SEMINÁRIO

Anderson Soares da Silva 2150875
Maria Eduarda Pedroso 2150336
Mariana Gonçalves Rodrigues 2151014

1-Dentre os SGBDs citados, escolhemos o PostgreSQL. Ele é um SGBD gratuito e de código aberto, com uma grande comunidade de desenvolvedores e suporte para diversos tipos de dados, incluindo geoespaciais.

2-SQL Injection é um tipo de ataque cibernético que explora vulnerabilidades em aplicativos que utilizam banco de dados. Uma das formas de realizar o ataque é por meio da inserção de código malicioso na consulta SQL. Por exemplo, suponha que um formulário de login seja vulnerável a SQL Injection. O atacante pode digitar no campo de nome de usuário uma entrada mal-intencionada como " ' or 1=1; --", que, quando enviado para o banco de dados, faz com que a consulta SQL resultante seja algo como:

SELECT * FROM users WHERE username='' or 1=1; --' AND password=''

Nesse caso, o ataque injetou código malicioso no campo de nome de usuário para que a consulta SQL retorne todos os registros da tabela de usuários (1=1 sempre é verdadeiro) e comente o restante da consulta para evitar erros. O atacante pode, em seguida, acessar a conta de qualquer usuário sem precisar saber a senha.

3-Há várias maneiras de proteger um aplicativo contra ataques de SQL Injection. Uma delas é através do uso de parâmetros preparados (prepared statements), que permitem que os dados de entrada sejam tratados como valores em vez de código SQL. Os parâmetros preparados impedem que o SQL injetado afete o comportamento da consulta, pois o SGBD trata o valor inserido como um dado e não como uma instrução SQL.
Outra maneira é através da validação dos dados de entrada, restringindo os caracteres especiais que podem ser inseridos em campos como nome de usuário e senha. Além disso, é recomendado manter o SGBD atualizado com as últimas correções de segurança e evitar o uso de contas com privilégios elevados para o acesso ao banco de dados.