Boston University Metropolitan College

MET CS 674 Database Security

Instructor Name: Shengzhi Zhang
Email: shengzhi@bu.edu

LfA classroom: HAR-211
Office hours: Tuesday 10am – 11am and 10pm- 11pm (EDT) or by appointment

Course Description

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 advanced topics such as SQL injection, database management security issues such as securing the DBMS, enforcing access controls, and related issues.

Prerequisites

You are required to have working knowledge of a programming language or DBMS. It is assumed that you have taken CS579 or CS 669, or have equivalent knowledge. Please contact the instructor if you have questions about prerequisites.

Reference TextBook

HOWTO Secure and Audit Oracle 10g and 11g by Ron Ben-Natan Publisher: Auerbach Publications; 1 edition (March 10, 2009) ISBN-10: 1420084127 ISBN-13: 978- 1420084122

Course Objectives

The objective we share in this course is that each student understands the application of security concepts to database technology and demonstrate the ability to work hands-on. Specific topic objectives are:

- Explain the fundamentals of cybersecurity, and how it relates to database systems
- Implement administration policies for users
- Understand DAC, MAC, and RBAC
- Describe database security models and their advantages or disadvantages.
- Discuss auditing fundamentals and implement auditing.
- Implement user authentication on Oracle.
- Implement access controls for database use, including virtual private database.

Assessments

- Final project
- 6 Labs
- 6 Quizzes
- Final Exam

Courseware
https://learn.bu.edu/

Fall 2020 COVID-19 Policies

Classrooms on campus have new capacities that follow guidelines issued by state and local health and government authorities related to COVID-19 and physical distancing. Before the beginning of the class, and throughout the semester, I will be asking if students want to attend the classroom in-person or not. Our classroom is with the LfA capacity of 14, which is enough to hold all students.

Compliance: All students returning to campus will be required, through a digital agreement, to commit to a set of Health Commitments and Expectations including face coverings, symptom attestation, testing, contact tracing, quarantine, and isolation. The agreement makes clear that compliance is a condition of being a member of our on-campus community.

You have a critical role to play in minimizing transmission of COVID-19 within the University community, so the University is requiring that you make your own health and safety commitments. Additionally, if you will be attending this class in person, you will be asked to show your Healthway badge on your mobile device to the instructor in the classroom prior to starting class, and wear your face mask over your mouth and nose at all times. If you do not comply with these rules you will be asked to leave the classroom. If you refuse to leave the class, the instructor will inform the class that they will not proceed with instruction until you leave the room. If you still refuse to leave the room, the instructor will dismiss the class and will contact the academic Dean's office for follow up.

Boston University is committed to offering the best learning environment for you, but to succeed, we need your help. We all must be responsible and respectful. If you do not want to follow these guidelines, you must participate in class remotely, so that you do not put your classmates or others at undue risk. We are counting on all members of our community to be courteous and collegial, whether they are with classmates and colleagues on campus, in the classroom, or engaging with us remotely, as we work together this fall semester.

Class Policies

1. **Attendance & Absences**: Attendance, either in classroom or online, is expected at all class meetings. Students with legitimate reasons who contact the professor before class begins can ask for a leave, but watching the recorded classes is required to catch up.

2. **Assignment Late Policy:** Each assignment, including lab, quiz, discussion, etc., has a deadline. All assignments are assessed a 33% per-day late penalty, up to a maximum of 3 days. No assignments will be accepted four days after the deadline. Students with legitimate reasons who contact the professor before the deadline may apply for extension. There are milestone deadlines for the final project, which is firm. A deadline miss means zero for the grade of that phase. It is the students' responsibility to keep secure backups of all assignments and project milestones.

3. **Academic Conduct Code:** Cheating and plagiarism will not be tolerated in any Metropolitan College course. They will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code: http://www.bu.edu/met/for-students/met-policies-procedures-resources/academic-conduct-code/**.**
   NOTE: [This should not be understood as a discouragement for discussing the material or your particular approach to a problem with other students in the class. On the contrary – you should share your thoughts, questions and solutions. Naturally, if you choose to work in a group, you will be expected to come up with more than one and highly original solutions rather than the same mistakes.]

4. **Grading Criteria:** The grade that a student receives in this class will be based on the class participation, quizzes, labs, discussion the project and the final exam. The grade is breakdown as below. All percentages are approximate and the instructor reserves the right to make necessary changes.
   Final Project (25%)
   Quizzes (20%)
   Lab exercises (25%)
   Discussion and class participation (5%)
   Final exam (25%)

   Letter grade/numerical grade conversion is shown below:

A (94-100)	A- (90-93)	B+ (85-89)	B (80-84)	B- (79-77)
C+ (74-76)	C (70-73)	C- (65-70)	D (60-65)	F (0 – 59)

Course Outline

(This is a tentative schedule. It is subject to change based on the class progress and students' feedback) This course is organized into six modules of about 2 lectures each.

Module 1 Security fundamentals

Topics:

1. Motivation to study cybersecurity, real world examples of cyberattacks.
2. Basic concepts: CIA, vulnerability, threat, risk, attack, compromise
3. Threat model, trust model, security model
4. Bug, worm, virus, rootkit, buffer overflow
5. TOCTTOU, covert channel
6. Kernel and user mode

Module 2 Database Auditing and hardening

Topics:

1. Database ACID
2. Database hardening techniques
3. Database auditing techniques

Module 3 Introduction to Crypto

Topics:

1. The role and property of crypto
2. Terminology: Alice, Bob, Eve, encrypt, decrypt, cryptography, cryptanalysis
3. Classical encryption: Caesar Cipher, ROTx, substitution cipher
4. Symmetric encryption: DES, AES
5. Key negotiation: DH
6. Asymmetric encryption: RSA and digital signature
7. Hash: MD, MAC, HMAC
8. Certificate and PKI

Module 4 Authentication and Authorization

Topics:

1. Something you know, you are, and you have.
2. Access policy, access control matrix, access control list, DAC, MAC RBAC
3. Oracle authentication: password, Kerberos

4. Oracle authorization: privileges, roles

Module 5 Virtual Private Database and SQL Injection

Topics:

1. Necessity of VPD
2. How to implement VPD
3. Problems of VPD
4. Launch SQL injection attacks
5. Countermeasures

Module 6 Database as a service

Topics:

1. Challenges in outsourced database
2. Merke Hash Tree
3. Data confidentiality: relational encryption

Course Schedule

Lectures, Readings, and Assignments subject to change, and will be announced in class as applicable within a reasonable time frame.

Class	Date	Topics	Assignment Release	Assignment Due
1	09/02	Module 1, Topic 1, 2, 3	Lab 1	
2	09/09	Module 1, Topic 4, 5, 6	Quiz 1	Lab 1
3	09/16	Module 2, Topic 1, 2	Lab 2	Quiz 1
4	09/23	Module 2, Topic 3	Quiz 2, final project	Lab 2
5	09/30	Module 3, Topic 1, 2, 3, 4, 5	Lab 3	Quiz 2

6	10/07	Module 3, Topic 6, 7, 8	Quiz 3	Lab 3
7	10/14	Module 4, Topic 1, 2,	Lab 4	Quiz 3
8	10/21	Module 4, Topic 3, 4	Quiz 4	Lab 4
9	10/28	Module 5, Topic 1, 2, 3	Lab 5	Quiz 4
10	11/4	Module 5, Topic 4, 5	Quiz 5	Lab 5
11	11/11	Module 6, Topic 1, 2	Lab 6	Quiz 5
12	11/18	Module 6, Topic 3	Quiz 6	Lab 6
13	12/02	Final Review		Quiz 6, final project