Tarefa realizada no dia : 18/04

Representando a atividade: **Consulta Servidor - 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 Consulta servidor de modo a fazer a aplicação web executar ações não autorizadas. Exemplos: expor dados de usuários cadastrados na base de dados.

**Resultados**:

**Tentativa 1:** Verificar se o campo Siape é vulnerável à 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 siape FROM servidores WHERE siape= 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: Siape= 1000’

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

**Tentativa 2:** Inserir uma string com uma distribuição adequada de aspa simples e comentários inline como entrada para o campo Siape 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.

Entradas:

1000 or 1=1 #

1000 or 1=1 --

obs.: Não apenas o servidor com siape 1000 seria consultado, mas qualquer usuário cadastrado no sistema já que 1=1 é sempre verdadeiro.

**Resultado**: Passou no teste.