Guía Práctica de Ejercicios Nº 11

En nuestra ante última práctica veremos conceptos de seguridad en aplicaciones Web, principalmente desarrolladas en PHP. Pero también veremos la manera de configurar nuestro lenguaje por medio del archivo php.ini que define las capacidades del mismo.

Objetivo: Comprender los conceptos básicos de seguridad Web con PHP como lenguaje del lado del servidor. Definir, desarrollar y utilizar los métodos de seguridad básicos para proteger nuestra aplicación Web a posibles ataques de tipo CSS, SQL Injection, Remote Code, entre otros. Desarrollar e implementar el filtrado de datos en nuestra aplicación Web. Entender y configurar las capacidades del lenguaje PHP desde un script o utilizando el archivo php.ini.

Introducción: En nuestra actualidad vemos que el desarrollo de Internet ha sido inminente y con ello las aplicaciones Web, por lo tanto, se hace indispensable el uso de un lenguaje que permita desarrollar aplicaciones Web como PHP, entre otros. Teniendo en cuenta la situación anterior es que veremos la como desarrollar aplicaciones Web que se ejecutarán del lado del servidor utilizando uno de los mejores lenguajes del ambiente del Software Libre. Teniendo en cuenta la magnitud del proyecto a desarrollar veremos la necesidad de emplear el paradigma orientado a objetos con PHP; que nos dará la posibilidad de diseñar, desarrollar y mantener el Software de manera profesional utilizando un paradigma antes mencionado.

Construcciones (palabras clave), variables globales y funciones que estudiaremos en esta unidad.

Construcciones del lenguaje con las que trabajaremos.

ctpye_alpha verifica si todos los caracteres en la cadena entregada $texto, son alfabéticos.

ctype_digit verifica si todos los caracteres en la cadena entregada $texto, son numéricos.

ctype_alnum chequea si todos los caracteres en la cadena entregada $texto, son alfanuméricos.

ctype_graph verifica si todos los caracteres en la cadena entregada $texto, generan una salida visible.

md5 nos permite calcular el hash md5 de una cadena.

uniqueid devuelve un identificador único con prefijo, basado en la hora actual en microsegundos.

rand nos permite generar un valor entero aleatorio.

htmlentities convierte todos los caracteres a su entidad HTML aplicable.

htmlspecialchars convierte caracteres especiales a entidades HTML.

init_set nos permite establecer una nueva configuración de alguna capacidad del lenguaje.

init_get nos permite obtener la configuración de alguna capacidad del lenguaje.

init_get_all nos permite obtener la configuración de todas las capacidades del lenguaje.

Ejercicios

Utilizar los conceptos de programación Web y de base de datos

1) – Escriba los scripts PHP necesarios para desarrollar un formulario de login. Tenga en cuenta que deberá tener creada una base de datos y una tabla con usuarios de acceso (utilice la herramienta phpmyadmin para crear la base de datos y la tabla).

login.php

```
<?php
// Se inicia o reanuda una sesion
session_start();
// Se agrega el formulario de login
echo "<form action='proceso.php' method='post'>";
echo "<table>";
echo "<tr>";
echo "<td>";
echo "Nombre de usuario: ";
echo "</td>";
echo "<td>";
echo "<input type='text' name='username' id='username'>";
echo "</td>";
echo "</tr>";
echo "<tr>";
echo "<td>";
echo "Contrase&ntilde;a: ";
echo "</td>";
echo "<td>";
echo "<input type='password' name='password' id='password'>";
echo "</td>";
echo "</tr>";
echo "<tr>";
echo "<td>";
echo "<input type='submit' name='entrar' id='entrar' value='Entrar'>";
echo "</td>";
echo "<td>";
echo "</td>";
echo "</tr>";
echo "</table>";
echo "</form>";
```

proceso.php

```
<?php
// Se inicia o reanuda una sesion
session_start();

// Si fue enviado el formulario se procesara
if (isset($_POST['entrar']) && $_POST['entrar'] == 'Entrar') {
```

```
	// Se verifican los datos de login
	if (isset($_POST['username'])) {
		$username = trim($_POST['username']);
	}
	if (isset($_POST['password'])) {
		$password = trim($_POST['password']);
	}

	$enlace = mysql_connect('127.0.0.1', 'root', '');
	mysql_select_db('sgu', $enlace);
	$consulta = "SELECT * FROM Usuarios WHERE username = '".$username."' AND
password = '".$password."'";
	$resultado = mysql_query($consulta, $enlace);
	// Se evalua si el usuario existe y se encuentra habilitado
	if (mysql_num_rows($resultado) > 0) {
		// Registrar variables de sesion
		$_SESSION['usuarioRegistrado'] = true;
		$_SESSION['username'] = $username;
		// Se direcciona a la pagina de aplicaciones
		header("Location: loginok.php");
	} else {
		// Se hace una redireccion por un mal login
		header("Location: loginfail.php");
	}
}
```

loginok.php

```
<?php
session_start();

echo "Login Ok!!!";
echo "<br/>";
echo "Usuario: ".$_SESSION['username'];
```

loginfail.php

```
<?php
session_start();

echo "Login Fail!!!";
```

2) – Del ejercicio anterior se le pedirá que realice un filtrado del ingreso de datos y la salida del mismo.

proceso.php

```
<?php
// Se inicia o reanuda una sesion
session_start();

// Si fue enviado el formulario se procesara
if (isset($_POST['entrar']) && $_POST['entrar'] == 'Entrar') {
	// Se verifican los datos de login
	if (isset($_POST['username'])) {
```

```
		$username = htmlentities(trim($_POST['username']));
	}
	if (isset($_POST['password'])) {
		$password = htmlentities(trim($_POST['password']));
	}

	$enlace = mysql_connect('127.0.0.1', 'root', '');
	mysql_select_db('sgu', $enlace);
	$consulta = "SELECT * FROM Usuarios WHERE username = '".$username."' AND
password = '".$password."'";
	$resultado = mysql_query($consulta, $enlace);
	// Se evalua si el usuario existe y se encuentra habilitado
	if (mysql_num_rows($resultado) > 0) {
		// Registrar variables de sesion
		$_SESSION['usuarioRegistrado'] = true;
		$_SESSION['username'] = $username;
		// Se direcciona a la pagina de aplicaciones
		header("Location: loginok.php");
	} else {
		// Se hace una redireccion por un mal login
		header("Location: loginfail.php");
	}
}
```

loginok.php

```
<?php
session_start();

echo "Login Ok!!!";
echo "<br/>";
echo "Usuario: ".htmlentities($_SESSION['username']);
```

3) – Partiendo del ejercicio anterior se le solicitará que mitigue amenazas de tipo SQL Injection.

proceso.php

```
<?php
// Se inicia o reanuda una sesion
session_start();

// Si fue enviado el formulario se procesara
if (isset($_POST['entrar']) && $_POST['entrar'] == 'Entrar') {
	// Se verifican los datos de login
	if (isset($_POST['username'])) {
		$username = htmlentities(trim($_POST['username']));
	}
	if (isset($_POST['password'])) {
		$password = htmlentities(trim($_POST['password']));
	}

	$enlace = mysql_connect('127.0.0.1', 'root', '');
	mysql_select_db('sgu', $enlace);
```

```
	$consulta = "SELECT * FROM Usuarios WHERE username =
'".mysql_escape_string($username)."' AND password = '".mysql_escape_string($password)."'";
	$resultado = mysql_query($consulta, $enlace);
	// Se evalua si el usuario existe y se encuentra habilitado
	if (mysql_num_rows($resultado) > 0) {
		// Registrar variables de sesion
		$_SESSION['usuarioRegistrado'] = true;
		$_SESSION['username'] = $username;
		// Se direcciona a la pagina de aplicaciones
		header("Location: loginok.php");
	} else {
		// Se hace una redireccion por un mal login
		header("Location: loginfail.php");
	}
}
```

4) – Tomando el ejercicio anterior realice los cuidados necesarios para mantener las credenciales de acceso seguras.

db.php

```
<?php

$host = '127.0.0.1';
$user = 'root';
$password = '';
$db = 'sgu';

$enlace = mysql_connect($host, $user, $password);
mysql_select_db($db, $enlace);
```

proceso.php

```
<?php
// Se inicia o reanuda una sesion
session_start();

// Se requiere del archivo db.php
require_once 'db.php';

// Si fue enviado el formulario se procesara
if (isset($_POST['entrar']) && $_POST['entrar'] == 'Entrar') {
	// Se verifican los datos de login
	if (isset($_POST['username'])) {
		$username = htmlentities(trim($_POST['username']));
	}
	if (isset($_POST['password'])) {
		$password = htmlentities(trim($_POST['password']));
	}

	$consulta = "SELECT * FROM Usuarios WHERE username =
'".mysql_escape_string($username)."' AND password = '".mysql_escape_string($password)."'";
	$resultado = mysql_query($consulta);
	// Se evalua si el usuario existe y se encuentra habilitado
```

```
        if (mysql_num_rows($resultado) > 0) {
                // Registrar variables de sesion
                $_SESSION['usuarioRegistrado'] = true;
                $_SESSION['username'] = $username;
                // Se direcciona a la pagina de aplicaciones
                header("Location: loginok.php");
        } else {
                // Se hace una redireccion por un mal login
                header("Location: loginfail.php");
        }
}
```

5) – Para terminar y tomando el resultado del ejercicio anterior se le solicitará mitigar la amenaza de tipo XSS (cross-site scriptng) y CSRF (cross-site request forgery).

login.php

```
<?php
// Se inicia o reanuda una sesion
session_start();

// Se agrega el formulario de login
echo "<form action='proceso.php' method='post'>";
// Se genera el token para evitar algunos ataques
$token = md5(uniqid(rand(), true));
// Se guarda el token en la sesion
$_SESSION['token'] = $token;
// Se guarda el token como un componente oculto en el formulario
echo "<input type='hidden' name='token' value=".$token." />";
// Se crea una tabla con los elementos del formulario
echo "<table>";
echo "<tr>";
echo "<td>";
echo "Nombre de usuario: ";
echo "</td>";
echo "<td>";
echo "<input type='text' name='username' id='username'>";
echo "</td>";
echo "</tr>";
echo "<tr>";
echo "<td>";
echo "Contrase&ntilde;a: ";
echo "</td>";
echo "<td>";
echo "<input type='password' name='password' id='password'>";
echo "</td>";
echo "</tr>";
echo "<tr>";
echo "<td>";
echo "<input type='submit' name='entrar' id='entrar' value='Entrar'>";
echo "</td>";
echo "<td>";
echo "</td>";
echo "</tr>";
```

```
echo "</table>";
echo "</form>";

proceso.php
<?php
// Se inicia o reanuda una sesion
session_start();

// Se requiere del archivo db.php
require_once 'db.php';

// Si fue enviado el formulario se procesara
if (isset($_POST['entrar']) && $_POST['entrar'] == 'Entrar' && isset($_POST['token']) &&
$_POST['token'] == $_SESSION['token']) {
        // Se verifican los datos de login
        if (isset($_POST['username'])) {
                $username = htmlentities(trim($_POST['username']));
        }
        if (isset($_POST['password'])) {
                $password = htmlentities(trim($_POST['password']));
        }

        $consulta = "SELECT * FROM Usuarios WHERE username =
'".mysql_escape_string($username)."' AND password = '".mysql_escape_string($password)."'";
        $resultado = mysql_query($consulta);
        // Se evalua si el usuario existe y se encuentra habilitado
        if (mysql_num_rows($resultado) > 0) {
                // Registrar variables de sesion
                $_SESSION['usuarioRegistrado'] = true;
                $_SESSION['username'] = $username;
                // Se direcciona a la pagina de aplicaciones
                header("Location: loginok.php");
        } else {
                // Se hace una redireccion por un mal login
                header("Location: loginfail.php");
        }
}
```

Anotaciones de los Ejercicios