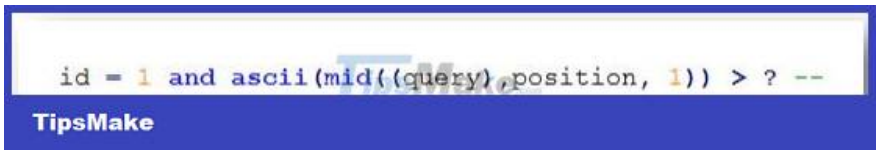
Web3: SQL injection - Exploit directions

In this article, TipsMake.com will learn about SQL Injection exploits with you.

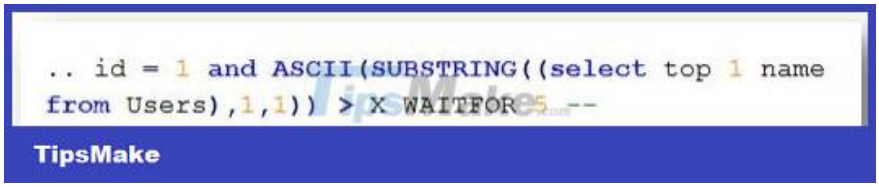
1. Boolean based and Time based Blind SQL injection

Boolean based: The basis of this technique is the comparison of true and false to find each character of information such as table name, column name. Therefore, with the range of alphanumeric values ??(including uppercase, normal), and some special characters, the matching becomes very difficult and requires a lot of time. Therefore, exploiting bugs is mainly carried out using tools.

In the Blind SQLi technique, we also have many different methods. The difference between these methods is the optimization of time. We will learn about blind SQL injection and its methods in the following topics.



Time based: Like boolean based attacks, differing only in inference, it relies on the processing time of the database and then returns the results to determine whether the SQL query executed successfully.



2. Union query based

This is a common method when exploiting SQL injection. Its basis is to use the union keyword to combine the results of select clauses, thereby obtaining information from the database. You can see examples of using this method in SQL injection exploitation in the previous topics: Web1: SQL Injection - The most common exploit route and Web2: SQL Injection - Other exploits.

3. Batch query

This is a method to apply the ability to execute multiple SQL statements at the same time of several database management systems and the support of programming languages. This method is very powerful and causes

immediate danger to the system. By adding an Update, Insert or Delete command line, the data in the web application's database is no longer intact.

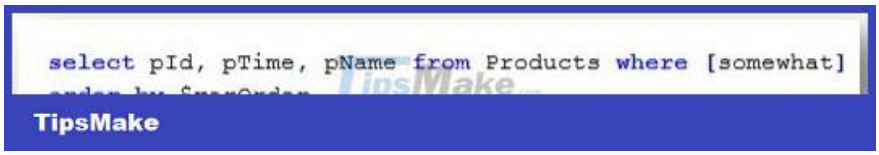
We can insert the following SQL statement to delete a table in the database:

4. Order by clause

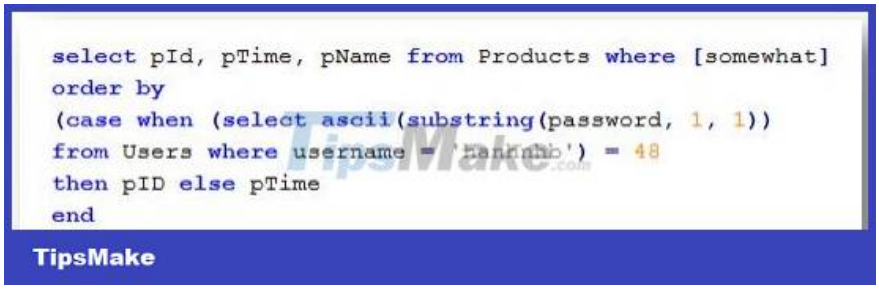
Unlike the above methods, the inject content is in the where clause. In this method, we will try to inject script code into the order clause. Let's take a look at the following scenario:

The programmer wants to list the company's products including the following information: Product Code, Product Name, Date . and has the function for users to customize whether they want to sort by date, according to product name or code.

The query is constructed as follows:



In this case we cannot directly add a sub select clause via the union keyword as always. One way to exploit that is to use BATCHED QUERY or you can refer to the following way:



In the above method, we were able to inject a sub select, but obviously this implementation must now be combined with the BOOLEAN BASED BLIND SQLI technique.

You finished reading the article "**Web3: SQL injection - Exploit directions**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
