hash_file »
« hash_copy

- Manual de PHP
- Referencia de funciones
- Extensiones criptográficas
- Hash
- Funciones de hash

Change language: Spanish

Submit a Pull Request Report a Bug

# hash_equals

(PHP 5 >= 5.6.0, PHP 7, PHP 8)

hash_equals — Comparación de strings segura contra ataques de temporización

## Descripción ¶

**hash_equals**(string `$known_string`, string `$user_string`): bool

Compara dos strings empleando el mismo tiempo, sin importar si son iguales o no.

Esta función debería utilizarse para mitigar los ataques de temporización, por ejemplo, al probar hash de contraseñas de crypt().

## Parámetros ¶

`known_string`

El string de longitud conocida con el que comparar

`user_string`

El string proporcionado por el usuario

## Valores devueltos ¶

Devuelve **`true`** cuando los dos strings son iguales, o **`false`** si no.

## Errores/Excepciones ¶

Emite un mensaje de nivel **`E_WARNING`** cuando ninguno de los parámetros proporcionados es un string.

## Ejemplos ¶

### Ejemplo #1 Ejemplo hash_equals()

```
<?php
$esperado   = crypt('12345', '$2a$07$usesomesillystringforsalt$');
$correcto   = crypt('12345', '$2a$07$usesomesillystringforsalt$');
$incorrecto = crypt('apple', '$2a$07$usesomesillystringforsalt$');

var_dump(hash_equals($esperado, $correcto));
```

```
var_dump(hash_equals($esperado, $incorrecto));
?>
```

El resultado del ejemplo sería:

```
bool(true)
bool(false)
```

## Notas ¶

> **Nota**:
>
> Ambos argumentos deber tener la misma longitud para que se puedan comparar. Cuando se proporcionan argumentos con diferente longitud, se devuelve **`false`** inmediatamente, pudiéndose filtrar la longitud del string conocido en caso de un ataque de temporización.
>
> **Nota**:
>
> Es importante proveer el string proporcionado por el usuario como segundo parámetro, en vez de como el primero.

+ add a note

## User Contributed Notes

There are no user contributed notes for this page.