

Prevenção

Como podemos evitar o SQL Injection?

Selecione uma alternativa

- A** O desenvolvedor deve colocar na query que vai para o banco de dados os parâmetros que estão sendo passados pelo usuário, pois dessa forma, o processo de consulta será mais rápido, não permitindo assim possíveis tentativas de SQL Injection
- B** Não há como ser evitado, a esperança é que nenhum usuário tente algo parecido.
- C** O desenvolvedor deve separar os parâmetros que são enviados pelo usuário, da query que está indo ao banco de dados, através por exemplo, do uso da classe PreparedStatement em Java.
- D** A única forma seria comprar uma solução proprietária da Oracle, capaz de verificar a existência dessas vulnerabilidades em nossas aplicações WEB.