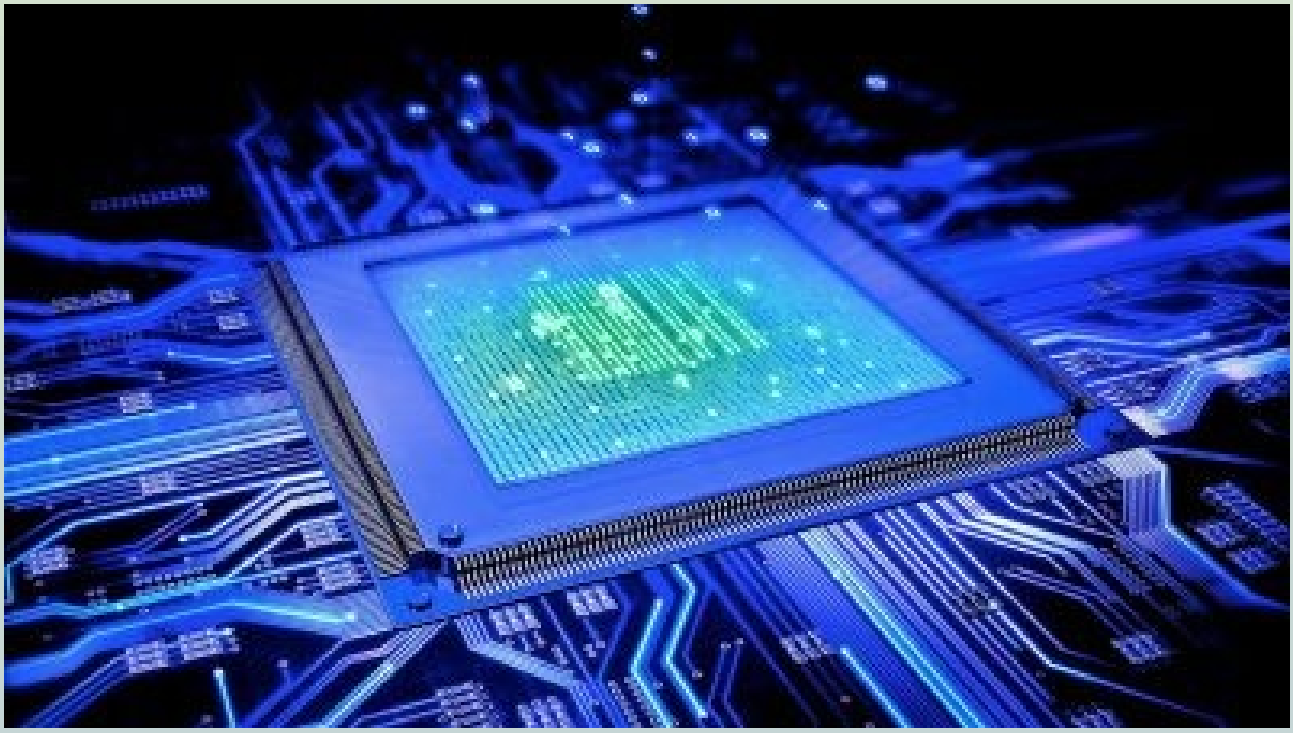
Adrià Llinares Arroyo 1rASIX
20 de març de 2025

Titol

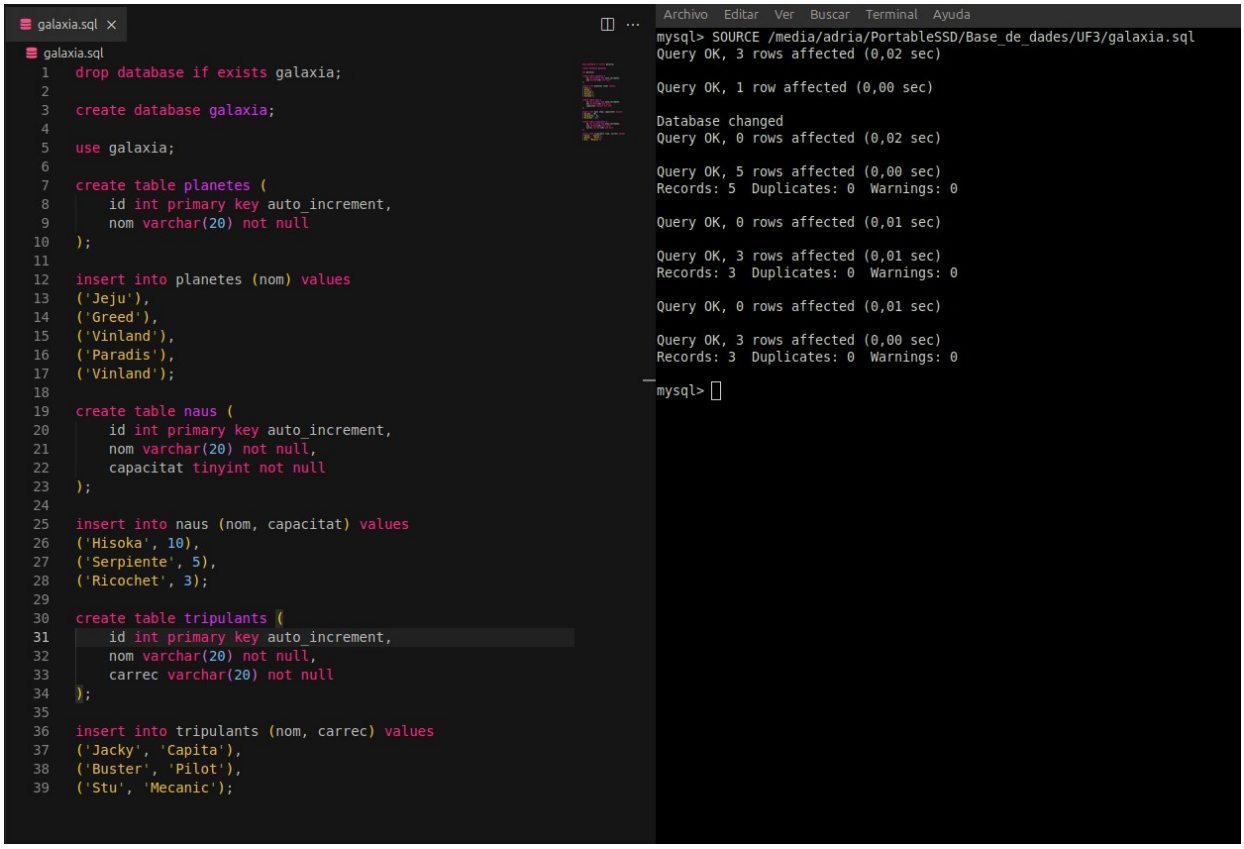
M02UF3-ASSEGURAMENT DE LA INFORMACIÓ



Índex

Practica resposta:

En aquesta activitat final, treballarem diferents aspectes del control i seguretat en un SGBD. L'activitat es distribueix entre 3 apartats: a) Usuaris, privilegis i rols. b) Catàleg de metadades. c) Seguretat i amenaces. Nota: S'ha de fer un mínim de cada apartat per a poder aprovar. Els apartats que no arribin a la nota mínima s'hauran de recuperar.
Rúbrica d'avaluació:
UF3_AA1 - Rúbrica
Abans de començar, necessites crear la base de dades galaxia amb les següents taules i alguns registres inserits:
PLANETES (id, nom)
NAUS(id, nom, capacitat)



TRIPULANTS (id, nom, càrrec)

1.1 Gestió d'usuaris locals

En un fitxer anomenat usuarislocal.sql, escriu les sentències SQL per a completar cadascun dels següents apartats, i fes una captura de pantalla executant cada consulta.

1. **Crea l'usuari alien@localhost amb permisos de només connexió a MySQL. Comprova que s'hagi creat l'usuari amb els seus permisos corresponents.**

He hagut d'afegir contrasenya degut a que tenia el seguent error.

```
mysql> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarislocal.sql
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
ERROR 1141 (42000): There is no such grant defined for user 'alien' on host 'localhost'
mysql>
```

Creacio de l'usuari alien.

```
-- 1
CREATE USER 'alien'@'localhost' IDENTIFIED BY 'Alumne.123';
SHOW GRANTS FOR 'alien'@'localhost';
```

```
mysql> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarislocal.sql
Query OK, 0 rows affected (0,00 sec)

+-----------------------------------------+
| Grants for alien@localhost              |
+-----------------------------------------+
| GRANT USAGE ON *.* TO `alien`@`localhost` |
+-----------------------------------------+
1 row in set (0,00 sec)

ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server versi
on for the right syntax to use near '' at line 1
mysql>
```

2. **Crea l'usuari clark@localhost identificat amb contrasenya i amb permisos de només connexió. Comprova que s'hagi creat l'usuari amb els seus permisos corresponents.**

Creacio usuari clark.

```
-- 2
CREATE USER 'clark'@'localhost' IDENTIFIED BY 'Alumne.123';
SHOW GRANTS FOR 'clark'@'localhost';
```

```
mysql> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarislocal.s
Query OK, 0 rows affected (0,00 sec)

+-----------------------------------------+
| Grants for clark@localhost              |
+-----------------------------------------+
| GRANT USAGE ON *.* TO `clark`@`localhost` |
+-----------------------------------------+
1 row in set (0,00 sec)
```

3. **Dona a clark permisos de SELECT sobre la taula tripulants. Comprova els permisos de clark i verifica que pot consultar la taula tripulants.**

D'aquesta manera clark tindra permisos de select a la taula tripulants.

```
-- 3
GRANT SELECT on galaxia.tripulants to 'clark'@'localhost';
SHOW GRANTS FOR 'clark'@'localhost';
SELECT * FROM galaxia.tripulants;
```

```
mysql> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarislocal.sql
Query OK, 0 rows affected (0,00 sec)

+-----------------------------------------------------------+
| Grants for clark@localhost                                |
+-----------------------------------------------------------+
| GRANT USAGE ON *.* TO `clark`@`localhost`                 |
| GRANT SELECT ON `galaxia`.`tripulants` TO `clark`@`localhost` |
+-----------------------------------------------------------+
2 rows in set (0,00 sec)

+----+--------+---------+
| id | nom    | carrec  |
+----+--------+---------+
|  1 | Jacky  | Capita  |
|  2 | Buster | Pilot   |
|  3 | Stu    | Mecanic |
+----+--------+---------+
3 rows in set (0,00 sec)
```

4. **Dona a alien permisos de SELECT, INSERT i UPDATE sobre totes les taules de la base de dades galaxia amb opció GRANT. Comprova els permisos de alien.**

Per donar permisos sobre totes les taules utilitzarem «*».

```
-- 4
GRANT SELECT, INSERT, UPDATE on galaxia.* to 'alien'@'localhost';
SHOW GRANTS FOR 'alien'@'localhost';
```

```
mysql> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarislocal.sql
Query OK, 0 rows affected (0,00 sec)

+-----------------------------------------------------------------+
| Grants for alien@localhost                                      |
+-----------------------------------------------------------------+
| GRANT USAGE ON *.* TO `alien`@`localhost`                       |
| GRANT SELECT, INSERT, UPDATE ON `galaxia`.* TO `alien`@`localhost` |
+-----------------------------------------------------------------+
2 rows in set (0,00 sec)
```

5. **Connecta't com a alien i concedeix a clark permisos de selecció sobre la taula naus. Comprova els permisos de clark.**

He iniciat sesi a alien, he executat el meu script, amb la part del root comentada, un cop he comprobat que alien ha pogut donar permisos de select des de el root he executat el script per comprobnar que s'habia modificat.

```
-- 5
GRANT SELECT ON galaxia.naus TO 'clark'@'localhost';
-- Al usuari root.
SHOW GRANTS FOR 'clark'@'localhost';
SELECT * FROM galaxia.naus;
```

```
adria@adria:~$ mysql -u alien -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 8.0.41-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2025, 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> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarislocal.sql
Query OK, 0 rows affected (0,00 sec)

mysql>
```

```
mysql> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarislocal.sql
+-----------------------------------------------------------+
| Grants for clark@localhost                                |
+-----------------------------------------------------------+
| GRANT USAGE ON *.* TO `clark`@`localhost`                 |
| GRANT SELECT ON `galaxia`.`naus` TO `clark`@`localhost`   |
| GRANT SELECT ON `galaxia`.`tripulants` TO `clark`@`localhost` |
+-----------------------------------------------------------+
3 rows in set (0,00 sec)

+----+-----------+-----------+
| id | nom       | capacitat |
+----+-----------+-----------+
|  1 | Hisoka    |        10 |
|  2 | Serpiente |         5 |
|  3 | Ricochet  |         3 |
+----+-----------+-----------+
3 rows in set (0,00 sec)

mysql>
```

1.2 Gestió d'usuaris remots

En un fitxer anomenat usuarisremot.sql, escriu les sentències SQL per a completar cadascun dels següents apartats, i fes una captura de pantalla executant cada consulta.

6. **Crea un usuari remot et@192.168.?.? amb permisos de INSERT sobre totes les taules de galaxia. Substitueix aquesta IP per una IP vàlida en el teu entorn i comprova els permisos de et des de root i fent un INSERT a tripulants des de la pròpia màquina client, connectat amb et.**

La IP que he afegit a l'usuari es la Ip de la meva maquina virtual, per per conectarme des de la maquina he hagut d'utilitzar la IP de la meva maquina real.

```
1   -- 1.2 Gestió d'usuaris remots
2
3   CREATE USER 'et'@'192.168.1.41' IDENTIFIED BY 'Alumne.123';
4   GRANT INSERT ON galaxia.* TO 'et'@'192.168.1.41';
5   SHOW GRANTS FOR 'et'@'192.168.1.41';
6
```

```
mysql> SOURCE /media/adria/PortableSSD/Base_de_dades/UF3/usuarisremot.sql
Query OK, 0 rows affected (0,01 sec)

Query OK, 0 rows affected (0,00 sec)

+--------------------------------------------------+
| Grants for et@192.168.1.41                       |
+--------------------------------------------------+
| GRANT USAGE ON *.* TO `et`@`192.168.1.41`        |
| GRANT INSERT ON `galaxia`.* TO `et`@`192.168.1.41` |
+--------------------------------------------------+
2 rows in set (0,00 sec)

mysql>
```

```
adria@adria-VirtualBox:~$ sudo mysql -h 192.168.1.36 -u et -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 8.0.41-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2025, 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> INSERT INTO galaxia.tripulants (nom, carrec) values ('Bull', 'Mecanic'
);
Query OK, 1 row affected (0,01 sec)

mysql>
```

Per demostrar que realment estic conectat a l'usuari que he creat he executat una comanda que no puc fer per que puguis veure el missatge d'error.

```
adria@adria-VirtualBox:~$ sudo mysql -h 192.168.1.36 -u et -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 8.0.41-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2025, 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> INSERT INTO galaxia.tripulants (nom, carrec) values ('Bull', 'Mecanic'
);
Query OK, 1 row affected (0,01 sec)

mysql> SELECT user, host FROM mysql.user;
ERROR 1142 (42000): SELECT command denied to user 'et'@'192.168.1.41' for tab
le 'user'
mysql>
```

7. **Dona a et permisos de SELECT sobre els camps nom i càrrec de la taula tripulants. Comprova els permisos de et i connectat amb ell per realitzar un SELECT sobre nom i càrrec de tripulants.**

S'ha de documentar:

- **Instrucció SQL**
- **Captura de pantalla amb l'execució de la instrucció SQL.**
- **Captura de pantalla amb la comprovació (si no es demana una comprovació específica, només cal comprovar-ho amb el SHOW GRANTS des de root)**

1.3 Creació i gestió de rols

En un fitxer anomenat gestiorols.sql, escriu les sentències SQL per a completar cadascun dels següents apartats, i fes una captura de pantalla executant cada consulta.

8. **Crea el rol xenomorf amb tots els privilegis sobre les taules planetes i tripulants i el rol metahuma amb tots els privilegis sobre la taula naus. Comprova que els rols creats apareixen a la taula mysql.user i comprova els privilegis que hi ha assignats a cada rol amb la comanda SHOW GRANTS.**
9. **Assigna el rol metahuma com a predeterminat a l'usuari clark. Comprova el seu rol actual amb SELECT CURRENT_ROLE();**
10. **Afegeix el rol xenomorf a l'usuari clark. Connectat amb clark i activa el nou rol a la sessió actual i comprova que pot accedir a les taules planetes i tripulants, i el nou rol actual amb SELECT CURRENT_ROLE();**

S'ha de documentar:

- **Instrucció SQL**
- **Captura de pantalla amb l'execució de la instrucció SQL.**
- **Captura de pantalla amb la comprovació (si no es demana una comprovació específica, només cal comprovar-ho amb el SHOW GRANTS des de root)**

2. Consulta al catàleg de metadades

En un fitxer anomenat metadades.sql, escriu les sentències SQL per a completar cadascun dels següents apartats, i fes una captura de pantalla executant cada consulta.

11. **Amb les taules mysql.user i mysql.tables_priv crea una consulta per a que et retorni els privilegis dels usuaris sobre les taules de la BD galaxia que tens dins SGBD.**
12. **Consulta a information_schema el nombre de files que té cada taula de la base de dades galaxia.**
13. **Consulta a information_schema les columnes de la taula tripulants de la base de dades galaxia.**

S'ha de documentar:

- **Instrucció SQL**
- **Captura de pantalla amb l'execució de la instrucció SQL.**

3.1 Seguretat:

Imagina que estàs auditant una empresa que mostra una llista d'informació a través d'un desplegable amb les opcions "nom", "premis" i "biografia".

Sembla que la base de dades no està normalitzada (no s'ha seguit un disseny basat en relacions 1:1, 1:N, etc.), i sembla que el desplegable correspon directament a una columna de la taula cantants.

Sospites que l'aplicació construeix la consulta SQL de manera dinàmica, sense cap validació i generant una crida com la següent:

SELECT {opcio_desplegable} FROM cantants WHERE id=1;

Aquest enfocament podria permetre una injecció SQL si un atacant manipula el valor de {opcio_desplegable}.

En el mateix fitxer anomenat UF3_AA1_[Cognom1Cognom2Nom]_DCL.pdf, respon amb les teves paraules les següents preguntes.

15. **Per què en aquest cas no podem aplicar la tècnica dels Prepared Statements per protegir-nos davant aquesta vulnerabilitat?**
16. **Quines quatre capes de seguretat proposaries per a que l'empresa millori la protecció d'aquesta aplicació?**

S'ha de documentar:

- **Punts 15,16:**
  - **Resposta escrita a cada pregunta.**

3.1 Amenaces:

Executa el fitxer lock_discografia i vulnera la base de dades generada. Aquest fitxer ha creat una base de dades amb taules i informació no securitzada. En algun lloc hi ha un camp "root" o "admin" amb una contrasenya guardada; aquesta contrasenya és la nova del teu propi sistema gestor. Executa un atac SQLi a través del fitxer discografia.

- **lock_discografia: Bloqueja el SGBD i prepara l'exercici.**
- **discografia: Formulari vulnerable a SQLi.**
- **unlock_discografia: Desbloqueja el SGBD deixant-lo amb les 4 BD inicials (mysql, information_schema, etc.).**

En un fitxer anomenat amenaces.sql, escriu les instruccions SQL utilitzades per aconseguir cadascun dels 4 punts següents.

17. **Troba la base de dades existent.**
18. **Troba el nom de la taula que guarda informació sensible sobre els usuaris.**
19. **Troba el nom de les columnes on es guarda informació sensible sobre els usuaris.**
20. **Troba la contrasenya de l'usuari amb més poder ('admin' o 'root').**

Aquest apartat no fa falta documentar-se.

Entrega un fitxer .zip anomenat "UF3_AA1_[Cognom1Cognom2Nom]_DCL.zip" amb:

- **UF3_AA1_[Cognom1Cognom2Nom]_DCL.pdf: Document pdf amb captures de pantalla demanades en cada apartat.**
- **usuarislocal.sql: Fitxer .sql que inclou les instruccions de l'apartat 1.1.**
- **usuarisremot.sql: Fitxer .sql que inclou les instruccions de l'apartat 1.2.**
- **gestiorols.sql: Fitxer .sql que inclou les instruccions de l'apartat 1.3.**

- **<u>metadades.sql:</u> Fitxer .sql que inclou les instruccions de l'apartat 2.**
- **<u>amenaces.sql:</u> Fitxer .sql que inclou les instruccions de l'apartat 3.2.**

<u>Exemple:</u> UF3_AA1_GarciaReverterEric_DCL.zip

|
|--> UF3_AA1_GarciaReverterEric_DCL.pdf
|--> usuarislocal.sql
|--> usuarisremot.sql
|--> gestiorols.sql
|--> metadades.sql
|--> amenaces.sql

Web grafía