**Almacenar contraseñas en MySQL**

Si queremos que nuestros usuarios se sientan seguros utilizando nuestros sistemas, debemos proporcionarles un nivel superior de protección. Esto se basa en crear una tabla con contraseñas totalmente accesibles es un fallo de seguridad tremendo.

Algunos tipos de almacenamiento de contraseñas son:

**1.-Password**

Esta función está presente desde hace unas cuantas versiones, pero sin embargo se ha demostrado que es fácilmente vulnerable por lo que no merece la pena explicarla.

**2.-MD5**

Para guardar una contraseña encriptada con MD5 necesitaremos una tabla con un campo de 32 caracteres, aunque se ha demostrado que el algoritmo MD5 puede ser vulnerado, la práctica es tan compleja que no merece la pena el esfuerzo, el algoritmo MD5 no puede ser revertido, es decir, no se pueden recuperar contraseñas de este sistema.

Insertar una contraseña con MD5:

|||| mysql> INSERT INTO usuarios VALUES('usuario',MD5('contraseña')); |||||

**3.-SHA o SHA1**

La función SHA y SHA1 son sinónimos, por lo que hacen el mismo efecto, al igual que MD5 no puede ser revertido y este necesita un campo de 40 caracteres para su almacenamiento, es más seguro que MD5 ya que calcula el cheksum SHA de 160 bits de una cadena, mientras que MD5 la calcula de 128.

Insertar una contraseña con SHA:

|||| mysql> INSERT INTO usuarios VALUES('usuario',SHA('contraseña')); |||||

En resumen el algoritmo de encriptación que utilizaremos seria el de sha1 ya que:

1.- Es el mas seguro

2.-Es de campo de 40 caracteres ya que calcula el cheksum SHA de 160 bits

3.-Y de fácil utilidad en php,java etc