Evidencia de Seguridad en la Base de Datos - Proyecto Trimestre 3

1. Encriptación de Contraseña

Se utiliza la función password_hash() con PASSWORD_DEFAULT para encriptar la contraseña antes de ser almacenada en la base de datos.
Esto garantiza que las contraseñas no se guarden en texto plano, cumpliendo con las buenas prácticas de seguridad.

Código relevante:
```
$hashed_password = password_hash($contraseña, PASSWORD_DEFAULT);
```

2. Inserción Segura en la Base de Datos

Se utiliza una sentencia preparada con bind de parámetros para evitar inyecciones SQL. La contraseña ya encriptada es insertada en la base de datos de forma segura.

Código relevante:
```
$sentencia = $base_de_datos->prepare("INSERT INTO registro (...) VALUES (?, ?, ..., ?, ?);");
$resultado = $sentencia->execute([... , $hashed_password, ...]);
```

3. Validación de Archivos Subidos

Se valida que el archivo de imagen se haya subido correctamente antes de procesarlo.
También se renombra con un nombre único para evitar conflictos.

Código relevante:
```
if (!isset($_FILES["foto_perfil"]) || $_FILES["foto_perfil"]["error"] !== UPLOAD_ERR_OK) {
    exit("Falta la foto de perfil.");
}
$foto_perfil_new_name = uniqid() . "_" . $foto_perfil;
```

4. Comentario Final

Estas implementaciones permiten evidenciar que se aplican medidas de seguridad en el manejo de datos sensibles, como las contraseñas y los archivos subidos, dentro del proyecto correspondiente al Trimestre 3.