III Lista de Exercícios de Segurança de Sistemas
Prof. Manoel Ribeiro

1) A melhor forma para descobrir se uma aplicação está vulnerável a este tipo de ataque é verificar se todos os usos dos interpretadores separam claramente os dados não confiáveis do comando ou consulta. Para chamadas em linguagem estruturada de consulta, isso significa utilizar variáveis de ligação em todas as instruções preparadas e procedimentos armazenados, e evitar consultas dinâmicas.

O tipo de ataque citado no texto é conhecido como
A Key Logging.
B Buffer overflow.
C SQL Injection.
D Cross-Site Scripting (XSS).
E Cross-Site Request Forgery (CSRF).

2) Sabendo-se que ataques do tipo SQL Injection provocam a execução de comandos diretos no banco de dados da aplicação, uma das ações recomendadas para se diminuir o risco de ocorrência desses ataques é a de
A instalação de antivírus no servidor de banco de dados.
B utilização de funções que retirem a interpretação de caracteres especiais nas consultas SQL.
C mudança da linguagem de programação da aplicação.
D configuração de um serviço de monitoramento SNMP.
E mudança do servidor de banco de dados.

3) A ameaça de segurança em que o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação da entrada de dados de uma aplicação é conhecida como
A SQL Mixing.
B SQL False Query.
C SQL Fake Query.
D SQL Query Attack.
E SQL Injection.

4) Se houver suspeita de que um dos sistemas web da rede de uma organização está sob ataque do tipo SQL injection, é recomendada ao administrador do sistema web a ofuscação de nomes das tabelas e dos campos do SGBD usados por esse sistema, o que pode reduzir as chances de que tal ataque seja bem-sucedido. O simples aumento da segurança no acesso ao host em que se encontra o SGBD não fará que os dados armazenados no banco de dados deixem de ser expostos a consultas indevidas decorrentes de ataques do tipo SQL injection.
C Certo
E Errado

5) O Cross-Site Scripting (XSS)
I. executa no cliente web um código malicioso que, necessariamente, está armazenado no servidor acessado;
II. explora vulnerabilidades relacionadas à falta de validação dos dados de entrada do usuário em uma página web;
III. serve de base técnica para a realização de ataques como o SQL Injection e Script Injection.
Está correto o que se afirma em
A I, apenas.
B I e II, apenas.
C I e III, apenas.
D II e III, apenas.
E I, II e III.

5) Um ataque de SQL injection tenta explorar as características da linguagem SQL, principalmente do interpretador de comandos SQL, podendo danificar as informações armazenadas em um servidor, sem, entretanto, conseguir quebrar a confidencialidade desse conteúdo.
C Certo
E Errado

6) Os ataques de SQL Injection do tipo code injection se caracterizam por tentar modificar um comando SQL já existente mediante a adição de elementos à cláusula WHERE ou a extensão do comando SQL com operadores como UNION, INTERSECT ou MINUS.
C Certo
E Errado

7) Uma aplicação WEB de uma empresa foi invadida e, após análise, descobriram que o ataque utilizou a técnica de SQL Injection. Sobre essa situação, afirma-se que
A filtros de pacote podem ser configurados como mecanismo de proteção eficiente.
B a aplicação necessita de manutenção para correção desse tipo de falha.
C o kernel do sistema operacional do servidor envolvido estava desatualizado.
D o servidor envolvido precisará de mais placas de rede para evitar novos ataques.
E o banco de dados envolvido sofreu, na ocasião, um DoS, tornando-se indisponível.