IT6863 Database Security and Auditing (summer 2018)

Dr. Svetlana Peltsverger

IT Department

Kennesaw State University

Contents

Catalog Description

Prerequisites: IT 5433 Databases: Design and Applications.
This course provides students with an understanding of security concepts and practices in general and those specific to database security in a highly detailed implementation. Students will learn fundamental principles of database security and how to develop database applications embedding from simple to sophisticated security and auditing models using advanced database systems and software tools.

Course Outcomes

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.
- Explain principles of database auditing.
- Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).

Module 1 SQL Review

Introduction and Module Summary

In this module, you will review database design and Structured Query Language (SQL). SQL is the standard language for relational database management systems. SQL knowledge is the prerequisite to this course. Depending on when you took an introduction to databases course, this module will take you anywhere from 4 to 12 hours of work. Spending enough time on this review will help you to complete other modules in this course.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

1. **Evaluate vulnerabilities of Database Management Systems.**
2. Describe the methods for controlling database security.
3. Explain principles of database auditing.
4. Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).

Module outcomes and activities:

After completing this module, students will be able:	to develop conceptual, logical and physical data models	to use SQL for data manipulation and data extraction
Readings	introduced	introduced
Practice exercise	reinforced	reinforced
SQL quiz	reinforced	reinforced
Lab 1	mastered	mastered

Assigned Reading

1. SQL http://docs.oracle.com/database/121/CNCPT/sqllangu.htm#CNCPT015
2. Readings linked through the module
3. Intro to SQL 1-10 http://sqlcourse.com/intro.html
4. Intro 2 to SQL 1-10 http://sqlcourse2.com/

Optional Reading

1. Oracle Relational Data Structures https://docs.oracle.com/cd/E11882_01/server.112/e40540/part_datstr.htm
2. Oracle 12c https://docs.oracle.com/database/121/nav/portal_4.htm

   MS SQL 2016 http://msdn.microsoft.com/en-us/library/ms187875.aspx

Module 2 Security Architecture

Introduction and Module Summary

This module introduces basic concepts of database security. First, we will discuss basic definitions of database management systems. Then we will discuss information security and information security architecture followed by description of database security methods.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- **Evaluate vulnerabilities of Database Management Systems.**
- Describe the methods for controlling database security.
- Explain principles of database auditing.
- Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).

Module outcomes and activities:

After completing this module, students will be able:	Describe an information system and its components	Define database management system functionalities	Outline the concept of information security	Protect database driven applications from SQL Injections
Readings	introduced	introduced	introduced	introduced
SQLi quiz				reinforced/mastered
Lab 1	reinforced/ mastered	reinforced/ mastered	reinforced/ mastered	

Assigned Reading

1. SQL Injections https://www.owasp.org/index.php/SQL_Injection and https://www.acunetix.com/websitesecurity/sql-injection/ and http://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm
2. Prepared Statement paper http://ksuweb.kennesaw.edu/~speltsve/files/sql_files/prepared_statement.doc
3. Invoker rights http://www.dba-oracle.com/t_authid_definer_rights.htm and http://psoug.org/definition/authid.htm
4. Input Validation and Data Sanitization https://wiki.sei.cmu.edu/confluence/display/java/Input+Validation+and+Data+Sanitization

Optional Reading

1. Managing Security for Definer's Rights and Invoker's Rights http://docs.oracle.com/database/121/DBSEG/dr_ir.htm#DBSEG659
2. Brief history of the Committee on National Security Systems (CNSS) https://www.cnss.gov/CNSS/about/history.cfm

Module 3 Securing Database Environment

Introduction and Module Summary

In this module, you will learn how to protect the database environment. You will also learn about Oracle multitenant architecture and continue SQL review.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- **Describe the methods for controlling database security.**
- Explain principles of database auditing.
- Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).

Module outcomes and activities:

After completing this module, students will be able:	Describe database environment	Outline several server administration best practices	Explain the differences between authentication methods	Use SQL for data manipulation and data extraction
Readings	reinforced	Introduced/ reinforced	introduced/ reinforced	
Lab 1				Reinforced/ mastered

Assigned Reading

1. Security Considerations for a SQL Server Installation https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-sql-server-installation

2. Azure Data Security and Encryption Best Practices https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices
3. Dealing with NIST's about-face on password complexity https://www.networkworld.com/article/3199607/linux/dealing-with-nists-about-face-on-password-complexity.html
4. Authentication Methods https://docs.oracle.com/cd/B19306_01/network.102/b14266/authmeth.htm#BABCGGEB

Optional Reading

1. Oracle Securing the Database Installation and Configuration https://docs.oracle.com/database/121/TDPSG/GUID-3EC7A894-D620-4497-AFB1-64EB8C33D854.htm#TDPSG60000
2. Digital Identity Guidelines https://pages.nist.gov/800-63-3/sp800-63b.html#singlefactorOTP

Module 4 SQL Procedures and Functions

Introduction and Module Summary

In this module, you will learn benefits of using procedural SQL and how to write, execute and test SQL procedures and functions.
SQL has limitations, it can execute one statement at a time. PL/SQL is executed as a block of code. Moreover, you can repeat execution of any named black as many times as you wish.
PL/SQL is used to write triggers, functions, procedures and packages. You can call PL/SQL functions from SQL statement.
Why use PL/SQL?
By Bryn.Llewellyn https://blogs.oracle.com/plsql-and-ebr/entry/why_use_pl_sql
"Large software systems must be built from modules. A module hides its implementation behind an interface that exposes its functionality. This is computer science's most famous principle. For applications that use an Oracle Database, the database is, of course, one of the modules. The implementation details are the tables and the SQL statements that manipulate them. These are hidden behind a PL/SQL interface. This is the Thick Database paradigm: select, insert, update, delete, merge, commit, and rollback are issued only from database PL/SQL. Developers and end-users of applications built this way are happy with their correctness, maintainability, security, and performance."

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.
- Explain principles of database auditing.
- **Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).**

Module outcomes and activities:

After completing this module, students will be able:	to list benefits of procedural SQL	differentiate when to use function and when to use procedures	develop procedural SQL code	test and execute procedural SQL code
Read PL/SQL Language Fundamentals and the module (2 hours)	introduced	introduced	introduced	
Execute PL/SQL code from the module (2 hour)	reinforced	reinforced	introduced	introduced
Complete Module Lab (1 hour 40 min)			mastered	mastered

Assigned Reading

1. Introduction to PL/SQL part I and II (except cursors) http://w2.syronex.com/jmr/edu/db/introduction-to-plsql/

Optional Reading

1. Date functions examples http://psoug.org/reference/date_func.html

2. PL/SQL Language Fundamentals
http://docs.oracle.com/database/121/LNPLS/fundamentals.htm#LNPLS99920

3. PL/SQL Subprograms
http://docs.oracle.com/database/121/LNPLS/subprograms.htm#LNPLS008

4. Variables and Types http://infolab.stanford.edu/~ullman/fcdb/oracle/or-plsql.html#variables%20and%20types

5. Oracle Procedures http://www.psoug.org/reference/procedures.html

6. Oracle Functions http://www.psoug.org/reference/functions.html

7. PL/SQL FAQ http://www.orafaq.com/wiki/PL/SQL_FAQ

Module 5 Triggers

Introduction and Module Summary

In this module, you will learn how to write PL/SQL and T-SQL triggers. A trigger is a named structural SQL block (PL/SQL or T-SQL) that is stored in the database and executed (fired) in response to a specified event that occurs in the database.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.
- Explain principles of database auditing.
- **Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).**

Module outcomes and activities:

After completing this module, students will be able:	to develop, test and debug Oracle PL/SQL triggers	to develop, test and debug MS SQL Server T-SQL triggers
Read assigned materials	introduced	introduced
Read and execute code from the module	reinforced	reinforced
Complete Module Lab	mastered	mastered

Assigned Reading

1. Oracle Triggers
http://docs.oracle.com/database/121/CNCPT/srvrside.htm#CNCPT218

2. T-SQL Triggers http://msdn.microsoft.com/en-us/library/ms189799.aspx

Optional Reading

1. Oracle triggers reference http://psoug.org/reference/table_trigger.html

2. Triggers in Pl/SQL includes: definition, trigger event, main parts of a trigger, types of trigger, syntax with example of creating triggers https://www.youtube.com/watch?v=FS1be-wl7Bc

3. DML triggers in SQL server https://www.youtube.com/watch?v=JNb54seLzZY

Module 6 User Administration: Oracle

Introduction and Module Summary

In this module, you will learn how to create/remove users using Oracle. How to modify an existing user and the difference between common and local users in Oracle pluggable database. You will take the first look at object permissions in Oracle and use data dictionary to report quota usage by users.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.
- Explain principles of database auditing.
- **Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).**

Module outcomes and activities:

After completing this module, students will be able:	Create/remove/modify users accounts using Oracle	List best practices for user administration
Read assigned materials	introduced	introduced
Read and execute code from the module	reinforced	reinforced
Complete Module Lab	mastered	mastered

Assigned Reading

1. Multitenant Architecture
https://docs.oracle.com/database/121/CNCPT/cdbovrvw.htm#CNCPT89234
2. Managing Security for Oracle Database Users
https://docs.oracle.com/database/121/DBSEG/users.htm
3. SYS vs SYSTEM https://docs.oracle.com/database/121/ADMQS/GUID-CF1CD853-AF15-41EC-BC80-61918C73FDB5.htm
4. SYSDBA and SYSOPER System Privileges https://docs.oracle.com/database/121/ADMQS/GUID-2033E766-8FE6-4FBA-97E0-2607B083FA2C.htm

Optional Reading

1. Documentation library Release 2 (11.2) http://www.oracle.com/pls/db112/homepage

Module 7 User Administration: SQL Server

Introduction and Module Summary

In this module, you will learn how to create/remove users and logins using SQL Server. You will also learn

how to modify an existing user and how to list all default users using SQL servers.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.
- Explain principles of database auditing.
- **Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).**

Module outcomes and activities:

After completing this module, students will be able:	Create/remove/modify users accounts using MS SQL Server	List elements of password policy
Read assigned materials	introduced	introduced
Read and execute code from the module	reinforced	reinforced
Complete Module Lab	mastered	mastered

Assigned Reading

1. Database permissions https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/getting-started-with-database-engine-permissions

2. Create login https://docs.microsoft.com/en-us/sql/t-sql/statements/create-login-transact-sql

3. Create user https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-database-user

4. Roles https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/join-a-role

Optional Reading

1. Documentation library https://docs.microsoft.com/en-us/sql/relational-databases/security/security-center-for-sql-server-database-engine-and-azure-sql-database

Module 8 Profiles, Passwords, Privileges, and Roles

Introduction and Module Summary

In this module, you will learn about four aspects of user administration and user security. These aspects are profiles, passwords, privileges, and roles.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.

- Describe the methods for controlling database security.
- Explain principles of database auditing.
- **Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).**

Module outcomes and activities:

After completing this module, students will be able:	Design and implement password policies	Grant and revoke user privileges	Create, assign, and revoke user roles
Read assigned materials	introduced	introduced	introduced
Read and execute code from the module	reinforced	reinforced	reinforced
Prepare for discussion topic and post your answer.	reinforced		
Complete Module Lab	mastered	mastered	mastered

Assigned Reading

1. Principal of least Privilege https://www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege

2. Oracle Profiles https://docs.oracle.com/database/121/SQLRF/statements_6012.htm

3. Oracle roles http://docs.oracle.com/database/121/SQLRF/statements_6014.htm

4. INFORMATION_SCHEMA reference https://docs.microsoft.com/en-us/sql/relational-databases/system-information-schema-views/system-information-schema-views-transact-sql

5. MS SQL Server Roles https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/join-a-role

6. Kerberos: http://web.mit.edu/kerberos/www/

Optional Reading

1. Oracle Data Dictionary https://docs.oracle.com/database/121/CNCPT/datadict.htm

2. Documentation library https://docs.microsoft.com/en-us/sql/relational-databases/security/security-center-for-sql-server-database-engine-and-azure-sql-database

3. Documentation library Release 2 (11.2) http://www.oracle.com/pls/db112/homepage

Module 9 Database Application Security Models

Introduction and Module Summary

In this module, you will learn about different types of users in a database environment and the related security model concepts. It also lists and describes the most commonly used application types.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.

- Explain principles of database auditing.

- **Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).**

Module outcomes and activities:

After completing this module, students will be able:	Describe the different types of users in a database environment and the distinct purpose of each	Explain the use of data encryption within database applications
Read assigned materials	introduced	introduced
Read and execute code from the module	reinforced	reinforced
Complete Module Lab	mastered	mastered

Assigned Reading

1. SQL Server application role https://msdn.microsoft.com/en-us/library/ms181491.aspx

2. SQL Server: Dynamic Data Masking https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking

3. Oracle Data Redaction https://docs.oracle.com/cloud/latest/db121/ASOAG/redaction.htm#ASOAG594

4. Oracle Data Masking http://www.oracle.com/technetwork/database/options/data-masking-subsetting/overview/index.html read and watch 35 min video

Optional Reading

1. What the difference between "Data Redaction" and "Data Masking"? http://www.dbaces.com/resources/knowledge-base/117-what-should-i-us
2. Oracle application users and roles https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dbfsg/configuring-application-sessions.html#GUID-BF0AACF5-D06C-47E1-B83C-1D354C2CF2F3

Module 10 Database Auditing: Oracle

Introduction and Module Summary

This module discusses the role of audit in cybersecurity and explains database auditing, which together with database security ensures that your data is protected. You guard your data by enforcing database security, and you ensure that data is well guarded through database auditing.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.

- Describe the methods for controlling database security.

- **Explain principles of database auditing.**

- Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).

Module outcomes and activities:

After completing this module, students will be able:	Explain role of auditing in cybersecurity	Select appropriate auditing model and	Define the differences between auditing	Describe Audit Vault and Unified

		objectives for a project	classifications and types	auditing in Oracle.
Read assigned materials	introduced	introduced	introduced	introduced
Complete Module Lab	reinforced	reinforced	reinforced	

Assigned Reading

1. A framework for continuous auditing: Why companies don't need to spend big money https://www.journalofaccountancy.com/issues/2017/mar/continuous-auditing.html

2. (Video) Advanced Auditing & Information Systems https://www.youtube.com/watch?v=hAHB0REPLvY (first 30 min)

3. Why You Need a Database Audit Trail https://www.imperva.com/blog/2017/04/why-you-need-a-database-audit-trail/

4. Introduction to auditing
https://docs.oracle.com/database/121/DBSEG/auditing.htm#DBSEG1023

5. Oracle Audit Vault and Database Firewall
http://www.oracle.com/technetwork/products/audit-vault/downloads/owp-audit-vault-db-firewall-122-2844505.pdf

Optional Reading

1. Data Privacy vs. Data Protection: Reflecting on Privacy Day and GDPR
https://www.welivesecurity.com/2018/01/25/data-privacy-vs-data-protection-gdpr/
2. Configuring Audit Policies
https://docs.oracle.com/database/121/DBSEG/audit_config.htm#DBSEG1025

Module 11 Database Auditing Models MS SQL Server

Introduction and Module Summary

This module discusses how to use SQL Server audit to create server audits that include server audit specifications for server level events, and database audit specifications for database level events.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.
- **Explain principles of database auditing.**
- Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).

Module outcomes and activities:

After completing this module, students will be able:	Describe anatomy of SQL Server audit	Configure auditing in SQL Server
Read assigned materials	introduced	introduced
Watch assigned videos	reinforced	reinforced

Complete Module Lab		

Assigned Reading

1. SQL Server Audit https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine

2. Get started with SQL database auditing https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine

3. Create a Server Audit and Server Audit Specification https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/create-a-server-audit-and-server-audit-specification

4. (video) SQL Server 2016 https://www.youtube.com/watch?v=Xh3WRDGWpq0

5. (video) SQL Server 2014 https://www.youtube.com/watch?v=EefIHhT78I0

Optional Reading

1. DDL Triggers in SQL Server - audit database objects https://www.sqlbook.com/sql-server/using-ddl-triggers-in-sql-server-to-audit-database-objects/

Module 12 Virtual Private Databases

Introduction and Module Summary

This module illustrates the concept of a virtual private database—a shared database schema containing data that belongs to many different users and each user can view or update only the data he or she owns. Three ways of implementing a virtual private database in Oracle: using the VIEW database object, using Oracle's application context and using Oracle's virtual private database feature.
Two ways of implementing a virtual private database in MS SQL Server: using the VIEW database object and using MS SQL Server Row-Level. You will also learn how to mask data in MS SQL Server tables.

Objectives and Outcomes

This module directly supports **highlighted** course outcome(s)

Students who complete this course successfully will be able to

- Evaluate vulnerabilities of Database Management Systems.
- Describe the methods for controlling database security.
- Explain principles of database auditing.
- **Develop and implement a security plan for an enterprise level database (password policies, auditing policies, user privileges, profile, and roles).**

Module outcomes and activities:

After completing this module, students will be able:	Define the term "virtual private database" and explain its importance	Implement a virtual private database in Oracle	Implement a virtual private database in MS SQL Server
Read assigned materials	introduced	introduced	introduced
Read and execute code from the module	reinforced	reinforced	
Prepare for discussion topic and post your answer.	Reinforced, mastered		
Complete Module Lab			reinforced

Assigned Reading
1. VPD Oracle: Using Oracle Virtual Private Database to Control Data Access https://docs.oracle.com/database/121/DBSEG/vpd.htm 2. VPD MS SQL Server: Row-Level Security https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security
Optional Reading
1. Virtual Private Database (Part 1) https://www.red-gate.com/simple-talk/sql/oracle/virtual-private-database-part-1/ 2. Virtual Private Database (Part 2) https://www.red-gate.com/simple-talk/sql/oracle/virtual-private-database-part-2/