MySQL + Docker + phpMyAdmin para practicar ciberseguridad

Muchos estudiantes aprenden SQL haciendo consultas sin contexto.

El problema es que memorizar SELECT * FROM tabla no enseña realmente cómo se usa SQL en seguridad.

Una forma mucho más práctica es montar un pequeño laboratorio donde los datos representen eventos reales:

- intentos fallidos de acceso
- conexiones sospechosas
- actividad fuera de horario
- posibles fugas de información

1□□ Levantar el entorno con Docker

```
docker run --platform linux/amd64 --name myXampp \
-p 41061:22 \
-p 41062:80 \
-d \
-v ~/my_web_pages:/www \
tomsik68/xampp:8
```

Abrimos phpMyAdmin:

- http://localhost:41062/phpmyadmin/

2□□ Crear la base de datos

```
CREATE DATABASE IF NOT EXISTS ciberseguridad_sql;
USE ciberseguridad_sql;
```

3□□ Crear una tabla de intentos fallidos

```
CREATE TABLE intentos_fallidos (
    id INT AUTO_INCREMENT PRIMARY KEY,
    usuario VARCHAR(50),
    ip_origen VARCHAR(45),
    fecha_hora DATETIME,
    intentos_fallidos INT,
    servicio VARCHAR(30)
);
```

4□□ Insertar datos de ejemplo

Aquí es donde realmente empieza la práctica.

```
INSERT INTO intentos_fallidos
(usuario, ip_origen, fecha_hora, intentos_fallidos, servicio)
VALUES
('admin','192.168.1.10','2026-03-12 08:15:00',2,'SSH'),
('admin','192.168.1.10','2026-03-12 08:20:00',3,'SSH'),
('maria','10.0.0.5','2026-03-12 09:00:00',1,'VPN'),
('root','203.0.113.45','2026-03-12 02:18:00',6,'SSH');
```

Ahora ya tenemos eventos que analizar.

5□□ Ver todos los registros

SELECT * FROM intentos_fallidos;

Resultado esperado:

usuario	ip_origen	intentos_fallidos	servicio
admin	192.168.1.10	2	SSH
admin	192.168.1.10	3	SSH
maria	10.0.0.5	1	VPN
root	203.0.113.45	6	SSH

6□□ Detectar posibles ataques de fuerza bruta

Ahora sí tiene sentido hacer consultas de análisis.

```
SELECT
    ip_origen,
    SUM(intentos_fallidos) AS total_intentos
FROM intentos_fallidos
GROUP BY ip_origen
HAVING SUM(intentos_fallidos) >= 5;
```

Esto permite localizar IPs con muchos intentos acumulados.

Resultado:

ip_origen	total_intentos
192.168.1.10	5
203.0.113.45	6