MySQL

SQL Injection - UNION Attack

Descobrir Número de Colunas

Anteriormente verificamos que podemos descobrir o numero de colunas de uma determinada tabela através do operador order by. No entanto, também podemos descobrir o número de colunas através do **UNION,** dependendo da query que está a ser feita.

IMPORTANTE: Para utilizar o operador UNION o número de colunas seleccionadas deve ser igual para os diferentes SELECTs. Ou seja, se o primeiro select for um SELECT * (todas as colunas), através do UNION conseguimos saber quantas colunas tem a tabela.

Tabela: Conta_Usuario

nome	cidade	idade
Barbara	Rússia	25
Joana	Argentina	30
Wendell	Portugal	10

Query: SELECT * FROM Conta_Usuario UNION SELECT null;
Resultado: ERRO - Número de colunas seleccionadas diferentes

Query: SELECT * FROM Conta_Usuario UNION SELECT null, null;
Resultado: ERRO - Número de colunas seleccionadas diferentes

Query: SELECT * FROM Conta_Usuario UNION SELECT null, null, null;
Resultado:

Barbara	Rússia	25
Joana	Argentina	30
Wendell	Portugal	10
null	null	null

Descobrir Número de Colunas

IMPORTANTE: Para utilizar o operador UNION o número de colunas seleccionadas deve ser igual para os diferentes SELECTs. Ou seja, se o primeiro select for um SELECT nome (apenas uma coluna), através do UNION conseguimos apenas saber quantas colunas estão a ser seleccionadas e não quantas colunas tem a tabela.

Tabela: Conta_Usuario

nome	cidade	idade
Barbara	Rússia	25
Joana	Argentina	30
Wendell	Portugal	10

Query: `SELECT nome FROM Conta_Usuario UNION SELECT null;`
Resultado:
Barbara
Joana
Wendell
null

Query: `SELECT * FROM Conta_Usuario UNION SELECT null, null;`
Resultado: ERRO - Número de colunas seleccionadas diferentes

Query: `SELECT * FROM Conta_Usuario UNION SELECT null, null, null;`
Resultado: ERRO - Número de colunas seleccionadas diferentes

Descobrir Colunas com texto

IMPORTANTE: Quando utilizamos o operador UNION, as colunas seleccionadas nos diferentes SELECTs devem, de forma correspondente, ser do mesmo data type (INT, VARCHAR, etc..).

Tabela: Conta_Usuario

nome	n_irmaos	idade
Barbara	0	25
Joana	3	30
Wendell	2	10

Query: `SELECT * FROM Conta_Usuario UNION SELECT 'a', null, null;`
Resultado:

Barbara	Rússia	25
Joana	Argentina	30
Wendell	Portugal	10
a	null	null

Query: `SELECT * FROM Conta_Usuario UNION SELECT null, 'a', null;`
Resultado: ERRO - 2ª coluna não é do tipo String

Query: `SELECT * FROM Conta_Usuario UNION SELECT null, null, 'a';`
Resultado: ERRO - 3ª coluna não é do tipo String