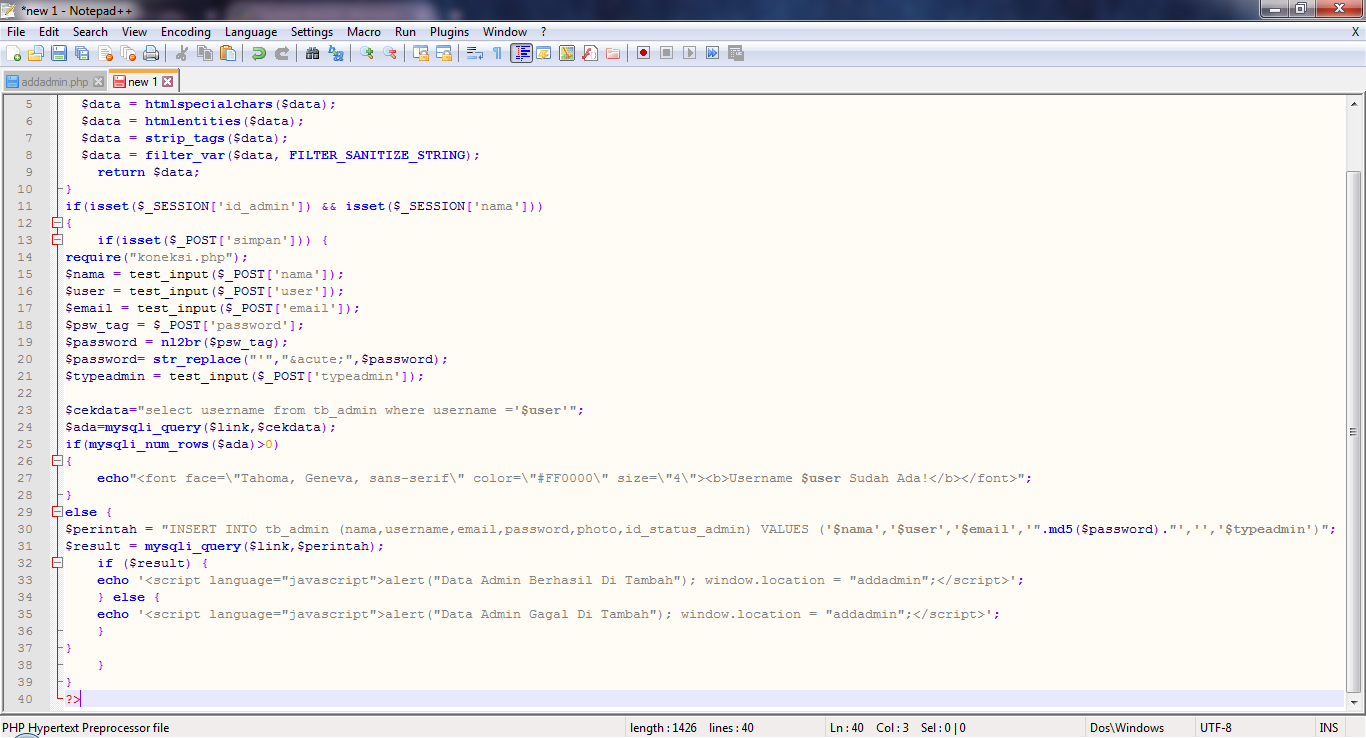
**BACK END DATABASE**



**Figure 3.3 MD5 Example of encrypted data 3**

There is many step for create the MD5 hash on line code, this time the authors implement the MD5 algorithm in code PHP for security password in database.

1. Initiate the code of program. At this time the authors using PHP for web development using SQL database.



**Figure 3.4 Initiate the MD5 hash 1**

1. Insert the value type of the data. At this time, The value of data is Name, Userame, Email, Pssword, and Type Admin.
2. Initiate the MD5 hash on the value. MD5 hash initiated on the password value, the hash can be initiated in PHP by added *.md5(value).*
3. The MD5 hash is simply using with one way hash*.* With one way hash, then the method used for the algorithm becomes simpler and easier to use. MD5 algorithm may be the most time efficient method to use, maintain and improve the effectiveness of time used. Usually for load security in the data requires a lot of time to make a hash.



**Figure 3.5 Initiate the MD5 hash 2**

1. **How to Work of MD5 Algorithm**

The MD5 algorithm first divides the input in blocks of 512 bits each. 64 Bits are inserted at the end of the last block. These 64 bits are used to record the length of the original input. If the last block is less than 512 bits, some extra bits are padded to the end. Each **block** is divided into 16 **words** of 32 bits each. These are denoted as M0 until M15. MD5 algorithm calculates process as follow:

1. **Appending Padding Bits**

The b-bit message is padded so that a single 1 bit is added into the end of the message. Then 0 bits are added until the length of the message is congruent to 448, modulo 512.

1. **Appending Length**

A 64-bit representation of b is appended to the result of the padding. Thus, the resulted message is a multiple of 512 bits.

1. **Buffer Initialization**

Bit A, B, C and D will be 32-bit registers. These registers are used in derivation of the 128-bit message digest. At the beginning, they are initialized as follows:

*A = x67452301*

*B = xe f cdab89*

*C = x98badc f e*

*D = x10325476*

1. **Processing of the Message**

The heart of MD5 is an algorithm which is used for the processing of the message. The message M is divided into 512-bit blocks which are processed separately.

The algorithm consists of four rounds, each of which comprised 16 steps. Hence, 64 steps are performed in the algorithm. The algorithm is performed as follows: first, values of A, B, C and D are stored into temporary variables AA, BB, CC and DD. Then, the following operations are performed for i = 0 to 63:

*A = B+ ((A+Func(B,C,D) +Xj[k] +T[i])≪ s) A ← D, B ← A, C ← B, D ← C*

Func(X,Y,Z) is different for every round. Function F(X,Y,Z) is used for the first round (0 ≤ i ≤ 15), G(X,Y,Z) for the second (16 ≤ i ≤ 31), H(X,Y,Z) for the third (32 ≤ i ≤ 47) and I(X,Y,Z) for the final round (48 ≤ i ≤ 63). The functions are defined as follows:

*F(X,Y,Z)=(X ∧Y)∨(¬X ∧Z)*

*G(X,Y,Z)=(X ∧Z)∨(Y ∧ ¬Z)*

*H(X,Y,Z) = X ⊕ Y ⊕ Z*

*I(X,Y,Z) = Y ⊕ (X ∨ ¬Z)*

Where ∨ is a bitwise or-operation, ¬ is a bitwise complement, ⊕ is a bitwise exclusive or operation (xor) and ∧ is a bitwise and-operation. Finally, the values of the temporary variables are added to the values obtained from the algorithm.

*A = A+AA*

*B = B+BB*

*C = C +CC*

*D = D+DD*

1. **Output**

When all bit have been processed with the algorithm, the message digest of M is in A, B, C, and D. The low-order byte of A is the first byte of the digest and the high-order byte of D is its last byte.

Put simply, MD5 is a block chained digest algorithm, computed over the data in phases of 512-byte blocks organized as little-endian 32-bit. The first block is processed with an initial seed, resulting in a digest that becomes the seed for the next block. When the last block is computed, its digest is the digest for the entire stream. This chained seeding prohibits parallel processing of the blocks.

1. **Advantages of MD5 Algorithm**

The advantages of MD5 algorithm analysis of which have been discussed are as follows:

1. **Utilizes a Fast Computation Algorithm**

MD5 algorithm may be the most time efficient method to use, maintain and improve the effectiveness of time used. Usually for load security in the data requires a lot of time to make a hash.

1. **Provides Collision Resistance**

Using the MD5 algorithm integrated data will not collide and crash on the server or in a database. Peoples can freely save the data to server and expand the data without having to fear the crash data.

1. **Widespread Used**

Used by many people, because this algorithm is commonly used in the present era. Thus, to study it will be very easy because many use and references available on the internet

1. **Provide a One Way Hash**

With one way hash, then the method used for the algorithm becomes simpler and easier to use

1. **Disadvantages of MD5 Algorithm**

While it is true that the information and data secured with MD5 algorithm that can be accessed anytime and from anywhere at all, there are times when this system can have some serious dysfunction are as follows:

1. **Security Flaws and Vulnerability**

MD5 algorithm is commonly used in data security, so it is easy to be learned by others and frail against hacking activities. Ordinary people usually do not realize the purpose of the algorithm that protects data, but for an IT Professional it will be very fatal in case of data leakage

1. **Less Secure than SHA-1 Security**

MD5 algorithm uses a much simpler method than SHA-1 so that the effectiveness SHA-1 being superior and more secure.

1. **Slower**

MD5 algorithm is slightly slower than MD4, but is more conservative in design. MD5 algorithm was designed because it was felt that MD4 was perhaps being adopted for use more quickly than justified by the existing critical review. MD4 was designed to be exceptionally fast, it is at the edge in terms of risking successful cryptanalytic attack.