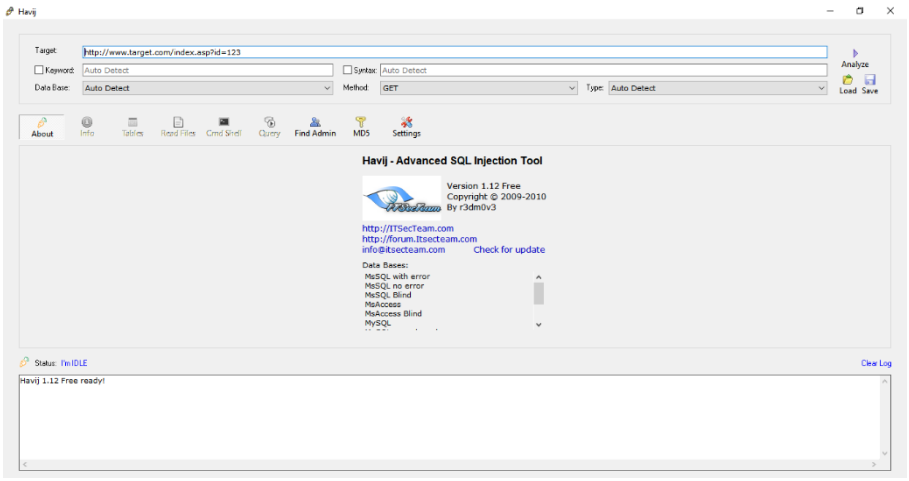
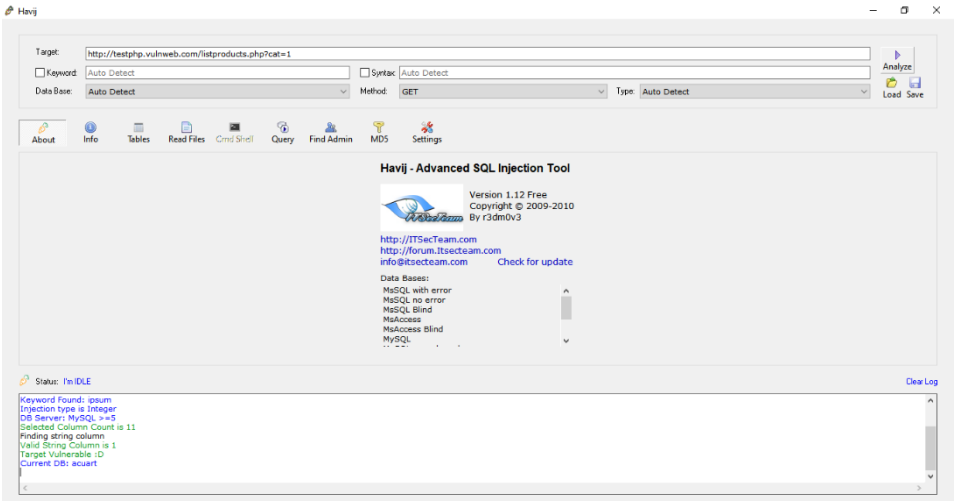
Perform SQL injection on a website by using Havij Tool

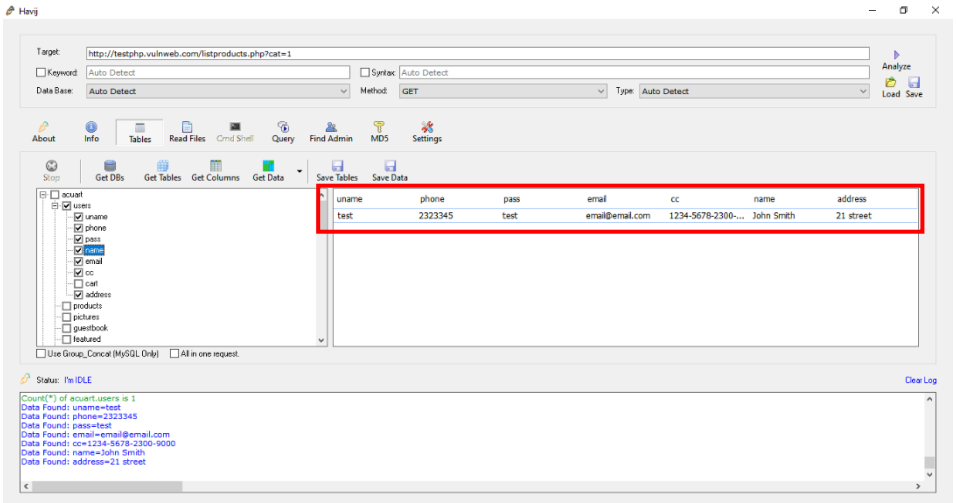
1.SQL injection is used to designed with a user-friendly GUI that makes it easy for an operator to retrieve the desired data. Such ease of use may be the reason behind the transition from attacks deployed by code-writing hackers to those by non-technical users.



2. Injection on the website http://testphp.vulnweb.com .



3.Checking for the user data which is stored in the website database.



We can observe that, there is user data which are username, phone number, email-id, password, address, etc. Hence, using “havij tool” will be useful to obtain information about the clients from the company or education website.

How to Prevent an SQL Injection

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes.

It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

If you discover an SQL Injection vulnerability, for example using an Acunetix scan, you may be unable to fix it immediately. For example, the vulnerability may be in open source code. In such cases, you can use a web application firewall to sanitize your input temporarily.

One of the best practices to identify SQL injection attacks is having a web application firewall (WAF). A WAF operating in front of the web servers monitors the traffic which goes in and out of the web servers and identifies patterns that constitute a threat. Essentially, it is a barrier put between the web application and the Internet.

A WAF operates via defined customizable web security rules. These sets of policies inform the WAF what weaknesses and traffic behaviour it should search for. So, based on that information, a WAF will keep monitoring the applications and the GET and POST requests it receives to find and block malicious traffic.