**MYSQL – SEGURANÇA E CONTROLE DE ACESSO**

LUCAS LAMOUNIER GONCALVES DUARTE - 2016012688

KEVIN VIEIRA PEREIRA - 2016015385

RODRIGO APARECIDO SILVA MAIA - 2016013095

Itajubá, 20 de março de 2018

**Questão 1: Estudar as estruturas de índices disponíveis no seu SGBD. Detalhe a sintaxe de criação e remoção de índices.**

**Questão 2: Como listar os índices de uma tabela do banco?**

**Questão 3: Criar uma view no banco. É possível indexar essa view?**

**Questão 4: Quais ferramentas de análise de consulta seu SGBD oferece?**

**Questão 5: Implemente uma consulta ‘pesada’ no seu banco.**

**a) Verifique o tempo necessário para processar essa consulta.**

**b) Agora crie um índice e refaça a consulta. Diminuiu o tempo de consulta? Justifique o índice criado.**

**Questão 6: Avalie por meio de consultas e descreva a impressão do grupo sobre:**

**a) Índice de Hash**

**b) Índice composto**

**c) Índice em um campo BLOB**

**Questão 7: Quais são as formas possíveis de iniciar uma transação no SGBD?**

**Questão 8: Pesquise sobre o chamado SQL Injection (o que é, como prevenir).**

O chamado SQL Injection é um tipo de ataque que se baseia na manipulação do código SQL. Quando uma aplicação recebe um valor digitado pelo usuário e concatena isso a uma string com código SQL para uma consulta em um banco de dados, a maneira que esta string é concatenada pode gerar uma abertura para que partes de código SQL sejam enviadas para a variável que coleta os dados digitados pelo usuário e enviem para manipular a consulta pré-determinada no momento em que a concatenação é feita.

**Referências:**

BOROVSKA, Plamenka; LAZAROVA, Milena. Efficiency of parallel minimax algorithm for game tree search. In: **Proceedings of the 2007 international conference on Computer systems and technologies**. ACM, 2007. p. 14.