Tarefa realizada no dia : 07/04

Representando a atividade **Login - SQL Injection**

Duração dos testes: 1 horas

Duração total da atividade: 1 horas e 40 min.

**Objetivo**: Submeter entradas maliciosas no sistema através de injeção de códigos SQL na página de Login de modo a fazer a aplicação web executar ações não autorizadas. Exemplos: expor dados de usuários cadastrados na base de dados e tipo de SGBD utilizado por essa base de dados.

**Resultados**:

**Tentativa 1:** Verificar se o campo Login é vulnerável a injeção de código SQL fazendo uso da técnica de concatenação de aspas simples.

Supondo que fazendo uso dos dados de entrada a aplicação aguarda receber as informações e executar a seguinte consulta na base de dados: SELECT login FROM usuarios WHERE login = ‘DadoFornecido’ , inserir uma string com uma aspa simples extra como entrada para o campo Login para tentar provocar falha na instrução a ser executada no interpretador de SQL da aplicação.

Entradas: Login = admin’

**Resultado**: Passou no teste. A aplicação está fazendo tratamento de dados de entrada não permitindo a injeção de instruções SQL através do campo de Login.

**Tentativa 2:** Inserir uma string com uma distribuição adequada de aspa simples e comentários inline como entrada para o campo Login para não provocar falha na instrução a ser executada no interpretador de SQL da aplicação. Dessa forma, tentar forçar o interpretador de SQL da aplicação a ignorar tudo que vier após o comentário inline.

Fonte sintaxe utilizada para comentários inline SBGDS:

<http://dev.mysql.com/doc/refman/5.7/en/comments.html>

<http://docs.oracle.com/cd/B28359_01/appdev.111/b28370/comment.htm>

<https://technet.microsoft.com/pt-br/library/ms188621(v=sql.105).aspx>

Entradas:

admin’ or 1=1 #

admin’ or 1=1 --

obs.: Não apenas o usuário admin seria consultado, mas qualquer usuário cadastrado no sistema já que 1=1 é sempre verdadeiro.

**Resultado**: Passou no teste.

**Tentativa 3:** Inserir uma string com fazendo uso de aspa simples sozinha para completar a entrada ao efetuar a pesquisa. Esperando que uma possível query de consulta semelhante a essa seja executada SELECT login from usuarios WHERE login = ‘admin’ or ‘a’=’a’.

Entradas:

admin’ or ‘a’=’a

**Resultado:** Passou no teste