junio 2017

## 

# BORJA LORENZO FERNÁNDEZ

# GUILLERMO RIUS García

# AXEL JUNESTRAND LEAL

# ANDRÉS HERRANZ gonzález

# ÍNDICE

## INTRODUCCIÓN

## DESCRIPCIÓN DETALLADA DE LA APLICACIÓN

## ARQUITECTURA DE LA APLICACIÓN

### Diseño

### Base de datos

### Principales decisiones de diseño

## SEGURIDAD

### SQL Injection

### xss

### encriptado de contraseñas

### FUERZA BRUTA

## INSTRUCCIONES DE USO

# INTRODUCCIÓN

Pachanga es una red social para amantes del fútbol que permite organizar partidos con otros usuarios.

La idea surgió porque ninguno de nosotros conoce otras aplicaciones que enfaticen en el deporte de equipo y cuenten con una comunidad que permita la práctica del mismo. Creemos, además, que es una buena forma de fomentar el deporte en una sociedad tan vinculada a la tecnología como la nuestra.

Pachanga posee un sistema de puntuación que permite a los usuarios ganar o perder puntos (“Pachanga points”) en función de los resultados obtenidos en los partidos.

De momento, la aplicación sólo permite organizar partidos en la zona de Madrid, es decir, en cada uno de los 21 distritos de la capital, teniendo cada uno varios polideportivos en los que se podrán jugar estos partidos. En total, Pachanga tiene registrados 52 polideportivos.

De esta forma, mediante el sistema de puntuación y de distritos, el usuario podrá ver un ranking con los mejores de su zona, ya que al registrarse tiene que proporcionar el distrito al que pertenece.

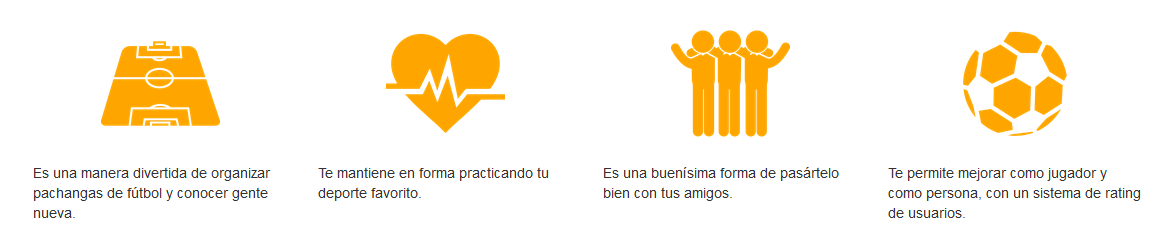
La aplicación permite también buscar partidos según la fecha, el distrito o el nombre de un partido que desee el usuario, dando total libertad a éste para elegir los partidos que quiera sin ningún tipo de restricción por zona.

# DESCRIPCIÓN DETALLADA DE LA APLICACIÓN

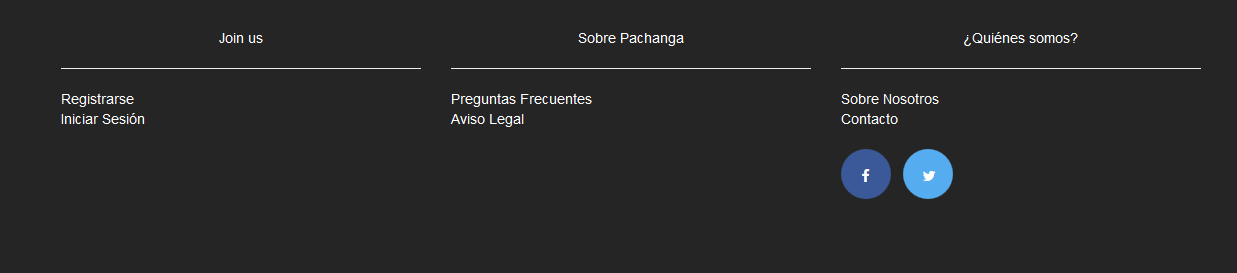
## Página principal:

La aplicación cuenta con una página principal en la que un usuario que no haya iniciado sesión podrá leer toda la información necesaria para poder hacer uso de las funcionalidades de la misma. Esta página cuenta con un “slider” que contiene información sobre proyectos (en este caso no reales) en los que está vinculado Pachanga como, por ejemplo, proyectos contra la obesidad infantil.



También contiene un párrafo con una breve descripción de la funcionalidad principal de la página, y otro para explicar al usuario la forma en la que se estructura el tema de los polideportivos y las zonas. Además, contiene una línea con las ventajas principales de Pachanga. Hemos añadido también un mapa de Madrid, para que el usuario pueda ver todos los distritos, y una zona para banners en la que se podrán incluir anuncios.

En el “footer” de la página, el usuario encontrará información detallada de la página, como las preguntas frecuentes (FAQ), información sobre los creadores de la página, un aviso legal y una página de contacto, la cual permite al usuario transmitir directamente cualquier duda o queja sobre la aplicación.



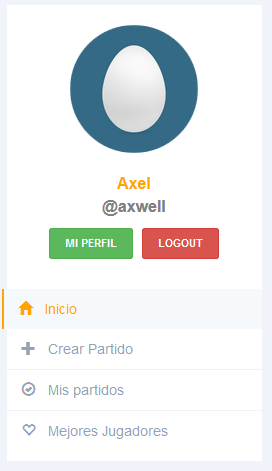
En la barra superior de la página, se encuentran los botones de inicio de sesión y registro, que al ser pulsados muestran un formulario sobre la misma página.

Si el inicio de sesión se realiza con éxito, el usuario es redirigido a la página de perfil del mismo. En caso de que las credenciales proporcionadas por el usuario sean erróneas, éste será redirigido a otra página de registro con un re-captcha de Google.



## Página de inicio:

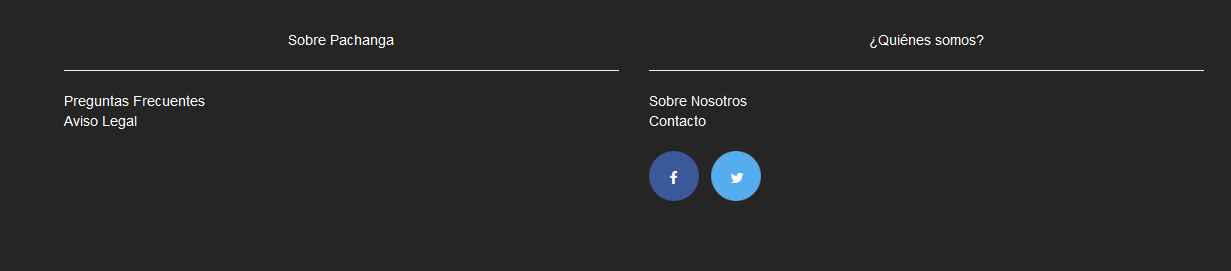
La página de inicio cuenta con un menú desde el que el usuario podrá ver su perfil, cerrar sesión, crear un partido nuevo, ver los partidos en los que está inscrito y ver la lista con los mejores jugadores de su zona.



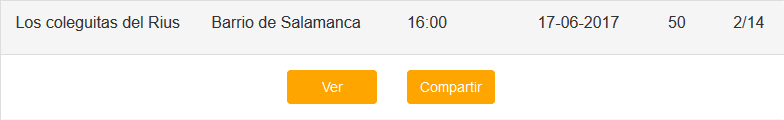
Esta vista cuenta también con una barra de búsqueda, mediante la cual, el usuario, puede filtrar partidos según le sea conveniente.



Es importante mencionar también que cuando el usuario está logeado, no se mostrará ninguna opción incoherente con la sesión iniciada, es decir, no habrá ninguna opción para iniciar sesión o registrarse. Por ejemplo, en el “footer” desaparece por completo la columna de la izquierda.

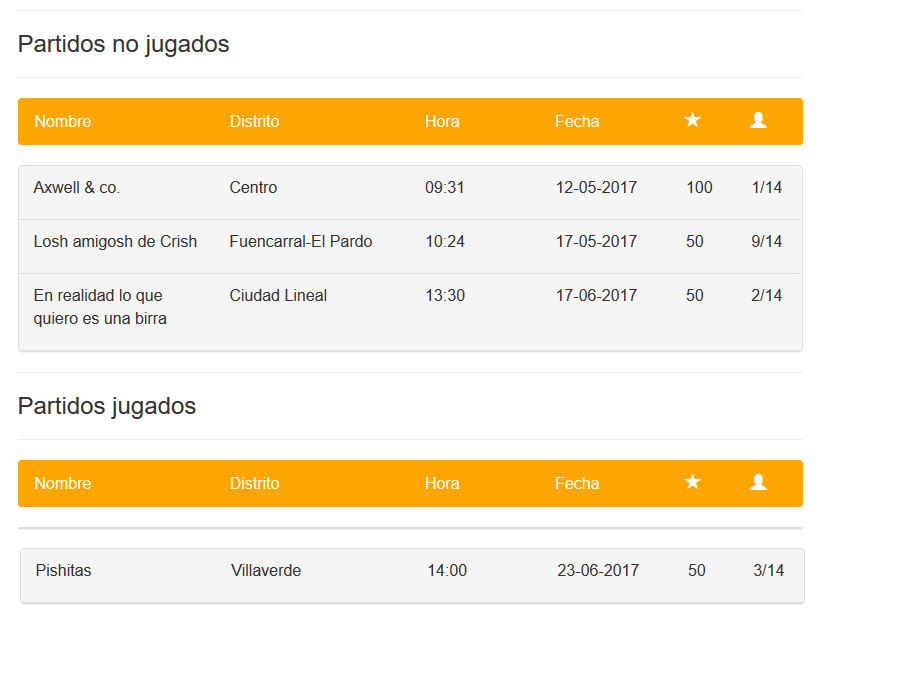


Los partidos mostrados en la aplicación tienen un desplegable (collapse) al ser pulsados, con la opción de ver y compartir. Además, de cada partido se muestra el nombre, el distrito en el que se juega, la fecha, la skill recomendada en puntos y el número de usuarios actualmente registrados.



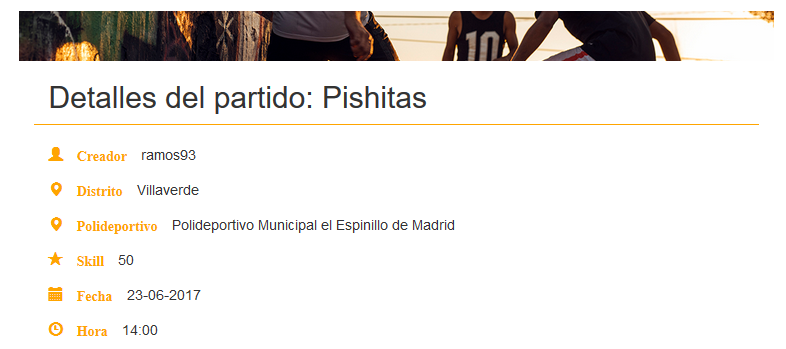
## Mis partidos:

Esta vista muestra todos los partidos en los que está apuntado el usuario, dividiéndolos en partidos jugados y partidos no jugados.

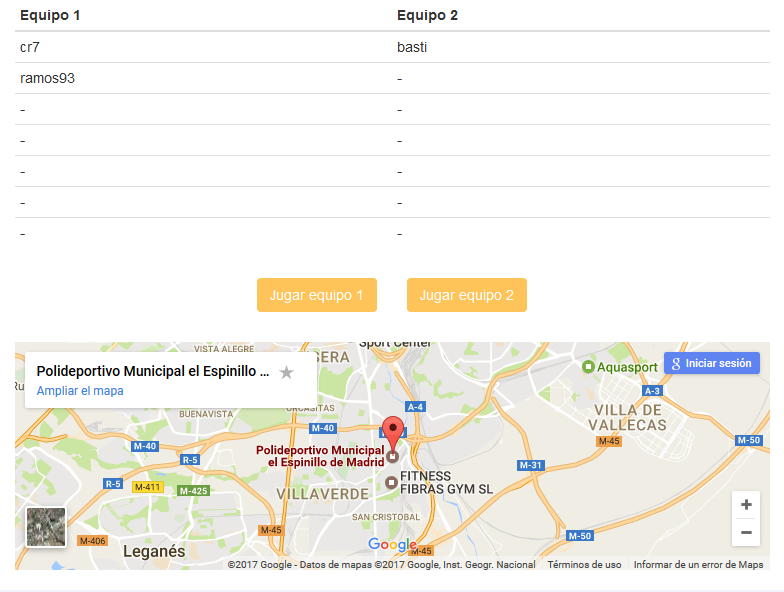


Esta vista nos permite ver también el partido al pulsar en él, llevándonos a la vista de un partido. Desde esta vista podremos ver los participantes de cada partido, y unirnos a cualquiera de los dos equipos.

Se mostrará una descripción detallada del partido



También se pueden ver los participantes de cada partido, además de un mapa de Google con la localización del polideportivo.



## Mejores jugadores:

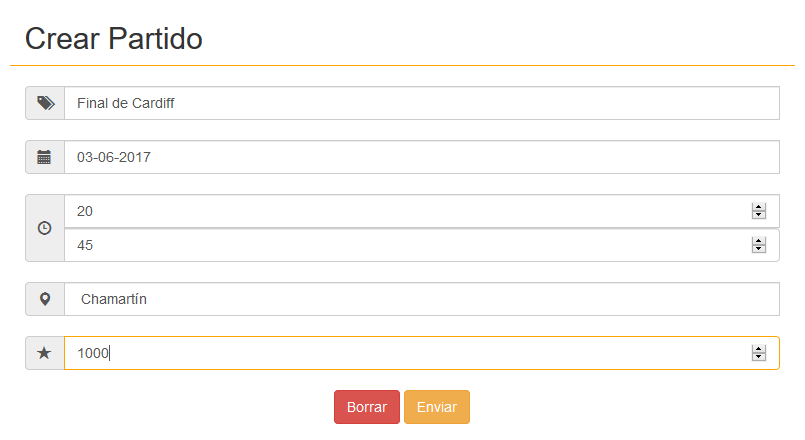
En la vista de mejores jugadores, el usuario podrá ver el ranking mencionado anteriormente, con los mejores jugadores de su zona. La lista estará ordenada por puntos de manera descendiente.



Se mostrará también un mapa del distrito. Si el usuario logeado pulsa en el botón para ver el perfil de alguno de los usuarios del ranking, este podrá ver la información detallada de ese usuario. También podrá ver los partidos en los que esté registrado este usuario, obteniendo así un apartado social en la aplicación.

## Crear partido:

Esta vista permite al usuario crear partidos con un nombre, una fecha, una hora, un distrito y un skill mínimo recomendado. Además, se ha incluido con AJAX un desplegable que muestra los polideportivos según el distrito que elija el usuario.



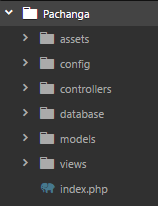
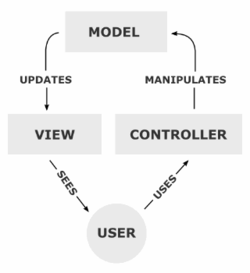


Cuando el usuario crea el partido, será redirigido a la ventana de detalles de ese partido y le saltará una alerta informando de que se ha creado correctamente.

# arquitectura de la aplicación

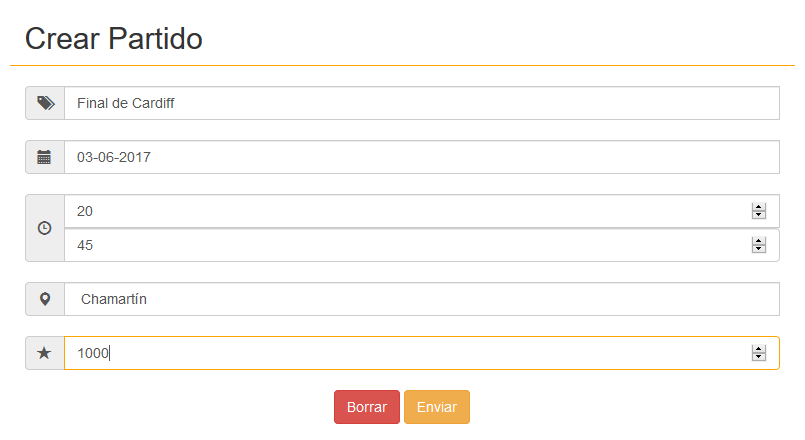
## Diseño:

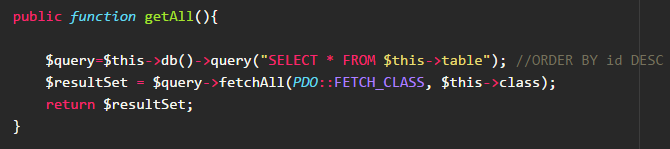
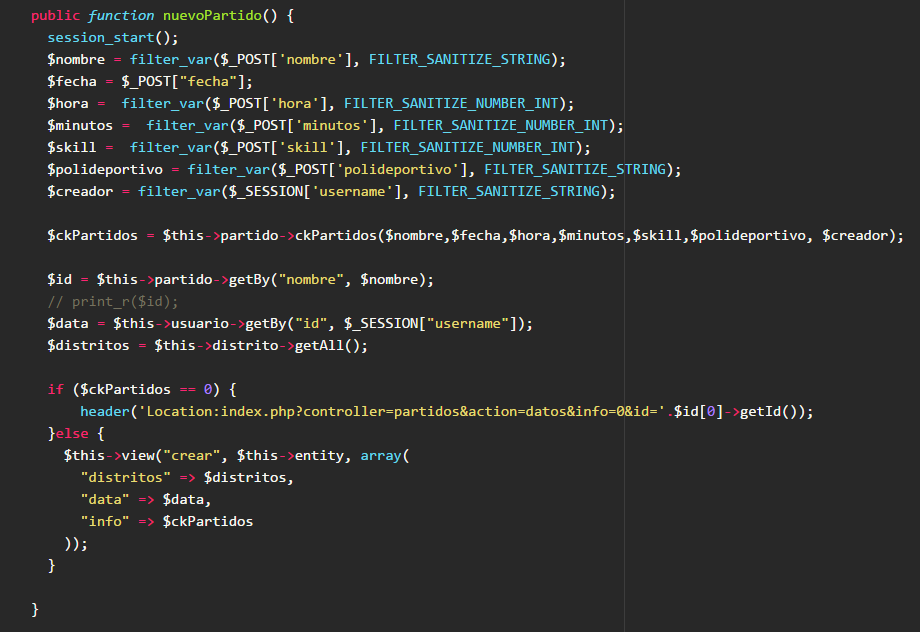
En cuanto a la arquitectura de nuestra aplicación, hemos utilizado el patrón de diseño Modelo-Vista-Controlador (MVC), ya que creemos que es el que mejor representa la interacción del cliente con el servidor y viceversa, y porque es el patrón más utilizado actualmente en el diseño de aplicaciones web. Además, hemos utilizado el patrón Singleton para el acceso a base de datos, permitiendo sólo una instancia del objeto que accede a la misma.

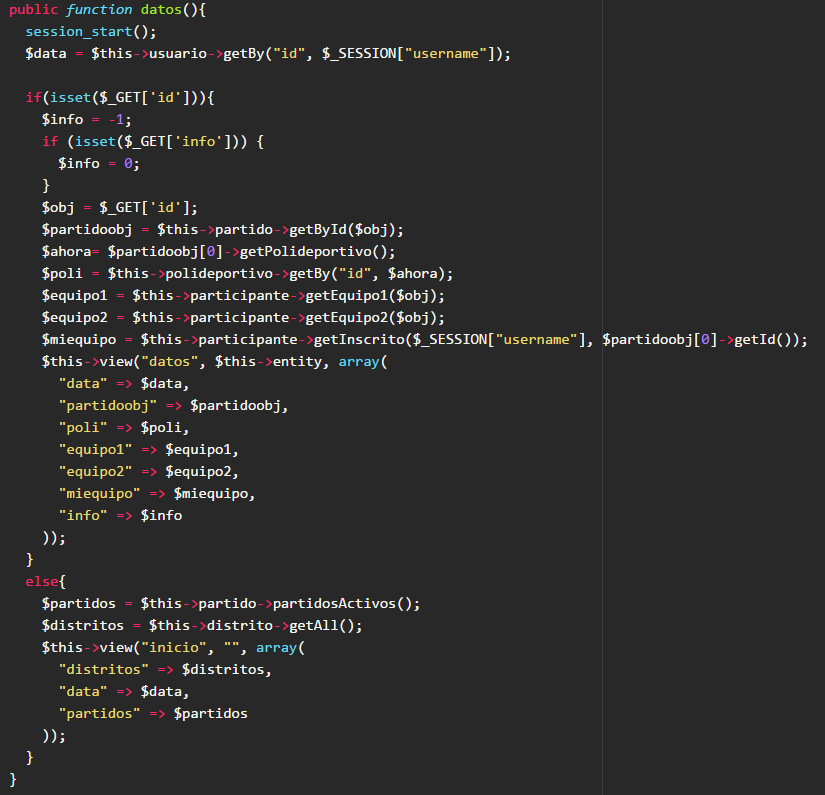
 

Un ejemplo de la utilización de este patrón sería, la funcionalidad de “Crear partido”. Así, cuando el usuario rellena los datos del partido y pulsa en enviar, se llamaría al controlador de partidos, con el método (action) “crearPartido”.

En la siguiente página se explica esta interacción gráficamente







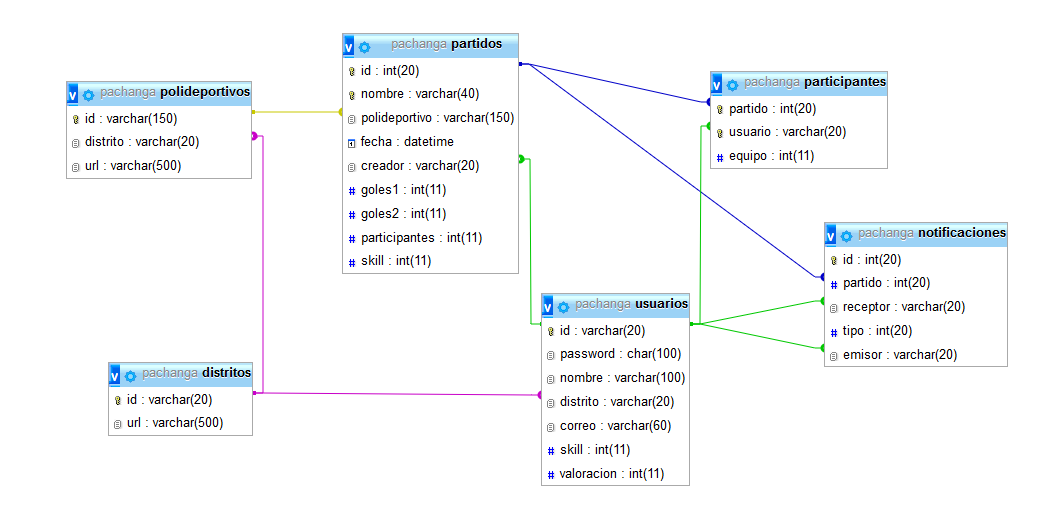


## Base de datos:

Para el diseño de la base de datos hemos utilizado la herramienta de phpMyAdmin que viene incluida en el paquete XAMPP, tal y como se vio en clase.

Hemos dividido la base de datos (“pachanga”) en seis tablas: “polideportivos”, “partidos”, “distritos”, “usuarios”, “notificaciones” y “participantes”, siendo esta última necesaria para representar la relación de muchos a muchos (N-N) que hay entre los usuarios y los partidos.

El diseño de la base de datos es el siguiente:



El acceso a la base de datos desde la aplicación se hace con la clase PDO (PHP Data Object), que es una interfaz ligera para poder acceder a bases de datos en PHP. Hemos decidido utilizar PDO porque permite la utilización de sentencias preparadas (PDOStatement), utilizadas para ejecutar la misma sentencia repetidamente con gran eficiencia.

## Decisiones de diseño:

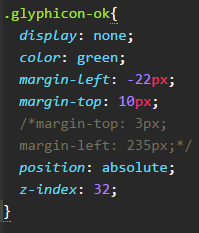
Para el diseño hemos decidido utilizar Bootstrap (<http://getbootstrap.com>), porque creemos que el diseño “mobile first” es un apartado muy importante en una aplicación como Pachanga, ya que mejora la accesibilidad y usabilidad de la misma.

Hemos descargado e incluido el CSS de Bootstrap en la librería de la aplicación (“library.php”) y el Javascript (“script.php”):





Hemos modificado también ciertas clases de Bootstrap según la necesidad de diseño, pero siempre en otros archivos CSS.

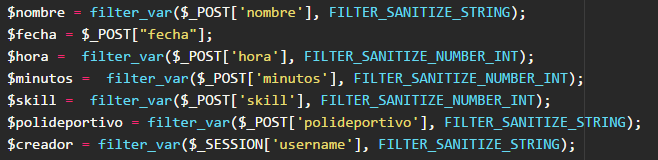




# Seguridad

## SQL Injection:

Para proteger la página frente a ataques de SQL Injection, hemos saneado todos los parámetros proporcionados por el usuario antes de realizar las queries.



A parte del saneado, hemos utilizado las sentencias preparadas de PDO mencionadas en el apartado anterior. La característica principal de las sentencias preparadas es que la consulta y los datos se envían al servidor SQL de manera separada. Esto es importante, porque la base del ataque SQL Injection es aprovechar la mezcla de código y datos en las consultas SQL.

## Directory listing:

Hemos impedido el listado de directorios mediante un fichero de configuración de apache (.htaccess).



## XSS (Cross Site Scripting):

Para proteger a los usuarios de Pachanga frente a este tipo de ataques, cuando el usuario intenta acceder a alguna página mediante URL sin haber iniciado sesión, el sistema redirige a la página de home. Esto lo hemos hecho mediante una función de filtrado de la URL que redirige según convenga. Además, esto nos ha permitido ahorrar bastante código, ya que no hemos tenido que hacer las comprobaciones en todos los archivos, sino sólo en uno (“functions.php”).



## Encriptado de contraseñas:

Todas las contraseñas son encriptadas antes de ser incluidas en la base de datos. Cuando el usuario inicia sesión, se hashea la contraseña proporcionada por este y se compara con la que hay en la base de datos. Nunca se desencriptan las contraseñas que hay en la base de datos.

El algoritmo utilizado para encriptar es SHA-512. La encriptación, paso por paso, es la siguiente:

* Se genera un string ($salt) de 16 caracteres con md5 en base 64.
* Este string se hashea 10.000 veces ($rounds=10000).
* Se encripta la contraseña con la función “crypt()”, que utiliza el algoritmo de encriptación SHA-512.



Después, para comparar las contraseñas, se realiza la misma operación con la contraseña proporcionada por el usuario.

## Fuerza bruta:

La protección frente ataques de fuerza bruta se ha hecho incluyendo el RE-CAPTCHA de Google, para requerir confirmación si se proporciona erróneamente una contraseña, evitando así cualquier ataque de fuerza bruta a los formularios de inicio de sesión y registro.

# instrucciones de uso

Lo primero que debe hacer el usuario para utilizar Pachanga es registrarse en la aplicación, escogiendo el distrito al que pertenece, pudiendo elegir entre los 21 distritos de Madrid.

Una vez registrado, podrá ver una página de inicio con todos los partidos que hay registrados, y filtrar los mismos por nombre, distrito y fecha.

Tendrá, además, un menú en la parte lateral izquierda (o pulsando el menú Burger en la versión responsive), desde el que podrá crear un partido, ver sus partidos registrados, y ver los mejores jugadores de su distrito (siempre con la opción de volver a la página de inicio pulsando el logo de Pachanga o seleccionando “Inicio” en el menú).

El usuario puede interactuar con otros compartiendo los partidos que desee con los demás usuarios de la aplicación.

Cuando los partidos registrados por el usuario hayan acabado (cuando se pase la fecha), pasarán a formar parte de los partidos jugados, y se enviará una notificación al usuario informando al mismo de que puede puntuarlo. Cuando lo puntúa, el resto de los usuarios que han jugado este partido podrán ver el resultado del mismo.