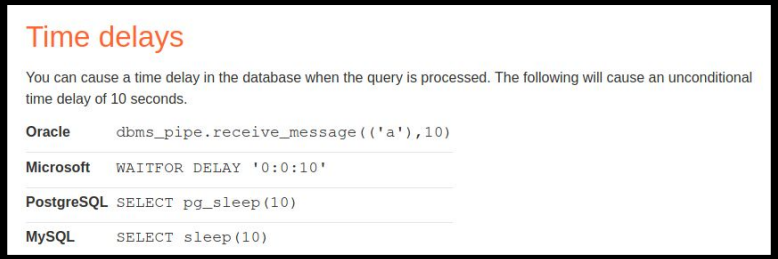
SQL Injection

Blind SQL Injection

Delays Temporais

Ataques de SQL Injection com a técnica de delays temporais consiste na análise do tempo demorado pela aplicação para devolver as respostas, com o intuito de entender se estas injeções foram ou não interpretadas e executadas. Assim sendo será necessário adaptar a injeção para este efeito. No entanto, dependendo do banco de dados da aplicação, as funções utilizadas para criar os delays temporais poderão ser diferentes.
Exemplo:



Time delays

You can cause a time delay in the database when the query is processed. The following will cause an unconditional time delay of 10 seconds.

Oracle	`dbms_pipe.receive_message(('a'),10)`
Microsoft	`WAITFOR DELAY '0:0:10'`
PostgreSQL	`SELECT pg_sleep(10)`
MySQL	`SELECT sleep(10)`

SELECT trackid **FROM** TrackedUsers **WHERE** tracking_id = '**$tracking_cookie**';

Injeção: ' || (SELECT pg_sleep(10))--
Query: **SELECT** trackid **FROM** TrackedUsers **WHERE** tracking_id = ' || (SELECT pg_sleep(10))--';

Explicação da Injeção

Neste caso, utilizamos a função pg_sleep(10). Assim sendo, se a resposta da aplicação demorar 10 segundos, podemos concluir que estamos perante um banco de dados PostgreSQL e que a aplicação é vulnerável a SQL Injection.