

Proiect – Securitatea bazelor de date

1. Introducere	2
Prezentarea modelului proiectat și a regulilor sale.....	2
Diagrama conceptuală	2
Schemele relaționale	3
Crearea tabelelor	3
Prezentarea regulilor de securitate care vor fi aplicate asupra modelului	3
2. Criptarea datelor.....	4
3. Auditarea activităților asupra bazelor de date	5
A) Auditare standard	5
B) Triggeri de auditare.....	6
C) Politici de auditare	7
4. Gestiunea utilizatorilor unei baze de date și a resurselor computaționale	8
A) Proiectarea configurației de management a identităților în baza de date (matricile proces-utilizator, entitate-proces, entitate-utilizator)	8
B) Implementarea configurației de management a identităților în baza de date.....	10
5. Privilegii și roluri	11
6. Aplicațiile pe baza de date și securitatea datelor	13
A) Contextul aplicației	13
B) SQL Injection.....	15
7. Mascarea datelor	17

1. Introducere

Prezentarea modelului proiectat și a regulilor sale

Proiectul reprezintă crearea unei baze de date pentru un lanț de farmacii la care se pot efectua comenzi online.

Structura bazei de date se găsește în diagrama următoare:

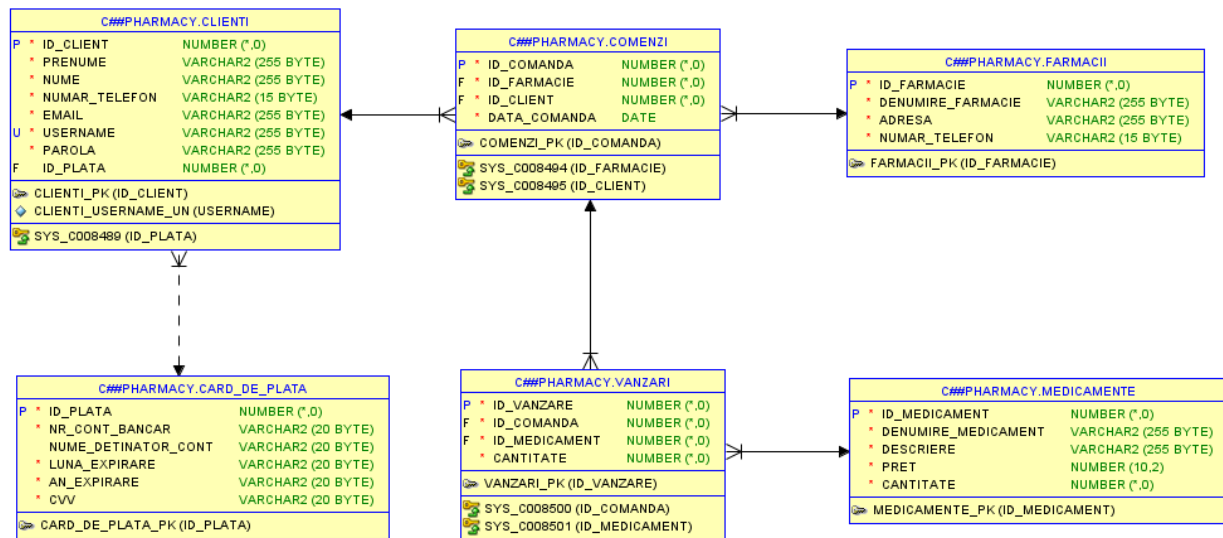
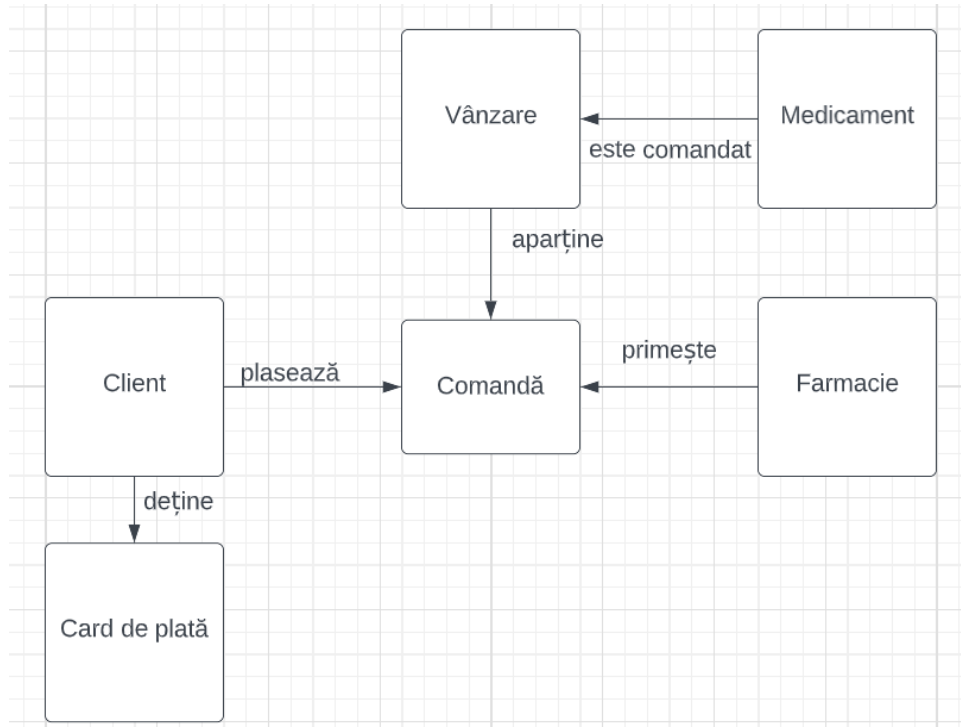


Diagrama conceptuală



Schemele relaționale

CARD_DE_PLATA (id_plata#, nr_cont_bancar, nume_detinator_cont, luna_expirare, an_expirare, CVV)

CLIENTI (id_client#, prenume, nume, numar_telefon, email, username, parola, id_plata)

COMENZI (id_comanda#, id_farmacie, id_client, data_comanda)

FARMACII (id_farmacie#, denumire_farmacie, id_client, data_comanda)

MEDICAMENTE (id_medicament#, denumire_medicament, descriere, pret, cantitate)

VANZARI (id_vanzare#, id_comanda, id_medicament, cantitate)

Crearea tabelelor

Script-urile care conțin comenzile de creare și inserare în tabel sunt atașate separat.

Prezentarea regulilor de securitate care vor fi aplicate asupra modelului

Parolele clienților vor fi procesate cu ajutorul funcției hash din pachetul dbms_crypto.

Clienții vor trebui să salveze datele unui card de plată pentru a putea să își creeze un cont. Aceste date sensibile vor fi criptate.

Anumite comenzi date de utilizatori vor fi auditate.

Utilizatorii nu vor avea drepturi nelimitate asupra obiectelor din baza de date. De asemenea, cu excepția utilizatorului admin, aceștia nu vor avea spațiu nelimitat.

2. Criptarea datelor

- Înainte de fiecare inserare în tabelul “Clienți” se va declanșa trigger-ul “hash_parole” definit astfel:

```
CREATE OR REPLACE TRIGGER hash_parole
BEFORE INSERT ON clienti
FOR EACH ROW
BEGIN
    :new.parola:=dbms_crypto.hash(utl_i18n.string_to_raw(:new.parola), dbms_crypto.HASH_SH1);
END;
/
```

- Pentru a cripta datele sensibile despre cardurile cu care clienții vor efectua plata, se va folosi procedura auxiliară “criptare”, definită astfel:

```
create or replace procedure criptare(text in varchar2, text_criptat out varchar2) as
    raw_text raw(100);
    raw_cheie raw(100);
    cheie varchar2(8) := '12345678';
    mod_operare pls_integer;
begin
    raw_text := utl_i18n.string_to_raw(text, 'AL32UTF8');
    raw_cheie := utl_i18n.string_to_raw(cheie, 'AL32UTF8');

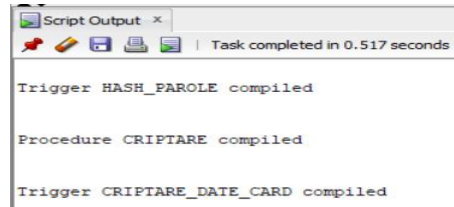
    mod_operare := dbms_crypto.encrypt_des + dbms_crypto.pad_zero + dbms_crypto.chain_ecb;
    text_criptat := dbms_crypto.encrypt(raw_text, mod_operare, raw_cheie);
end;
/
```

Această procedură va fi aplicată valorilor corespunzătoare câmpurilor “nr_cont_bancar”, “luna_expirare”, “an_expirare” și “CVV” din tabelul “card_de_plată” înainte de inserarea lor, folosind trigger-ul “criptare_date_card”.

```
CREATE OR REPLACE TRIGGER criptare_date_card
BEFORE INSERT ON card_de_plata
FOR EACH ROW
declare
    nr_cont_bancar_criptat varchar2(200);
    luna_expirare_criptat varchar2(200);
    an_expirare_criptat varchar2(200);
    CVV_criptat varchar2(200);
BEGIN
    criptare(:new.nr_cont_bancar, nr_cont_bancar_criptat);
    criptare(:new.luna_expirare, luna_expirare_criptat);
    criptare(:new.an_expirare, an_expirare_criptat);
    criptare(:new.CVV, CVV_criptat);

    :new.nr_cont_bancar := nr_cont_bancar_criptat;
    :new.luna_expirare := luna_expirare_criptat;
    :new.an_expirare := an_expirare_criptat;
    :new.CVV := CVV_criptat;
END;
/
```

Cele 3 script-uri sunt aplicate cu succes.



Tabelul "Clienti":

ID_CLIENT	PRENUME	NUME	NUMAR_TELEFON	EMAIL	USERNAME	PAROLA	ID_PLAT
1	John	Doe	555-555-5555	john.doe@example.com	johndoe	1D96E4206BEA782AC246C56F5A96FF8A1C6A06CF	
2	Jane	Smith	555-555-5556	jane.smith@example.com	janesmith	484C825FD6AF44672CFC62A3E8B91A7ABDD44B5C	
3	Bob	Johnson	555-555-5557	bob.johnson@example.com	bobjohnson	B8C3FA2A4530920CBFB8ED59288ED07B6EDA70D4	
4	Amy	Williams	555-555-5558	amy.williams@example.com	amywilliams	F583DF6D795629648EE69F8AE24224E33AF7E64	
5	Michael	Jones	555-555-5559	michael.jones@example.com	michaeljones	328F36F928D6F35121DFB42C6A7C8A347B30882	

Tabelul "Card de plata":

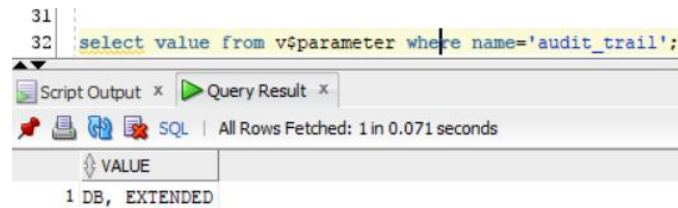
ID_PLATA	NR_CONT_BANCAR	NUME_DETINATOR_CONT	LUNA_EXPIRARE	AN_EXPIRARE	CVV
1	1 09A5451ACECA5F8A	John Doe	1E552C75E644F442	3E8C87D32E899022	C91D449B8AB46AF
2	2 6210D9321BC91C4C	Jane Smith	11FE1D8FEEA13428	56BDC0DF4AB7C240	C91D449B8AB46AF
3	3 D2F82FBEA0261BBC	Luna Johnson	FE3EC63267DE1F28	CC6671ADF4C4FD17	C91D449B8AB46AF
4	4 A23FB5B86D036DBE	Amy Williams	311DCA128CC14035	3E8C87D32E899022	C91D449B8AB46AF
5	5 A23FB5B86D036DBE	Michael Jones	3CEAE8C6AC8712E5	DF49754BAC6FF5DA	C91D449B8AB46AF

3. Auditarea activităților asupra bazelor de date

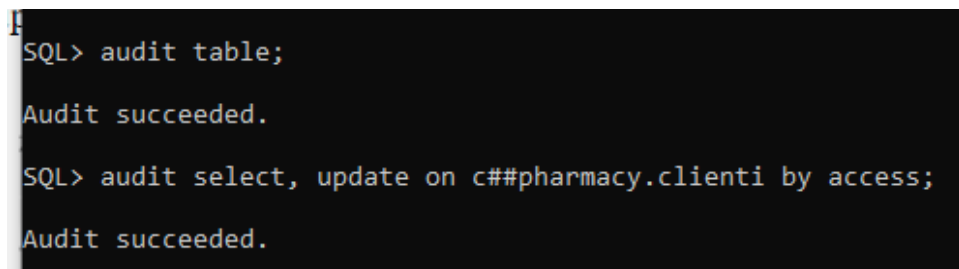
A) Auditare standard

Auditarea se realizează asupra bazei de date pentru ștergerea sau inserarea în tabelul "Clienti".

SYS as SYSDBA: Valoarea parametrului audit_trail a fost schimbată la "DB, Extended" folosind comanda "alter system set audit_trail=db,extended scope=spfile;" și restartând baza de date ("shutdown immediate" și "startup").



SYS as SYSDBA: se execută următoarele comenzi:



User C##PHARMACY:

```
select * from clienti;  
update clienti set nume = 'Popescu' where id_client = 1;
```

SYS as SYSDBA:

```
SQL> select * from (select os_username, username, owner, timestamp, action, sql_text from dba_audit_trail where lower(owner) = 'c##pharmacy' order by timestamp desc) where rownum <= 5;
```

OS_USERNAME	USERNAME	OWNER	TIMESTAMP	ACTION	SQL_TEXT
oana_	C##PHARMACY	C##PHARMAC	24-JAN-23	6	update clienti set nume = 'Popescu' where id_client = 1
		Y		t = 1	
oana_	C##PHARMACY	C##PHARMAC	24-JAN-23	3	select * from clienti
		Y			

Se oprește auditarea:

```
SQL> noaudit table;  
Noaudit succeeded.  
  
SQL> noaudit select table;  
Noaudit succeeded.
```

B) Triggeri de auditare

Crearea unui trigger pentru a reține toate ștergerile care au loc pe tabelul “Vânzări”. Datele vor fi reținute în tabelul “tabel_audit_vanzari”

SYS as SYSDBA: creare tabel audit, secvență și triggeri

```
create table tabel_audit_vanzari(  
    id_secv number(4) primary key,  
    user_ varchar2(20),  
    session_ number(10),  
    host_ varchar2(100),  
    data_stergere date,  
    nr_randuri_sterse number(5)  
);  
create sequence secv_audit_vanzari;  
  
create or replace trigger trigger_audit_before_stergere_vanzari  
before delete on c##pharmacy.vanzari  
declare  
    nr_randuri number;  
begin  
    select count(*) into nr_randuri from c##pharmacy.vanzari;  
  
    insert into tabel_audit_vanzari  
    values(secv_audit_vanzari.nextval, sys_context('userenv', 'session_user'),  
          sys_context('userenv', 'sessionid'), sys_context('userenv', 'host'), sysdate, nr_randuri);  
end;  
/  
  
create or replace trigger trigger_audit_after_stergere_vanzari  
after delete on c##pharmacy.vanzari  
declare  
    nr_randuri_after number;
```

```
nr_randuri_before number;  
current_session varchar2(100);  
id_rec_audit number;  
begin  
    select count(*) into nr_randuri_after from c##pharmacy.vanzari;  
    select sys_context('userenv', 'sessionid') into current_session from dual;  
  
    select max(id_secv) into id_rec_audit from tabel_audit_vanzari where session_ = current_session;  
  
    select nr_randuri_sterse into nr_randuri_before  
    from tabel_audit_vanzari  
    where id_secv = id_rec_audit;  
  
    update tabel_audit_vanzari  
    set nr_randuri_sterse = nr_randuri_before - nr_randuri_after  
    where id_secv = id_rec_audit;  
end;  
/
```

Conectare ca c##pharmacy:

```
-- 30 de înregistrări în tabelul vanzari (id_vanzare apartine [1, 30])  
delete from vanzari where id_vanzare = 10;  
delete from vanzari where id_vanzare > 37;  
delete from vanzari where id_comanda < 2;  
delete from vanzari where id_vanzare > 20;  
commit;
```

SYS as SYSDBA:

```
select * from tabel_audit_vanzari;
```

ID_SECV	USER_	SESSION_	HOST_	DATA_STERGERE	NR_RANDURI_STERSE
1	1 C##PHARMACY	120115	DESKTOP-L33FRNV	24-JAN-23	1
2	2 C##PHARMACY	120115	DESKTOP-L33FRNV	24-JAN-23	0
3	3 C##PHARMACY	120115	DESKTOP-L33FRNV	24-JAN-23	9
4	4 C##PHARMACY	120115	DESKTOP-L33FRNV	24-JAN-23	7

C) Politici de auditare

Politică de auditare care să înregistreze încercările de modificare a parolei unui client.

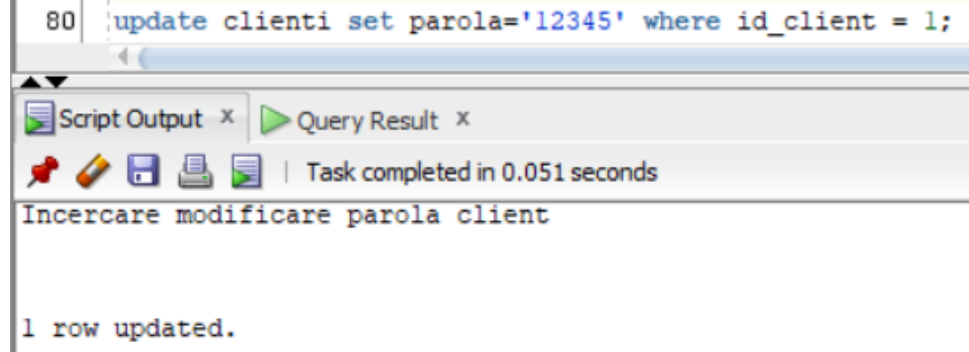
SYS as SYSDBA:

```
create or replace procedure alerta_modif_parole (object_schema varchar2, object_name varchar2,  
policy_name varchar2)  
as  
begin  
    dbms_output.put_line('Incercare modificare parola client');  
end;  
/  
  
create or replace procedure procedura_audit_parole as  
begin  
    dbms_fga.add_policy(  
        object_schema => 'C##PHARMACY',  
        object_name => 'CLIENTI',  
        policy_name => 'policy_modif_parole',  
        enable => true,  
        statement_types => 'UPDATE',  
        handler_module => 'ALERTA_MODIF_PAROLE');  
end;  
/
```

```
execute procedura_audit_parole;
```

Conectare ca c##pharmacy:

```
update clienti set parola='12345' where id_client = 1;
```



SYS as SYSDBA:

```
select db_user, userhost, policy_name, to_char(timestamp, 'dd/mm/yyyy hh24:mi:ss') Time, sql_text  
from dba_fga_audit_trail  
order by timestamp desc;
```

Rezultat:

The screenshot shows the result of the query in the 'Query Result' tab. The table has 5 columns: DB_USER, USERHOST, POLICY_NAME, TIME, and SQL_TEXT. There is one row of data.

DB_USER	USERHOST	POLICY_NAME	TIME	SQL_TEXT
C##PHARMACY	DESKTOP-L33FRNV	POLICY_MODIF_PAROLE	24/01/2023 17:20:39	update clienti set parola='12345' where id_client = 1

4. Gestiunea utilizatorilor unei baze de date și a resurselor computaționale

A) Proiectarea configurației de management a identităților în baza de date (matricile proces-utilizator, entitate-proces, entitate-utilizator)

Utilizatori:

- Clienți
- Angajați
- Admin

Procese:

- P1: Creare cont client.
- P2: Afișare conturi client.
- P3: Actualizare informații client.
- P4: Ștergere cont client.
- P5: Adăugare card de plată.
- P6: Vizualizare card de plată.
- P7: Actualizare informații card de plată.
- P8: Adăugare medicament.
- P9: Actualizare informații medicament.
- P10: Ștergere medicament.

- P11: Vizualizare informații medicament.
- P12: Adăugare comandă.
- P13: Afișare comandă.
- P14: Ștergere comandă.
- P15: Adăugare farmacie.
- P16: Actualizare informații farmacie.
- P17: Vizualizare informații farmacie.
- P18: Ștergere farmacie.

Matricea Proces – Utilizator:

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18
Client	x		x								x	x					x	
Angajat		x						x	x	x	x		x	x			x	
Admin		x		x				x	x	x	x		x	x	x	x	x	x

Matricea Entitate – Proces

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18
Card de plata	I	S	I, U		I	S	U											
Clienți	I	S	U	D									S					
Medicamente								I, U	U	D	S		S					
Vânzări												I, U	S	D				
Comenzi												I, U	S	D				
Farmacii															I	U	S	D

Matricea Entitate – Utilizator:

	Clienți	Angajați	Admin
Card de plata	I, S, U	S	S
Clienți	I, U	S	S, D

Medicamente	S	I, S, U, D	I, S, U, D
Vânzări	I	S	S
Comenzi	I	S	S, D
Farmacii	S	S	I, S, U, D

B) Implementarea configurației de management a identităților în baza de date

- Crearea utilizatorilor:

```

13 -- Creare utilizator Administrator
14 create user c##admin identified by "admin";
15
16 -- Creare utilizatori - clienti
17 create user c##client1 identified by "client";
18 create user c##client2 identified by "client";
19 create user c##client3 identified by "client";
20 create user c##client4 identified by "client";
21
22 -- Creare utilizatori - angajati
23 create user c##angajat1 identified by "angajat";
24 create user c##angajat2 identified by "angajat";
25 create user c##angajat3 identified by "angajat";
26
27 select * from all_users;

```

USERID	USERNAME	USERID	CREATED	COMMON	ORACLE_MAINTAINED	INHERITED	DEFAULT_COLLATION	IMPLICIT	ALL_SHARD
42	C##CLIENT1	113	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO
43	C##ADMIN	112	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO
44	C##CLIENT2	114	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO
45	C##CLIENT3	115	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO
46	C##CLIENT4	116	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO
47	C##ANGAJAT1	117	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO
48	C##ANGAJAT2	118	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO
49	C##ANGAJAT3	119	24-JAN-23	YES	N	NO	USING_NLS_COMP	NO	NO

- Asignare spațiu:

```

39 -- GRANT QUOTA: nelimitat pentru admin, 100 pentru angajati, 50 pentru clienti
40 alter user c##admin quota unlimited on USERS;
41 alter user c##client1 quota 50M on USERS;
42 alter user c##client2 quota 50M on USERS;
43 alter user c##client3 quota 50M on USERS;
44 alter user c##client4 quota 50M on USERS;
45 alter user c##angajat1 quota 100M on USERS;
46 alter user c##angajat2 quota 100M on USERS;
47 alter user c##angajat3 quota 100M on USERS;
48
49 select *
50 from DBA_TS_QUOTAS
51 where ((username like 'C##CLIENT%' or username like 'C##ANGAJAT%') or username = 'C##ADMIN')
52 order by username;
53

```

TABLESPACE_NAME	USERNAME	BYTES	MAX_BYTES	BLOCKS	MAX_BLOCKS	DROPPED
1 USERS	C##ADMIN	0	-1	0	-1	NO
2 USERS	C##ANGAJAT1	0	104857600	0	12800	NO
3 USERS	C##ANGAJAT2	0	104857600	0	12800	NO
4 USERS	C##ANGAJAT3	0	104857600	0	12800	NO
5 USERS	C##CLIENT1	0	52428800	0	6400	NO
6 USERS	C##CLIENT2	0	52428800	0	6400	NO
7 USERS	C##CLIENT3	0	52428800	0	6400	NO
8 USERS	C##CLIENT4	0	52428800	0	6400	NO

5. Privilegii și roluri

- Creare și asignare roluri:

```
19 -- Creare roluri
20 CREATE ROLE C##administrator;
21 CREATE ROLE C##client;
22 CREATE ROLE C##angajat;
23
24 -- Asignare roluri utilizatorilor
25 GRANT C##administrator to c##admin;
26 GRANT C##client to c##client1;
27 GRANT C##client to c##client2;
28 GRANT C##client to c##client3;
29 GRANT C##client to c##client4;
30 GRANT C##angajat to c##angajat1;
31 GRANT C##angajat to c##angajat2;
32 GRANT C##angajat to c##angajat3;
33
34 select *
35 from dba_role_privs
36 where ((grantee like 'C##CLIENT%' or grantee like 'C##ANGAJAT%') or grantee = 'C##ADMIN')
37 order by grantee;
```

Script Output x Query Result x

All Rows Fetched: 10 in 0.157 seconds

GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	COMMON	INHERITED
1 C##ADMIN	C##ADMINISTRATOR	NO	NO	YES	NO	NO
2 C##ANGAJAT	RESOURCE	NO	NO	YES	NO	NO
3 C##ANGAJAT1	C##ANGAJAT	NO	NO	YES	NO	NO
4 C##ANGAJAT2	C##ANGAJAT	NO	NO	YES	NO	NO
5 C##ANGAJAT3	C##ANGAJAT	NO	NO	YES	NO	NO
6 C##CLIENT	RESOURCE	NO	NO	YES	NO	NO
7 C##CLIENT1	C##CLIENT	NO	NO	YES	NO	NO
8 C##CLIENT2	C##CLIENT	NO	NO	YES	NO	NO
9 C##CLIENT3	C##CLIENT	NO	NO	YES	NO	NO
10 C##CLIENT4	C##CLIENT	NO	NO	YES	NO	NO

- Asignare permisiuni inserare/selectare/actualizare/ștergere în tabele în funcție de rol.

```
-- Permisuni pentru tabelul "Card de plata"
GRANT SELECT ON c##pharmacy.card_de_plata TO c##admin;
GRANT SELECT, INSERT, UPDATE ON c##pharmacy.card_de_plata TO C##client;
GRANT SELECT ON c##pharmacy.card_de_plata TO C##angajat;

-- Permisuni pentru tabelul "Clienti"
GRANT SELECT, DELETE ON c##pharmacy.clienti TO c##admin;
GRANT INSERT, UPDATE ON c##pharmacy.clienti TO C##client;
GRANT SELECT, UPDATE, DELETE ON c##pharmacy.clienti TO C##angajat;

-- Permisuni pentru tabelul "Medicamente"
GRANT SELECT, INSERT, UPDATE, DELETE ON c##pharmacy.medicamente TO c##admin;
GRANT SELECT ON c##pharmacy.medicamente TO C##client;
GRANT SELECT, INSERT, UPDATE, DELETE ON c##pharmacy.medicamente TO C##angajat;

-- Permisuni pentru tabelul "Vanzari"
GRANT SELECT ON c##pharmacy.vanzari TO c##admin;
GRANT SELECT ON c##pharmacy.vanzari TO C##client;
GRANT INSERT ON c##pharmacy.vanzari TO C##angajat;

-- Permisuni pentru tabelul "Comenzi"
GRANT SELECT, DELETE ON c##pharmacy.comenzi TO c##admin;
GRANT INSERT ON c##pharmacy.comenzi TO C##client;
GRANT SELECT ON c##pharmacy.comenzi TO C##angajat;
```

```
-- Permisuni pentru tabelul "Farmacii"
GRANT SELECT, INSERT, UPDATE, DELETE ON c##pharmacy.farmacii TO c##admin;
GRANT SELECT ON c##pharmacy.farmacii TO C##client;
GRANT SELECT ON c##pharmacy.farmacii TO C##angajat;

grant ALL ON dbms_crypto TO c##admin;
GRANT EXECUTE ON dbms_crypto TO C##client;
GRANT EXECUTE ON dbms_crypto TO C##angajat;

GRANT EXECUTE ON dbms_fga TO c##admin;
GRANT EXECUTE ON dbms_fga TO C##client;
GRANT EXECUTE ON dbms_fga TO C##angajat;
```

```
101 SELECT grantee, table_name, privilege
102 FROM dba_tab_privs
103 where ((grantee like 'C##CLIENT%' or grantee like 'C##ANGAJAT%') or grantee = 'C##ADMIN')
104 order by grantee;
```

Script Output x Query Result x
SQL | All Rows Fetched: 41 in 1.162 seconds

	GRANTEE	TABLE_NAME	PRIVILEGE
1	C##ADMIN	DBMS_CRYPTO	EXECUTE
2	C##ADMIN	DBMS_FGA	EXECUTE
3	C##ADMIN	MEDICAMENTE	UPDATE
4	C##ADMIN	FARMACII	UPDATE
5	C##ADMIN	VANZARI	SELECT
6	C##ADMIN	COMENZI	SELECT
7	C##ADMIN	CLIENTI	SELECT
8	C##ADMIN	CARD_DE_PLATA	SELECT
9	C##ADMIN	MEDICAMENTE	SELECT
10	C##ADMIN	FARMACII	SELECT
11	C##ADMIN	MEDICAMENTE	INSERT
12	C##ADMIN	FARMACII	INSERT
13	C##ADMIN	COMENZI	DELETE
14	C##ADMIN	CLIENTI	DELETE
15	C##ADMIN	MEDICAMENTE	DELETE
16	C##ADMIN	FARMACII	DELETE
17	C##ADMIN	DBMS_CRYPTO	DEBUG
18	C##ANGAJAT	MEDICAMENTE	INSERT
19	C##ANGAJAT	DBMS_CRYPTO	EXECUTE
20	C##ANGAJAT	DBMS_FGA	EXECUTE

21	C##ANGAJAT	MEDICAMENTE	DELETE
22	C##ANGAJAT	CLIENTI	DELETE
23	C##ANGAJAT	FARMACII	SELECT
24	C##ANGAJAT	MEDICAMENTE	SELECT
25	C##ANGAJAT	MEDICAMENTE	UPDATE
26	C##ANGAJAT	COMENZI	SELECT
27	C##ANGAJAT	CLIENTI	SELECT
28	C##ANGAJAT	CARD_DE_PLATA	SELECT
29	C##ANGAJAT	CLIENTI	UPDATE
30	C##ANGAJAT	VANZARI	INSERT
31	C##CLIENT	FARMACII	SELECT
32	C##CLIENT	CARD_DE_PLATA	INSERT
33	C##CLIENT	CLIENTI	INSERT
34	C##CLIENT	MEDICAMENTE	SELECT
35	C##CLIENT	CLIENTI	UPDATE
36	C##CLIENT	COMENZI	INSERT
37	C##CLIENT	VANZARI	SELECT
38	C##CLIENT	DBMS_CRYPTO	EXECUTE
39	C##CLIENT	DBMS_FGA	EXECUTE
40	C##CLIENT	CARD_DE_PLATA	UPDATE
41	C##CLIENT	CARD_DE_PLATA	SELECT

6. Aplicațiile pe baza de date și securitatea datelor

A) Contextul aplicației

Programul angajaților farmaciilor este între orele 9:00 - 18:00 de luni până vineri, prin urmare nu se pot face operațiuni specifice doar angajaților în afara programului (exemplu: introducerea de noi medicamente). Pentru asta se va salva în contextul aplicației atributul "farmacii_deschise" care va fi calculat la momentul logării utilizatorilor și poate avea valorile "true" sau "false".

Conectat ca SYS as DBA:

```
set serveroutput on;

-- creare context aplicatie
create context aplicatie_farmacie_ctx using proced_aplicatie_farmacie_ctx;

-- definire procedura
create or replace procedure proced_aplicatie_farmacie_ctx is
    ora_curenta number(3);
    ziua_saptamanii number(10);
begin
    select to_number(to_char(sysdate, 'hh24')) into ora_curenta from dual;
    select to_number(to_char(sysdate, 'd')) into ziua_saptamanii from dual;

    dbms_output.put_line(to_char(sysdate, 'day dd-mm-yyyy hh24:mi'));

    if ziua_saptamanii in (7, 1) then
        dbms_output.put_line('In week-end angajatii farmaciei nu lucreaza.');
```

```
        dbms_session.set_context('aplicatie_farmacie_ctx', 'farmacii_dechise', 'false');
    else
        if (ora_curenta < 9 and ora_curenta > 18) then
            dbms_output.put_line('Angajatii farmaciei lucreaza doar in intervalul 9 - 18.');
```

```
            dbms_session.set_context('aplicatie_farmacie_ctx', 'farmacii_dechise', 'false');
        else
```

```
        dbms_session.set_context('aplicatie_farmacie_ctx', 'farmacii_dechise', 'true');
    end if;
end if;

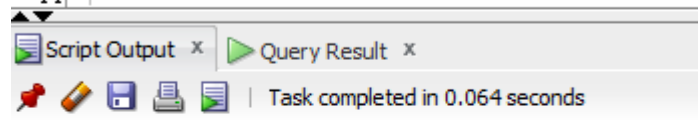
end;
/

-- Testare
exec proced_aplicatie_farmacie_ctx();

-- creare trigger de logon

create or replace trigger trigger_logon
after logon on database
begin
    proced_aplicatie_farmacie_ctx();
end;
/
```

```
41
42 -- Testare
43 exec proced_aplicatie_farmacie_ctx();
44
```



Procedure PROCED_APLICATIE_FARMACIE_CTX compiled

sunday 29-01-2023 19:21
In week-end angajatii farmaciei nu lucreaza.
fals

PL/SQL procedure successfully completed.

Conectat ca c##admin

```
create or replace trigger inainte_modificare_medicamente
before insert or update or delete on c##pharmacy.medicamente
for each row
declare
    v_farmacii_deschise varchar(5);
begin
    v_farmacii_deschise := sys_context('aplicatie_farmacie_ctx', 'farmacii_dechise');

    if (v_farmacii_deschise = 'nu') then
        RAISE_APPLICATION_ERROR(-20001, 'In acest moment nu sunt permise modificari asupra medicamentelor.');
```

Conectat ca c##angajat1

```
set SERVEROUTPUT on;
INSERT INTO c##pharmacy.medicamente (id_medicament, denumire_medicament, descriere, pret, cantitate)
```

```
VALUES (121, 'Claritromicina', 'antibiotic din clasa macrolidelor utilizat pentru a trata infectii ale tractului respirator superior, infectii ale pielii si alte infectii bacteriene', 25.99, 10);
```

```
74
75 -- Conectat ca c##angajat1
76
77
78 set SERVEROUTPUT on;
79 INSERT INTO c##pharmacy.medicamente (id_medicament, denumire_medicament, descriere, pret, cantitate)
80 VALUES (119, 'Claritromicina', 'antibiotic din clasa macrolidelor utilizat pentru a trata infectii ale tractului respirator superior, infectii ale pielii si alte infectii bacteriene', 25.99, 10);
```

Script Output x Query Result x

Task completed in 0.07 seconds

Error starting at line : 79 in command -
INSERT INTO c##pharmacy.medicamente (id_medicament, denumire_medicament, descriere, pret, cantitate)
VALUES (119, 'Claritromicina', 'antibiotic din clasa macrolidelor utilizat pentru a trata infectii ale tractului respirator superior, infectii ale pielii si alte infectii bacteriene', 25.99, 10)
Error report -
ORA-20001: in acest moment nu sunt permise modificari asupra medicamentelor.
ORA-06512: at "C##ADMIN.INAINTE_MODIFICARE_MEDICAMENTE", line 11
ORA-04088: error during execution of trigger 'C##ADMIN.INAINTE_MODIFICARE_MEDICAMENTE'

B) SQL Injection

Cerință: crearea unei proceduri care să afișeze denumirea farmaciilor unde au fost plasate comenzi într-o anumită zi.

Procedura nesigură:

```
-- procedura care afiseaza numele farmaciilor de unde s-au comandat medicamente intr-o anumita zi

-- conectat ca admin
-- procedura nesigura:
create or replace procedure lista_farmacii_comenzi(p_data_comanda varchar2) as
    type vector is table of c##pharmacy.comenzi%rowtype;
    v_lista_id_farmacii vector;
    v_farmacie c##pharmacy.farmacii%rowtype;
    v_id number(38);
begin
    execute immediate 'SELECT * FROM c##pharmacy.comenzi WHERE TO_CHAR(data_comanda, 'DD-MM-YYYY
HH24:MI:SS') LIKE '%' || p_data_comanda || '%' '
        bulk collect into v_lista_id_farmacii;

    for i in 1..v_lista_id_farmacii.count loop
        v_id := v_lista_id_farmacii(i).id_farmacie;

        select unique * into v_farmacie
        from c##pharmacy.farmacii f
        where f.id_farmacie = v_id;

        dbms_output.put_line('Farmacie: ' || v_farmacie.denumire_farmacie);
    end loop;
end;
/

GRANT EXECUTE ON lista_farmacii_comenzi TO c##angajat;

-- conectat ca angajat1:

set serveroutput on;
-- afisare farmacii la care s-au facut plasat intr-o anumita zi
exec c##admin.lista_farmacii_comenzi('01-01-2022');
-- afisare farmacii la care utilizatorii cu numele de familie 'Popescu' au plasat comenzi comenzi in
anul 2022
execute c##admin.lista_farmacii_comenzi('2022%' and id_client in (select id_client from
c##pharmacy.clienti where nume = 'Popescu') and 'AAA' like '');
```

Ivan Oana Mariana

Grupa 505

```
29 -- conectat ca angajat1:
30 set serveroutput on;
31 -- afisare farmacii la care s-au facut plasat intr-o anumita zi
32 exec c##admin.lista_farmacii_comenzi('01-01-2022');
33
34 -- afisare farmacii la care utilizatorii cu numele de familie 'Popescu' au plasat comenzi comenzi in anul 2022
35 execute c##admin.lista_farmacii_comenzi('2022%' and id_client in (select id_client from c##pharmacy.clienti where nume = 'Popescu') and 'AAA' like '');
36
37
```

Script Output x Query Result x Query Result 1 x

Task completed in 0.185 seconds

Farmacie: Pharmacy A
Farmacie: Pharmacy A
Farmacie: Pharmacy A

PL/SQL procedure successfully completed.

Farmacie: Pharmacy E
Farmacie: Pharmacy E
Farmacie: Pharmacy E

PL/SQL procedure successfully completed.

Procedură sigură:

```
-- conectat ca admin

REVOKE EXECUTE ON lista_farmacii_comenzi FROM c##angajat1;

-- procedura sigura:
create or replace procedure lista_farmacii_comenzi_zi(p_data_comanda date) as
    type vector is table of c##pharmacy.comenzi%rowtype;
    v_lista_id_farmacii vector;
    v_farmacie c##pharmacy.farmacii%rowtype;
    v_id number(38);
begin
    SELECT * bulk collect into v_lista_id_farmacii
    FROM c##pharmacy.comenzi
    WHERE trunc(data_comanda) = to_date(p_data_comanda, 'DD-MM-YYYY');

    for i in 1..v_lista_id_farmacii.count loop
        v_id := v_lista_id_farmacii(i).id_farmacie;
        select unique * into v_farmacie
        from c##pharmacy.farmacii f
        where f.id_farmacie = v_id;

        dbms_output.put_line('Farmacie: ' || v_farmacie.denumire_farmacie);
    end loop;
end;
/

GRANT EXECUTE ON lista_farmacii_comenzi TO c##angajat;

-- conectat ca angajat1
-- afisare farmacii la care s-au facut plasat intr-o anumita zi
exec c##admin.lista_farmacii_comenzi_zi(to_date('01-01-2022', 'DD-MM-YYYY'));

execute c##admin.lista_farmacii_comenzi_zi('2022%' and id_client in (select id_client from
c##pharmacy.clienti where nume = 'Popescu') and 'AAA' like '');
```



```
66 -- conectat ca angajat1
67 exec c##admin.lista_farmacii_comenzi_zi(to_date('01-01-2022', 'DD-MM-YYYY'));
68 execute c##admin.lista_farmacii_comenzi_zi('2022%' and id_client in (select id_client from c##pharmacy.clienti where nume = 'Popescu') and 'AAA' like '');
69
70
```

Script Output x

Task completed in 0.056 seconds

Error starting at line : 68 in command -
BEGIN c##admin.lista_farmacii_comenzi_zi('2022%' and id_client in (select id_client from c##pharmacy.clienti where nume = 'Popescu') and 'AAA' like ''); END;
Error report -
ORA-01861: literal does not match format string
ORA-06512: at line 1
01861. 00000 - "literal does not match format string"
*Cause: Literals in the input must be the same length as literals in the format string (with the exception of leading whitespace). If the "FX" modifier has been toggled on, the literal must match exactly, with no extra whitespace.
*Action: Correct the format string to match the literal.

7. Mascarea datelor

```
-- creare folder (conectat ca SYS as DBA)
create or replace directory dir_export_clienti as 'C:\tmp\pharmacy_db_export';
grant read, write on directory dir_export_clienti to c##pharmacy;

-- creare pachet (conectat ca c##pharmacy)
create or replace package pachet_mascare is
    function f_mascare_text(text varchar2) return varchar2;
    function f_mascare_numar(nr number) return number;
end;
/

create or replace package body pachet_mascare is
    type tip_tabind is table of number index by pls_integer;
    v_tabind tip_tabind;

    function f_mascare_text(text varchar2) return varchar2 is
        v_sir varchar2(100);
        v_nr_cuv number;
    begin
        v_sir := substr(text, 1, 1);
        select length(text) into v_nr_cuv from dual;
        v_sir := rpad(v_sir, v_nr_cuv, '*');
        return v_sir;
    end f_mascare_text;

    function f_mascare_numar(nr number) return number is
        v_lungime number;
        v_min_nou number;
        v_max_nou number;
        l_seed VARCHAR2(100);
        v_nr_nou number;
    begin
        if v_tabind.exists(nr) then
            return v_tabind(nr);
        else
            v_lungime := length(to_char(nr));
            v_min_nou := to_number(rpad(substr(to_char(nr), 1, 1), v_lungime, '0'));
            v_max_nou := to_number(rpad(substr(to_char(nr), 1, 1), v_lungime, '9'));
            DBMS_RANDOM.seed (val => l_seed);

            v_nr_nou := round(DBMS_RANDOM.value (low => v_min_nou, high => v_max_nou), 0);
            v_tabind(nr):=v_nr_nou;

            return v_nr_nou;
        end if;
    end f_mascare_numar;
```

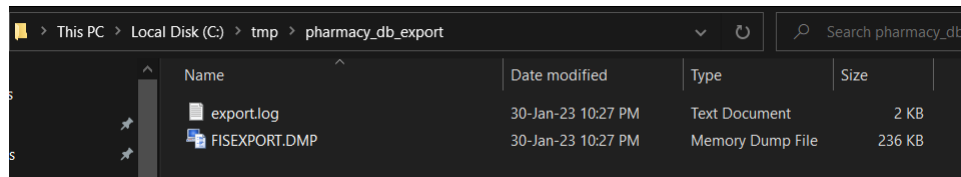
```
end f_mascare_numar;  
end;  
/
```

Comandă CMD:

```
expdp c##pharmacy/c##pharmacy@orcl tables=clienti  
remap_data=clienti.num: pachet_mascare.f_mascare_text  
remap_data=clienti.prenume: pachet_mascare.f_mascare_text  
remap_data=clienti.id_plata: pachet_mascare.f_mascare_numar  
directory=dir_export_clienti dumpfile=FISEXPORT.dmp
```

```
Starting "C##PHARMACY"."SYS_EXPORT_TABLE_01": c##pharmacy/***** tables=clienti remap_data=clienti.num:  
pachet_mascare.f_mascare_text remap_data=clienti.prenume: pachet_mascare.f_mascare_text remap_data=clienti.i  
d_plata: pachet_mascare.f_mascare_numar directory=dir_export_clienti dumpfile=FISEXPORT.dmp  
Processing object type TABLE_EXPORT/TABLE/TABLE_DATA  
Processing object type TABLE_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS  
Processing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS  
Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER  
Processing object type TABLE_EXPORT/TABLE/TABLE  
Processing object type TABLE_EXPORT/TABLE/GRANT/OWNER_GRANT/OBJECT_GRANT  
Processing object type TABLE_EXPORT/TABLE/AUDIT_OBJ  
Processing object type TABLE_EXPORT/TABLE/CONSTRAINT/CONSTRAINT  
Processing object type TABLE_EXPORT/TABLE/CONSTRAINT/REF_CONSTRAINT  
Processing object type TABLE_EXPORT/TABLE/TRIGGER  
.. exported "C##PHARMACY"."CLIENTI" 8.679 KB 6 rows  
Master table "C##PHARMACY"."SYS_EXPORT_TABLE_01" successfully loaded/unloaded  
*****  
Dump file set for C##PHARMACY.SYS_EXPORT_TABLE_01 is:  
C:\TMP\PHARMACY_DB_EXPORT\FISEXPORT.DMP  
Job "C##PHARMACY"."SYS_EXPORT_TABLE_01" successfully completed at Mon Jan 30 22:27:25 2023 elapsed 0 00:00:  
45  
C:\Users\oana_\Downloads\WINDOWS.X64_193000_db_home\bin>
```

Rezultă următorul conținut în folder:



Name	Date modified	Type	Size
export.log	30-Jan-23 10:27 PM	Text Document	2 KB
FISEXPORT.DMP	30-Jan-23 10:27 PM	Memory Dump File	236 KB

Comandă CMD – import:

```
impdp c##pharmacy/c##pharmacy@pharmacy directory=dir_export_clienti dumpfile=FISEXPORT.DMP  
TABLES=clienti remap_table=clienti:clienti_mask
```