
Security and access control

— DWES UD5.2 —

1.- Cookies

Cookies are text files that applications save on the client.

They are saved in the web browser environment and are associated with a specific website. Its typical use is the storage of user preferences:

- Language
- Colors
- Letter size
- ...

Normally, information that is not very sensitive is saved but that allows some tasks to be downloaded to the server.

1.- Cookies

To create a cookie in PHP, use the setcookie function.

The syntax of the setcookie function is:

```
setcookie(name, value, expire or [options], path, domain, secure, httponly);
```

The only required parameter is 'name', all the others are optional.
For example, to create a cookie that lasts 1 hour you would do this:

```
setcookie('nombre', 'valor', time()+3600);
```

Cookies will not be available the first time the page is accessed, they can be read from the next page request using the global array \$_COOKIE.

1.- Cookies

Code source

```
<!DOCTYPE html>

<?php
$cookie_name = "user";
$cookie_value = "John Doe";
setcookie($cookie_name, $cookie_value, time() + (86400 * 30), "/"); // 86400 = 1 day
?>

<html>
<body>

<?php
if(!isset($_COOKIE[$cookie_name])) {
    echo "Cookie named '" . $cookie_name . "' is not set!";
} else {
    echo "Cookie '" . $cookie_name . "' is set!<br>";
    echo "Value is: " . $_COOKIE[$cookie_name];
}
?>

</body>
</html>
```

1.- Cookies

The **expire** parameter indicates the validity period of the cookie.

UNIX time is used, in seconds, from 1-1-1970 00:00:00.

If it is left blank or a zero is entered, the cookie expires at the end of the **web session** → when the browser is closed.

To modify a cookie, you must make a **setcookie** with the new values

To delete a cookie, the expiration date must have passed:

```
setcookie('nombre', 'valor', time()-3600);  
setcookie('nombre', 'valor', 1); // recommended
```

1.- Cookies

For security it is important to use the **secure** and **httponly** options.

```
<?php
$arr_cookie_options = array (
    'secure' => true,    // The cookie will only be set if a HTTPS connection exists
    'httponly' => true, // Only accessible through the HTTP protocol
    'samesite' => 'Lax' // None || Lax || Strict
);
setcookie('MiCookie', 'ValorCookie', $arr_cookie_options);
?>
```

In order to consult the cookies received by the server, the superglobal **array** **\$_COOKIE** is used

1.- Cookies

You can create an array inside the cookie:

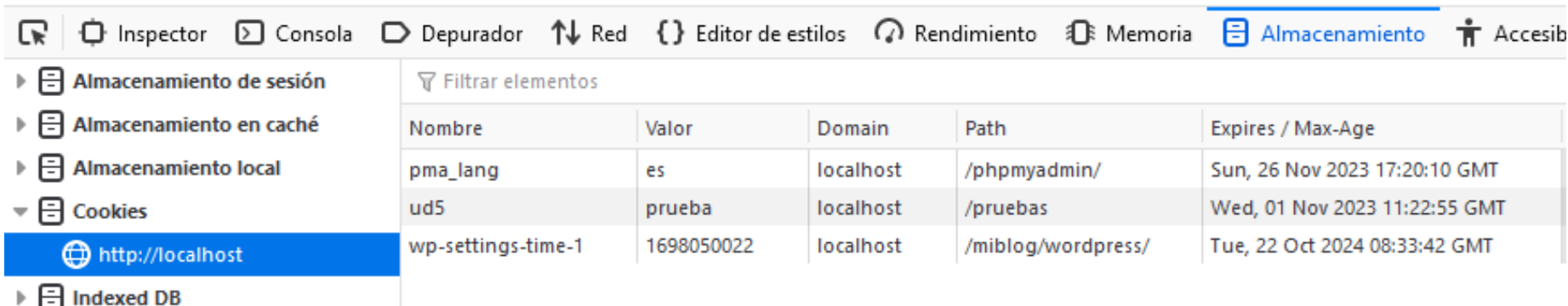
```
setcookie("cookie[tres]", "valor tres");  
setcookie("cookie[dos]", "valor dos");  
setcookie("cookie[uno]", "valor uno");
```

```
// print them  
if (isset($_COOKIE['cookie'])) {  
    foreach ($_COOKIE['cookie'] as $nombre => $valor) {  
        $name = htmlspecialchars($nombre);  
        $value = htmlspecialchars($valor);  
        echo '$nombre: '. $valor . '<br>';  
    }  
}
```

2.- Inspect cookies

To inspect the cookies of the current application you can do the following:

In Firefox → right click → Inspect → Storage → Cookies



The screenshot shows the Firefox DevTools Storage Inspector. The top toolbar includes icons for Inspector, Console, Debugger, Red, Editor de estilos, Rendimiento, Memoria, Almacenamiento (selected), and Accesib. The left sidebar shows a tree view with 'Almacenamiento de sesión', 'Almacenamiento en caché', 'Almacenamiento local', 'Cookies' (expanded), 'http://localhost' (selected), and 'Indexed DB'. The main panel displays a table of cookies for the selected site.

Nombre	Valor	Domain	Path	Expires / Max-Age
pma_lang	es	localhost	/phpmyadmin/	Sun, 26 Nov 2023 17:20:10 GMT
ud5	prueba	localhost	/pruebas	Wed, 01 Nov 2023 11:22:55 GMT
wp-settings-time-1	1698050022	localhost	/miblog/wordpress/	Tue, 22 Oct 2024 08:33:42 GMT

2.- Inspect cookies

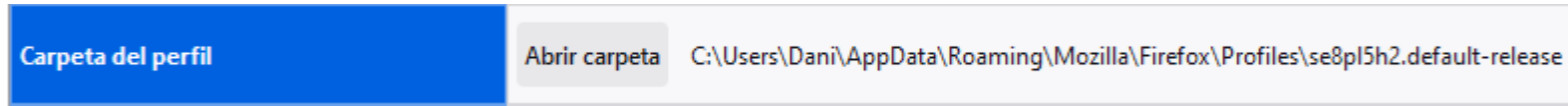
To inspect all cookies in Firefox:

1. Open the application menu



1. In “Help” → “More troubleshooting information”

1. Open the “Profile Folder”



1. Open the “cookies.sqlite” file (e.g. with DB Browser for SQLite)

1. Open the “Datasheet” tab

2.- Inspect cookies

DB Browser for SQLite - C:\Users\Dani\AppData\Roaming\Mozilla\Firefox\Profiles\se8pl5h2.default-release\cookies.sqlite

Archivo Editar Ver Herramientas Ayuda

Nueva base de datos Abrir base de datos Guardar cambios Deshacer cambios Abrir proyecto Guardar proyecto Anexar base de datos Cerrar base de datos

Estructura Hoja de datos Editar pragmas Ejecutar SQL

Tabla: moz_cookies

	id	originAttributes	name	
	Filtro	Filtro	Filtro	Filtro
1	9466		CONSENT	PENDING+888
2	10943		__qca	P0-583002089-163792:
3	10944		__fssid	c6037f3c-be10-4813-a0
4	10950		__gads	ID=c5ee98bd1f225ac8-
5	23355		__octo	GH1.1.367699169.1651
6	25178		ClientId	C02895EFCDD55401785:
7	27357	^partitionKey=%28https%2Coffice.com%29	OIDC	1
8	27359	^partitionKey=%28https%2Coffice.com%29	ClientId	513908F594A9485495C
9	27505	^partitionKey=%28https%2Coffice.com%29	__Host-GAPS	1:LWTh1vm6e2d18qb9
10	27507		django_language	es
11	29444	^partitionKey=%28https%2CCredit.com%29	__qca	P0-515079654-1654860
12	29540	^partitionKey=%28https%2Cwhatismyip.com%29	AVPUID	13a0bc9bd376d434fcec
13	31890	^partitionKey=%28https%2Coffice.com%29	ClientId	AF3DB1CDDF3649E08C
14	33060		__ga	GA1.1.268289565.1637
15	33081		qcSxc	1662285360952
16	33103		fs.session.id	fbccf48-41e5-4965-ac
17	33105		__pbjs_userid_consent_data	7571372671378286
18	33116		cookie	1f1c4015-7b26-420a-b0

1 - 18 de 531

Ir a: 1

Editar celda

Modo: Texto

1 9466

Tipo de datos actualmente en la celda: Texto / Numérico
4 caracteres

Aplicar

Remoto

Identidad Seleccione una identidad para conectar

DBHub.io Local Base de datos actual

Nombre Última modificación Tamaño

Historial de SQL Gráfica Esquema Remoto

Solo lectura UTF-8

3.- Good practices for the use of cookies

As seen, you can review all cookies and their value, then:

- Is it good practice to save passwords in cookies?
- And credit card numbers?

Avoid saving sensitive data as much as possible; if you need to do so, it is recommended to encrypt it and use https.

Before saving a cookie, the user must be informed and consent obtained.

If the cookie is going to be used only during the session, it is recommended to make it expire when the browser is closed (expire field set to 0)

Exercise

Modify the login screen from the last exercise so that:

- Save the user who authenticates correctly in a cookie
- When accessing the login screen, if there is a valid cookie with a user who has previously been successfully authenticated, instead of displaying the login form, it will display a message saying 'Do you want to log in as \$NAME?', allowing you to select 'Yes' or 'No'. If 'Yes' is selected, the message 'Access successful' will be displayed. If 'No' is selected, the cookie will be deleted and the login form will be displayed again.