Universidade Federal de Santa Catarina – UFSC
Departamento de Informática e Estatística – INE/CTC

Prof. Carina Friedrich Dorneles
dorneles@inf.ufsc.br

Leitura Complementar III

Nome: Fernando Paladini_____ Data de entrega: 29/12/2015

Instruções:

1. Ler o texto em http://en.wikipedia.org/wiki/SQL_injection
2. Responder as questões abaixo.
3. Salvar o arquivo de respostas e postar no Moodle até o dia **29/12/2015**.
4. Todas as respostas devem ser descritas de forma pessoal, ou seja, respostas copiadas do texto não serão consideradas corretas.
5. ***Não esqueça***: a atividade é **individual**, leituras **fora do prazo não** serão contabilizadas na nota.

Questões:

1. O que é "SQL Injection"?.

SQL Injection é uma técnica de injeção de código em programas e sites vulneráveis. É uma falha muito comum em websites e permite que comandos SQL arbitrários sejam executados (tais como dump de banco de dados, deleção de dados, adição de dados, etc.). Sempre está presente como uma das vulnerabilidades mais comuns e perigosas da web por grupos respeitados de segurança como OWASP.

2. Como é possível injetar, maldosamente, comandos SQL que prejudiquem um Banco de Dados?

Um dos exemplos mais clássicos é inserir queries SQL em inputs de formulários de contato ou inputs de busca. Quando o SQL não é "escaped" pelo programa/site, esta query pode acabar sendo executada no servidor e agindo no BD (seja retornando dados que não deveriam ser retornados ou ainda algo pior, como por exemplo modificando, adicionando ou removendo dados).

3. Explique alguma das soluções apontadas pelo autor, para solucionar o problema.

Algumas das soluções propostas é utilizar (1) checagem de padrões, para descobrir se o valor de um campo é uma representação válida do tipo que este dado deveria ter; (2) modificar permissões de usuários do banco de dados – basicamente alterar o usuário utilizado pela aplicação web para um que possua menos permissões sobre os dados do banco (ou modificar as permissões do usuário utilizado pela aplicação web); (3) identificar comandos SQL, verificando os valores dos inputs para tentar encontrar valores que tem algum significado no SQL e então tratá-los adequadamente; (4) utilizar instruções parametrizadas, onde um campo só pode armazenar um valor do seu tipo, e não queries SQL.

4. O artigo mostra alguns exemplos de casos reais de "SQL Injection". Escolha dois deles e explique.

Em Julho de 2008 o site malasiano da empresa Kaspersky foi invadido por um hacker turco que disse utilizar SQL injection no seu ataque.
Em Agosto de 2009, o Departamento de Justiça dos EUA considerou culpado um cidadão norte-americano e dois russos pelo crime de roubar 130 milhões de cartões de crédito usando SQL injection.