Syllabus

The following are all pages from this module linked as a single file suitable for printing or saving as a PDF for offline viewing. Please note that some animations or images may not work.

Course Description

This module is also available as a concatenated page, suitable for printing or saving as a PDF for offline viewing.

MET CS674

Database Security

Prerequisite: MET CS 669 or proof of knowledge

The course provides a strong foundation in database security and auditing. This course utilizes Oracle scenarios and step-by-step examples. The following topics are covered: security, profiles, password policies, privileges and roles, Virtual Private Databases, and auditing. The course also covers a list of advanced topics, such as SQL injection. Database management security issues such as securing the DBMS, enforcing access controls, and related issues are also covered.

Technical Notes

The table of contents expands and contracts (+/- sign) and may conceal some pages. To avoid missing content pages, you are advised to use the next/previous page icons in the top right corner of the learning modules.

This course requires you to access files such as word documents, PDFs, and/or media files. These files may open in your browser or be downloaded as files, depending on the settings of your browser.

Course Objectives

At the completion of the course, you will fully understand how to implement database security on modern business databases by using practical scenarios and step-by-step examples. Hands-on projects using Oracle Database Management System are used to reinforce and showcase the topics presented.

By successfully completing this course, you will be able to:

- Describe the fundamentals of security, and how it relates to information systems.
- Identify assets in your organization and their values.
- Identify risks and vulnerabilities in operating systems from a database perspective.
- Explain good password policies and techniques to secure passwords in your organization.
- Implement administration policies for users.
- Use Oracle to create policies, profiles and roles.
- Compare the various database security models and their advantages or disadvantages.
- Implement a Virtual Private Database using views, roles, and application context.
- Summarize an overview of auditing fundamentals and create your own auditing model.
- Describe the purpose and use of data dictionaries, encryption, and SQL injection.
- Explore an interesting topic of your choice related to database security or related topic.

Course Outline

Module 1 – Information Security Fundamentals and the Types of Attacks

- Lecture 1 – Information Security Fundamentals
- Lecture 2 – Attackers and their Attacks
- Lecture 3 – Information Security Framework

Module 2 – Operating Systems and User Administration

- Lecture 4 – Operating Systems
- Lecture 5 – User Administration

Module 3 – Profiles, Passwords, Privileges and Roles

Due to a heavy workload in this third week, it is recommended that you get started on the assignments as early as possible (particularly the Research Paper Proposal).

- Lecture 6 – Authorization
- Lecture 7 – Database Applications Security

Module 4 - Virtual Private Database

- Lecture 8 – Virtual Private Database
- Lecture 9 – How the Virtual Private Database Works

Module 5 - Auditing and Encryption with Oracle

- Lecture 10 – Auditing
- Lecture 11 – Encryption with Oracle

Module 6 - Advanced Topics (Data Dictionary and SQL Injection)

- Lecture 12 – Data Dictionary
- Lecture 13 – SQL Injection

Module 7 - Final Exam

- **Proctored Final Exam** – There will be a proctored final exam for this course.

Instructor: Shengzhi Zhang, Ph.D.

Assistant Professor
Computer Science Department
Metropolitan College
Boston University
Email: shengzhi@bu.edu

Dr. Shengzhi Zhang earned his PhD in Computer Science and Engineering from Penn State University in 2012. His research focuses on cybersecurity, including but not limited to Internet of Things (IoT) security, automobile

security, mobile security, and operating system security, among others. He has most recently worked as an assistant professor in the Department of Computer Science at the Florida Institute of Technology. Prior to academia, Dr. Zhang conducted various research projects in Cisco, IBM, and Honeywell Aerospace labs. His existing partnerships, both nationally and internationally, include researchers from Ford Motor, IBM, GE, Indiana University, Penn State, Kuwait University, and the Chinese Academy of Sciences. Dr. Zhang has published many papers and served as program committee members in top-tier security conferences and journals.

Course Resources

Required Book

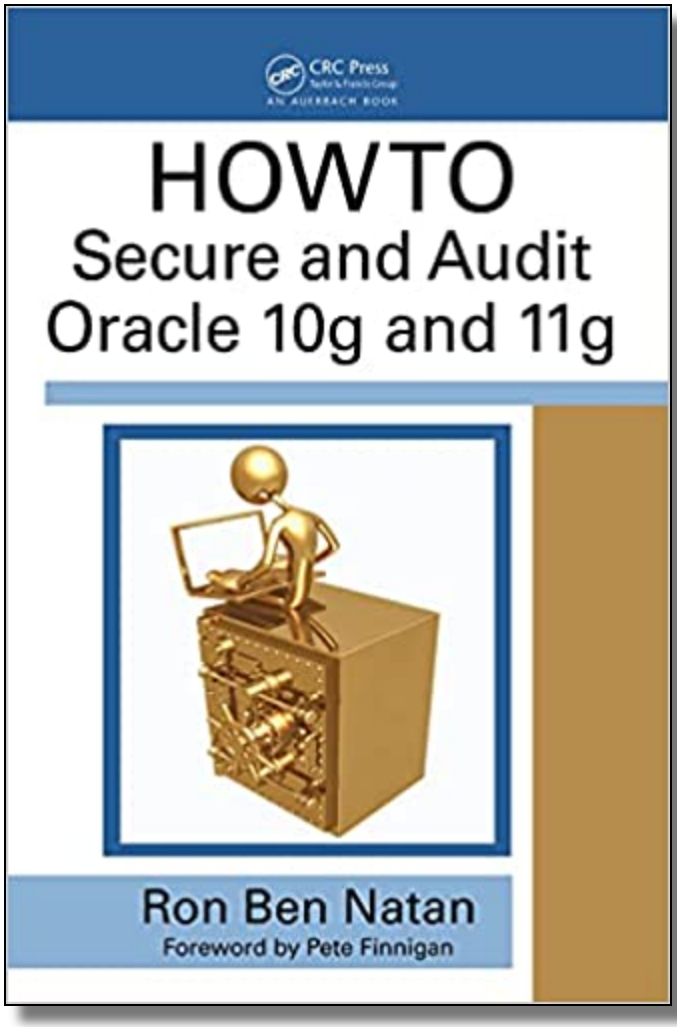
There is NO required textbook for this course.

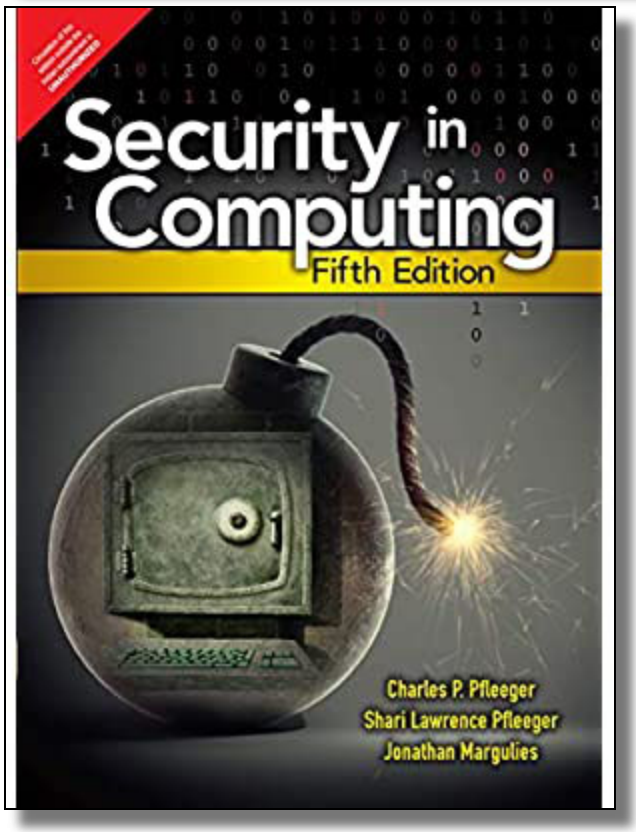
Recommended Book

Ben-Natan, R. (2009). ***HOWTO Secure and Audit Oracle 10g and 11g*****.**
Publisher: Auerbach Publications

ISBN-13: 978-1420084122
ISBN-10: 1420084127

This book can be purchased from Barnes & Noble at Boston University.





Pfleeger, C. P. & Pfleeger, S. L. (2018). ***Security in Computing*****.**

Publisher: Pearson India

ISBN-13: 978-9352866533

ISBN-10: 9789352866533

This book can be purchased from Barnes & Noble at Boston University.

Tutorials and Handouts

Lab Assignment Instructions

Advanced SQL Injection In SQL Server Applications (available in Module 6, as well)

SQL Injection: Are your Web Applications Vulnerable? (available in Module 6, as well)

Oracle Error Codes Resource

Included for your convenience is a link of searching for standard Oracle database error messages, provided by Oracle.

There are more than 40,000 of these error codes, each with a code, cause, and what to do about it. For example:

ORA-12537: TNS:connection closed

Cause: "End of file" condition has been reached; partner has disconnected.

Action: None needed; this is an information message.

ORA-12538: TNS:no such protocol adapter

Cause: The protocol adapter requested (by way of the "(PROTOCOL=..)" keyword-value pair in a TNS address) is unknown. If the supplied address is typographically correct then the protocol adapter is not installed.

Action: Install the protocol adapter or correct typographical error, as appropriate. Note: if the supplied address was derived from resolving the service name, check the address in the appropriate file (TNSNAMES.ORA, LISTENER.ORA or SQLNET.ORA).

Glossary

For your convenience, there is a link to the glossary on each page. It is accessible by clicking the Glossary icon (G).

Boston University Library Information

Boston University has created a set of videos to help orient you to the online resources at your disposal. An introduction to the series is below:

met_ode_library_14_sp1_00_intro video cannot be displayed here

All of the videos in the series are available on the Online Library Resources page, which is also accessible from the Campus Bookmarks section of your Online Campus Dashboard. Please feel free to make use of them.

As Boston University students, you have full access to the BU Library. From any computer, you can gain access to anything at the library that is electronically formatted. To connect to the library, use the link http://www.bu.edu/library. You may use the library's content whether you are connected through your online course or not, by confirming your status as a BU community member using your Kerberos password.

Once in the library system, you can use the links under “Resources” and “Collections” to find databases, eJournals, and eBooks, as well as search the library by subject. Some other useful links follow:

Go to Collections to access eBooks and eJournals directly.

If you have questions about library resources, go to Ask a Librarian to email the library or use the live-chat feature.

To locate course eReserves, go to Reserves.

Please note that you are not to post attachments of the required or other readings in the water cooler or other areas of the course, as it is an infringement on copyright laws and department policy. All students have access to the library system and will need to develop research skills that include how to find articles through library systems and databases.

Free Tutoring Service

Free online tutoring services by Tutor.com are available to BU online students for the duration of their eligible online course. Tutor.com is a web-based service that provides an online writing lab and access to on-demand and scheduled tutoring sessions for writing, math, business, coding languages, and other subjects. Students can submit a question to a tutor, submit a paper for feedback about writing and grammar, or schedule a live session with a tutor.

You can log in directly to Tutor.com from Blackboard Online Campus by clicking the link in the left-hand navigation menu within your online course. All activity in the Tutor.com classroom is recorded for learner review and quality control. Transcripts will be available afterward in My Account under My Locker in your Tutor.com account.

Please Note

Tutor.com services may be used only for current Boston University online courses and career services. Use of this service for purposes other than current coursework or career services may result in deactivation of your Tutor.com account.

Study Guide

Module 1 Study Guide and Deliverables
September 5 - September 11

Topics: Information Security Fundamentals and the Types of Attacks

Readings:
- Online lectures 1–3
- Module 1 live classroom slides and recording (will be shared after the live classroom session)

Discussions: Discussion 1 postings end Tuesday, September 12 at 6:00 AM ET

- Participate into the group discussions at the “My Group” section on the left-hand course menu.
- Discussion Rubric

Assignments: Assignment 1 due Tuesday, September 12 at 6:00 AM ET

- Submit the assignment at the “Assignments” section on the left-hand course menu.
- Lab Assignment Instructions

Assessments: Quiz 1 due Tuesday, September 12 at 6:00 AM ET

- Take the quiz at the “Assessments” section on the left-hand course menu.

Live Classroom:

- Module 1 – lecture: Wednesday, September 6 from 7:30 – 9:00 PM ET
- Module 1 – office hour: Saturday, September 9 from 8:00 – 9:00 PM ET
- Join the live session at the “Live Classrooms/Offices” section on the left-hand course menu.

Module 2 Study Guide and Deliverables
September 12 - September 18

Topics: Operating Systems and User Administration

Readings:

- Online lectures 4 and 5
- Module 2 live classroom slides and recording (will be shared after the live classroom session)

Discussions: Discussion 2 postings end Tuesday, September 19 at 6:00 AM ET

- Participate into the group discussions at the “My Group” section on the left-hand course menu.
- Discussion Rubric

Assignments: Assignment 2 due Tuesday, September 19 at 6:00 AM ET

- Submit the assignment at the “Assignments” section on the left-hand course menu.
- Lab Assignment Instructions

Assessments: Quiz 2 due Tuesday, September 19 at 6:00 AM ET

- Take the quiz at the “Assessments” section on the left-hand course menu.

Live Classroom:

- Module 2 – lecture: Wednesday, September 13 from 7:30 – 9:00 PM ET

- Module 2 – office hour: Saturday, September 16 from 8:00 – 9:00 PM ET
- Join the live session at the “Live Classrooms/Offices” section on the left-hand course menu.

Module 3 Study Guide and Deliverables
September 19 - September 25

Topics: Profiles, Passwords, Privileges and Roles

Readings:
- Online lectures 6 and 7
- Module 3 live classroom slides and recording (will be shared after the live classroom session)

Discussions: *Open* Discussion

Assignments: Assignment 3 due Tuesday, September 26 at 6:00 AM ET

Assessments: Quiz 3 due Tuesday, September 26 at 6:00 AM ET

Live Classroom:
- Module 3 – lecture: Wednesday, September 20 from 7:30 – 9:00 PM ET
- Module 3 – office hour: Saturday, September 23 from 8:00 – 9:00 PM ET

Module 4 Study Guide and Deliverables
September 26 - October 2

Topics: Virtual Private Database

Readings:
- Online lectures 8 and 9
- Module 4 live classroom slides and recording (will be shared after the live classroom session)

Discussions: Discussion 4 postings end Tuesday, October 3 at 6:00 AM ET

Assignments: Assignment 4 due Tuesday, October 3 at 6:00 AM ET

Assessments: Quiz 4 due Tuesday, October 3 at 6:00 AM ET

Live Classroom:	• Module 4 – lecture: Wednesday, September 27 from 7:30 – 9:00 PM ET • Module 4 – office hour: Saturday, September 30 from 8:00 – 9:00 PM ET

Module 5 Study Guide and Deliverables
October 3 - October 9

Topics:	Auditing and Encryption with Oracle
Readings:	• Online lectures 10 and 11 • Module 5 live classroom slides and recording (will be shared after the live classroom session)
Discussions:	Discussion 5 postings end Tuesday, October 10 at 6:00 AM ET
Assignments:	Assignment 5 due Tuesday, October 10 at 6:00 AM ET
Assessments:	Quiz 5 due Tuesday, October 10 at 6:00 AM ET
Live Classroom:	• Module 5 – lecture: Wednesday, October 4 from 7:30 – 9:00 PM ET • Module 5 – office hour: Saturday, October 7 from 8:00 – 9:00 PM ET

Module 6 Study Guide and Deliverables
October 10 - October 16

Topics:	Advanced Topics (Data Dictionary and SQL Injection)
Readings:	• Online lectures 12 and 13 • Read the two PDF handouts on SQL Injections: *Advanced SQL Injection* and *SQL Injection: Are your Web Applications Vulnerable?*
Course Evaluation:	• Course Evaluation opens on Tuesday, October 10, at 10:00 AM ET and closes on Tuesday, October 17 at 11:59 PM ET.

- Please complete the course evaluation. Your feedback is important to MET, as it helps us make improvements to the program and the course for future students.

Discussions: Discussion 6 postings end Tuesday, October 17 at 6:00 AM ET

Assignments:
- Research Paper due Tuesday, October 17 at 6:00 AM ET
- Assignment 6 due Tuesday, October 17 by 6:00 AM ET

Assessments: Quiz 6 due Tuesday, October 17 at 6:00 AM ET

Live Classroom:
- Module 6 – lecture: Wednesday, October 11 from 7:30 – 9:00 PM ET
- Course Wrap-up and Final Exam Review: Saturday, October 14 from 8:00 – 9:00 PM ET

Final Exam Details

The Final Exam is a proctored exam available from **Wednesday, October 18 at 6:00 AM ET to Saturday, October 21 at 11:59 PM ET**.

The Computer Science department requires that all final exams be administered using an online proctoring service called Examity that you will access via your course in Blackboard. In order to take the exam, you are required to have a working webcam and computer that meets Examity's system requirements. A detailed list of those requirements can be found on the How to Schedule page ("Proctored Final Exam Information" module at the course home page). Additional information regarding your proctored exam will be forthcoming from the Assessment Administrator. You will be responsible for scheduling your own appointment within the defined exam window.

The Final Exam is open book and accessible only during the final exam period. You can access it from the Assessments section of the course. Your proctor will enter the password to start the exam.

Final Exam Duration: three hours.

Student Research Presentations

The presentations linked below are samples from the classroom version of MET CS 674 and are meant to give you an idea of the scope of research topics. These are not all necessarily exceptional presentations (i.e., some are "B" grade). Also they were graded on a different rubric. Regardless, the presentations have a consistent theme – a research topic component and a "lab" component. Please note that on the bottom of most slides, narrative is documented. You have to view/print the slides in NOTES MASTER mode. In the online version of MET CS 674 you will be writing a research paper vs. creating a presentation.

- SQL Injection Attacks with SQL 2000
- AppDetective
- XMLWebSecurity (including Oracle)
- WebServices and DB Security
- Data Storage Security
- Web Application Security
- Disaster Recovery
- Access Control
- Rootkits
- Secure and Monitor Mobile Databases
- SQL Server Authentication Modes

Lab Assignment Instructions

Some assignments include hands-on lab exercises. Doing such labs helps to increase your understanding of the lecture material. Typically, we illustrate such concepts in a lab setting at Boston University. We are trying to replicate that approach in this course.

In your lab documents, you should include:

- Explanations of the work performed in the lab
- All SQL input and output used in the labs. You can use the SPOOL Command to save your Oracle code to a text file. This text file can then be pasted into the Word document
- Screen captures
- Websites - that you either used in completing the lab work or used as a resource
- Any other item that shows completion of the lab work
- Your submitted lab document should also include the following formatting at a minimum:
    - Your name
    - Lab title
    - Date
    - Table of contents
    - Clearly marked answers for each step in the labs

- Page numbers in your document

An Example of Lab Submission

These submissions consist of a sentence or two describing the SQL query and a SPOOLed version of the code. For example:

I have created a new user called yourName, I used the following syntax:

```
SQL> CREATE USER yourName IDENTIFIED BY tiger01
     etc…
     8 /
     User created
```

Course Grading Structure

The course will be conducted by means of a sequence of lectures in text and graphic form. Each week will cover one or more core database security concepts and will have at least one lab component, along with a short quiz based on the topics covered that week. There is one major assignment: the Research Paper. Students will be able to demonstrate their understanding of the fundamentals of database security through these assignments. In the final module of the course there is a comprehensive final exam, and it is proctored.

Grading Policy

All students will be expected to demonstrate database security knowledge and techniques. To obtain an exceptional grade, you have to exceed expectations in your projects, quizzes, and assignments.

Grading Structure and Distribution

The grade for the course is determined by the following:

Overall Grading Percentages	
Quizzes	15
Labs/Assignment	20

Discussions/Participation	10
Research Paper	25
Final Examination	30

The following grades will be assigned for your assignments.

A	4.0
A-	3.7
B+	3.3
B	3.0
B-	2.7
C+	2.3
C	2.0
Fail	0

Grades will be curved to maintain academic standards at Boston University.

Assignments, Exams and Discussions

Participation

Graded Discussions – all discussions will be graded on a 100-point scale: Discussion Rubric.

Assignments

Some assignments include hands-on labs. Instructions for submitting your lab work are available by clicking the following link: Lab Assignment Instructions.

Quizzes

There will be six 1-hour quizzes comprised of a combination of multiple-choice and true/false questions.

Research Paper

You are asked to research and provide a summary report on the latest security features of one of the database management systems, or a Database Security topic, as specified in the Research Paper Details.

Final Exam

There will be a proctored Final Exam in this course. The type and nature of questions in the final exam will be very similar to your quiz questions.

Expectations

Many learning activities require sharing your assignments and opinions with you classmates. For example, you may be given a set of criteria on the basis of which to evaluate other classmates' assignments, and asked to submit the results to your facilitator by a specified day of the week. It is, therefore, very important that you, as well as your classmates, submit your assignments on a timely basis. Timely submission by all will result in each of you being able to evaluate each other's assignments.

Delays

If, for any reason, you are unable to meet any assignment deadline, contact your Course Facilitator. All assignments must be completed. Extensions may be granted under mitigating circumstances.

Discussion Grading Rubric

Graded discussion periods are held Day 1 of each module until 6:00 AM ET on Day 1 of the following module. You're certainly welcome to continue a discussion past the grading period, but that additional posted material will not affect your discussion grade. The discussion grading rubric below is the guide we use to evaluate your discussion contributions.

Discussion Grading Rubric					
Criteria	**51–60**	**61–70**	**71–80**	**81–90**	**91–100**

Participation	Very limited participation	Participation generally lacks frequency or relevance	Reasonably useful relevant participation during the discussion period	Frequently relevant and consistent participation throughout the discussion period	Continually relevant and consistent participation throughout the discussion period
Community	Mostly indifferent to discussion	Little effort to keep discussions going or provide help	Reasonable effort to respond thoughtfully, provide help, and/or keep discussions going	Often responds thoughtfully in a way that frequently keeps discussions going and provides help	Continually responds thoughtfully in a way that consistently keeps discussions going and provides help
Content	No useful, on-topic, or interesting information, ideas or analysis	Hardly any useful, on-topic, or interesting information, ideas or analysis	Reasonably useful, on-topic, and interesting information, ideas and/or analysis	Frequently useful, on-topic, and interesting information, ideas and analysis	Exceptionally useful, on-topic, and interesting information, ideas and analysis
Reflection and Synthesis	No significant effort to clarify, summarize or synthesize topics raised in discussions			Contributes to group's effort to clarify, summarize or synthesize topics raised in discussions	Leads group's effort to clarify, summarize or synthesize topics raised in discussions