PRÁCTICA 1: CRACKEANDO PASSWORDS CON PHP

IMPORTANTE:

Esta práctica es obligatoria. Se calificará con un máximo de 10 puntos. La nota de aprobado es un 5.

ESCENARIO:

Un sitio web de comercio electrónico ha almacenado las password encriptadas de los usuarios en su base de datos. Han utilizado el algoritmo MD5.

De alguna forma, hemos podido acceder a los contenidos de la base de datos y tenemos las passwords encriptadas de todos los usuarios.

Queremos “crackear” esos códigos hash MD5, para obtener las passwords de los usuarios.

Sabemos que las passwords tienen 4 caracteres numéricos del 0 al 9.

A continuación, se tiene la tabla que almacena los códigos hash de algunos de los usuarios:

email	clave	Código hash de la clave (MD5)
marta@europa.es	????	91e50fe1e39af2869d3336eaaeebdb43
pedro@europa.es	????	3c0aec8e759a22ef8b2c6498b3f85a9f
juan@europa.es	????	b75bd27b5a48a1b48987a18d831f6336
alberto@europa.es	????	977f25398b95e1c577802c84a3d90d98
carlos@europa.es	????	581b41df0cd50ace849e061ef74827fc
nacho@europa.es	????	d74a214501c1c40b2c77e995082f3587

Vas a poder crackear todas las passwords excepto una.

La aproximación por la fuerza bruta se hace normalmente escribiendo una serie de bucles anidados que pasan por todas las combinaciones posibles de caracteres. Esta es una de las razones por las que las políticas de password requieren la inclusión de mayúsculas, minúsculas, números, y signos de puntuación, para que crackear sea más difícil. Cuantos más caracteres tiene la password, más bucles anidados tienes que poner. Si además las password son largas, es aún más difícil.

PISTAS

Se proporciona el código fuente de un programa que crackea passwords de dos caracteres numéricos de longitud. Te servirá de plantilla para que escribas el tuyo, que crackeará passwords de cuatro caracteres numéricos de longitud. El que se adjunta se llama crackeo_2.php.

SE PIDE:

Vais a realizar un programa en PHP que utilice la fuerza bruta (ensayo y error) para obtener una password a partir de su código MD5.

No existe ningún algoritmo matemático capaz de calcular la password a partir del código hash MD5.

Por medio de ensayo y error (a lo bruto), puedes calcular el código hash de todas las passwords posibles, y luego compararlo con los códigos almacenados.

1. Haz el programa PHP tunombre_crackea_4.php, que:
    a. Crackee la tabla del enunciado: Tu programa será capaz de crackear passwords de 4 dígitos numéricos.
    b. Muestre una salida en forma de tabla: Se visualizará en cada fila el email y la password de cada usuario.
2. Como no vas a poder crackear una de las claves, escribe un breve documento que indique cuál es. Si lo sabes, indica también por qué no has podido crackearla. Reflexiona sobre ello y escribe lo que piensas en este documento.
3. Cuando termines, sube al aula virtual un zip con:
    a. El código fuente de tu programa
    b. Un pantallazo de la solución
    c. El documento explicativo del punto 2.

Calificación:

1. El programa PHP funciona y obtiene correctamente las passwords (6 puntos)
2. La salida del programa se visualiza estéticamente en forma de tabla (1 punto)
3. Has averiguado el código no crackeable, y has aventurado una causa realista de por qué no has podido crackearlo (2 puntos)
4. En vista de los resultados, has realizado una reflexión sobre la seguridad de las passwords (1 punto)