Respostas - SQL Injection

Pergunta 1: Explique com suas palavras qual o papel do caractere Apostrofo (') na parte grifada em amarela abaixo, do Ponto e Virgula (;) na parte grifada em amarelo e do caractere traco traco (--) parte grifada em amarelo, no exemplo dado abaixo, que representa um ataque de SQL INJECTION:

SELECT id, nome, sobrenome FROM autores WHERE nome =

'jo'; DROP TABLE autores ; --' AND sobrenome = 'silva';

RESPOSTA 1:

O caractere apostrofo (') e utilizado em SQL para delimitar valores de strings. No exemplo dado, quando o atacante insere o apostrofo apos "jo", ele finaliza a string de forma prematura, permitindo que a sequencia de comandos subsequentes seja interpretada como instrucoes SQL independentes.

O ponto e virgula (;) indica o final de uma instrucao SQL, permitindo que uma nova instrucao seja iniciada. Isso e explorado pelo atacante para adicionar uma nova consulta SQL, neste caso, um comando para excluir a tabela "autores".

O traco duplo (--) introduz um comentario em SQL, ignorando qualquer texto que venha apos ele na mesma linha. Isso garante que a parte restante da consulta original (AND sobrenome = 'silva') seja tratada como comentario e nao cause erros de sintaxe.

Pergunta 2: Considerando a tela de Login abaixo, e considerando que a mesma nao tem protecao alguma contra SQL Injection. Explique como um atacantes poderia se aproveitar dessa vulnerabilidade, para realizar o acesso sem saber o usuario ou a senha:

RESPOSTA 2:

Respostas - SQL Injection

Um atacante poderia explorar a vulnerabilidade de SQL Injection inserindo um payload no campo de login. Por exemplo, no campo de "usuario", o atacante poderia inserir:

' OR '1'='1

E deixar o campo de senha vazio ou inserir qualquer valor irrelevante. Isso geraria uma consulta SQL como:

SELECT * FROM usuarios WHERE username = '' OR '1'='1' AND password = '';

A condicao '1'='1' sempre sera verdadeira, permitindo que o atacante acesse o sistema sem precisar de um nome de usuario ou senha valido.