IFSP Araraquara Programação Web – TA
Prova Teórica Parte 1
Gabriel Albino (AQ3004775)

1. (1,5) Sobre SQL Injection (Injeção de comandos SQL), especifique se cada afirmação é verdadeira (V) ou falsa (F).
(V) As consultas SQL podem ser manipuladas para tentativa de desvio do processo de autenticação elaborado pelo desenvolvedor.
(F) A injeção direta de comandos SQL é uma técnica na qual se tenta criar ou alterar comandos SQL para expor dados sensíveis.
(F) Comandos de UPDATE não são suscetíveis a ataques de SQL Injection pelo fato de não ser possível manipular a cláusula SET.

Observação: Dados sensíveis são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

2. (1,0) Verifique cada item, de a) até d), e realize a correspondência entre o nome da função e sua descrição.
Observação: Deixe em branco para funções sem uma descrição correspondente.

a) Retorna um conjunto de resultados a partir da execução da declaração preparada.
b) Utilizada para preparar a instrução SQL possibilitando que ela seja executada diversas vezes no banco de dados.
c) Vincula os parâmetros a uma instrução SQL preparada.
d) Retorna a quantidade de linhas alteradas por uma instrução SQL válida.

(c) $stmt->bind_param()
( ) $stmt->execute()
(b) $conexao->prepare($sql)
(a) $stmt→get_result()
(d) $stmt->affected_rows