

Rezumat

În acest referat se efectuează o analiză detaliată a mecanismelor de securitate disponibile în ediția "Community a PostgreSQL", demonstrând cum pot fi utilizate pe o bază de date medicală simplă formată din trei entități principale: "pacient", "personal_medical" și "fișă_medicală". Lucrarea abordează mai multe straturi de securitate, inclusiv securitatea rețelei prin utilizarea metodelor de autentificare sigure "(scram-sha-256)" și configurarea fișierului "pg_hba.conf" pentru controlul accesului bazat pe IP. Cele paradigmă fundamentale ale controlului accesului sunt examineate: Gestionarea accesului bazat pe rol "(RBAC)", controlul accesului discreționar "(DAC)" și controlul accesului obligatoriu "(MAC)" care sunt implementate prin siguranța nivelului rândului "(RLS)". Referatul prezintă modul de implementare a unui sistem de auditare care utilizează trigger-uri PostgreSQL pentru înregistrarea tuturor operațiunilor legate de date sensibile, precum și metode de prevenire a atacurilor de tip "SQL Injection" prin utilizarea declarațiilor pregătite. În ceea ce privește criptarea, există o serie de metode diferite. Acestea includ criptarea la nivel de disc complet folosind programe precum "FileVault", "BitLocker" și "LUKS"; criptarea la nivel de coloană folosind extensia "pgcrypto"; criptarea în tranzit prin "SSL/TLS". În cele din urmă, se arată cum se utilizează vizualizările "(Views)" pentru a îmbunătăți securitatea datelor prin ascunderea structurii tabelelor și limitarea accesului la date. Totul este și visibil public în repozitory-ul meu de Github la urmatorul Link: https://github.com/iamxorum/Master_Unibuc/tree/main/SBD/Report

Cuprins

1 Pregătirea mediului pentru referat	4
1.1 Cerințe	4
1.2 Pornirea mediului	4
2 Schema bazei de date	5
3 Securitatea Rețelei	6
4 Controlul Accesului	8
4.1 Role Based Access Control	8
4.2 Discretionary Access Control	10
4.3 Mandatory Access Control	10
5 Auditare	11
5.1 Trigger	11
5.2 pgAudit	12
6 Prevenirea SQL Injection	13
7 Criptarea Datelor	14
7.1 Full Disk Encryption - La nivel de disk	14
7.2 File System Encryption - La nivel de os	15
7.3 Criptarea la nivel de coloană	15
7.4 Criptare la nivel de rețea	16
7.5 Criptarea parolelor	16
8 Visualizări pentru Securitate	17
9 Concluzii	18
Bibliografie	19

Capitolul 1

Pregătirea mediului pentru referat

Instalarea PostgreSQL Community Edition și configurarea unui mediu de testare sunt necesare pentru a rula exemplele prezentate în acest referat. Pentru a face configurarea mediului proiectului mai simplă, Docker este folosit. Mediul este pe un VPS închiriat (securizat prin regulile de firewall iptables) și accesat doar prin VPN (Wireguard); Subnet-ul de rețea prin care se poace accessa (prin VPN) este 10.80.0.0/16 unde userii coneptați prin VPN sunt pe subnet-ul 10.80.1.0/24 și VPS-urile/Nodurile pe subnet-ul 10.80.0.0/24.

1.1 Cerințe

- **Docker și Docker Compose:** utilizate pentru containerizarea și orchestrarea serviciilor;
- **PostgreSQL Community Edition** (versiunea 14 sau superioară): sistemul de gestiune a bazelor de date relaționale;
- **Acces la linia de comandă:** necesar pentru execuția scripturilor SQL și administrarea containerelor.

1.2 Pornirea mediului

Mediul poate să fie rulat oriunde, important că este instalat Docker și Docker Compose. Comanda necesară pentru pornire este urmatoarea

```
docker-compose up -d
```

Capitolul 2

Schema bazei de date

Pentru referatul acesta (care va fi implementat în continuare pentru aplicația de evaluare SBD) o să mă folosesc de un DB Schema simplu compus de 3 entități:

- pacient;
- personal_medical;
- fisa_medicala;

Relațiile sunt următoarele:

- Pacient (1) - (N) Fisa_medicala;
- Personal_medical (1) - (N) Fisa_medicala;

Jos puteți observa rularea creării a schemei:

```
[2025-12-30 20:06:57] Connected
referat_db.public> CREATE TABLE pacient (
    id_pacient SERIAL PRIMARY KEY,
    nume VARCHAR(50) NOT NULL,
    prenume VARCHAR(50) NOT NULL,
    cnp VARCHAR(13) UNIQUE NOT NULL,
    telefon VARCHAR(15),
    adresa TEXT
)
[2025-12-30 20:06:57] completed in 101 ms
referat_db.public> CREATE TABLE personal_medical (
    id_personal SERIAL PRIMARY KEY,
    nume VARCHAR(50) NOT NULL,
    prenume VARCHAR(50) NOT NULL,
    specializare VARCHAR(50),
    username_db VARCHAR(60) UNIQUE NOT NULL,
    grad_acreditare INT NOT NULL DEFAULT 1
)
[2025-12-30 20:06:58] completed in 92 ms
referat_db.public> CREATE TABLE fisa_medicala (
    id_fisa SERIAL PRIMARY KEY,
    id_pacient INT REFERENCES pacient(id_pacient),
    id_medic INT REFERENCES personal_medical(id_personal),
    diagnostic TEXT NOT NULL,
    tratament TEXT,
    data_consultatie TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    nivel_clasificare INT NOT NULL DEFAULT 1 CHECK (nivel_clasificare IN (1, 2, 3))
)
[2025-12-30 20:06:58] completed in 91 ms
```

Figura 2.1: Creare schema

Capitolul 3

Securitatea Rețelei

Primul pas în securizarea bazei de date este de a determina cine și cum poate accesa baza de date în fișierul pg_hba.conf, unde se stabilește ce intervale de IP sunt permise sau respinse pentru acces. Este util să se protejeze accesul la nivel de firewall, dar este util să existe încă un strat de securitate în cazul în care firewall-ul nu funcționează.

TYPE	DATABASE	USER	ADDRESS	METHOD
local	all	all		scram-sha-256
host	all	all	127.0.0.1/32	scram-sha-256
host	all	all	10.80.0.0/16	scram-sha-256
host	all	all	0.0.0.0/0	reject
host	all	all	::/0	reject

Asta este o configurație minimală care permite acces-ului la baza de date în local cu parolă de autentificare; permite access-ului prin parola la userii care provin din range-ul de IP 10.80.0.0/16 (VPN în cazul acesta) și localhost; în final se dă reject la restul userilor care provin de altundeva la nivelul IPv4 și IPv6.

O vulnerabilitate era să fie trecut pentru tipul de conexiune "local" metoda "trust" unde se permitea conexiunea fară parolă.

O altă vulnerabilitate era folosirea metodei "md5" în loc de "scram-sha-256" deoarece md5 este mai nesigur (și-a pierdut setarea by default de la PostgreSQL 14 unde scram-sha-256 este acum setat default).

MD5 ca să fie considerat sigur trebuie să îndeplinească următoarele: - Ar trebui să fie capabil să convertească ușor informații digitale, cum ar fi un mesaj, într-o valoare hash cu lungime fixă. - Hash-ul trebuie să fie imposibil de decriptat din punct de vedere computational pentru a obține orice informații despre mesajul de intrare. - Din punct de vedere computational, trebuie să fie imposibil să se găsească două fișiere cu un hash identic.

Din păcate al treilea punct nu este îndeplinit deoarece este posibil să se genereze același hash pentru două fișiere diferite; situația asta aduce la atacuri de tip coliziune,

o vulnerabilitate extrem de ridicată, deoarece pot să generez același hash pentru o altă parolă spre exemplu. [3]

O altă metodă bună pentru securizarea accesului prin rețea este setarea tipului de conexiune în loc de "host" cu "hostssl". Pentru referat nu vom folosi SSL.

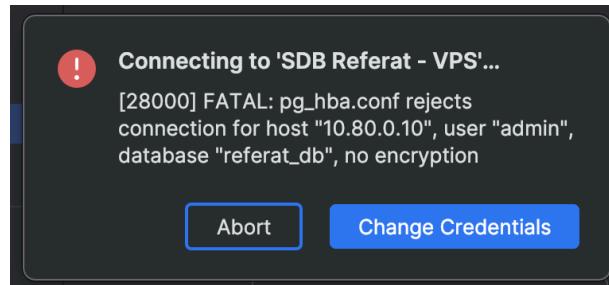


Figura 3.1: Conexiune cu Hostssl



Figura 3.2: Conexiune cu Host

Capitolul 4

Controlul Accesului

Pentru referatul acesta, o să abordez 3 tipuri de access control (menționate și la cursul SBD):

- **RBAC:** Role Based Access Control;
- **MAC:** Mandatory Access Control;
- **DAC:** Discretionary Access Control;

4.1 Role Based Access Control

Acest tip de access control bazează accesul prin roluri. În loc de a configura pentru fiecare personal_medical ce are voie să facă, să vadă, să modifice, să steargă (CRUD), stabilim asta pe baza de rol aşa că dacă e nevoie să se steargă/adauge/modifice o regulă de access, este mai ușor de întreținut/mentinut pentru ca se face doar odată schimbarea.

```
referat_db:public> CREATE ROLE rol_medic
[2025-12-30 20:47:03] completed in 86 ms
referat_db:public> CREATE ROLE rol_asistent
[2025-12-30 20:47:03] completed in 83 ms
referat_db:public> CREATE ROLE rol_rezident
[2025-12-30 20:47:03] completed in 83 ms
referat_db:public> GRANT ALL ON fisa_medicala TO rol_medic
[2025-12-30 20:47:04] completed in 84 ms
referat_db:public> GRANT ALL ON pacient TO rol_medic
[2025-12-30 20:47:04] completed in 84 ms
referat_db:public> GRANT ALL ON personal_medical TO rol_medic
[2025-12-30 20:47:04] completed in 83 ms
referat_db:public> GRANT SELECT ON pacient TO rol_asistent
[2025-12-30 20:47:05] completed in 83 ms
referat_db:public> GRANT SELECT ON fisa_medicala TO rol_asistent
[2025-12-30 20:47:05] completed in 83 ms
referat_db:public> GRANT SELECT ON personal_medical TO rol_asistent
[2025-12-30 20:47:05] completed in 83 ms
referat_db:public> GRANT SELECT ON fisa_medicala TO rol_rezident
[2025-12-30 20:47:06] completed in 83 ms
referat_db:public> CREATE USER "ana.popescu" WITH PASSWORD 'parola123'
[2025-12-30 20:47:06] completed in 87 ms
referat_db:public> GRANT rol_medic TO "ana.popescu"
[2025-12-30 20:47:06] completed in 86 ms
referat_db:public> CREATE USER "mihai.marinescu" WITH PASSWORD 'parola123'
[2025-12-30 20:47:07] completed in 90 ms
referat_db:public> GRANT rol_asistent TO "mihai.marinescu"
[2025-12-30 20:47:07] completed in 83 ms
referat_db:public> CREATE USER "elena.constantinescu" WITH PASSWORD 'parola123'
[2025-12-30 20:47:07] completed in 93 ms
referat_db:public> GRANT rol_rezident TO "elena.constantinescu"
[2025-12-30 20:47:08] completed in 83 ms
[2025-12-30 20:47:12] transaction committed: @console [SDB Referat - VPS]
```

Figura 4.1: Configurare RBAC

După ce am creat rolurile/userii pentru acces, putem testa (prin linie de comandă).

Se poate observa că medicul chiar are acces la orice (poate să adauge/șteargă pacienți noi spre exemplu), când asistentul vede totul dar nu are drept de modificare/ștergere/adăugare a datelor. În final, rezidentul are acces doar la fișele medicale.

```
[XRM-SRV01] iomxorum[XRM-SRV01]~ 
→ psql -h 10.80.0.40 -p 5432 -U "ana.popescu" -d referat_db
Password for user ana.popescu:
psql (17.6 (Debian 17.6-0+deb13u1), server 16.11 (Debian 16.11-1.pgdg13+1))
Type "help" for help.

referat_db=> \dp patient
          Access privileges
Schema | Name | Type | Access privileges | Column privileges | Policies
-----+-----+-----+-----+-----+-----+
public | patient | table | admin=updxt/admin +| | 
       |         |         | rol_medic=updxt/admin+| | 
       |         |         | rol_asistent=r/admin | | 
       |         |         | rol_rezident=r/admin | | 
(1 row)

referat_db=> SELECT * FROM patient LIMIT 1;
 id_patient | name | prenume | cnp | telefon |           adresă
-----+-----+-----+-----+-----+-----+
 1 | Popescu | Ion | 19800123456789 | 07123456789 | Strada Mihai Eminescu, Nr. 10, București
(1 row)

referat_db=> INSERT INTO patient (name, prenume, cnp, telefon, adresă)
VALUES ('Test', 'Medic', '20000123456789', '0711111111', 'Test Address')
RETURNING *;
ERROR: permission denied for sequence patient_id_patient_seq
referat_db=> INSERT INTO patient (id_patient, name, prenume, cnp, telefon, adresă)
VALUES (4, 'Test', 'Medic', '20000123456789', '0711111111', 'Test Address')
RETURNING *;
 id_patient | name | prenume |   cnp |   telefon |           adresă
-----+-----+-----+-----+-----+-----+
 4 | Test | Medic | 20000123456789 | 0711111111 | Test Address
(1 row)

INSERT 0 1
referat_db=> DELETE FROM patient WHERE cnp = '20000123456789';
DELETE 1
referat_db=> \dp fisa_medicala
          Access privileges
Schema | Name | Type | Access privileges | Column privileges | Policies
-----+-----+-----+-----+-----+-----+
public | fisa_medicala | table | admin=updxt/admin +| | 
       |         |         | rol_medic=updxt/admin+| | 
       |         |         | rol_asistent=r/admin +| | 
       |         |         | rol_rezident=r/admin +| | 
(1 row)

referat_db=> \dp personal_medical
          Access privileges
Schema | Name | Type | Access privileges | Column privileges | Policies
-----+-----+-----+-----+-----+-----+
public | personal_medical | table | admin=updxt/admin +| | 
       |         |         | rol_medic=updxt/admin+| | 
       |         |         | rol_asistent=r/admin +| | 
       |         |         | rol_rezident=r/admin +| | 
(1 row)

referat_db=> \dp
referat_db=>
```

Figura 4.2: Rol Medic

```
[XRM-SRV01] iomxorum[XRM-SRV01]~ 
→ psql -h 10.80.0.40 -p 5432 -U "mihai.morinescu" -d referat_db
Password for user mihai.morinescu:
psql (17.6 (Debian 17.6-0+deb13u1), server 16.11 (Debian 16.11-1.pgdg13+1))
Type "help" for help.

referat_db=> \dp patient
          Access privileges
Schema | Name | Type | Access privileges | Column privileges | Policies
-----+-----+-----+-----+-----+-----+
public | patient | table | admin=updxt/admin +| | 
       |         |         | rol_medic=updxt/admin+| | 
       |         |         | rol_asistent=r/admin | | 
       |         |         | rol_rezident=r/admin | | 
(1 row)

referat_db=> SELECT * FROM patient;
 id_patient | name | prenume |   cnp |   telefon |           adresă
-----+-----+-----+-----+-----+-----+
 1 | Popescu | Ion | 19800123456789 | 07123456789 | Strada Mihai Eminescu, Nr. 10, București
 2 | Ionescu | Maria | 19980607890123 | 0723456789 | Bulevardul Unirii, Nr. 25, Cluj-Napoca
 3 | Georgescu | Andrei | 1985123456789 | 074567890 | Strada Republicii, Nr. 5, Timișoara
(3 rows)

referat_db=> \dp fisa_medicala
          Access privileges
Schema | Name | Type | Access privileges | Column privileges | Policies
-----+-----+-----+-----+-----+-----+
public | fisa_medicala | table | admin=updxt/admin +| | 
       |         |         | rol_medic=updxt/admin+| | 
       |         |         | rol_asistent=r/admin +| | 
       |         |         | rol_rezident=r/admin +| | 
(1 row)

referat_db=> SELECT * FROM fisa_medicala;
referat_db=> SELECT * FROM fisa_medicala;
referat_db=> INSERT INTO patient (id_patient, name, prenume, cnp, telefon, adresă) VALUES (4, 'Test', 'Asistent', '2000123456789', '0711111111', 'Test Address')
ERROR: permission denied for table patient
referat_db=>
```

Figura 4.3: Rol Asistent

```
[XRM-SRV01] iomxorum[XRM-SRV01]~ 
→ psql -h 10.80.0.40 -p 5432 -U "elena.constantinescu" -d referat_db
Password for user elena.constantinescu:
psql (17.6 (Debian 17.6-0+deb13u1), server 16.11 (Debian 16.11-1.pgdg13+1))
Type "help" for help.

referat_db=> \dp fisa_medicala
          Access privileges
Schema | Name | Type | Access privileges | Column privileges | Policies
-----+-----+-----+-----+-----+-----+
public | fisa_medicala | table | admin=updxt/admin +| | 
       |         |         | rol_medic=updxt/admin+| | 
       |         |         | rol_asistent=r/admin +| | 
       |         |         | rol_rezident=r/admin +| | 
(1 row)

referat_db=> SELECT * FROM fisa_medicala;
referat_db=> SELECT * FROM patient;
ERROR: permission denied for table patient
referat_db=> SELECT * FROM personal_medical;
ERROR: permission denied for table personal_medical
referat_db=>
```

Figura 4.4: Rol Rezident

```
referat_db=# SELECT r.role_name AS role_name, m.member_name AS member_name
FROM pg_roles r
JOIN pg_auth_members m ON r.oid = m.roleid
JOIN pg_roles m ON m.member = m.old
WHERE r.role_name LIKE '%rol_%'
ORDER BY r.role_name, m.role_name;
role_name           member_name
-----+-----+-----+
rol_asistent | mihai.morinescu
rol_medic    | ana.popescu
rol_rezident | elena.constantinescu
(3 rows)

referat_db=# SELECT
grantee AS role_name,
table_name,
string_agg(privilege_type, ',' ORDER BY privilege_type) AS privileges
FROM information_schema.table_grants
WHERE grantee LIKE 'rol_%'
AND table_schema = 'public'
GROUP BY grantee, table_name;
role_name           table_name           privileges
-----+-----+-----+
rol_asistent | fisa_medicala | SELECT
rol_asistent | patient      | SELECT
rol_asistent | personal_medical | SELECT
rol_medic    | fisa_medicala | DELETE, INSERT, REFERENCES, SELECT, TRIGGER, UPDATE
rol_medic    | patient      | DELETE, INSERT, REFERENCES, SELECT, TRIGGER, UPDATE
rol_medic    | personal_medical | DELETE, INSERT, REFERENCES, SELECT, TRIGGER, UPDATE
rol_rezident | fisa_medicala | SELECT
(7 rows)

referat_db=#
```

Figura 4.5: Verificare Roluri

4.2 Discretionary Access Control

Acest tip de access control permite proprietarului unui obiect (tabel, înregistrare) să decidă direct cine are acces. Permișunile sunt acordate individual fiecărui utilizator, oferind control granular asupra accesului la date.

Cum se poate observa, după ce medicul a primit rolul de SELECT access pe ”fisa_medicala” cu opțiune de a da mai departe, userul ”elena.constantinescu” (asistent) a primit permisiunea de SELECT pe același tabel și se poate observa că a primit accesul.

```
* [DB:referat] [elena:constantinescu]: 
* !psql -h 192.168.0.40 -p 5432 -U "elena.popescu" -d referat_db
Password for user elena.popescu: 
SSL connection (cipher: ECDHE-RSA-AES256-GCM-SHA384), server: 16.12 (DellEMC 16.12.1-p0gpl1+1)
Type 'help' for help.

referat_db> GRANT SELECT ON fisa_medicala TO "elena.constantinescu";
referat_db>
referat_db> 
* [DB:referat] [elena:constantinescu]: 
* !psql -h 192.168.0.40 -p 5432 -U "elena.popescu" -d referat_db
Password for user elena.popescu: 
SSL connection (cipher: ECDHE-RSA-AES256-GCM-SHA384), port 5432 failed: FATAL:  password authentication failed for user "elena.popescu"
* [DB:referat] [elena:constantinescu]: 
* !psql -h 192.168.0.40 -p 5432 -U "elena.popescu" -d referat_db
Password for user elena.popescu: 
SSL connection (cipher: ECDHE-RSA-AES256-GCM-SHA384), server: 16.12 (DellEMC 16.12.1-p0gpl1+1)
Type 'help' for help.

referat_db> SELECT * FROM fisa_medicala;
   id_fisa | id_pacient | id_medic | diagnostic | treatment | data_consultatie | nivel_clasificare
:-----:|:-----:|:-----:|:-----:|:-----:|:-----:|:-----:
  1 | 1 | 1 | Hipertensiune arterială | Lisinopril 10mg zilnic, monitorizare tensiune | 2024-01-15 10:30:00 | 3
  1 | 1 | 2 | Hipertensiune arterială | Lisinopril 10mg zilnic, monitorizare tensiune | 2024-01-15 10:30:00 | 3
  1 | 1 | 3 | Infecție respiratorie superioară | Amoxicilină 500mg de 3 ori pe zi timp de 7 zile | 2024-01-25 09:00:00 | 3
(3 rows)

referat_db> SELECT * FROM pacient;
ERROR: permission denied for table pacient
referat_db>
```

Figura 4.6: Testare DAC

4.3 Mandatory Access Control

Acest tip de access control este impus de sistem pe baza unor etichete de securitate și reguli stricte (în cazul acesta ”grad_acreditare” pentru personal și ”nivel_clasificare” pentru fișele medicale). Accesul este determinat de nivelul de clasificare al datelor și al utilizatorului, fără posibilitatea modificării de către utilizatori (prin intermediul RLS - Row Level Security).

După ce s-a rulat accesul pentru RLS, se poate vedea cum fiecare user poate să vadă doar înregistrările care au ”nivel_clasificare” mai mic sau egal cu propriul lor ”grad_acreditare”.

```
* [DB:referat] [elena:constantinescu]: 
* !psql -h 192.168.0.40 -p 5432 -U "elena.popescu" -d referat_db
Password for user elena.popescu: 
SSL connection (cipher: ECDHE-RSA-AES256-GCM-SHA384), server: 16.12 (DellEMC 16.12.1-p0gpl1+1)
Type 'help' for help.

referat_db> SELECT * FROM fisa_medicala;
   id_fisa | id_pacient | id_medic | diagnostic | treatment | data_consultatie | nivel_clasificare
:-----:|:-----:|:-----:|:-----:|:-----:|:-----:|:-----:
  1 | 1 | 1 | Hipertensiune arterială | Lisinopril 10mg zilnic, monitorizare tensiune | 2024-01-15 10:30:00 | 3
  1 | 1 | 2 | Hipertensiune arterială | Lisinopril 10mg zilnic, monitorizare tensiune | 2024-01-15 10:30:00 | 3
  1 | 1 | 3 | Infecție respiratorie superioară | Amoxicilină 500mg de 3 ori pe zi timp de 7 zile | 2024-01-25 09:00:00 | 3
(3 rows)

referat_db>
referat_db> 
* [DB:referat] [elena:constantinescu]: 
* !psql -h 192.168.0.40 -p 5432 -U "elena.popescu" -d referat_db
Password for user elena.popescu: 
SSL connection (cipher: ECDHE-RSA-AES256-GCM-SHA384), server: 16.12 (DellEMC 16.12.1-p0gpl1+1)
Type 'help' for help.

referat_db> SELECT * FROM fisa_medicala;
   id_fisa | id_pacient | id_medic | diagnostic | treatment | data_consultatie | nivel_clasificare
:-----:|:-----:|:-----:|:-----:|:-----:|:-----:|:-----:
  1 | 1 | 1 | Hipertensiune arterială | Lisinopril 10mg zilnic, monitorizare tensiune | 2024-01-15 10:30:00 | 3
  1 | 1 | 2 | Hipertensiune arterială | Lisinopril 10mg zilnic, monitorizare tensiune | 2024-01-15 10:30:00 | 3
  1 | 1 | 3 | Infecție respiratorie superioară | Amoxicilină 500mg de 3 ori pe zi timp de 7 zile | 2024-01-25 09:00:00 | 3
(3 rows)

referat_db> SELECT * FROM fisa_medicala;
   id_fisa | id_pacient | id_medic | diagnostic | treatment | data_consultatie | nivel_clasificare
:-----:|:-----:|:-----:|:-----:|:-----:|:-----:|:-----:
  2 | 2 | 2 | Cardiale tensionă | Diureză 40mg la revizie, tensiuni de relansare | 2024-01-20 14:15:00 | 2
  2 | 2 | 3 | Infecție respiratorie superioară | Amoxicilină 500mg de 3 ori pe zi timp de 7 zile | 2024-01-25 09:00:00 | 2
(2 rows)

referat_db>
```

Figura 4.7: Testare MAC

Capitolul 5

Auditare

5.1 Trigger

Auditarea permite înregistrarea tuturor operațiunilor efectuate asupra datelor sensibile pentru a putea urmări și analiza accesul la informații. În PostgreSQL, aceasta poate fi implementată folosind trigger-uri care înregistrează automat fiecare operațiune (INSERT, UPDATE, DELETE) într-un tabel de audit.

Implementarea folosește un tabel "audit_log" care stochează:

- **Tabelul afectat;**
- **Tipul operației (INSERT, UPDATE, DELETE);**
- **Utilizatorul care a efectuat operația (session_user);**
- **Timestamp-ul acțiunii;**
- **Datele vechi și noi (pentru UPDATE);**
- **Adresa IP a utilizatorului;**

Trigger-ele sunt configurate pentru toate tabelele sensibile (fisa_medicala, pacient, personal_medical) și se declanșează automat la fiecare modificare.

```
referat_db>> INSERT INTO personal_Medical (id_personal, nume, prenume, specializare, username_db, grad_acreditor) VALUES ('5', 'Dr. Popescu', 'Andrei', 'Cardiologie', 'and.popescu', 3);
INSERT 0 1
referat_db>>
```

Figura 5.1: Testare Insert

id	id_personal	username_db	grad_acreditor	data_crea	data_modif	last_login	last_logout	last_ip
1	5	and.popescu	3	2023-12-26 20:20:41	2023-12-26 20:20:41	2023-12-26 20:20:41	2023-12-26 20:20:41	127.0.0.1

Figura 5.2: Verificare Audit

5.2 pgAudit

Se poate folosi extensia "pgAudit" pentru medii de producție, care oferă auditare detaliată la nivel de sesiune și obiect. Toate operațiunile PostgreSQL sunt înregistrate de pgAudit și pot fi analizate folosind pgAudit Analyze, care încarcă datele într-un schema de bază de date pentru analiză. [1]

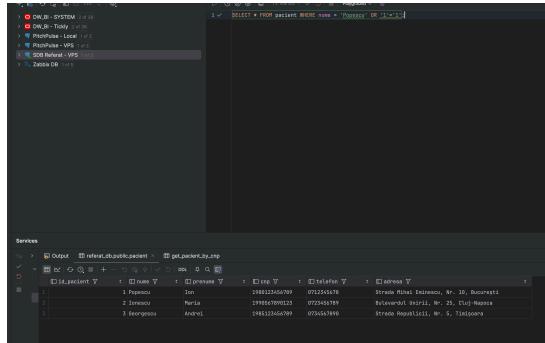
Beneficiile pgAudit includ auditare la nivel de sesiune (toate comenzi SQL), auditare la nivel de obiect (DDL, DML pe anumite tabele) și integrare cu sistemul de logare PostgreSQL. De asemenea, pgAudit Analyze permite analiză avansată. [1]

Capitolul 6

Prevenirea SQL Injection

SQL Injection este printre cele mai frecvente atacuri asupra bazelor de date, în care un atacator injectează cod SQL fals în interogări prin concatenarea string-urilor. Soluția implică interogările parametrizate pregătite, care separă codul SQL de datele utilizatorului.

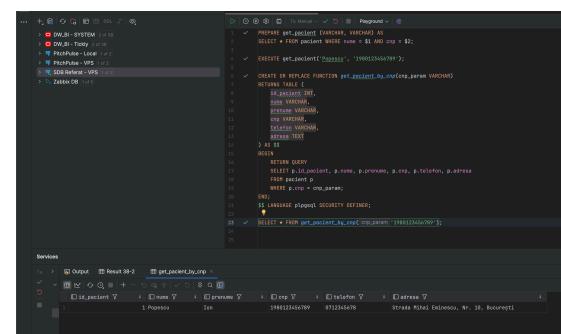
În PostgreSQL, se pot folosi prepared statements cu "PREPARE" și "EXECUTE", sau funcții PL/pgSQL care acceptă parametri. Acestea previne injectarea de cod SQL deoarece parametrii sunt tratați ca date, nu ca parte a comenzi SQL.



```
SELECT * FROM patient WHERE name = 'Thomas' OR 1=1;
```

id_patient	name	sex	age	telefon	adresa
1	Papucu	În	198812246789	072124678	Strada Mihai Eminescu, Nr. 10, București
2	Serbanu	Maria	19990709123	0721545899	Bulevardul Unirii, Nr. 23, Cluj Napoca
3	Iorgulescu	Andrei	198812246509	0721656789	Strada Revolutionii, Nr. 5, Timișoara

Figura 6.1: Testare Injection



```
CREATE OR REPLACE FUNCTION get_patient_by_name(p_name VARCHAR) AS
$BODY$
    SELECT * FROM patient WHERE name = $1 AND sex = $2;
$BODY$ LANGUAGE plpgsql SECURITY DEFINER;
CREATE OR REPLACE FUNCTION get_patient_by_id(id_patient INT) AS
$BODY$
    SELECT * FROM patient WHERE id_patient = $1;
$BODY$ LANGUAGE plpgsql SECURITY DEFINER;
```

```
SELECT * FROM get_patient_by_name('Thomas') OR 1=1;
```

Figura 6.2: Verificare Injection

Capitolul 7

Criptarea Datelor

Criptarea datelor este necesară pentru protejarea informațiilor sensibile împotriva accesului neautorizat.

7.1 Full Disk Encryption - La nivel de disk

Una dintre cele mai bune metode de protejare a datelor este criptarea completă a discului sau a partii. Această tehnică asigură protecția atât a fiecărui fișier, cât și a stocării temporare care poate conține părți ale acestora. Nu trebuie să te îngrijorezi să alegi ce fișier vrei să protejezi, deoarece criptarea completă a discului protejează toate fișierele. [2]

Avem diverse opțiuni (depinde de OS-ul pe care îl folosim): Implementarea folosește un tabel ”audit_log” care stochează:

- **MacOS - FileVault;**
- **Windows - BitLocker;**
- **Linux - LUKS (Linux Unified Key Setup).**

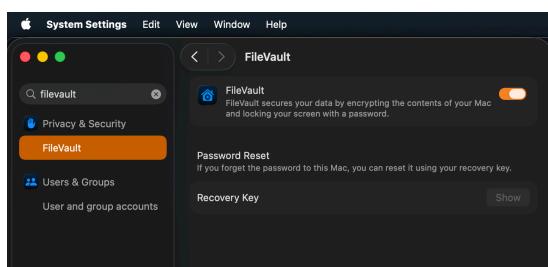


Figura 7.1: FileVault

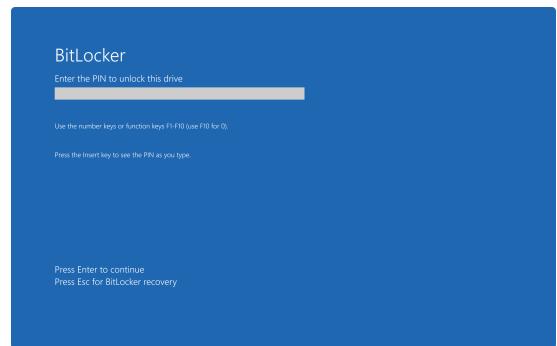


Figura 7.2: BitLocker

7.2 File System Encryption - La nivel de os

Criptarea la nivel de sistem de fișiere, denumită și criptare de fișiere sau directoare, este atunci când sistemul de fișiere însuși criptează fișierele sau directoarele. [2]

7.3 Criptarea la nivel de coloană

Pentru criptare la nivel de coloană, se poate folosi extensia "pgcrypto". Aceasta permite criptarea selectivă a coloanelor cu date sensibile, cum ar fi numerele CNP și cardurile de credit. [2]

```
RETURNS BYTEA AS $$  
BEGIN  
    RETURN pgp_sym_encrypt(cnp_plain, encryption_key);  
END;  
$$ LANGUAGE plpgsql;  
  
CREATE OR REPLACE FUNCTION decrypt_cnp(cnp_encrypted BYTEA, encryption_key TEXT)  
RETURNS VARCHAR AS $$  
BEGIN  
    RETURN pgp_sym_decrypt(cnp_encrypted, encryption_key);  
END;  
$$ LANGUAGE plpgsql;  
  
INSERT INTO pacient_encrypted (nume, prenume, cnp_encrypted, telefon, adresa)  
VALUES (  
    'Popescu',  
    'Ion',  
    encrypt_cnp('1980123456789', 'portocal12'),  
    '0712345678',  
    'Strada Mihai Eminescu, Nr. 10, București'  
);  
  
SELECT  
    id_pacient,  
    nume,  
    prenume,  
    decrypt_cnp(cnp_encrypted, 'portocal12') AS cnp_decriptat,  
    telefon,  
    adresa  
FROM pacient_encrypted  
WHERE nume = 'Popescu';  
  
ALTER TABLE pacient  
ALTER COLUMN cnp TYPE BYTEA  
USING encrypt_cnp(cnp, 'portocal12');  
| %L to chat, %K to generate
```

Figura 7.3: encryption.sql

În cazul tabelelor pe care le avem, am creat o entitate nouă pentru a arăta diferența între a citi având cheia de decriptare și fără cheie.

După ce am creat uneltele necesare (verificați "encryption.sql" din imagine), mai jos se poate observa diferența când, după ce s-a introdus pacientul cu criptarea CNP-ului, se face citirea fără sau cu cheie.

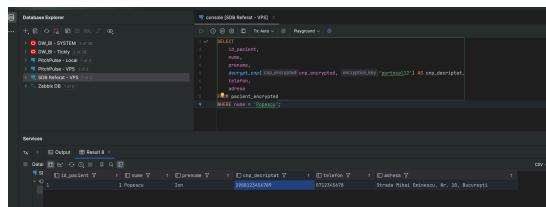


Figura 7.4: Cu cheie

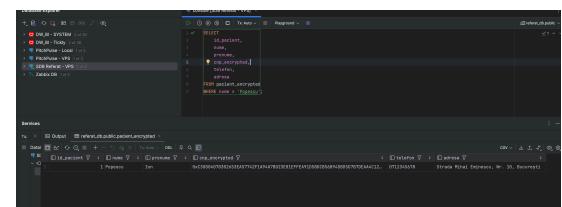


Figura 7.5: Fără cheie

Pentru tabelul curent "pacient", am criptat coloana prin comanda următoare:

```

ALTER TABLE pacient
ALTER COLUMN cnp TYPE BYTEA
USING encrypt_cnp(cnp, 'portocal12');

```

Listing 7.1: Migrarea coloanei CNP la format criptat (BYTEA)

Jos se poate observa coloana ”cnp” din tabelul ”pacient” criptat după rularea comenzi de mai sus:

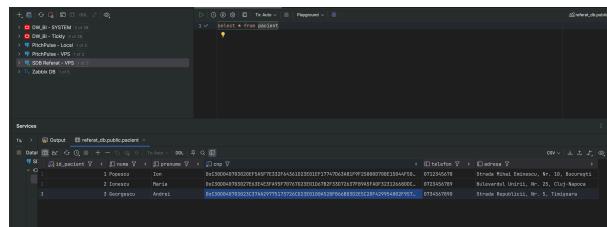


Figura 7.6: CNP Criptat

7.4 Criptare la nivel de rețea

Criptarea la nivel de rețea protejează datele în tranzit între client și server. În PostgreSQL, aceasta se realizează prin SSL/TLS. Am menționat anterior opțiunea ”hostssl” în ”pg_hba.conf” care necesită conexiuni SSL.

7.5 Criptarea parolelor

PostgreSQL folosește deja criptare pentru stocarea parolelor. Am menționat anterior folosirea ”scram-sha-256” în loc de ”md5” pentru autentificare.

Capitolul 8

Visualizări pentru Securitate

Views pot îmbunătăți securitatea datelor prin ascunderea structurii tabelelor și limitarea accesului. Putem face vizualizări care expun doar coloanele necesare și aplică filtrare automată în loc să acordăm permisiuni direct tabelelor.

```
1 now_z@host:~/automa (14u)
2 CREATE OR REPLACE VIEW pacient_public AS
3   SELECT
4     id_pacient,
5       nume,
6       prenume,
7       telefon
8   FROM pacient;
9
10 CREATE OR REPLACE VIEW personal_public AS
11   SELECT
12     id_personal,
13       nume,
14       prenume,
15       specializare
16   FROM personal_medical;
17
18 CREATE OR REPLACE VIEW fisa_medicala_personal AS
19   SELECT
20     f.id_fisa,
21     f.id_pacient,
22     p.nume AS nume_pacient,
23     p.prenume AS prenume_pacient,
24     f.diagnostic,
25     f.tratament,
26     f.data_consultatie
27   FROM fisa_medicala f
28   JOIN pacient p ON f.id_pacient = p.id_pacient
29   JOIN personal_medical pm ON f.id_medic = pm.id_personal
30   WHERE pm.username_db = current_user;
31
32 GRANT SELECT ON pacient_public TO rol_asistent;
33 GRANT SELECT ON personal_public TO rol_asistent;
34 GRANT SELECT ON fisa_medicala_personal TO rol_medic;
35
```

```
[XRM-SRV01] iamxorum@XRM-SRV01:~ ✓
→ psql -h 10.80.0.40 -p 5432 -U "mihai.marinescu" -d referat_db
Password for user mihai.marinescu:
psql (17.6 (Debian 17.6-0+deb13u1), server 16.11 (Debian 16.11-1.pgdg13+1))
Type "help" for help.

referat_db=> SELECT * FROM pacient;
ERROR: permission denied for table pacient
referat_db=> SELECT * FROM pacient_public;
id_pacient | nume | prenume | telefon
-----+-----+-----+-----
1 | Popescu | Ion | 0712345678
2 | Ionescu | Maria | 0723456789
3 | Georgescu | Andrei | 0734567890
(3 rows)

referat_db=>
```

Figura 8.2: Testare Visualizare

Figura 8.1: Creare Visualizări

Exemplu În loc să acordăm ”SELECT” pe întregul tabel ”pacient”, creăm un view ”pacient_public” care expune doar nume, prenume și telefon, ascunzând CNP-ul și adresa completă. (vedeți mai sus la imaginea 8.2)

Capitolul 9

Concluzii

Acest referat a demonstrat implementarea practică a multiple straturi de securitate în PostgreSQL, utilizând o bază de date medicală ca studiu de caz. Principalele concluzii sunt:

- **Securitatea rețelei:** prin configurarea corectă a "pg_hba.conf" și utilizarea metodelor de autentificare sigure precum "scram-sha-256";
- **Controlul accesului:** poate fi implementat prin trei paradigmă complementare (RBAC, DAC, MAC);
- **Auditare:** pentru urmărirea și analiza accesului la date sensibile, iar implementarea prin trigger-uri;
- **Prevenirea SQL Injection:** prin utilizarea prepared statements;
- **Criptarea:** la multiple niveluri (disc, coloană, rețea);
- **Visualizări:** pentru ascunderea structurii bazei de date și limitarea accesului la date sensibile;

Bibliografie

- [1] Crunchy Data Solutions, Inc., *pgAudit Analyze Documentation, Version 1.0.9*, Accesat la: 29 Decembrie 2025, Crunchy Data, 2021, URL: https://access.crunchydata.com/documentation/pgaudit-analyze/1.0.9/pdf/pgaudit_analyze.pdf.
- [2] EnterpriseDB, *PostgreSQL Security Best Practices*, White Paper, Accesat la: 29 Decembrie 2025, EnterpriseDB Corporation, 2020, URL: <https://info.enterprisedb.com/rs/069-ALB-339/images/Security-best-practices-2020.pdf>.
- [3] Marc Stevens, *On Overcoming the Many-to-One Nature of Hash Functions: MD5 Collisions*, Accesat la: 29 Decembrie 2025, 2009, URL: <https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/MD5%20Collisions.pdf>.