

Sesiones en PHP

Mantener y manejar información de los usuarios en el servidor mediante el array `$_SESSION`

Variable super global \$_SESSION

\$_SESSION es un **array especial** utilizado para guardar información a través de los requests que **un usuario** hace durante su visita a un sitio web o aplicación.

A cada usuario que accede a la aplicación e inicia sesión se le asigna un session ID único, y es lo que le permite identificar la sesión y que esté disponible para ese usuario en concreto.



Iniciar sesión

Se hace **al principio del código PHP**, y debe hacerse antes de que cualquier texto, HTML o JavaScript se envíe al navegador.

La función **session_start()** inicia la sesión entre el usuario y el servidor, y permite a los valores guardados en **\$_SESSION** ser accesibles después.



Iniciar sesión y acceso a \$_SESSION

// Comienzo de la sesión

```
session_start();
```

// Guardar datos de sesión

```
$_SESSION["usuario"] = "Pedro";
```

// Leer valores de sesión

```
echo "Nombre de usuario: " . $_SESSION["usuario"];
```



Eliminar un valor de \$_SESSION

Se realiza mediante la función **unset()** y facilitando la clave del valor a eliminar.

// Eliminar el nombre de usuario:

```
unset($_SESSION["usuario"]);
```



Eliminar TODOS los valores de \$_SESSION

Para desvincular todos los valores de sesión de vez se puede emplear `session_unset()`:

```
// Eliminar el valor de todo el array $_SESSION:
```

```
session_unset();
```

¡OJO! Todavía se pueden guardar nuevos valores en \$_SESSION.



Cerrar una sesión


Tan importante es iniciar una sesión como cerrarla. Incluso cuando realmente una sesión es sólo una forma temporal de almacenar datos, es importante limpiarla después por seguridad.

Esta acción se realiza, por ejemplo, cuando el usuario hace “log out”.

// Terminar la sesión:

`session_destroy();`

Si sólo se desvinculan los valores la sesión permanecerá activa, lo que deja la puerta abierta a intrusos.



Seguridad en las sesiones (ampliación)


Sesión Time-Outs; Establecer un tiempo de vida a las sesiones.

```
session_start();  
    // Establecer tiempo de vida de la sesión en segundos  
    $inactividad = 600;  
    // Comprobar si $_SESSION["timeout"] está establecida  
    if(isset($_SESSION["timeout"])){  
        // Calcular el tiempo de vida de la sesión (TTL = Time To Live)  
        $sessionTTL = time() - $_SESSION["timeout"];  
        if($sessionTTL > $inactividad){  
            session_destroy();  
            header("Location: /logout.php"); // redirección a página de logout  
        }  
    }  
    // El siguiente key se crea cuando se inicia sesión  
    $_SESSION["timeout"] = time();
```


Seguridad en las sesiones (ampliación)

Regenerar el Session ID: la función `session_regenerate_id()` crea un nuevo ID único para representar la sesión actual del usuario.

```
session_start();  
  
if($_POST["usuario"] = "admin" && $_POST["password"] == sha1($password)){  
    $_SESSION["autorizado"] = true;  
    session_regenerate_id();  
}
```



Origen y más info.

<https://diego.com.es/sesiones-en-php>

