Gorka Alvarez e Iñaki García

Tarea Opcional

Contenido

Enunciado

Guardar la contraseña cifrada en la BD. Para ello podéis usar funciones de cifrado de PHP, por ejemplo crypt(). Para probar esta tarea podéis usar vuestro email vip y el alumno: prueba0xx@ikasle.ehu.eus, donde xx es vuestro número de grupo(p.e. prueba010@ikasle.ehu.eus).Si se completa esta tarea, es necesario volver a registrar el usuario admin@ehu.es para que la contraseña se almacene cifrada en la BD.

Modificaciones en los ficheros

SignUp.php

Para cifrar las contraseñas de los usuarios se ha utilizado la función *password_hash()*.

```
$hashed_password = password_hash($pass, PASSWORD_DEFAULT);
```

Como se ve en la imagen, la función utiliza dos parámetros. El primero se corresponde con la contraseña que ha introducido el usuario en el formulario de registro, mientras que el segundo parámetro, hace referencia a la sal que usara la función para encriptar nuestra contraseña, en este caso, el algoritmo BCRYPT, predeterminado de PHP. Una vez encriptada la contraseña se sube a la Base de Datos tal como se hacía anteriormente.

LogIn.php

Al iniciar sesión, ahora, para comprobar la contraseña se debe realizar una ligera modificación. Anteriormente, únicamente comprobábamos si la contraseña que introducia el usuario era igual a la que estaba almacenada en la base de datos, sin embargo, esto, es ahora inviable. Por ello, se ha utilizado la función *has_equals()* de PHP, que permite comparar dos Strings de forma segura.

```
if(($row['email']==$email)and(hash_equals($row['pass'],crypt($pass,$row['pass'])))){
```

Ejemplo de Cifrado

El ejemplo más sencillo que podemos poner, es el correspondiente a la contraseña de administrador de nuestra aplicación:

Contraseña Original: *admin000*.

Contraseña Cifrada: *$2y$10$GB/.GZ2i0shUqLiKj1iBGeIRYwsc9UTlict/3m.SlxsNjJ3PXtONK.*