Oracle Security

WEEK 11

Topics

Basic Audit

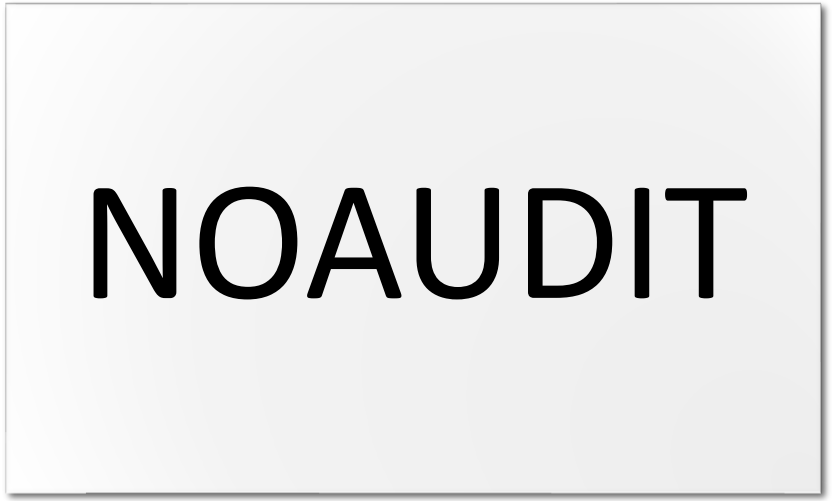
FGA – Fine Grained Audit

SQL Injection Challenge

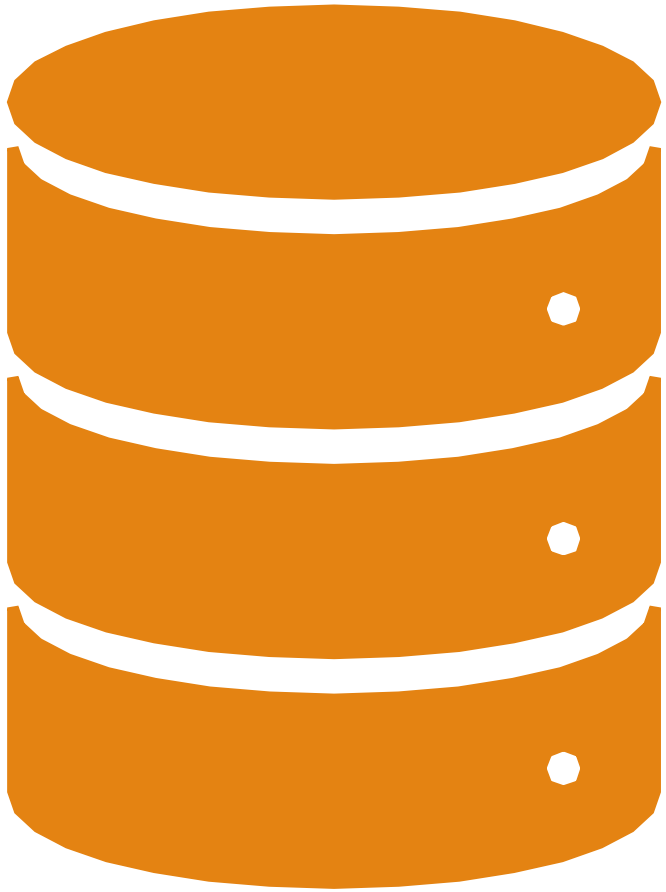
Basic Audit

When to Enable Audit?

- Suspicious activity
- Find out if an Oracle user is still used
- Who is deleting records from a specific table?
- Find out who is updating the SALARY table but only if the salary value is greater than 10000 (fine grained auditing is needed – enterprise edition)



Audit Statements



Step 1: What we want to audit?

Some database operations (drop table, truncate table etc.)

Database operations executed by a user (only DELETEs executed by Dorel)

Database operations on a table (only UPDATEs for VANZARI.FACTURI)

Step 2: When we want to audit?

- Whenever successful
- Whenever NOT successful
- By default both are enabled

Step 3: How to audit?

BY ACCESS

BY SESSION

Audit Examples

```
AUDIT UPDATE TABLE, INSERT TABLE, DELETE TABLE BY tmarin BY ACCESS;
AUDIT DELETE ON vanzari.clienti BY ACCESS WHENEVER NOT SUCCESSFUL;
AUDIT DELETE ON vanzari.facturi BY SESSION;
AUDIT UPDATE ON vanzari.liniifact WHENEVER NOT SUCCESSFUL;
```

Query the Audit Data

Audit Configuration

```
SYS@SQL> select user_name, audit_option, success, failure from dba_stmt_audit_opts where user_name in
('FMIHAI', 'PSILVIU', 'TMARIN');

USER_NAME            AUDIT_OPTION                               SUCCESS    FAILURE
-------------------- ------------------------------------------ ---------- ----------
TMARIN               INSERT TABLE                               BY ACCESS  BY ACCESS
TMARIN               UPDATE TABLE                               BY ACCESS  BY ACCESS
TMARIN               DELETE TABLE                               BY ACCESS  BY ACCESS
```

Audit Trail

```
SQL> SELECT USERNAME, TIMESTAMP, OWNER, OBJ_NAME, ACTION_NAME FROM DBA_AUDIT_TRAIL WHERE username IN
('FMIHAI', 'PSILVIU', 'TMARIN');

USERNAME             TIMESTAMP          OWNER      OBJ_NAME        ACTION_NAME
-------------------- ------------------ ---------- --------------- ----------------------------
PSILVIU              08-MAY-17          VANZARI    FACTURI         SESSION REC
PSILVIU              08-MAY-17          VANZARI    CLIENTI         DELETE
TMARIN               08-MAY-17          VANZARI    CLIENTI         DELETE
PSILVIU              08-MAY-17          VANZARI    LINIIFACT       UPDATE
TMARIN               08-MAY-17          VANZARI    LINIIFACT       UPDATE
```

Audit Challenge

You suspect that somebody is trying to connect to VANZARI schema using a brute force attack.

Implement the required audit to figure out what's going on.

FGA – Fine Grained Audit

When Should We Use FGA?

FGA Example

We want to audit in our own audit table all queries and inserts involving FACTURI table, but only when VALFACT > 2000.

STEP 1: Grant execute privileges on DBMS_FGA package.

STEP 2: Create a custom audit table

STEP 3: Create a FGA handler procedure to embed our audit logic

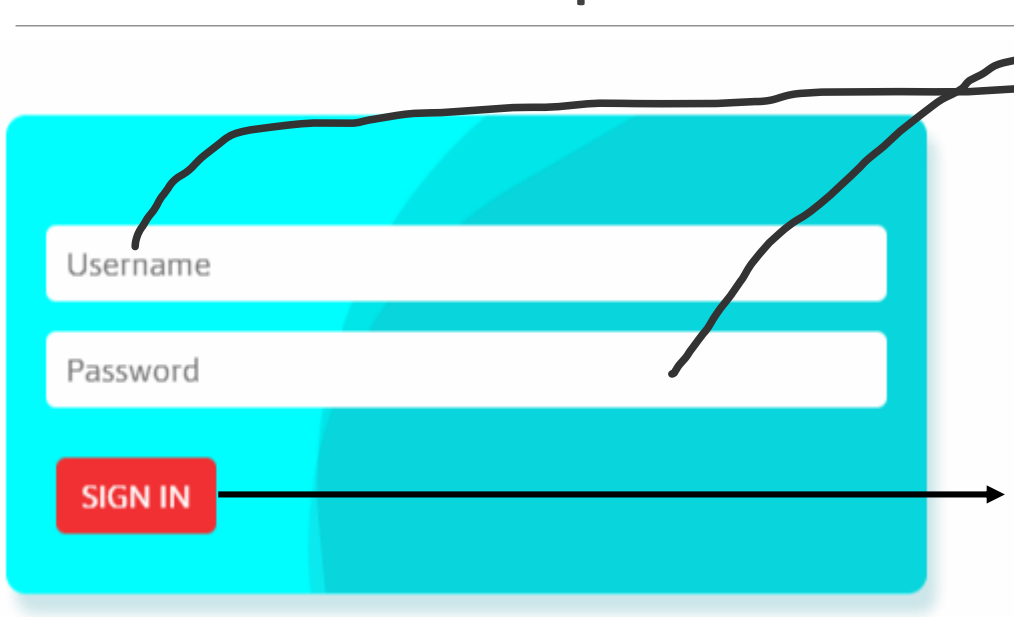
STEP 4: Add the audit policy using DBMS.FGA package

STEP 5: Test the FGA policy

*A step by step implementation may be found in **w10_securitate_si_audit_ro.pdf** file (on FEAA portal).*

SQL Injection

Basic Example




```
CREATE OR REPLACE FUNCTION LOGIN (EMAIL IN VARCHAR2, PWD IN VARCHAR2)
RETURN VARCHAR2 AS
  found_accounts integer;
BEGIN
  execute immediate 'select count(*) from accounts where email = '''
    || email || ''' and pwd = ''' || PWD || '''' into found_accounts;
  if found_accounts = 1 then
    return 'SUCCESS: You have succesfully logged in';
  else
    return 'FAILED: Invalid username or password';
  end if;
END LOGIN;
```

01

Connect to FB schema and create the LOGIN function from the previous slide (sql_injection_login.sql file)

02

Supposing that you don’t know the password of andra@gmail.com, how can you gain access into the system?

03

How can you fix the security problem in our LOGIN function?

Challenge: Be a hacker!

Quiz Time

Challenge your Oracle security knowledge with these 10 questions!

https://play.kahoot.it

That’s all folks!

THANK YOU AND SEE YOU NEXT WEEK…