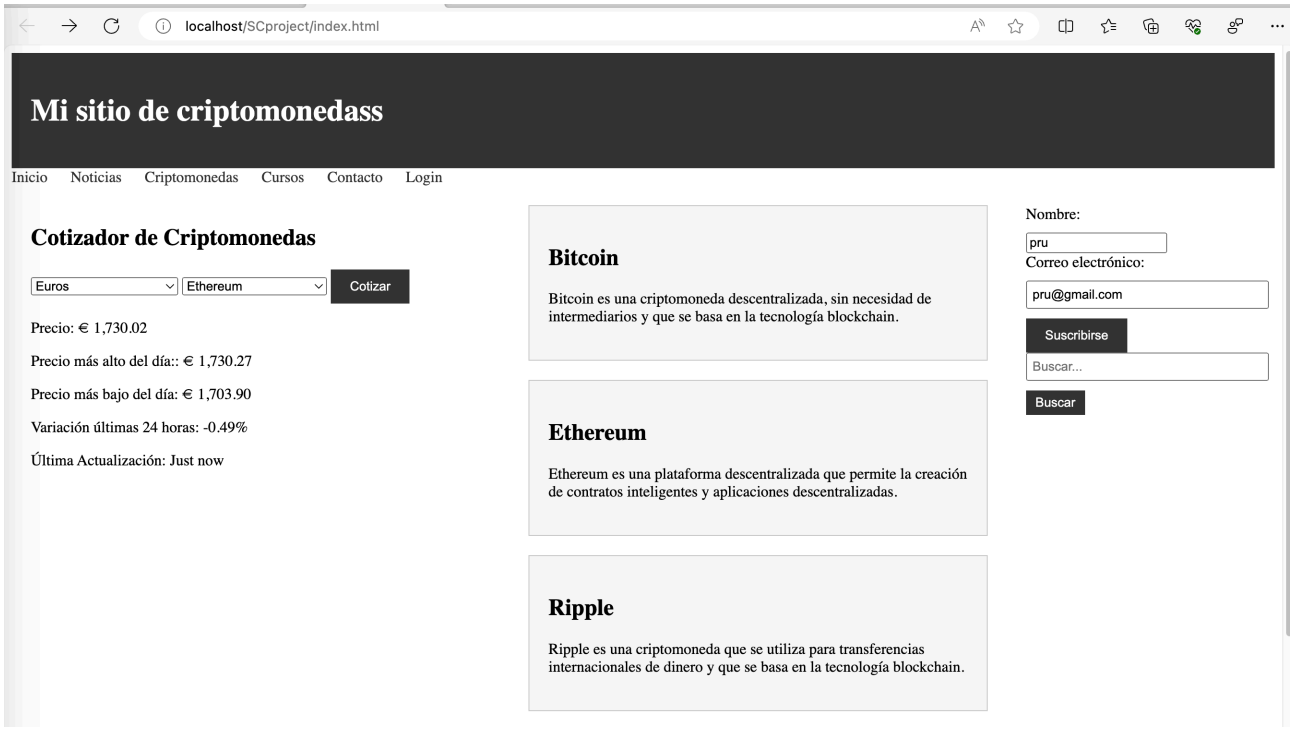
Franklin, Reyes Marchel.

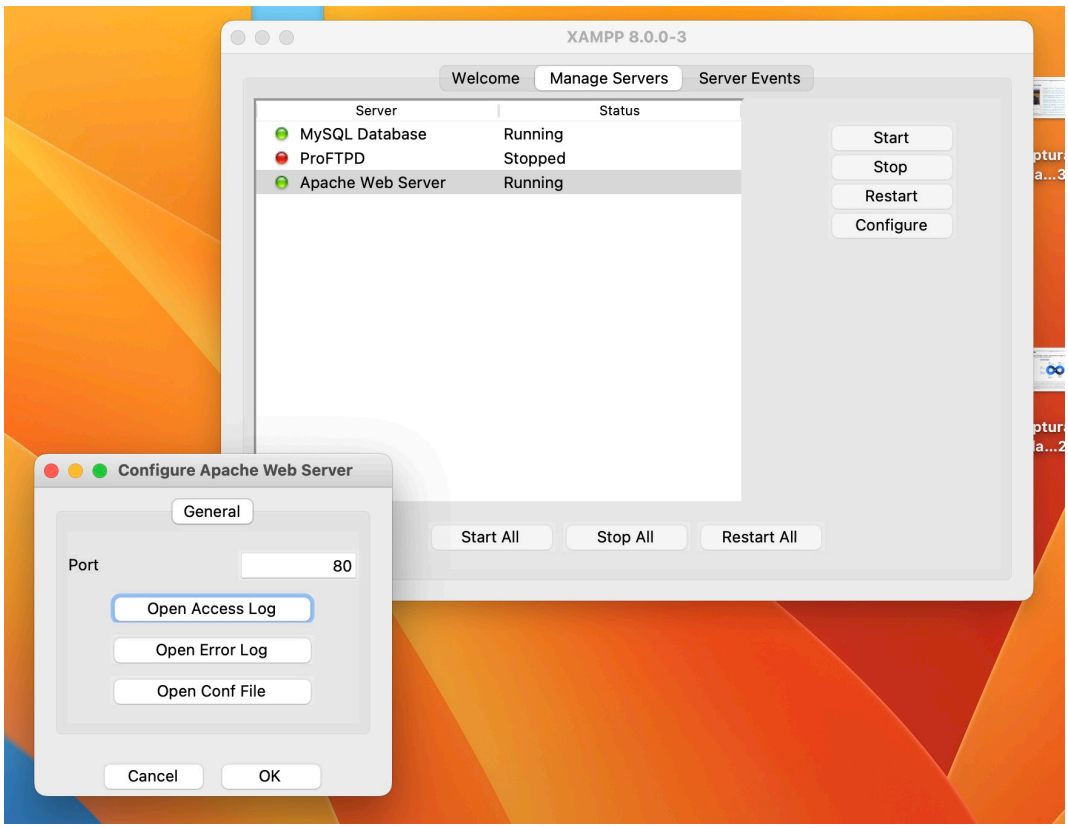
Proyecto de identificación y prevención de vulnerabilidades.

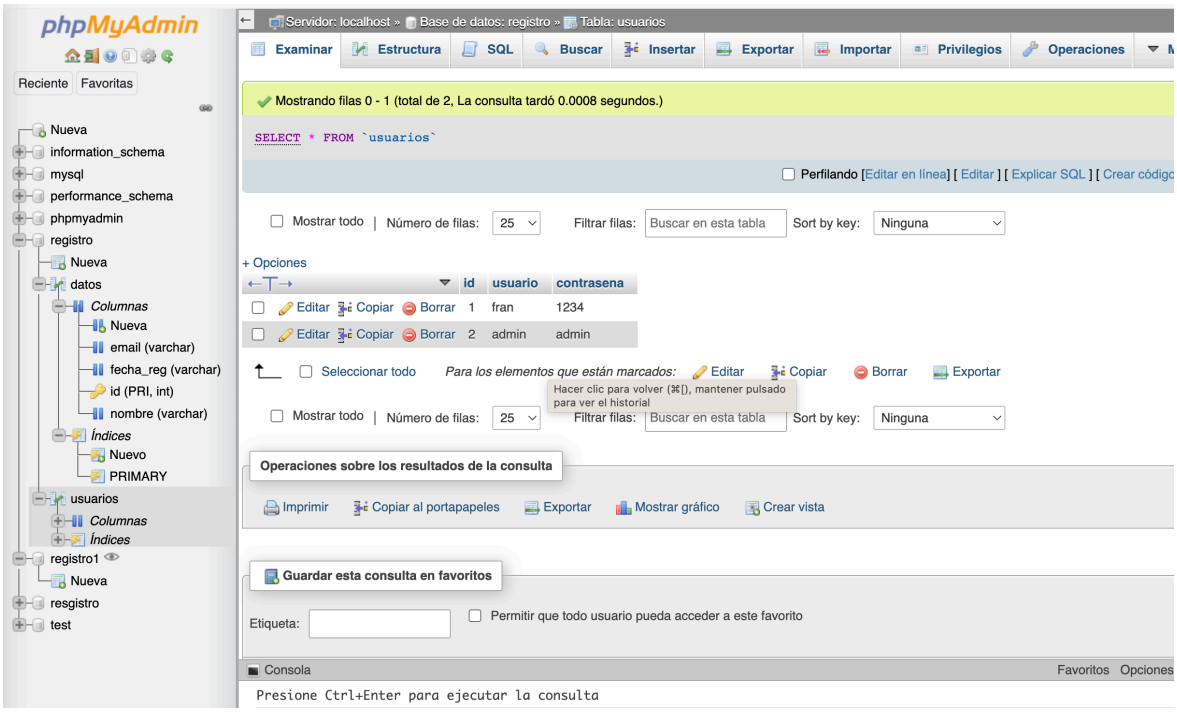
1. Idea de la aplicación:

Una web que dé información y noticias sobre criptomonedas y tecnología blockchain, permita cotizar criptomonedas en las principales divisas fiat usando una API y permita loguearse y suscribirse a un boletín de noticias. Se obtiene la mayor parte del código, usando un plugin de CHAT-GPT4 para Visual Studio Code, y repositorios de GITHUB.



2. Se plantea hacer una web en HTML, CCS y JS para el frontend, con una base de datos SQL y PHP para el backend. Se desarrolla usando servidor local con la herramienta XAMPP para el servidor local APACHE y la base de datos MySQL, en una Mac M1.


XAMPP 8.0.0-3
Welcome
Manage Servers
Server Events
Server
Status
MySQL Database
Running
ProFTPD
Stopped
Apache Web Server
Running
Start
Stop
Restart
Configure
Start All
Stop All
Restart All
Configure Apache Web Server
General
Port
80
Open Access Log
Open Error Log
Open Conf File
Cancel
OK


phpMyAdmin
Reciente
Favoritas
Nueva
information_schema
mysql
performance_schema
phpmyadmin
registro
Nueva
datos
Columnas
Nueva
email (varchar)
fecha_reg (varchar)
id (PRI, int)
nombre (varchar)
Índices
Nuevo
PRIMARY
usuarios
Columnas
Índices
registro1
Nueva
resgistro
test
Servidor: localhost » Base de datos: registro » Tabla: usuarios
Examinar
Estructura
SQL
Buscar
Insertar
Exportar
Importar
Privilegios
Operaciones
Mostrando filas 0 - 1 (total de 2, La consulta tardó 0.0008 segundos.)
SELECT * FROM `usuarios`
Perfilando [Editar en línea] [Editar] [Explicar SQL] [Crear código
Mostrar todo | Número de filas: 25 Filtrar filas: Buscar en esta tabla Sort by key: Ninguna
+ Opciones
id
usuario
contrasena
Editar Copiar Borrar 1 fran 1234
Editar Copiar Borrar 2 admin admin
Seleccionar todo
Para los elementos que están marcados:
Editar
Copiar
Borrar
Exportar
Hacer clic para volver (⌘[), mantener pulsado para ver el historial
Mostrar todo | Número de filas: 25 Filtrar filas: Buscar en esta tabla Sort by key: Ninguna
Operaciones sobre los resultados de la consulta
Imprimir
Copiar al portapapeles
Exportar
Mostrar gráfico
Crear vista
Guardar esta consulta en favoritos
Etiqueta:
Permitir que todo usuario pueda acceder a este favorito
Consola
Favoritos
Opciones
Presione Ctrl+Enter para ejecutar la consulta

Pie de foto

3. La la primera vulbnerabilidad a subsanar es INFORMATION LEAKAGE o goteo de información, ya que mostrar información sobre la tecnología utilizada, en este caso servidor APACHE con lenguaje PHP y sus versiones facilita a los atacantes la penetración del sistema.

Pie de foto

Para corregir la vulnerabilidad de goteo de información, se debe mostrar un mensaje de error genérico en lugar de información detallada del servidor, se debe agregar la siguiente línea al archivo .**htaccess** en el directorio raíz:

ErrorDocument 403 "Lo siento, no tienes permiso para acceder a este recurso.”

Luego añadimos una segunda vulnerabilidad a subsanar: SQL Injection. Para corregirla se debe usar declaraciones preparadas con PHP.

Se cambia el código de la consulta de la tabla de la base de datos INSERT INTO

```
      $consulta = "INSERT INTO datos(nombre, email, fecha_reg)
VALUES ('$name','$email','$fechareg')";
      $resultado = mysqli_query($conex,$consulta);
```

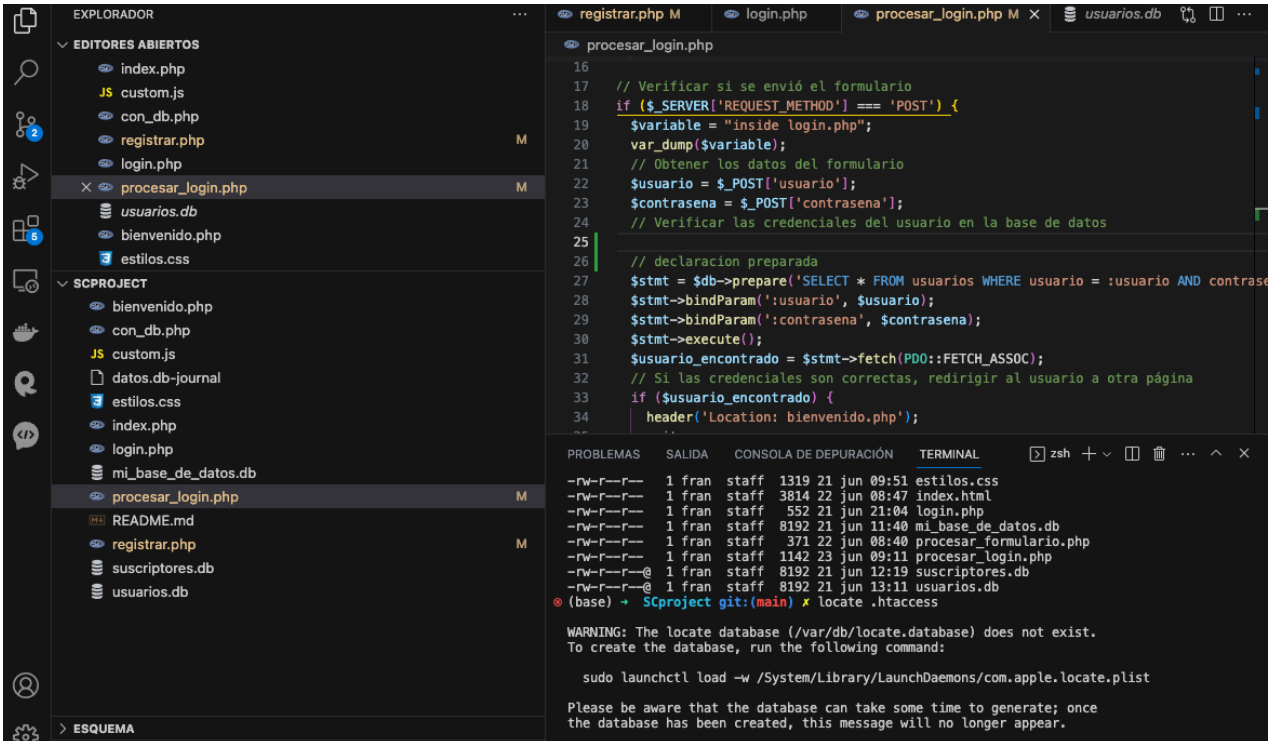
por la declaración preparada:

```
  $stmt = $db->prepare('SELECT * FROM usuarios WHERE usuario
= :usuario AND contrasena = :contrasena');
  $stmt->bindParam(':usuario', $usuario);
  $stmt->bindParam(':contrasena', $contrasena);
```

```
  $stmt->execute();
```

4. Repositorio: https://github.com/fran-immune/SCproject

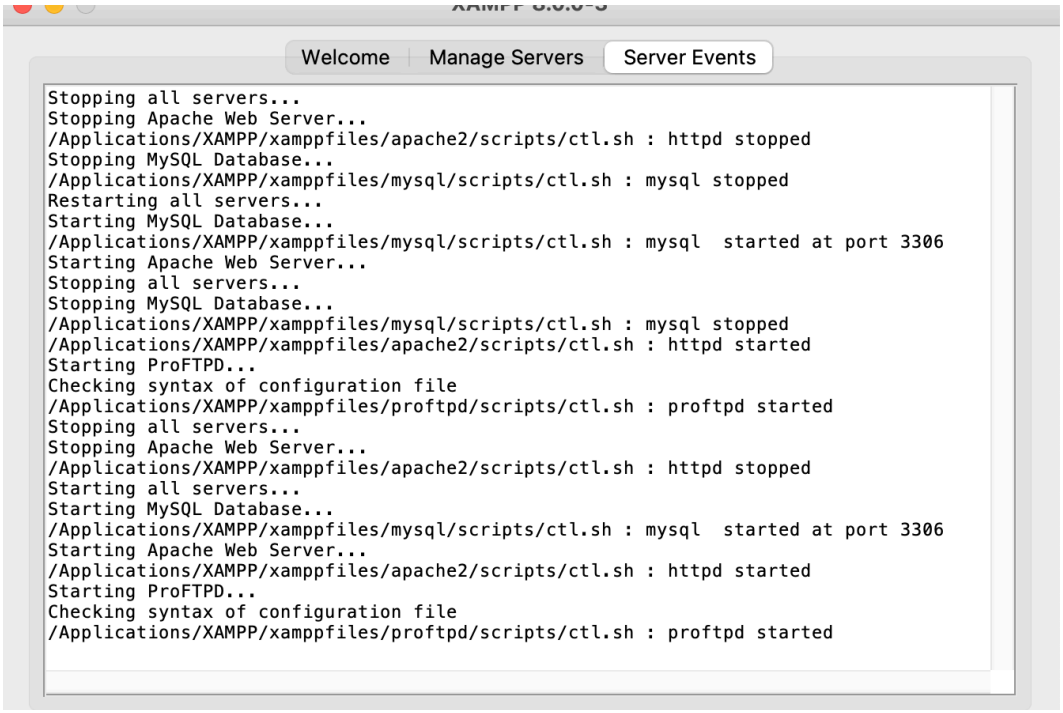
Anexos:
Código para evitar SQL Injection



Pie de foto

Fallo de servidor para abrir PHP

```
[Fri Jun 23 07:02:46.329180 2023] [suexec:notice] [pid 50496] AH01232: suEXEC mechanism enabled
(wrapper: /Applications/XAMPP/xamppfiles/bin/suexec)
[Fri Jun 23 07:02:46.472266 2023] [ssl:warn] [pid 50500] AH01906: www.example.com:443:0 server
certificate is a CA certificate (BasicConstraints: CA == TRUE !?)
[Fri Jun 23 07:02:46.472307 2023] [ssl:warn] [pid 50500] AH01909: www.example.com:443:0 server
certificate does NOT include an ID which matches the server name
[Fri Jun 23 07:02:46.472531 2023] [lbmethod_heartbeat:notice] [pid 50500] AH02282: No slotmem from
mod_heartmonitor
[Fri Jun 23 07:02:46.518948 2023] [mpm_prefork:notice] [pid 50500] AH00163: Apache/2.4.46 (Unix)
OpenSSL/1.1.1i PHP/8.0.0 mod_perl/2.0.11 Perl/v5.32.0 configured -- resuming normal operations
[Fri Jun 23 07:02:46.519013 2023] [core:notice] [pid 50500] AH00094: Command line: '/Applications/
XAMPP/xamppfiles/bin/httpd -E /Applications/XAMPP/xamppfiles/logs/error_log -D SSL -D PHP'
[Fri Jun 23 07:50:00.977126 2023] [php:error] [pid 50718] [client ::1:61806] script '/Applications/
XAMPP/xamppfiles/htdocs/conexion-a-mysql-con-php/login.php' not found or unable to stat, referer:
http://localhost/conexion-a-mysql-con-php/login.html
[Fri Jun 23 08:19:07.583313 2023] [php:error] [pid 50506] [client ::1:62194] script '/Applications/
XAMPP/xamppfiles/htdocs/conexion-a-mysql-con-php/procesar_login.php' not found or unable to stat
[Fri Jun 23 08:59:38.208192 2023] [php:error] [pid 50722] [client ::1:62810] script '/Applications/
XAMPP/xamppfiles/htdocs/conexion-a-mysql-con-php/procesar_login1.php' not found or unable to stat,
referer: http://localhost/conexion-a-mysql-con-php/login.php
[Fri Jun 23 09:01:00.212664 2023] [php:error] [pid 85527] [client ::1:62851] script '/Applications/
XAMPP/xamppfiles/htdocs/conexion-a-mysql-con-php/procesar_login1.php' not found or unable to stat
[Fri Jun 23 09:02:25.202902 2023] [php:error] [pid 50506] [client ::1:62898] script '/Applications/
XAMPP/xamppfiles/htdocs/conexion-a-mysql-con-php/procesar_login1.php' not found or unable to stat,
referer: http://localhost/conexion-a-mysql-con-php/login.php
[Fri Jun 23 09:48:29.970883 2023] [php:error] [pid 50721] [client ::1:65224] script '/Applications/
XAMPP/xamppfiles/htdocs/conexion-a-mysql-con-php/login2.php' not found or unable to stat
[Fri Jun 23 10:47:39.526862 2023] [php:error] [pid 50504] [client ::1:49417] script '/Applications/
XAMPP/xamppfiles/htdocs/conexion-a-mysql-con-php/login2.php' not found or unable to stat
```


Welcome
Manage Servers
Server Events
Stopping all servers...
Stopping Apache Web Server...
/Applications/XAMPP/xamppfiles/apache2/scripts/ctl.sh : httpd stopped
Stopping MySQL Database...
/Applications/XAMPP/xamppfiles/mysql/scripts/ctl.sh : mysql stopped
Restarting all servers...
Starting MySQL Database...
/Applications/XAMPP/xamppfiles/mysql/scripts/ctl.sh : mysql started at port 3306
Starting Apache Web Server...
Stopping all servers...
Stopping MySQL Database...
/Applications/XAMPP/xamppfiles/mysql/scripts/ctl.sh : mysql stopped
/Applications/XAMPP/xamppfiles/apache2/scripts/ctl.sh : httpd started
Starting ProFTPD...
Checking syntax of configuration file
/Applications/XAMPP/xamppfiles/proftpd/scripts/ctl.sh : proftpd started
Stopping all servers...
Stopping Apache Web Server...
/Applications/XAMPP/xamppfiles/apache2/scripts/ctl.sh : httpd stopped
Starting all servers...
Starting MySQL Database...
/Applications/XAMPP/xamppfiles/mysql/scripts/ctl.sh : mysql started at port 3306
Starting Apache Web Server...
/Applications/XAMPP/xamppfiles/apache2/scripts/ctl.sh : httpd started
Starting ProFTPD...
Checking syntax of configuration file
/Applications/XAMPP/xamppfiles/proftpd/scripts/ctl.sh : proftpd started

Logs Server