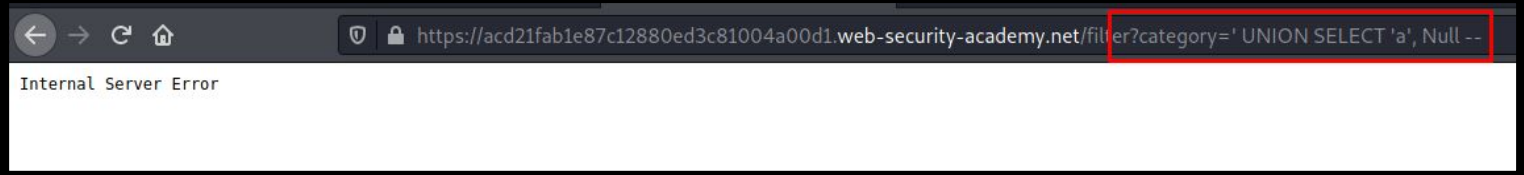
SQL Injection

Bancos de Dados Oracle

Descobrir Número de Colunas

Quando usamos o operador UNION em bancos de dados ORACLE, temos obrigatoriamente que especificar as tabelas dos respectivos SELECTs. Se as tabelas em cada SELECT não forem especificadas, vai ser gerado um erro SQL.



Embora o nome das tabelas do banco de dados não seja do nosso conhecimento, os bancos de dados ORACLE têm uma tabela default chamada "dual", a qual podemos utilizar para o efeito. Assim sendo, podemos usar a seguinte injeção SQL:

' UNION SELECT 'a', Null FROM dual--

https://docs.oracle.com/cd/B19306_01/server.102/b14200/queries004.htm