Web4: SQL injection - Exploitation steps

Web4: SQL injection - Exploit steps. In this article, TipsMake.com will learn about SQL Injection exploitation steps.

1. Detection

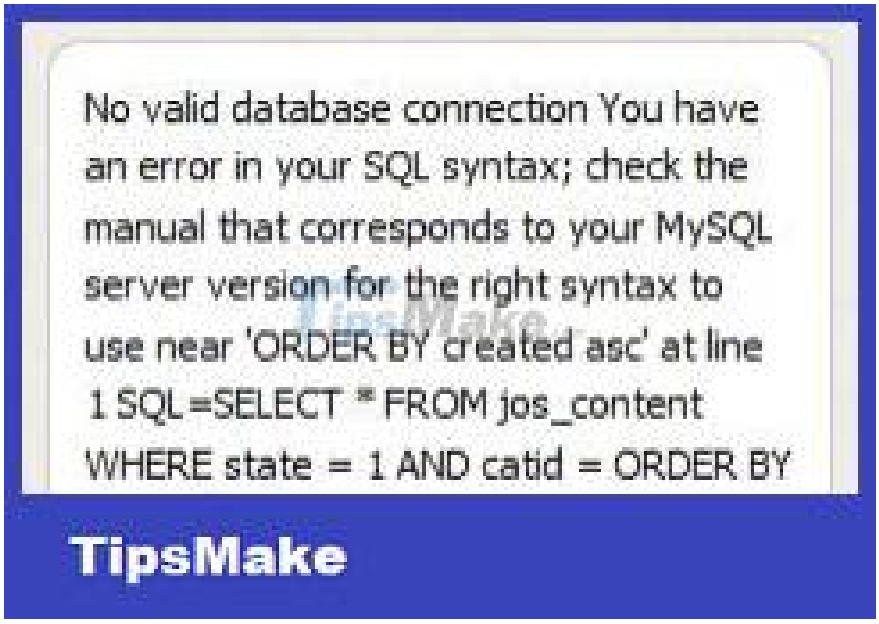
A common way to detect whether a web application has an SQL injection error is to add to the query meta characters in database management systems, such as single quote, comma. double quote, semi colon and comment characters (--, ##, /**/)… and wait and see how the web application will handle that query.

2. Collecting information about the database management system

When detecting an application that has SQL injection errors, the next job to do is to collect information about the database management system that the application is using, this information includes the type of database (mysql, mssql , oracle…) and its version.

To determine the type of administration that the application is using, we can evaluate it according to many criteria. Judging by the error message:

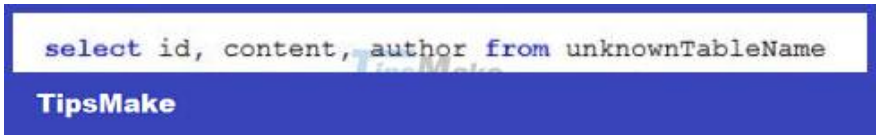
Error message from MS-SQL – IIS



In the case above, the error message says that the web application uses MySQL.

3. Specify the number of columns in the select . clause

When exploiting SQL injection, we often use one or more subselect clauses, this is done via the union keyword. Union is the keyword used to combine the results of many select clauses, so in each select clause, the number of fields must be equal and equal to the number of fields selected in the original select clause. Consider a specific example:



Here, in the initial select clause, select 3 fields: id, content and author. Therefore the select clause after the union keyword also needs to have exactly 3 fields. If the number of select fields in the select clause after the union is not equal to the number of fields selected in the first select clause, we will get an error message. So how to know exactly how many fields the first select clause selects. We can do a trial by incrementing the number of columns in the select clause after the union (starting at 1). When no error message appears, that is the number of columns to look for.

Another, faster way to do this is to use 'order by'. In DBMS the keyword 'order by' is used to sort the order of the records obtained in the select clause. After order by can be a column name to specify that the result will be sorted by the value of that column (can be ascending or descending). After order by can also be the ordinal number of that column. If the value after order is greater than the number of columns selected, we will see an error message.

4. Identify information

After getting the basic information, we will proceed to exploit SQL injection to get the database or perform other behaviors through this vulnerability.

Specify table and column names: we have many ways to do this, one of them is 'guess' because it is fast and in specific cases this is very useful. For example, some common table names such as: user, users, admin, administrator, staff, account, manager . (note the prefix tbl_ is very often used by programmers to name the table).

A more formal way to know the table and column names is to use the information_schema object. This object provides information about the tables, columns, views and procedures. of the database.