Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

PHP encryption symmetric program example using crypt to store password in a text file

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

Q. Symmetric encryption is a type of encryption where the same key is used to encrypt and decrypt the message. Can you explain how do I use symmetric encryption under PHP to store password in a text file and authenticate the user?

A. Symmetric encryption differs from asymmetric (also known as public-key) encryption, which uses one key to encrypt a message and another to decrypt the message.

PHP crypt() will return an encrypted string using the standard Unix DES-based encryption algorithm or alternative algorithms that may be available on the system. Arguments are a string to be encrypted and an optional salt string to base the encryption on. See the Unix man page for your crypt function for more information.

Syntax:
string crypt (string $str [, string $salt])

Consider following example.
$en_password : Stores encrypted password. You need to store this in database or flat text file.
$userPasswordInput : Holds user provided / supplied password via HTML page

If command is use to check encrypted password (hash) with user supplied password.

```
<?php
//Standard DES-based encryption with a two character salt called 'ge'
$en_password = crypt('secrete','ge');

if (crypt($userPasswordInput, $en_password) == $en_password) {
   echo "Password verified, you can login!";
}
?>
```

PHP Function to write / store password to a file called /home/secure/.password

```
function updateAdminLoginPassword($new){
  $encryptedPassword;
  //This is Blowfish encryption with a sixteen character salt starting with or $2a$
  $encryptedPassword = crypt($new, '$2a$didIL...fpSd78..$');
  // Open the file and erase the contents if any
  $fp = fopen("/home/secure/.password", "w");
  // Write the data to the file
  fwrite($fp, $Password);
  // Close the file
  fclose($fp);
  echo '<h3>Password has been updated!<h3>';
  echo '<SCRIPT>alert(\'Password changed! You must login again to use new password\');</SCR
  /* resetSession(); */
}
```

Function to verify a password (note we are using hash in both functions $2a$didIL...fpSd78..$):

```
function verifyPassword($password)
{
 $username= "admin";
 $encryptedpasswd="";
// read encrypted password
 $fp = fopen("/home/secure/.password", "r");
 while ( $line = fgets($fp, 1000) ) { $encryptedpasswd=$line; }
```

```
 if ( $_POST["username"] == $username && (crypt($password,'$2a$didIL...fpSd78..$') ==  $enc
 { // allow login
  session_start(); //Initialize session data
                //store user login name and password
  $_SESSION['user'] = $username;
                $_SESSION['pwd'] = $encryptedpasswd;
                // display main menu
  header( "Location: /welcome.php" );
 }
 else
 {       // password is not correct or session expired due to password change
 header( "Location: /login.php?sessionnotfound=1" );
 }
}
```

Above examples just provides you idea about php password encryptions and hash. You must consider other factors such as SSL http session, MD5 password / hash and mysql database to store password has etc.

Further readings:

- PHP crypt() [2]
- PHP's Encryption Functionality [3]

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/php/**
[2] PHP crypt(): **http://php.net/crypt**
[3] PHP's Encryption Functionality: **http://www.onlamp.com/pub/a/php/2001/07/26/encrypt.html**