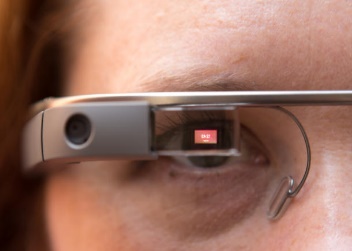
Trabajo Final de Seguridad en las Aplicaciones



Tema: CHAT ANONIMO SIN RASTROS

Alumno: Jorge Oscar Gamez

Universidad Nacional Arturo Jauretche

Introducción

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

Es por eso que cada vez más debemos resguardar y proteger la información como si nosotros mismos la fuésemos a divulgar , ya que sin darnos cuenta exponemos datos puntuales que afectan a nuestra privacidad

¿Porque este tipo de método sirve para brindar la seguridad necesaria que las personas necesitan para proteger su privacidad?

Con el simple hecho de utilizar un dispositivo externo como medio para descifrar y un mensaje cifrado, en este caso texto en pantalla, nos aseguramos de que solo nosotros podamos visualizar el contenido de la ventana del ordenador que en situaciones muy delicadas dan un valor agregado a la confidencialidad de nuestras conversaciones.

Resumen

El desarrollo no está basado en ningún sistema hecho hasta el momento, pero esta tecnología hoy en día está al alcance de todos de manera separada por lo que se tuvo que investigar y trabajar para permitir la fusión de las mismas en este proyecto

Utilizamos métodos de encriptación de texto para guardar las conversaciones en nuestra base de datos que gracias a un botón con el nombre “eliminar rastros” ejecuta la sentencia “Delete \* FROM chat “ en nuestra base de datos eliminando cualquier conversación registrada mas allá de estar encriptada con la función nativa de PHP base64\_encode y base64\_decode. , librerías externas y un lector desarrollado en Android Studio personalizado para este proyecto.

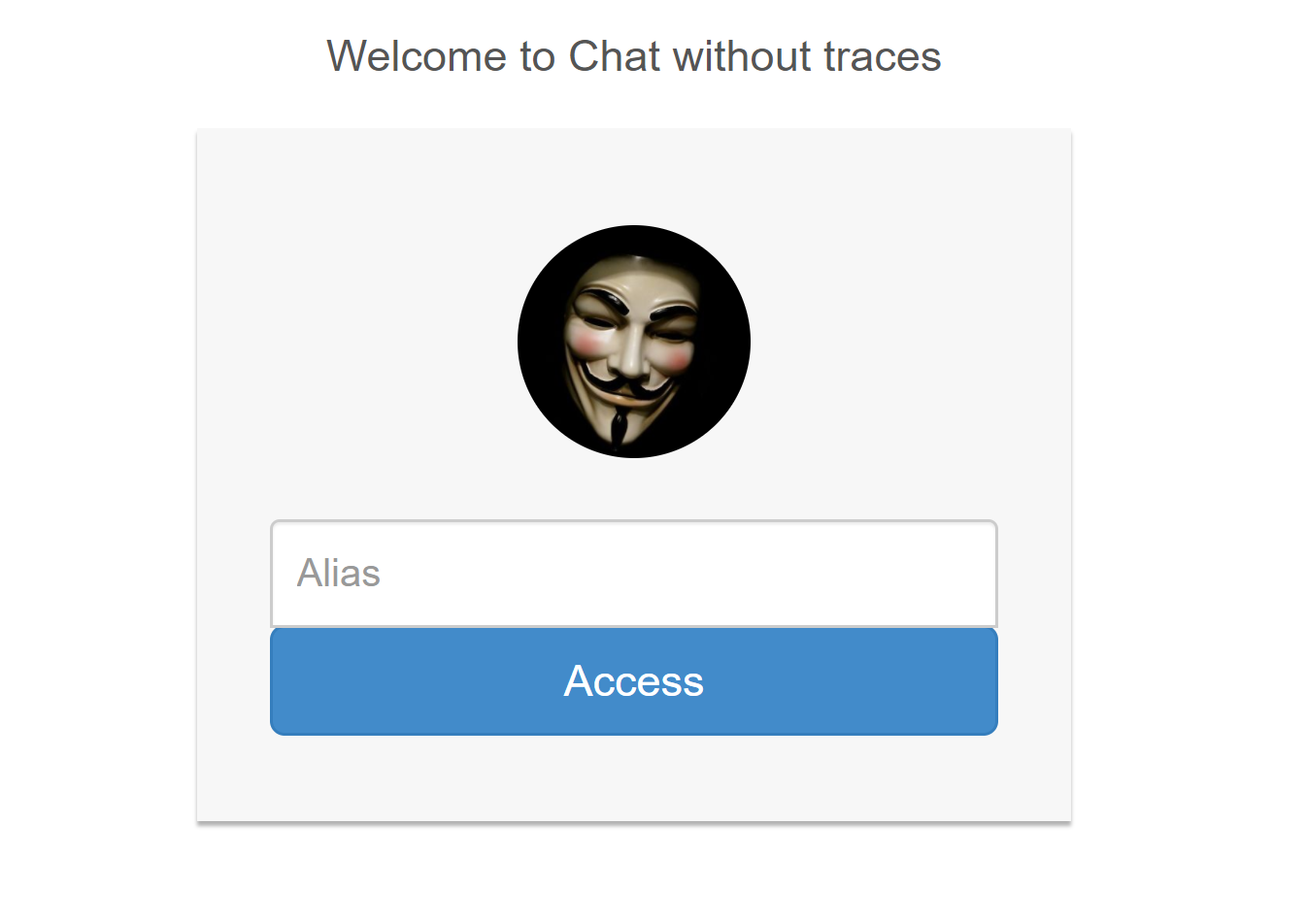
Desarrollo

Aplicación WEB

Para comenzar con el desarrollo utilizamos el lenguaje de programación PHP, base de datos MariaDB, y librerías externas de codificación QR basadas en JQuery del lado del cliente y algunas otras para el lado del servidor

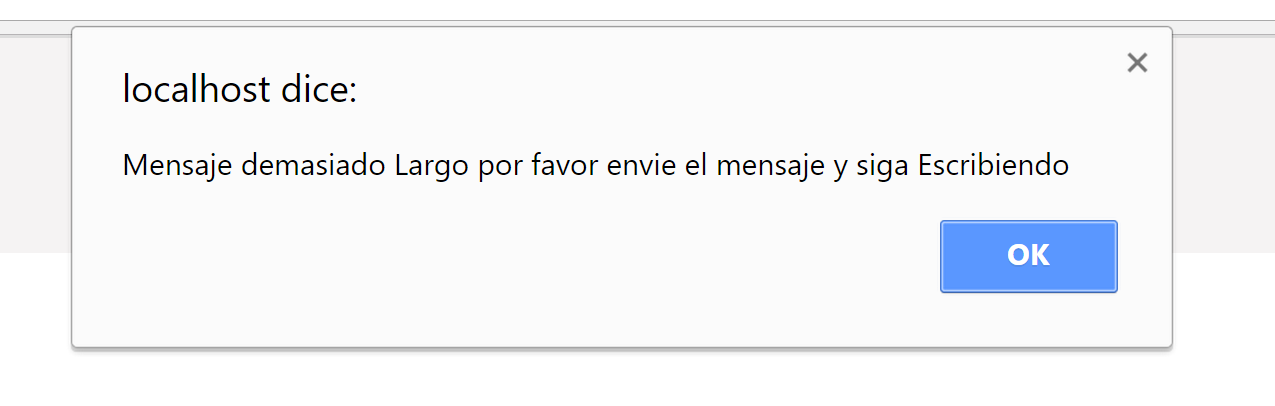
Logeo con Alias - Protección de datos de usuario

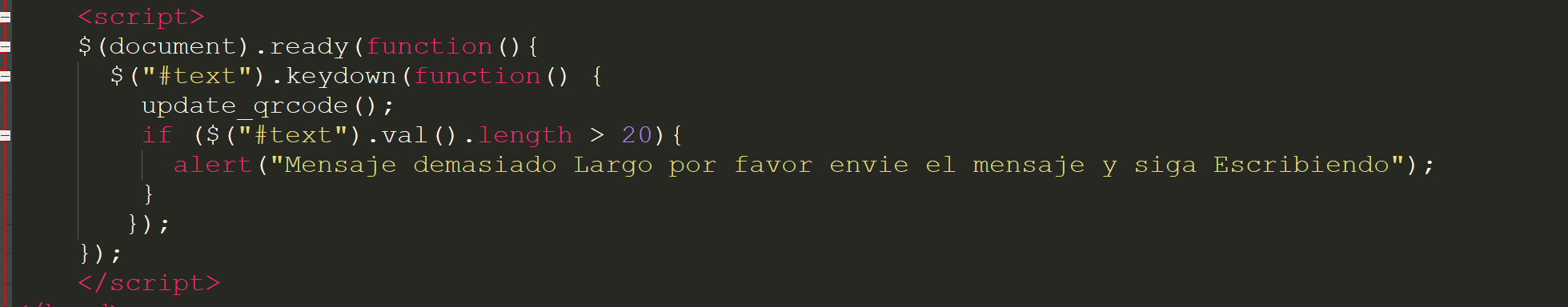
El iniciar nuestro sistema ingresamos con un alias para evitar registros de usuarios y solicitud de datos personales que se podrían exponer en el caso de un ataque a nuestra base de datos, como también evitamos especificar una política para la gestión de datos de usuario (control de acceso y reglas de flujo de información) manteniendo el anonimato de los usuarios.



Disponibilidad de nuestro servidor.

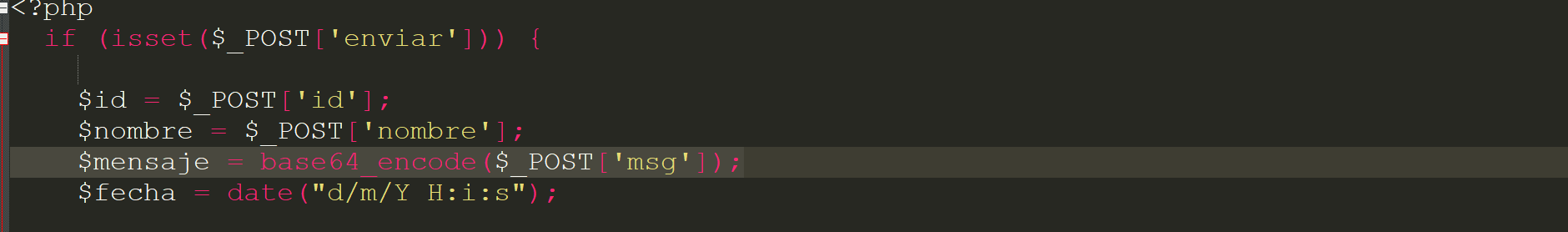
Con el siguiente script de JQuery podemos validar del lado del cliente antes de que viaje hacia nuestro servidor el largo de string a ingresar para evitar ataques por inundación tema de la Clase 1 con un mensaje que evita la continuación de ingreso de texto.





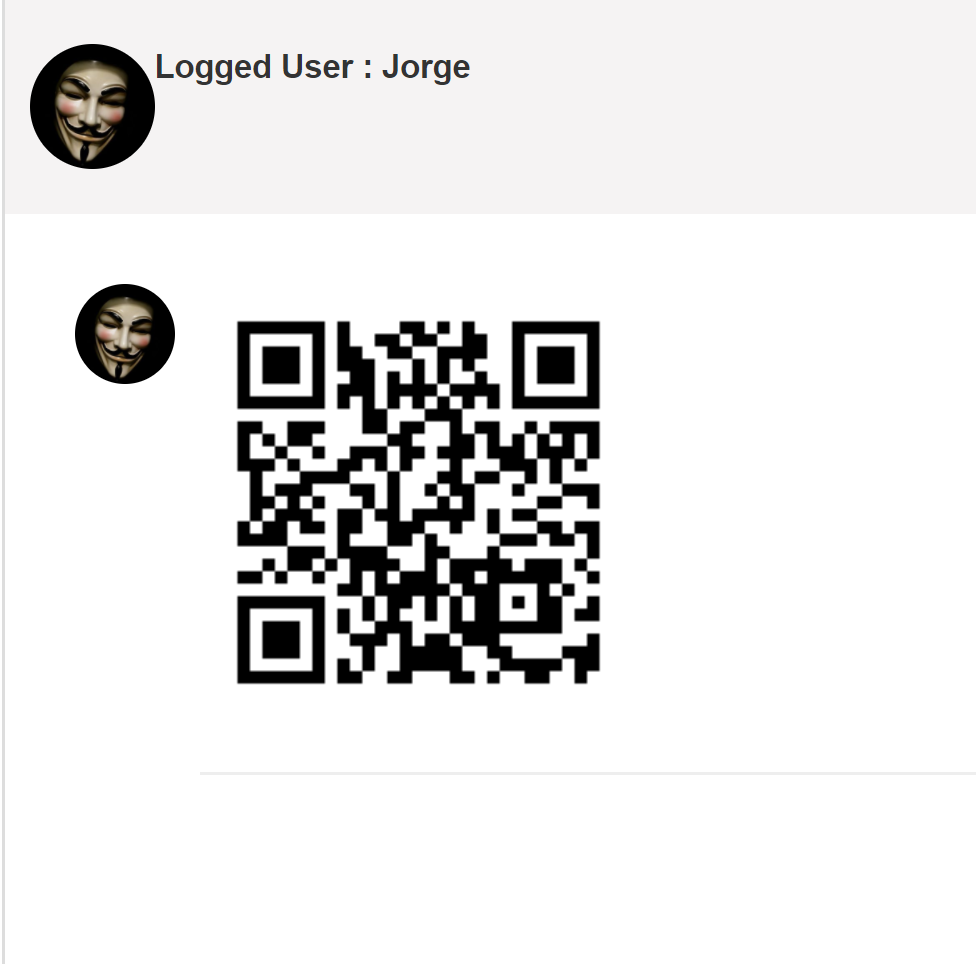
Encriptación Base64\_encode () de PHP

Del lado del cliente en el archivo sala.php encerramos la variable capturada por el método POST antes de guardarla en nuestra base de datos para encriptarla.

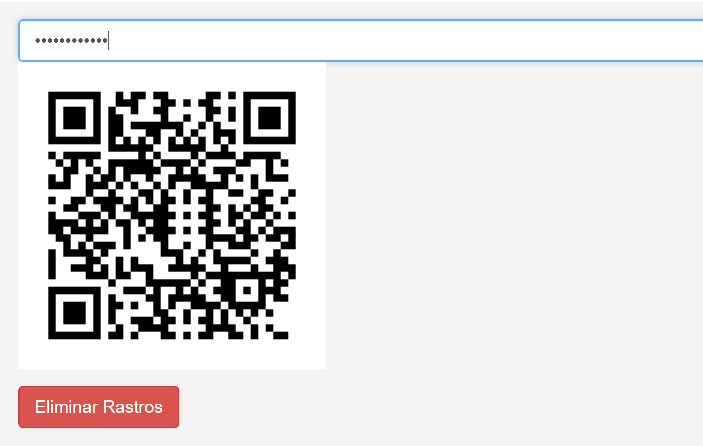




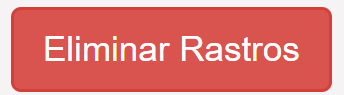
Print Screen de nuestra Base de datos para la palabra “Hola Carlos” que codificado en base64 es igual a SG9sYSBDYXJsb3Mg. Que luego llega desencriptada a la vista el cliente, pero codificada en código QR.



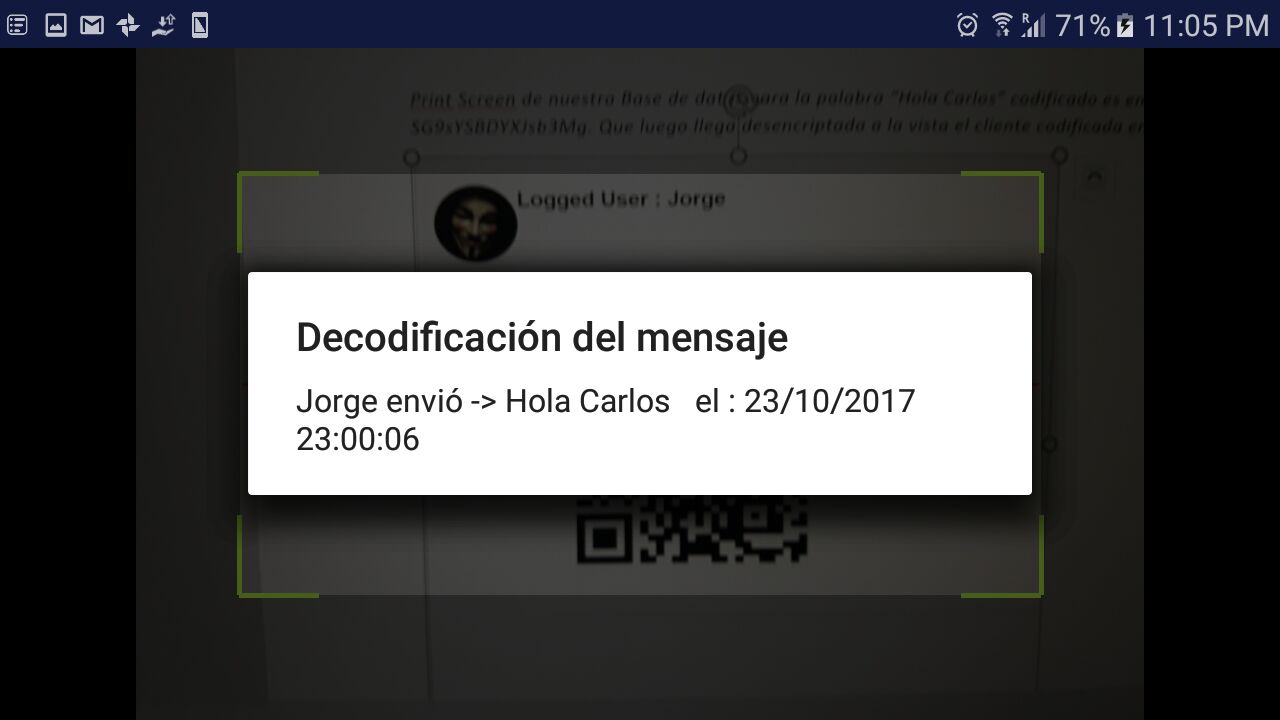
Codificación con librería externa en tiempo real JQuery y Ocultamiento de texto legible con un input box tipo password



Eliminar rastros de conversaciones

El botón  borra todo registro existente de nuestra base de datos para la tranquilidad de los usuarios.

Aplicación Android



En tiendas de archivos APK solo se pudo encontrar lectores que luego de la lectura te redirigían a una búsqueda en internet o simplemente a otra pantalla deteniendo la ejecución, por lo que se creó un lector constante QR personalizado para este proyecto con memoria interna de mensajes leídos y detección de nuevos mensajes en movimiento para que según donde este mirando el usuario con la cámara descifre el mensaje oculto, pensado para lentes como Google Glass o similares como VRBOX.

**Mejoras futuras**

Debemos reconocer que se peude mejorar la aplicaicon con la utilización de Sockets.io y tecnología como NodeJs , abarcando tanto del lado del cliente como del lado del servidor , y la utilización de Programación Orientada a Objetos con librerias incluidas como PDO pero de PHP. La visualización de usuario online , y la utilización de una clave en la operación de encriptación de algo como el imei del dispositivo externo de lectura , en este caso los lentes de Google glass

Apoyo bibliográfico

<http://php.net/>

<http://phpqrcode.sourceforge.net/>