Havij 1.15

Advanced SQL Injection Tool

User Manual

IT Security Research & Penetration Testing Team

http://ItSecTeam.com

Author:

r3dm0v3

What's new?

Features

Installation

- **What is Havij?**
- **What is SQL Injection?**
- **Who should use Havij?**
- **Installing Havij**
- **Uninstalling Havij**
- **Registering Havij**
- **Check for update**

Getting Started

- **Fast starting with Havij**
- **Saving and loading the project**
- **Getting Info**
- **Data base and tables data Extraction**
  - Data extraction
  - Filtering data
  - Changing data extraction start row
  - Using Group_Concat
  - Extracting data of one row at once
  - Saving data
  - Updating data
  - Deleting data
  - Inserting data
- **Reading files**
- **Executing system commands on target**
- **Query**
- **Finding admin login page**
- **Cracking MD5 hashes**

Manual Injection

- **Choosing Database**
- **Choosing Variable Type**
- **Defining Keyword**
- **Defining Syntax**
- **Defining Syntax for Blind injections**
- **Choosing Method**
- **Injecting into Forms (POST Method)**

Settings

- **Basic Settings**
  - Using proxy
  - Replacing Space character
  - Showing Injections
  - Injecting URL rewrite pages
  - Injecting into Cookie, User-Agent, etc
- **Advanced Settings**
  - Authentication is needed for injection
  - Defining character set to use in blind injections
  - Changing Headers
  - Time Out
  - Default Injection Value
  - Avoid using strings
  - Bypass illegal union
  - Try different syntaxes in union injection
  - Follow redirections
  - Column count
  - Do not find columns count in MsSQL with error
  - Bypass mod_security
  - Bypass WebKnight WAF
  - Custom Replacement
  - Time based method delay

- Blind table prefix
- Blind column prefix
- Table list for blind guessing
- Column list for blind guessing

What's new?

- Webknight WAF bypass added.
- Bypassing mod_security made better
- Unicode support added
- A new method for tables/columns extraction in mssql
- Continuing previous tables/columns extraction made available
- Custom replacement added to the settings
- Default injection value added to the settings (when using %Inject_Here%)
- Table and column prefix added for blind injections
- Custom table and column list added.
- Custom time out added.
- A new md5 cracker site added
- bugfix: a bug releating to SELECT command
- bugfix: finding string column
- bugfix: getting multi column data in mssql
- bugfix: finding mysql column count
- bugfix: wrong syntax in injection string type in MsAccess
- bugfix: false positive results was removed
- bugfix: data extraction in url-encoded pages
- bugfix: loading saved projects
- bugfix: some errors in data extraction in mssql fixed.
- bugfix: a bug in MsAccess when guessing tables and columns
- bugfix: a bug when using proxy
- bugfix: enabling remote desktop bug in windows server 2008 (thanks to pegasus315)
- bugfix: false positive in finding columns count
- bugfix: when mssql error based method failed
- bugfix: a bug in saving data
- bugfix: Oracle and PostgreSQL detection

Features

item	Free version	Pro version
1. Supported Databases with injec on method	✓	✓
MsSQL 2000/2005 with error	✓	✓
MsSQL 2000/2005 no error union based	✓	✓
MsSQL Blind	✗	✓
MsSQL time based	✗	✓
MySQL union based	✓	✓
MySQL Blind	✓	✓
MySQL error based	✓	✓
MySQL time based	✓	✓
Oracle union based	✓	✓
Oracle error based	✗	✓
PostgreSQL union based	✗	✓
MsAccess union based	✓	✓
MsAccess Blind	✗	✓
Sybase (ASE)	✓	✓
Sybase (ASE) Blind	✗	✓
2. HTTPS Support	✗	✓
3. Proxy support	✓	✓
4. Automa c database detec on	✓	✓
5. Automa c type detec on (string or integ	✓	✓
6. Automa c keyword detec on (finding difference between the posi ve and negative response)	✓	✓
7. Trying different injec on syntaxes	✓	✓
8. Op ons for replacing space by /**/,+,... against IDS or filter	✓	✓
9. Avoid using strings (magic_quotes similar filters bypass)	✓	✓
10. Manual injec on syntax suppo	✓	✓
11. Manual queries with result	✗	✓
12. Bypassing illegal union	✓	✓
13. Full customizable h p headers (like referer,user agent and ..	✓	✓
14. Load cookie from site for authen ca no	✓	✓
15. Http Basic and Digest authentication	✓	✓
16. Injecting URL rewrite pages	✗	✓
17. Bypassing mod_security web application firewall and similar firewalls	✗	✓
18. Bypassing WebKnight web application firewall and similar firewalls	✗	✓
19. Real time result	✓	✓
20. Guessing tables and columns in mysql<5 (also in blind) and MsAccess	✓	✓
21. Fast getting tables and columns for mysql	✓	✓
22. continuing previous tables/columns extraction session	✗	✓
23. Executing SQL query in Oracle database	✗	✓
24. Custom keyword replacement in inejctions	✗	✓
25. Getting one row in one request (all in one request)	✗	✓
26. Dumping data into file	✗	✓

27. Saving data as XML format	✗	✓
28. View every injection request sent by program	✗	✓
29. Enabling xp_cmdshell and remote desktop	✗	✓
30. Multiple tables/column extraction methods	✗	✓
31. Multi thread Admin page finder	✓	✓
32. Mul thread Online MD5 cracke	✓	✓
33. Getting DBMS Informations	✓	✓
34. Getting tables, columns and data	✓	✓
35. Command executation (mssql only)	✓	✓
36. Reading system files (mysql only)	✓	✓
37. insert/update/delete data	✓	✓
38. Unicode support	✗	✓

Installation

What is Havij?

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.
It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system.
The power of Havij that makes it different from similar tools is its injection methods. The success rate is more than 95% at injec ng vlnerable targets using Havij.
The user friendly GUI (Graphical User Interface) of Havij and automated settings and detections makes it easy to use for everyone even amateur users.

What is SQL Injection?

SQL Injection is common web application vulnerability due to insufficient validation on user inputs. An attacker can inject some SQL commands into the original query written by the developer to change the result to what he/she wants and execute his/her commands. This work (injecting SQL commands) is called Exploitation that can cause sensitive data disclosure, changing data, deleting data or even whole system compromise!

Who should use Havij?

All security professionals, Web administrators, web application developers, penetration testers, everyone who wants to test his/her sites security and all hack and security researchers can use Havij.

Installing Havij

Requirements for installing Havij:

- Windows operating system
- Havij setup file
- Internet Explorer 5.5 or above
- 8MB free space on hard disk

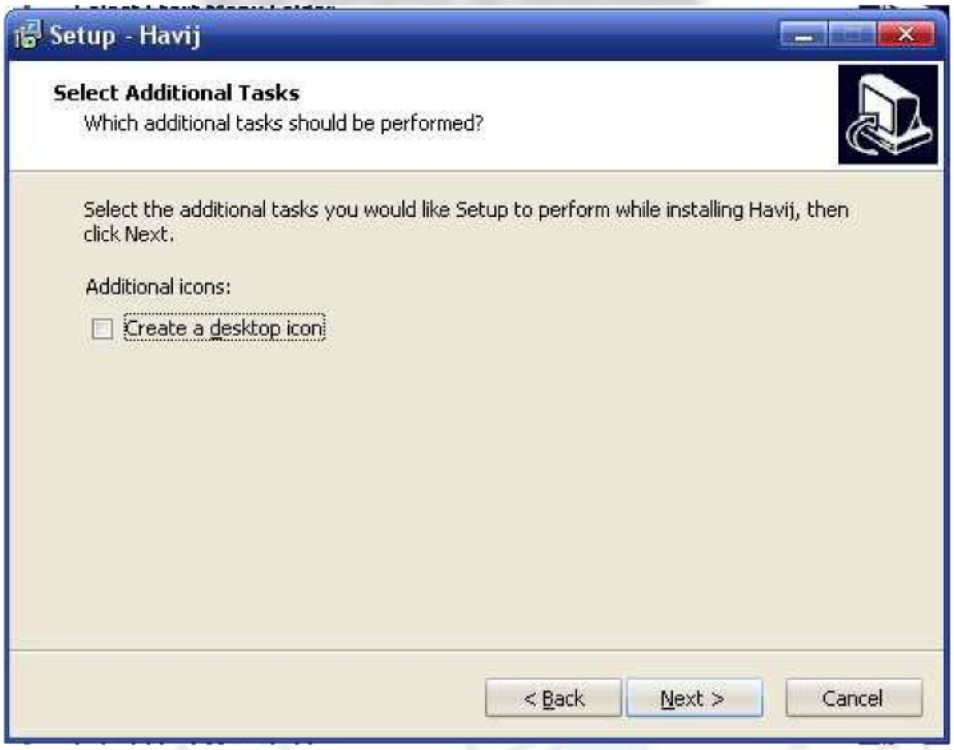
Make sure that you have downloaded the setup file from ItSecTeam.com or somewhere else that you trust.

For starting the installation run the setup file. Below window should be displayed.

Click on 'Next' to continue the installation and below window will be shown.

At the above window you should specify where you want to install Havij. You can use the default path and click on 'Next' to go to next step.

You should enter the Start Menu folder that will be created for program at the above screen. Click on 'Next' after doing it.

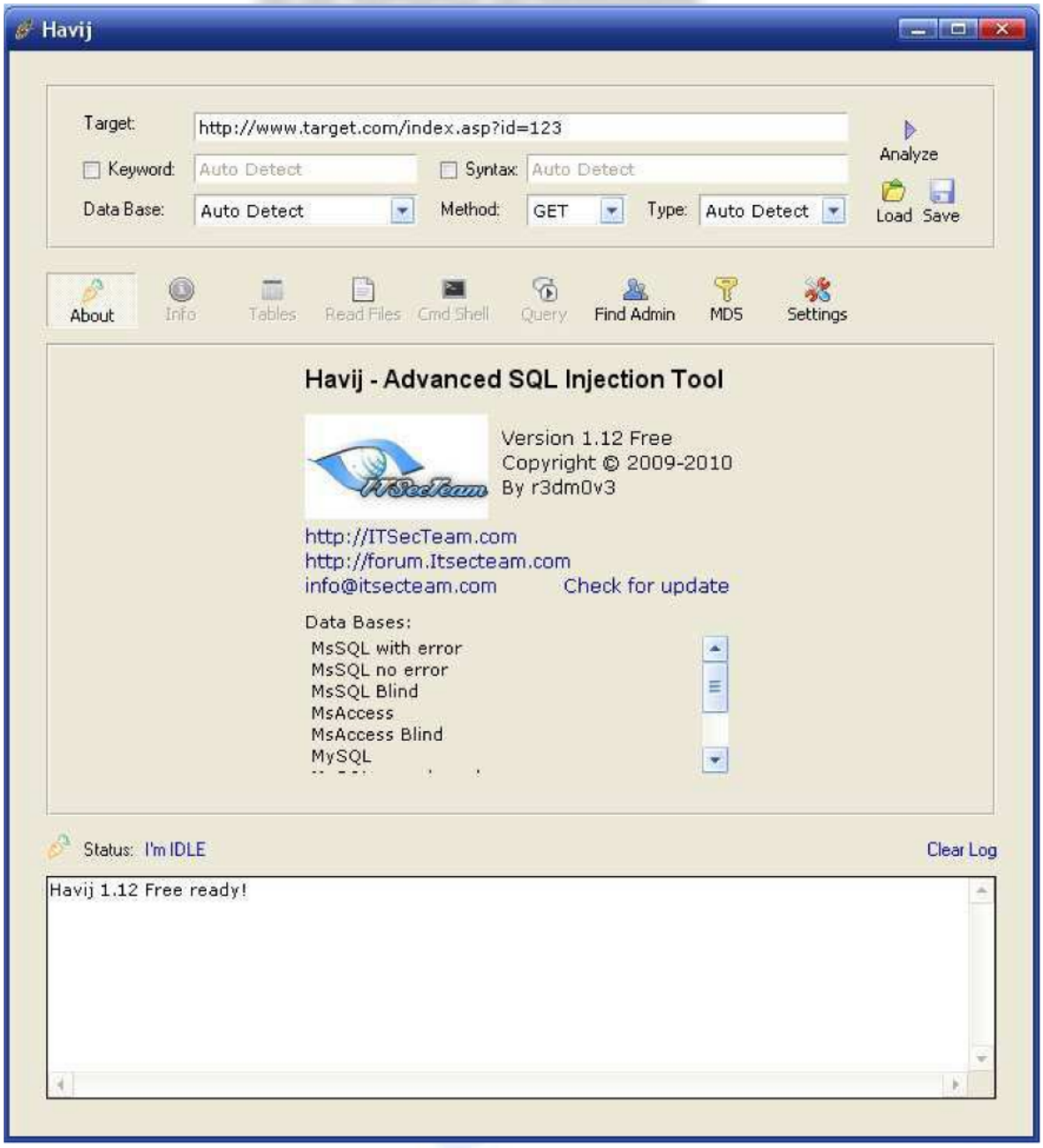


If you would like to create a shortcut for the Havij on your desktop check the 'Create a desktop icon' checkbox. With clicking on 'Next' button following information about the install should be shown.

Click on 'Install' to start the installation.

After the installation finished, following window will be shown.

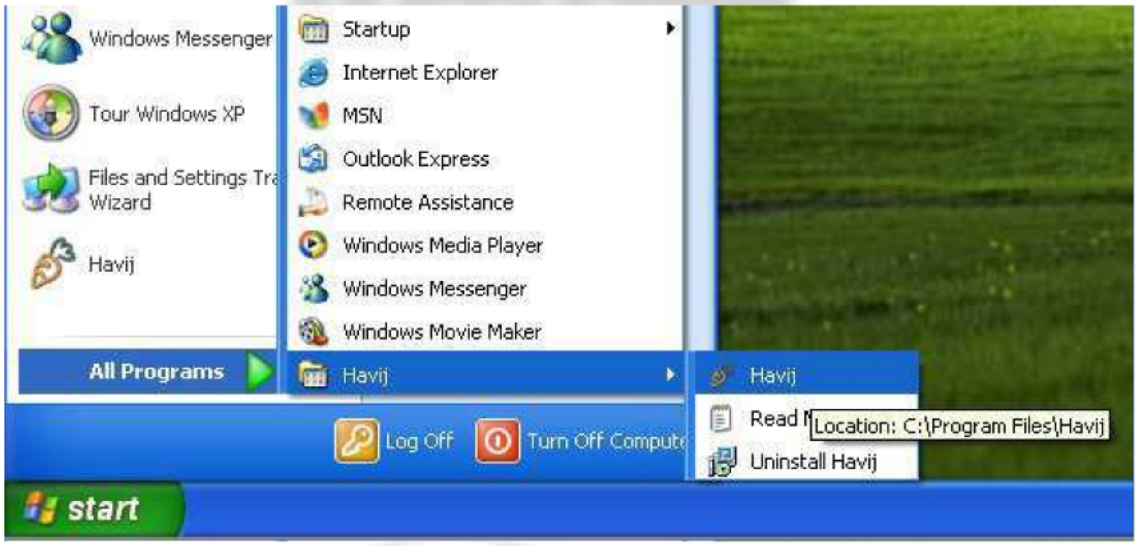
If you would like to run Havij after installation, check 'Launch Havij' checkbox and click 'Finish' button.



Havij installation successfully finished.

For running Havij you can click on Havij icon in Start Menu folder or run it from desktop shortcut.

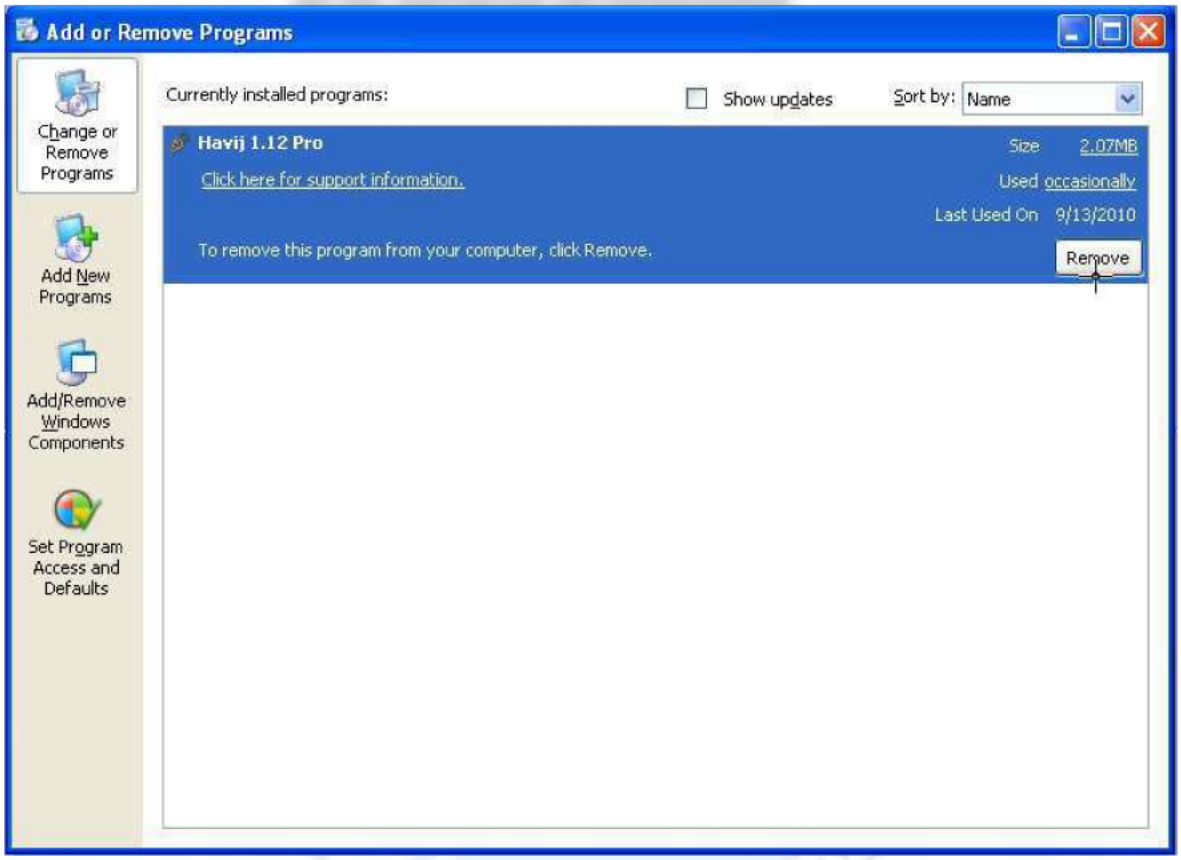
Important: Havij needs accessing to the internet for injecting the targets. If you use firewall software, give the required permissions to the Havij.



The above steps are same in all versions.

Uninstalling Havij

For uninstalling Havij go to Control Panel and open 'Add or Remove Programs' then find Havij in list.



Click on 'Remove' to uninstall begins. The uninstall program will ask you that are you sure you want to uninstall it or not, click on 'Yes'. Havij removal process will proceed automatically and at last the following message will be shown.

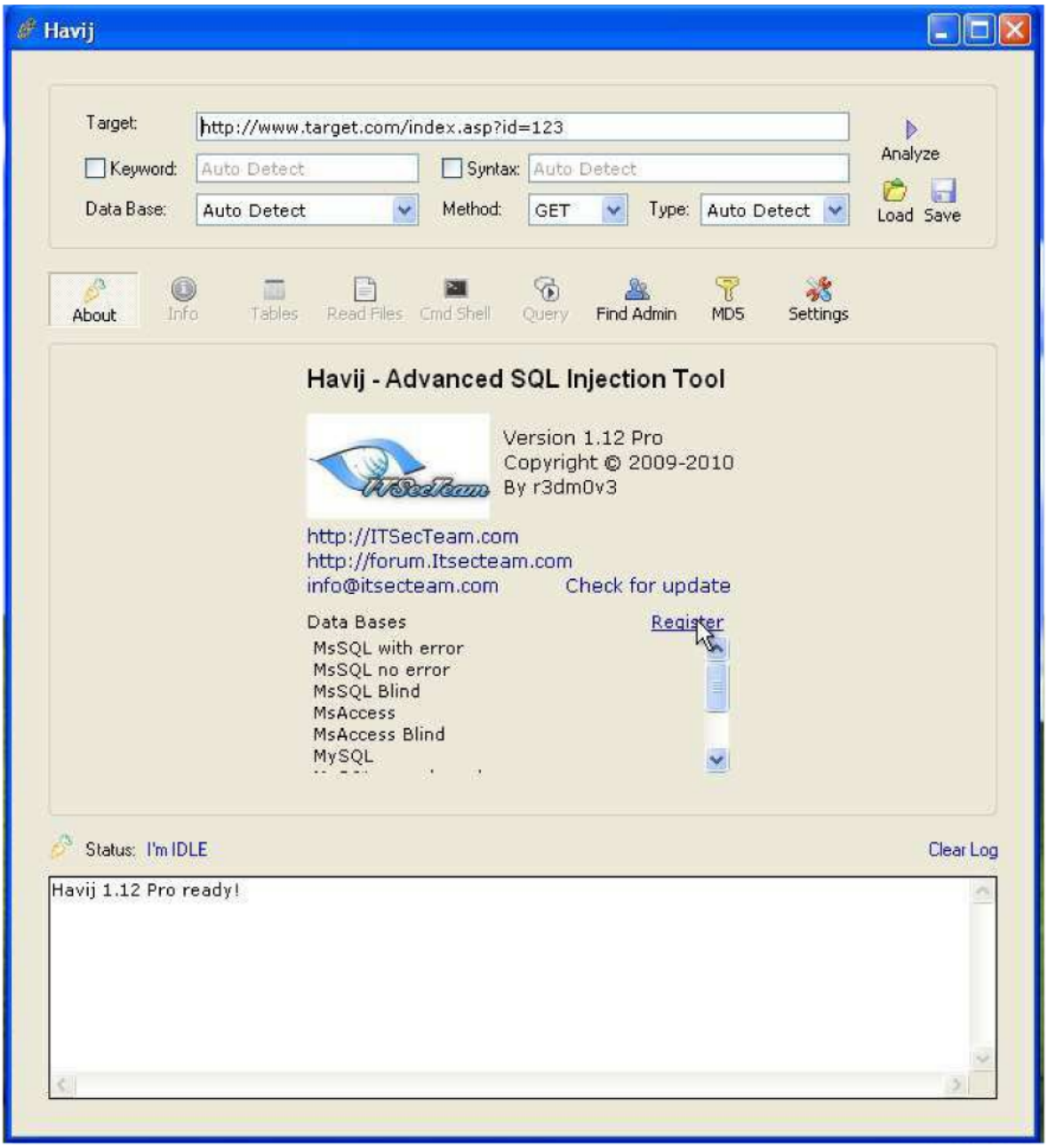
The above steps are same in all versions.

Registering the software

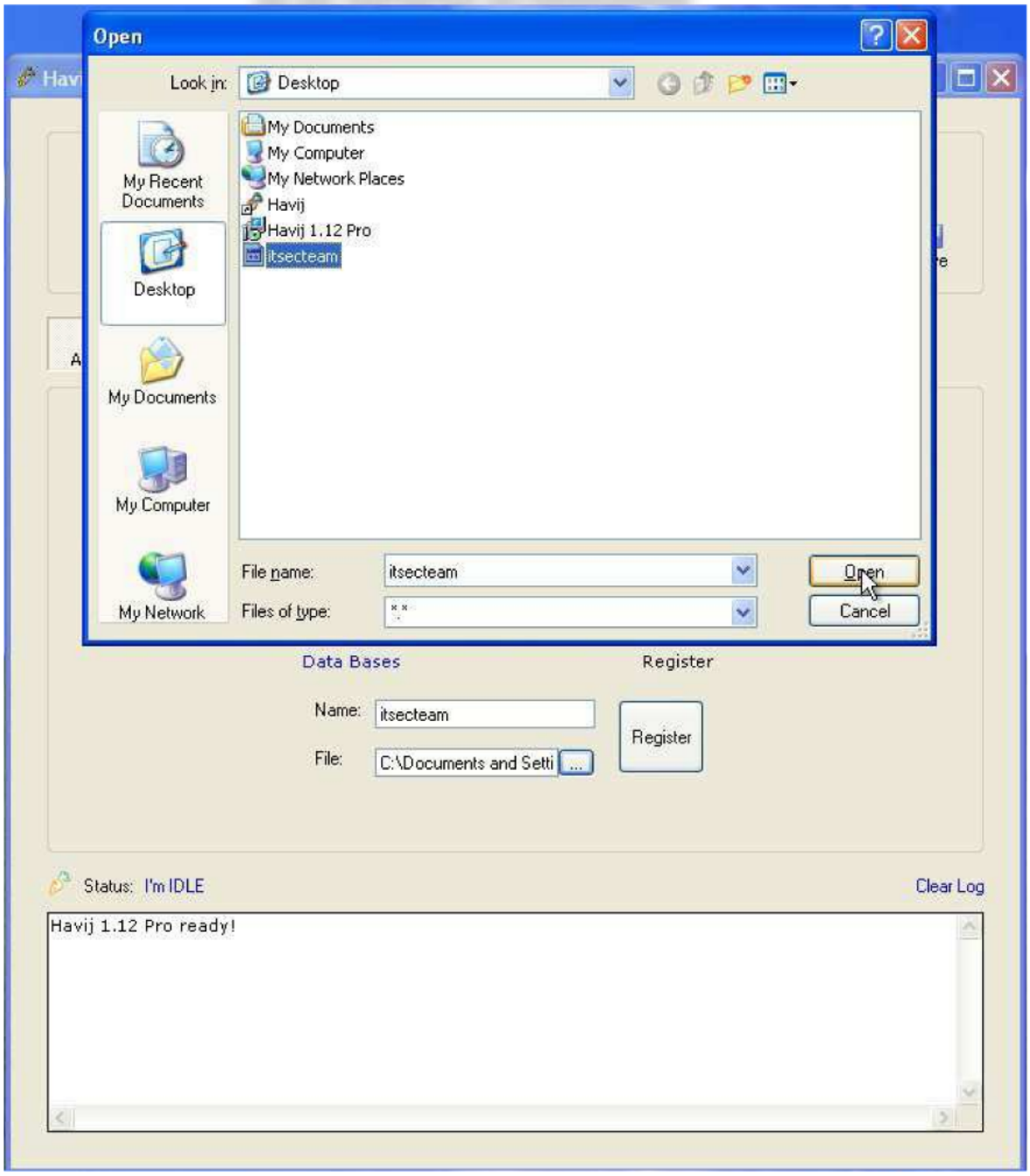
Before you can register the software you should buy a license. For purchase detail contact info@itsecteam.com

After receiving the license follow these steps to register.

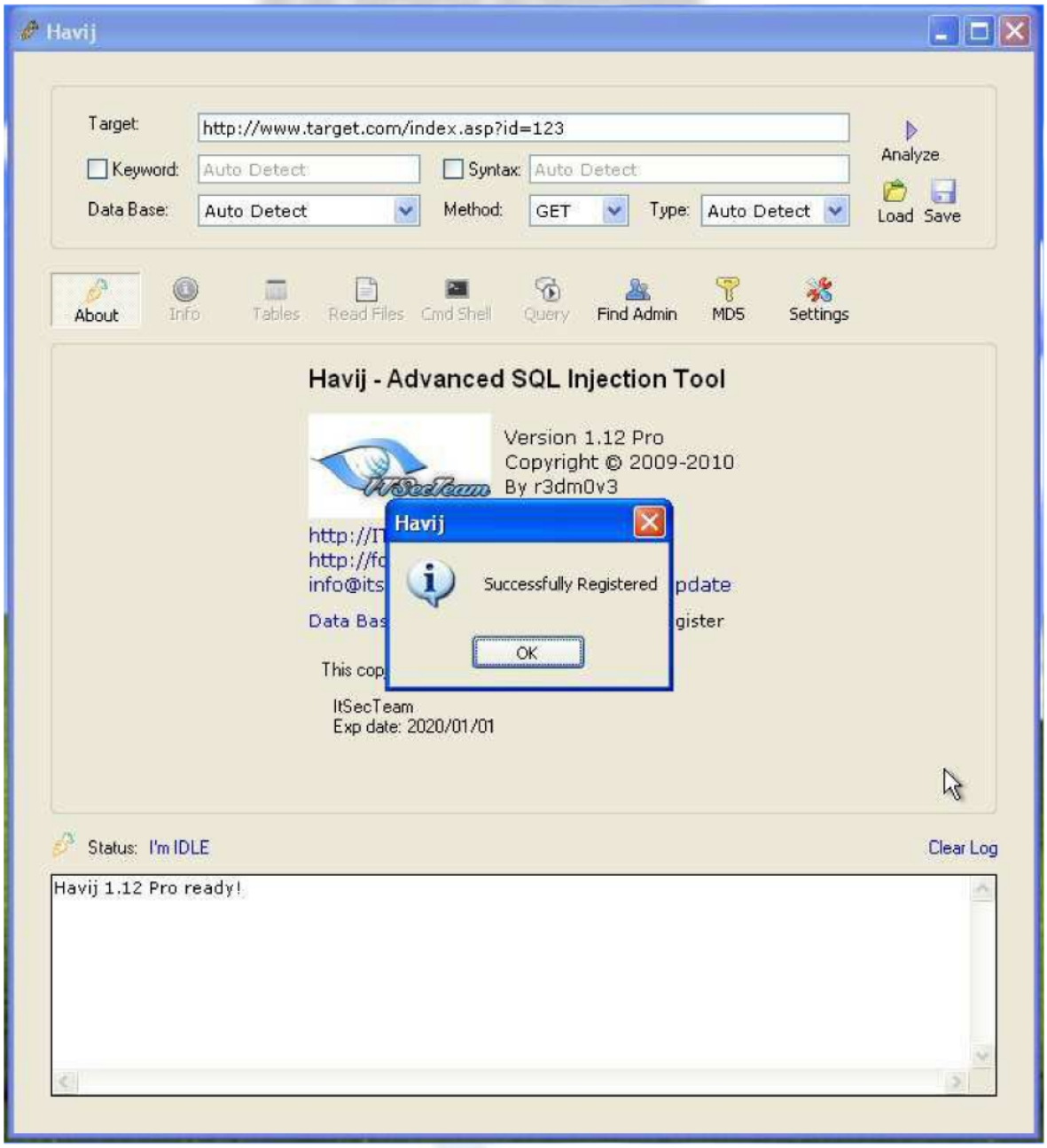
1- Connect to the internet
2- In about window click on 'Register'



3- In 'Name' text box enter the name that your license is registered to.
4- In 'File' text box browse the license file.
Important: both name and license file will be send to you after purchase.



5- Now click on 'Register' and wait until license validation process completes. The following message should be shown if everything is correct.



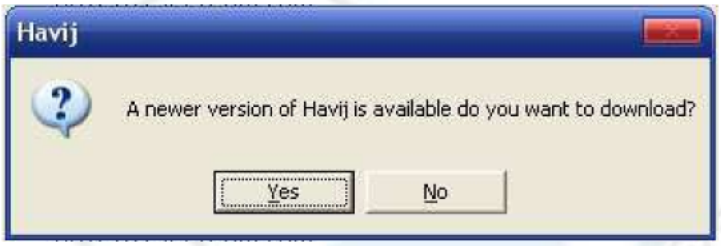
Important: if you use firewall, make sure that Havij has enough permission to access the internet. If you had problem with registering, turn off your firewall and repeat all steps.

Important: using one license at two or more different machines will make the license expired!

Check for update

In about window click on 'Check for update' to program automatically check for new updates. If there be no updates the following message will be shown.

If there is a new version available, this message will be displayed.



If you would like to download the new version, click on 'Yes' button.

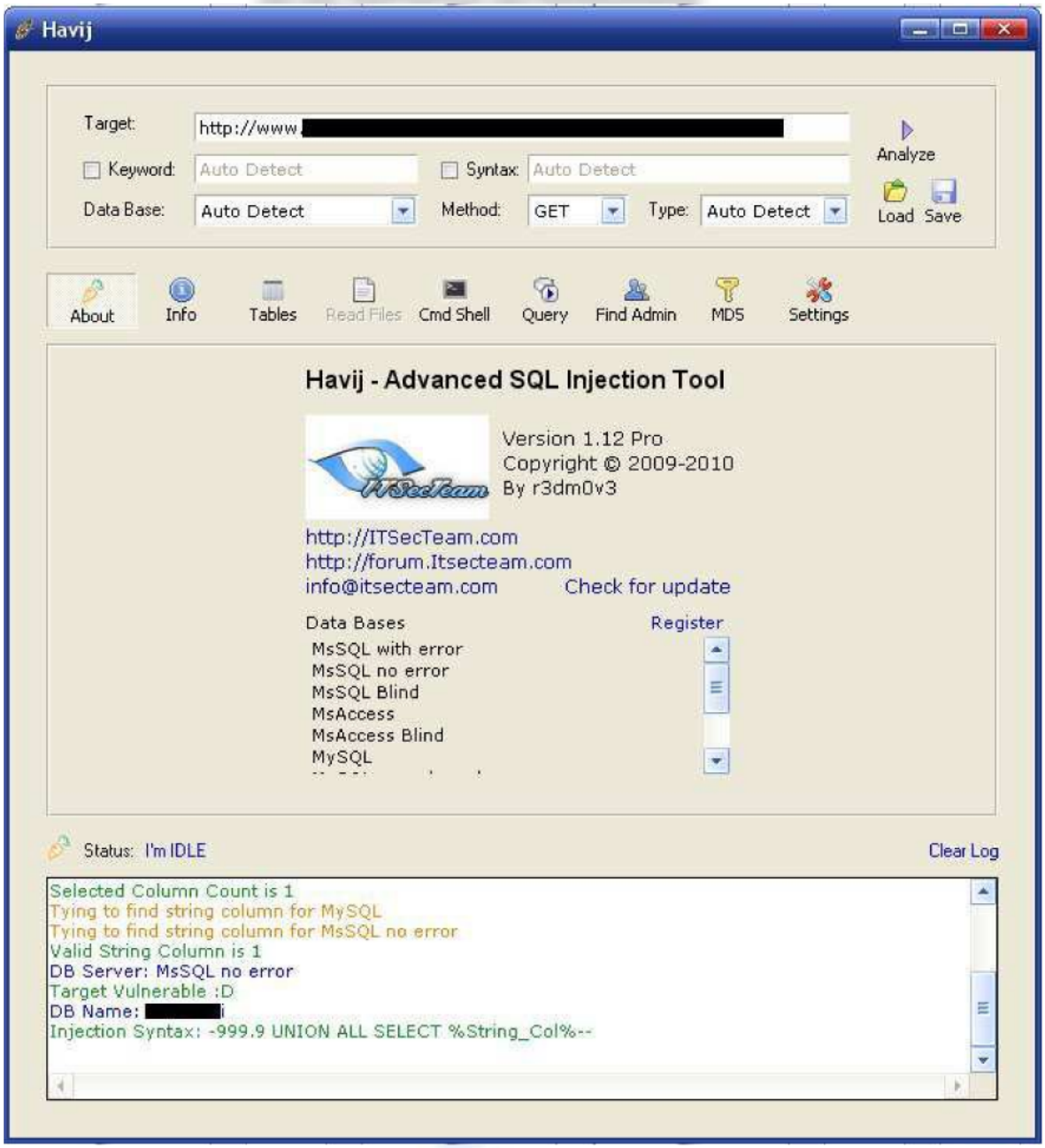
Getting Started

Fast starting with Havij

You don't need so much technical information for using Havij however it has a lot of settings for professional users. To start using Havij you just need a vulnerable URL to SQL Injection bug.

How to find a vulnerable web site? You can use web vulnerability scanner programs and available tools for finding SQL Injection vulnerabilities and also you can use Google. It doesn't matter if you are not sure that page is vulnerable or not, Havij will check it. You can use Havij to check security of your own website.

Why should the target address be like 'http://www.target.com/index.php**?id=123**'? Because the vulnerable page must have at least one input that Havij could inject into in.



Save and loading the project

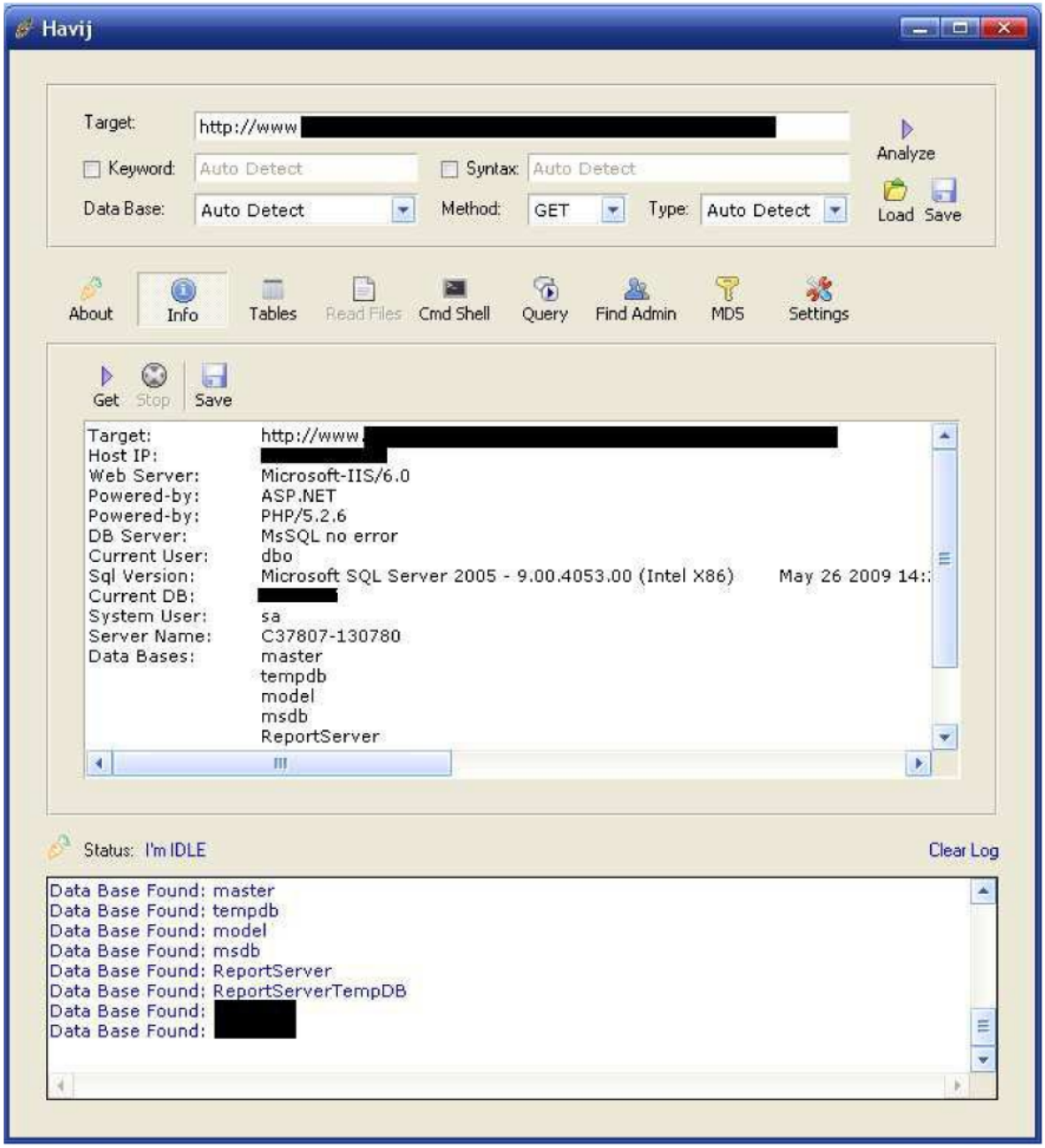
For increasing your speed in testing targets you can save them after analyze and injecting, so you won't need to analyze them again for further use.

To save the project after analyze, click on 'Save' button below the 'Analyze' and select a file.

For loading a project and continuing it click on 'Load' button near the 'Save' button and load the saved project.

Getting Info

After analyzing finished, if the target is vulnerable, the 'Info' button on the top menu will be activated. You can use this option to get some info like database username, current database, server name and more. To do this click on 'Info' then click on 'Get' extracted info will be shown in the text box. You can save this info by clicking on 'Save' button.

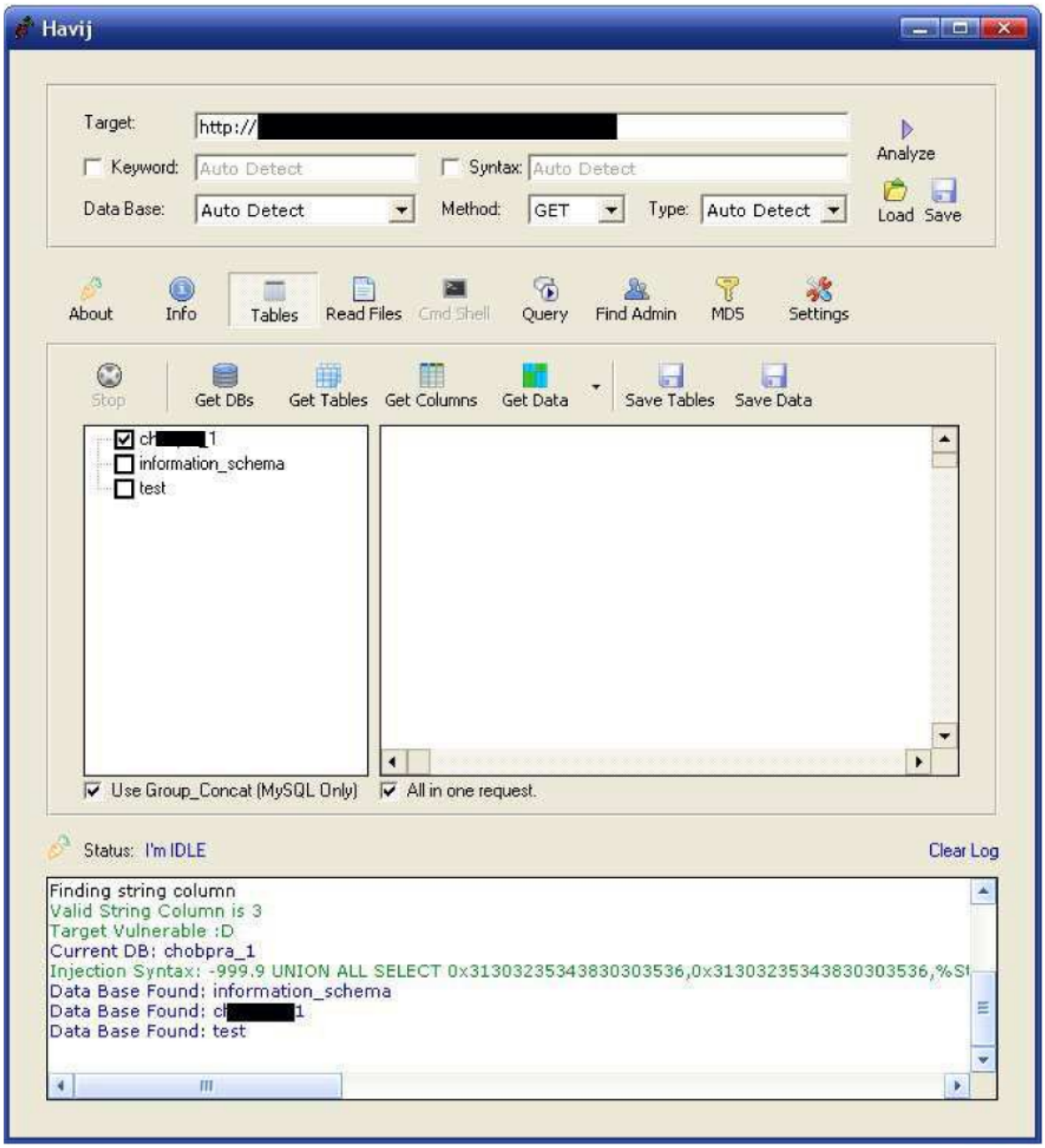


Data base and tables data Extraction

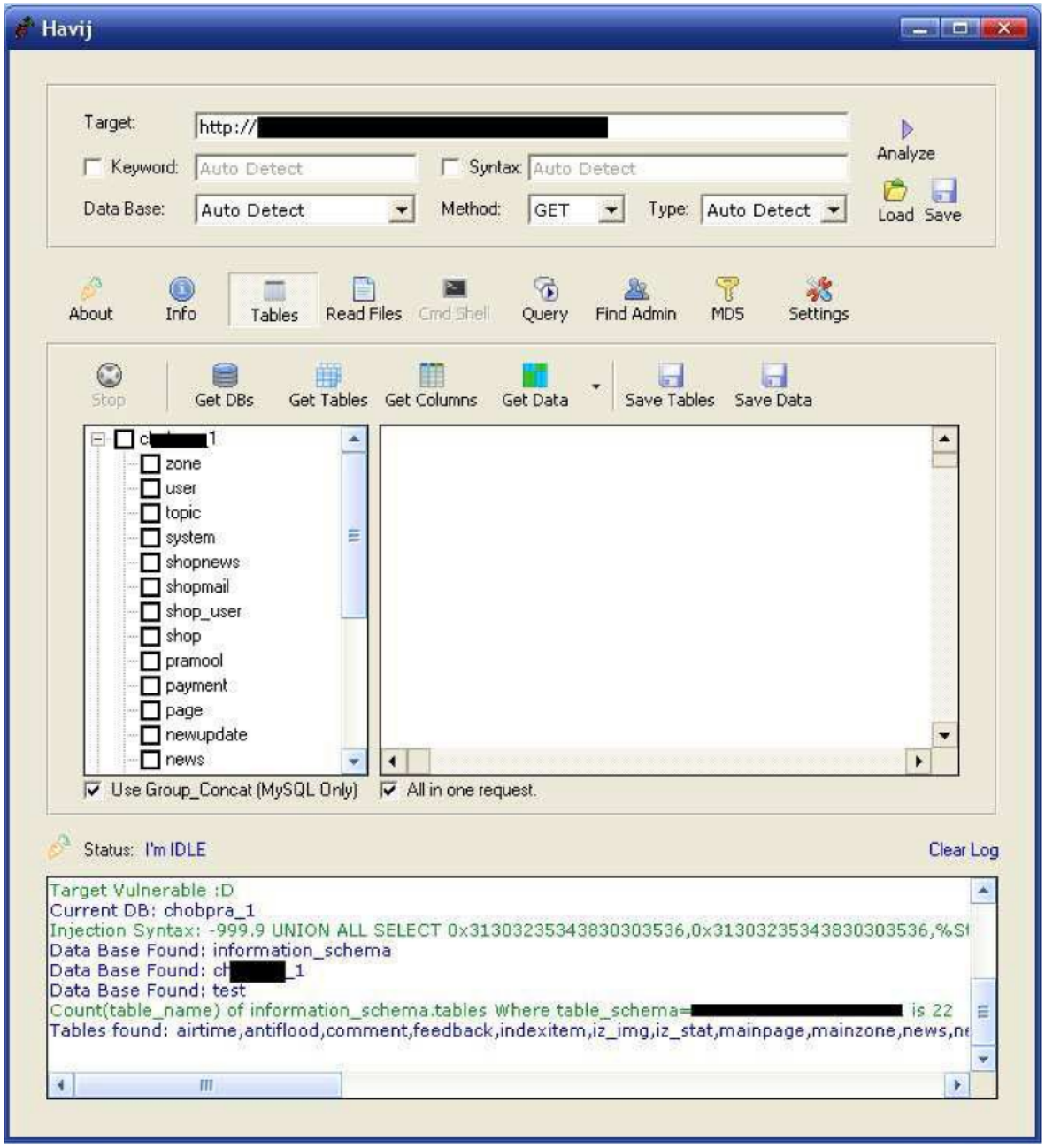
Data extraction

Using the 'Tables' button on the top menu you can find server's database and tables. Click on 'Tables' to display the data extraction window. On the left window databases and tables will be shown and on the right window extracted data. After analyzing, target's default database is selected in the left window, to get all databases click on 'Get DBs'.

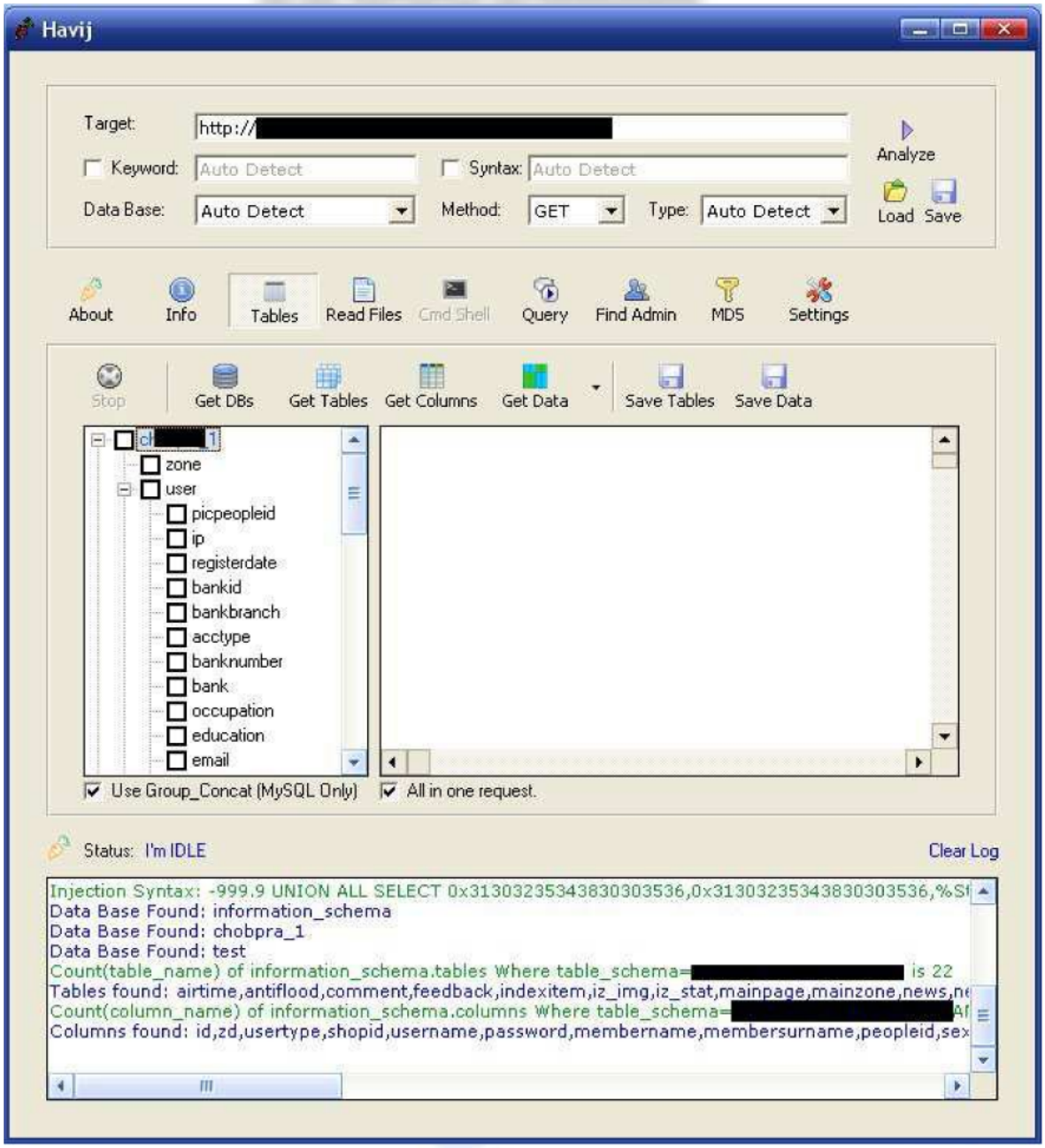
Important: the current database user may doesn't have enough privileged to access other databases.



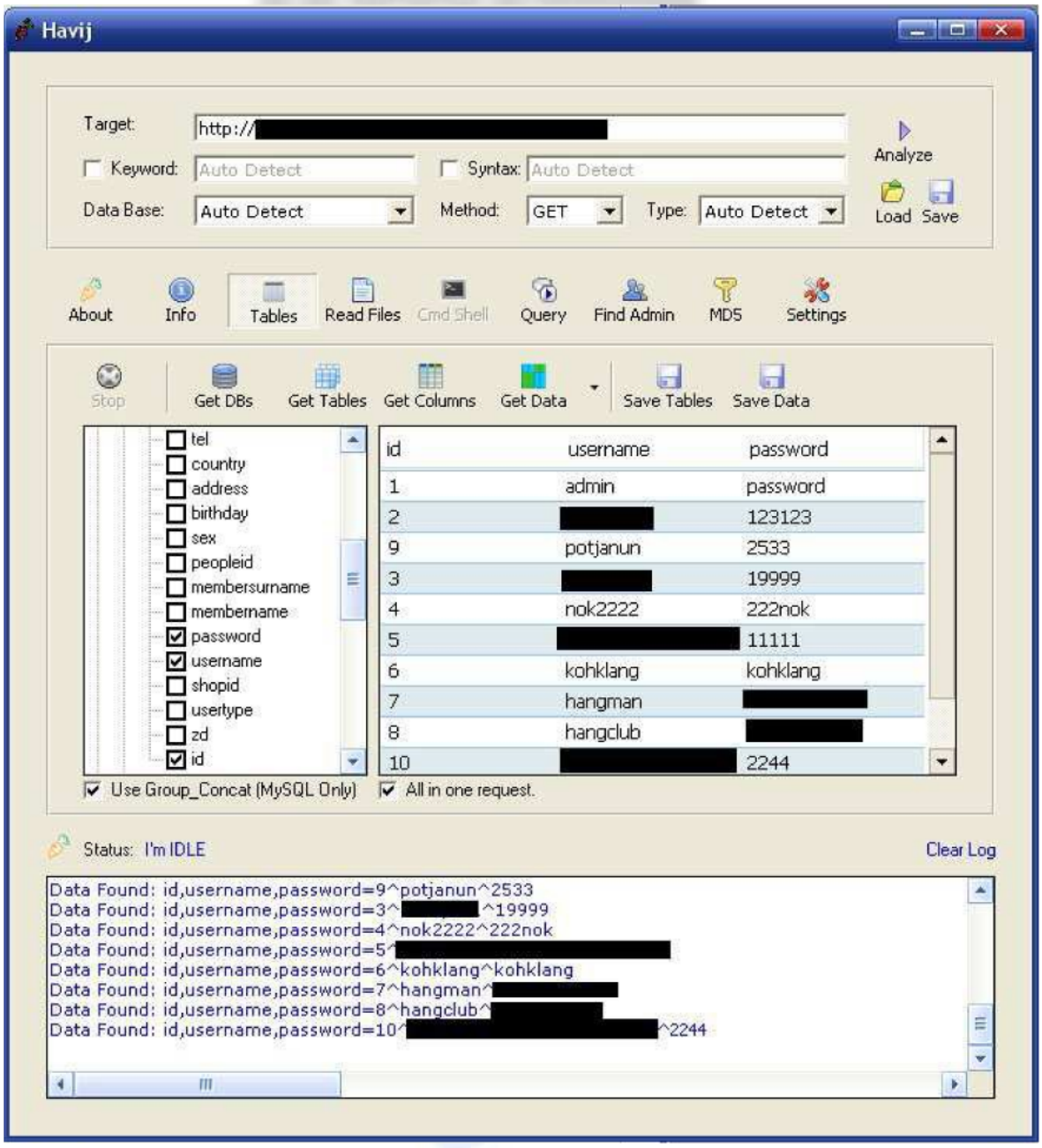
To view tables, check one or more database from the left list and click on 'Get Tables'. Tables will be listed under the databases.



To get columns first choose one or more tables and then click on 'Get Columns'.



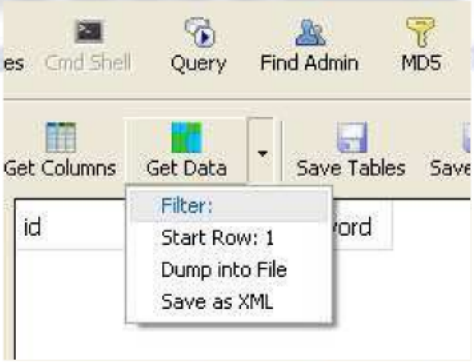
To get data from tables select some columns (check their checkbox) and then click on ‘Get Data’.



Filtering the data

Sometimes you're looking for a specific data in database, in these cases you can use filter to find what you want faster.

To set a filter on data extraction click on arrow near the 'Get Data' button and select 'Filter' from the opened menu. Now enter your condition and click on 'Get Data' to get all data that fit your condition.



For example if you want to get the record that its 'Username' column is 'Admin' enter the following condition as filter:

Username='Admin'

To remove filter leave it empty.

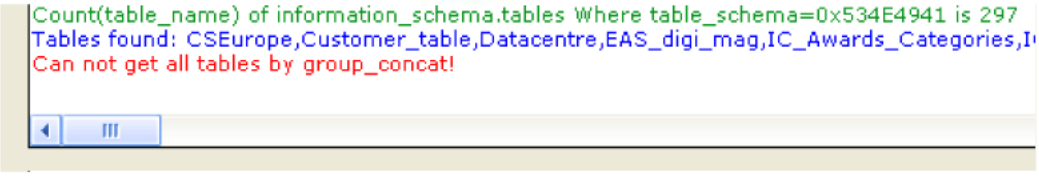
Changing Data extraction start row

The 'Get Data' extracts data from first row to the last row by default. If you want to change the start row click on arrow near the 'Get Data' and select 'Start Row' then enter the number of data extraction start row. Now click 'Get Data' to start data extraction. At any time you can click on 'Stop' to stop data extraction.

Using Group_Concat

This option is below the database and tables list. If it is activated it means that you can use Group_Concat function in MySQL database to extract all tables and databases in one request.

Important: if there are so many tables or columns, Havij may not be able to extract all of them using Group_Concat option. The following message will be displayed in this case.



To get tables or databases normally uncheck this Group_Concat and retry.

Extracting data of one row at once

Using 'All in one request' option below the extracted data window you can get 1 row data of all columns you selected in one request.

Important: if selected columns are too much, Havij may not be able to extract all data using this method. To get data normally uncheck 'All in one request' and retry.

Saving Data

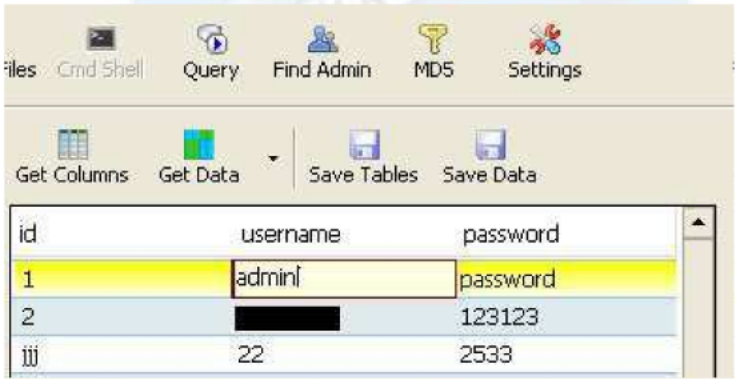
For saving tables in html format click on 'Save Tables' and for saving data click on 'Save Data'.

If you would like to save data in XML format click on arrow near the 'Get Data' and select 'Save as XML' then select a file to save. Now click on 'Get Data', extracted data won't be displayed in form and will be saved directly in XML file. This is good for getting so much data.

If you would like to dump data like MySQL, click on arrow near 'Get Data' and select 'Dump into File' then click 'Get Data' then extracted data won't be displayed and will be directly in file. This is good for getting so much data.

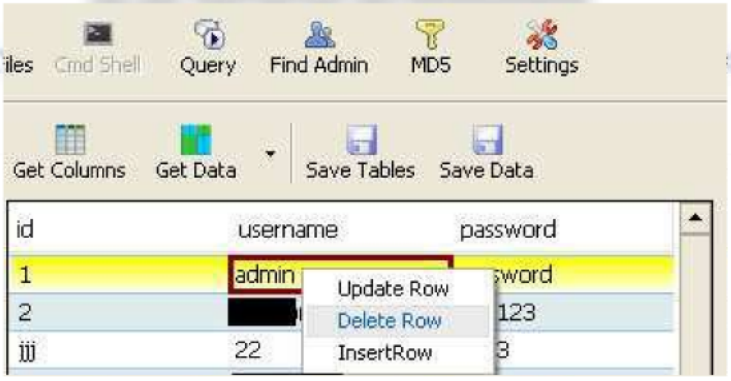
Updating data

For updating data double click on it and enter new data then press Enter key.



Deleting data

To delete a row right click on it and select 'Delete Row'.



Inserting Data

To insert a new record right click on a row and select 'Insert Row'.

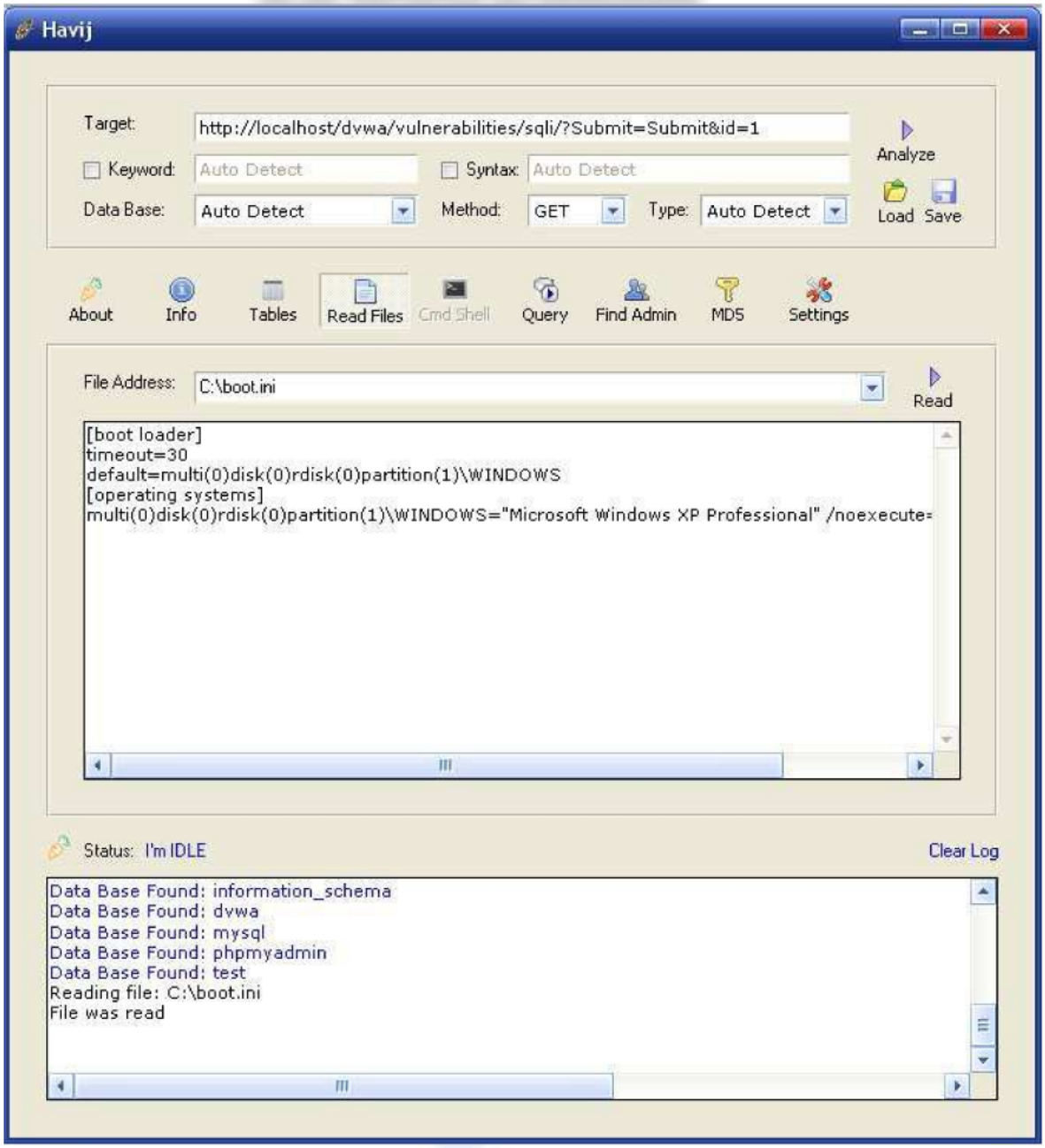
Important: it's not possible to update, insert or delete data in MySQL with PHP. It is shown in below table for other data bases and languages.

	SQL Server	MySQL	PostgreSQL	Oracle	MsAccess
ASP	Yes	?	?	?	No
ASP.NET	Yes	?	?	?	No
PHP	Yes	No	Yes	?	No
JAVA	?	No	?	No	No
ColdFusion	Yes	?	?	?	No

Reading Files

If the database is MySQL after analyze 'Read Files' will be activated and you can read files on MySQL server using it. To do this just enter the file address and click 'Read'

Important: if the file does not exist or the current database user doesn't have enough privilege to access the file, nothing will be displayed.

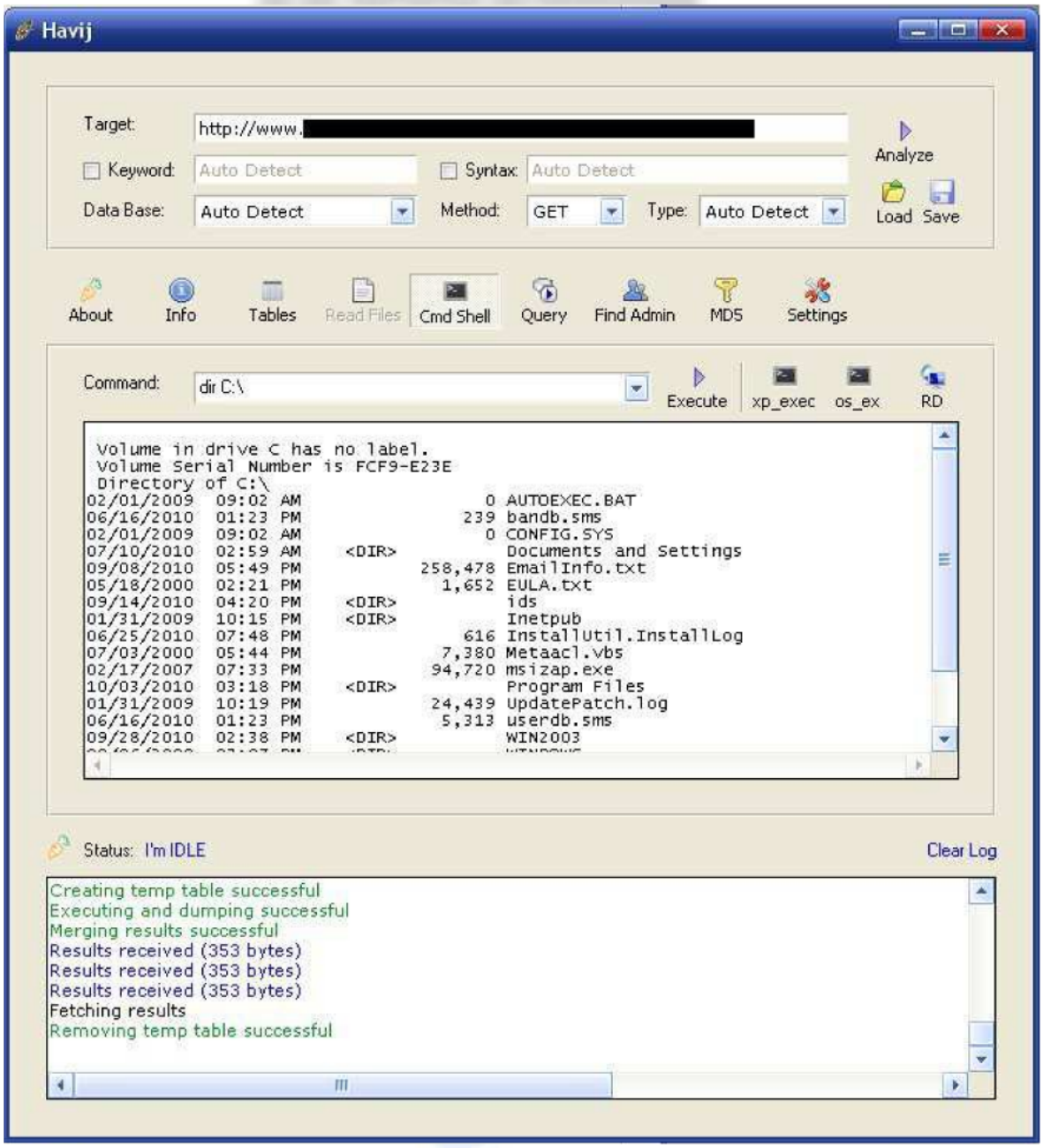


Executing system commands on target

When target's database is Microsoft SQL Server, 'CMD Shell' option will be activated and you can execute system commands on SQL server.

Enter your command and click 'Execute'. The result will be displayed if the command was executed.

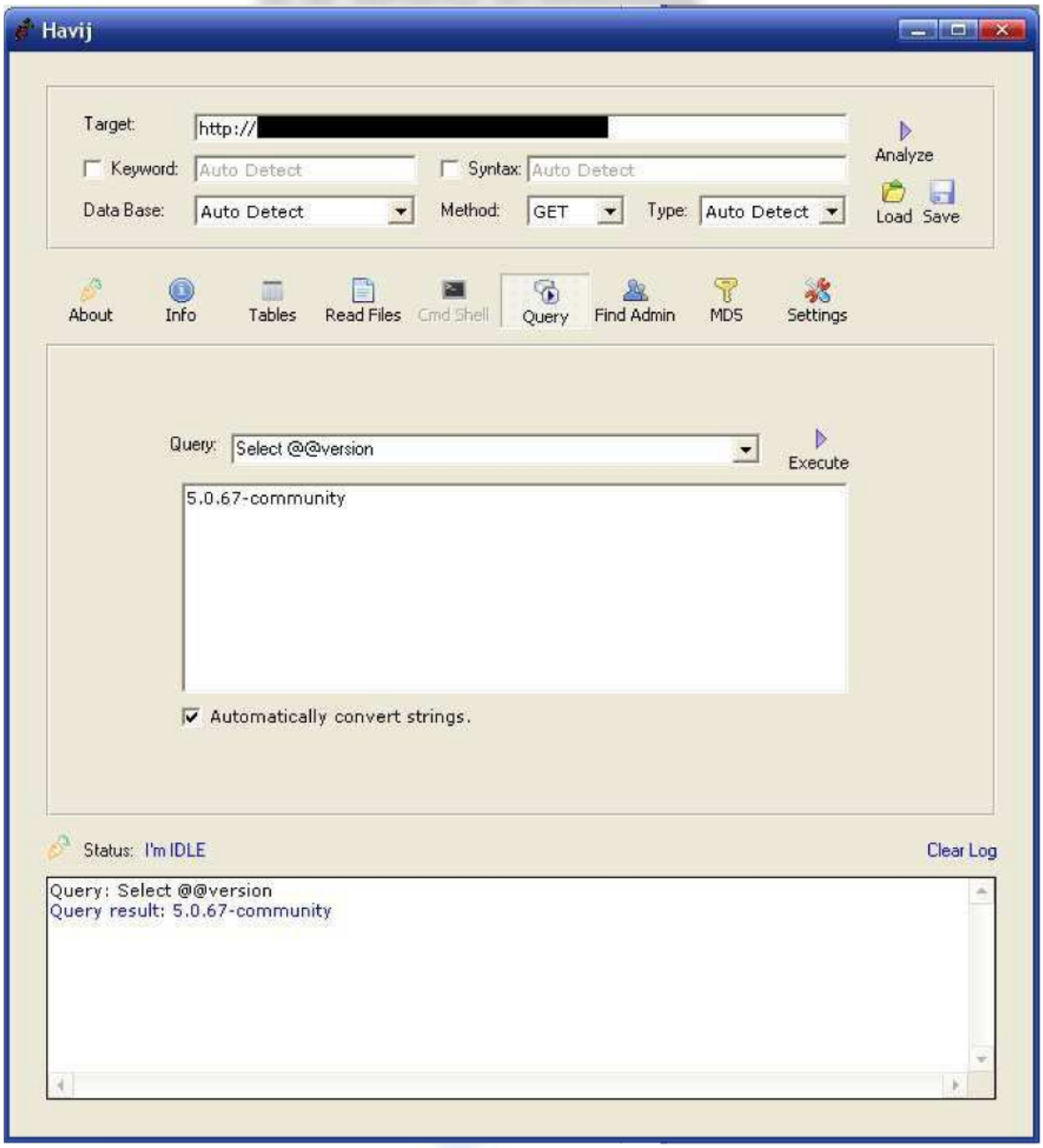
Important: for executing commands database user must have enough privilege.



Query

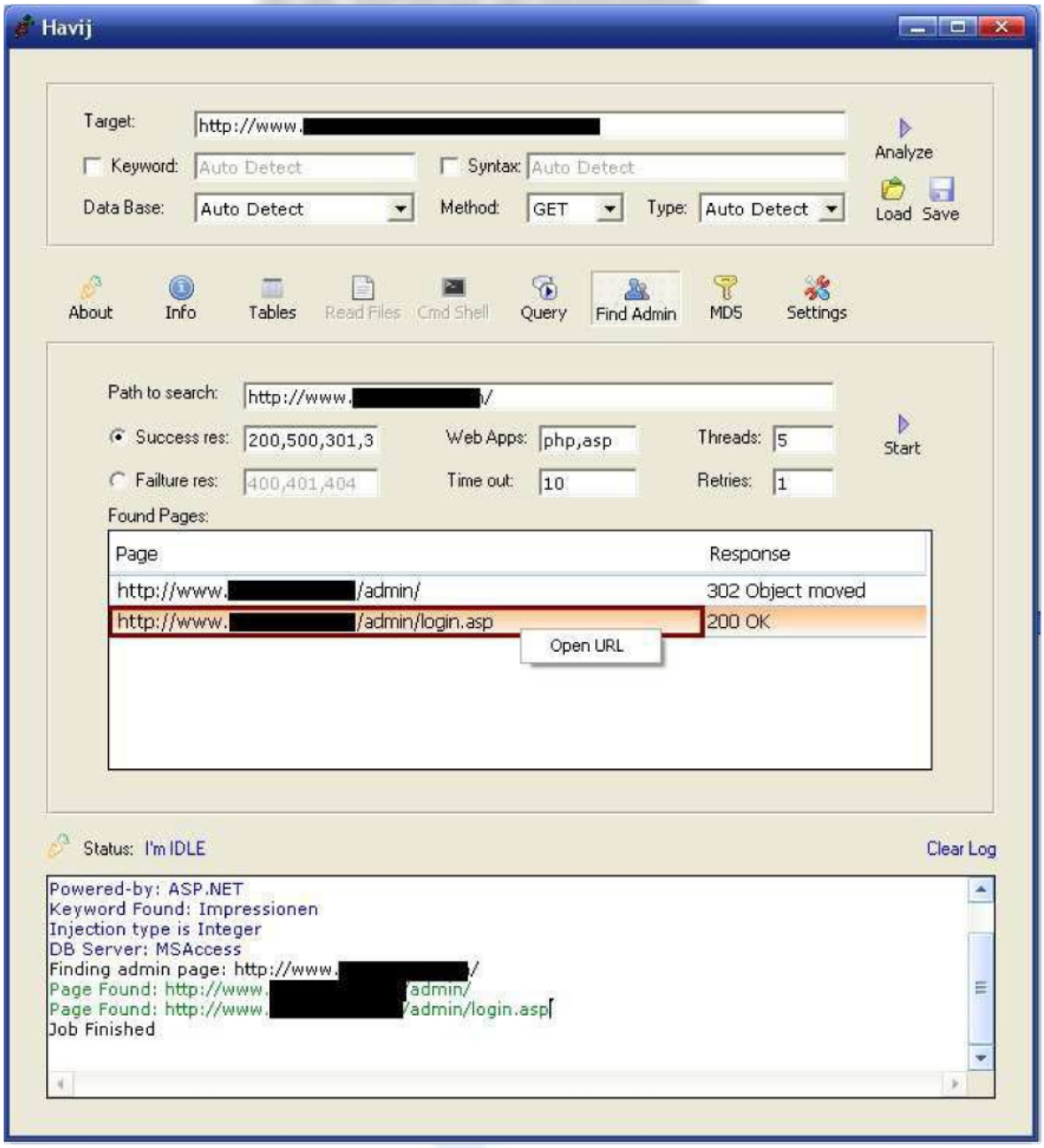
By using 'Query' on top menu you can run your own query on target's database.

Important: SQL queries should not return more than one row.



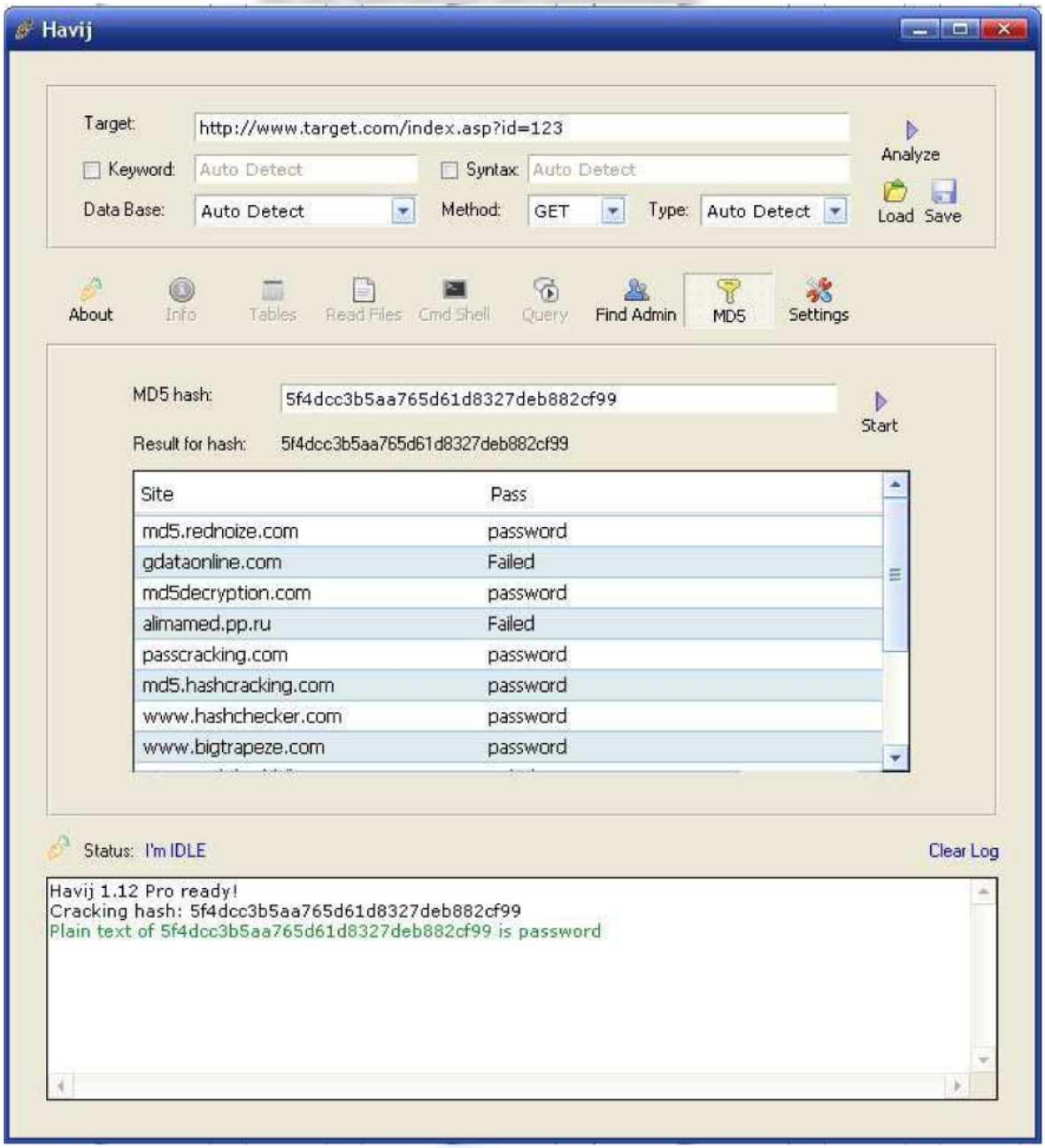
Finding admin login page

By using 'Find Admin' you can find any site's login page. Click on 'Find Admin', enter the site address in 'Path to search' and click 'Start' to find available login pages for that site. Found pages will be shown in list. You can right click on them and select 'Open URL' to open them in your browser.



Cracking MD5 Hashes

Havij has an online MD5 cracker. Click on 'MD5' on top menu and enter the hash you want to crack into 'MD5 hash' field and click 'Start'. Havij will look for hash in several sites in mul thread mode and displays the result.


Havij
Target:
http://www.target.com/index.asp?id=123
Analyze
Keyword:
Auto Detect
Syntax:
Auto Detect
Data Base:
Auto Detect
Method:
GET
Type:
Auto Detect
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
MD5 hash:
5f4dcc3b5aa765d61d8327deb882cf99
Start
Result for hash:
5f4dcc3b5aa765d61d8327deb882cf99
Site
Pass
md5.rednoize.com
password
gdataonline.com
Failed
md5decryption.com
password
alimamed.pp.ru
Failed
passcracking.com
password
md5.hashcracking.com
password
www.hashchecker.com
password
www.bigtrapeze.com
password
Status:
I'm IDLE
Clear Log
Havij 1.12 Pro ready!
Cracking hash: 5f4dcc3b5aa765d61d8327deb882cf99
Plain text of 5f4dcc3b5aa765d61d8327deb882cf99 is password

Manual Injection

Havij has manual injection settings that let the user to set them manually and use Havij advantages in injecting targets vulnerable to SQL Injection bug. By default all of these setting are set to 'Auto Detect' and Havij does everything needed. These settings are Keyword, Syntax, Database and Type (variable type). You can set one or all of these settings manually and start injecting.

Choosing Database

If you're sure what the target's database server is, you can select it from 'Database' list on the top of main program window. Havij supports following databases and injection methods.

- MsSQL with error: Microsoft SQL Server injection using error based method
- MsSQL no error: Microsoft SQL Server injection using union
- MsSQL Blind: Microsoft SQL Server injection using blind method
- MsSQL time based: Microsoft SQL Server injection using time based method
- MySQL unknown ver: MySQL injection using union
- MySQL Blind: MySQL injection using blind method
- MySQL error based: MySQL injection using error based method
- MySQL time based: MySQL injection using time based method
- Oracle: Oracle injection using union method
- Oracle error based: Oracle injection using error based method
- PostgreSQL: PostgreSQL injection using union method
- MsAccess: Microsoft Access injection using union method
- MsAccess Blind: Microsoft Access injection using blind method
- Sybase (ASE): Sybase (Adaptive Server Enterprise) using union
- Sybase (ASE): Sybase (Adaptive Server Enterprise) using blind method

Choosing Variable Type

Variable type is type of the input variable that Havij injects into it that can be integer or string. Integer type is variable that will be used directly in SQL query but string type will be used between quotation marks (' or ").

Defining Keyword

Keyword is a word that indicates true response. True response is the response that page returns to a SQL injection that returns some rows. The false response is the response page returns to an injection that cause the query to return no row. Keyword is a word from the html source code of true response page.

For finding keyword you can use following injections.

h p://site.com/index.php?id=52 and 1=1 that returns true response for integer variables

h p://site.com/index.php?id=52 and 1=0 that returns false response for integer variables

And

h p://site.com/index.php?id=52and 'x'='x that returns true response for string variables

h p://site.com/index.php?id=52and 'x'='y that returns false response for string variables

Keyword should exist in true response and shouldn't exist in false response. For example if you can see 'Hello' word in true response and couldn't see in false response (in html source code), 'Hello' is a good keyword to use.

Defining Syntax

In some targets because of specific SQL queries or conditions Havij can't inject automatically. In these cases you can still inject with Havij using manual syntax.

For example assume that you can inject into a target and see the SQL server version using the following injection.

http://site.com/index.php?id=-52 union all select 1,2,@@version,3—

To set syntax in Havij enter the following address as 'Target':

h p://site.com/index.php?id=52

And then check 'Syntax' checkbox and enter the following in textbox as 'Syntax':

-52 union all select 1,2,%String_Col%,3—

Important: we replaced @@version that will be returned in page with %String_Col%

Important: %String_Col% is case sensitive.

Now click on 'Analyze' to start injection.

Defining Syntax for Blind injections

In blind injections none of selected data by query won't be returned in vulnerable page, so it's not possible to extract data by union injection. In most of cases we can see two different response by various injections, one which indicates true response (SQL query with injection returns at least one row) and the other indicates false response (SQL query with injection returns no row). Please read 'Defining Keyword' for more.

For example assume that following injection returns true response in some page:

h p://site.com/index.php?id=52 and 1=1

Enter following URL as target:

http://site.com/index.php?id=52

And enter the following expression as syntax:

52 and %True_Expression%

Important: %True_Expression% is case sensitive.

If the variable type is string and you can see true response by the following injection:

http://site.com/index.php?id=52' and 'x'='x

Enter following URL as target:

h p://site.com/index.php?id=52

And enter this as syntax:

52' and %True_Expression and 'x'='x

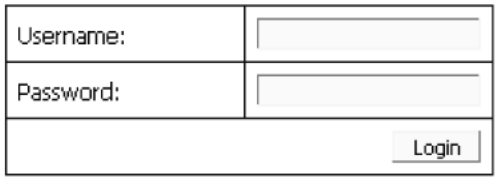
Important: if you set manual syntax, it's better to set keyword manually too (especially in blind injections).

Choosing Method

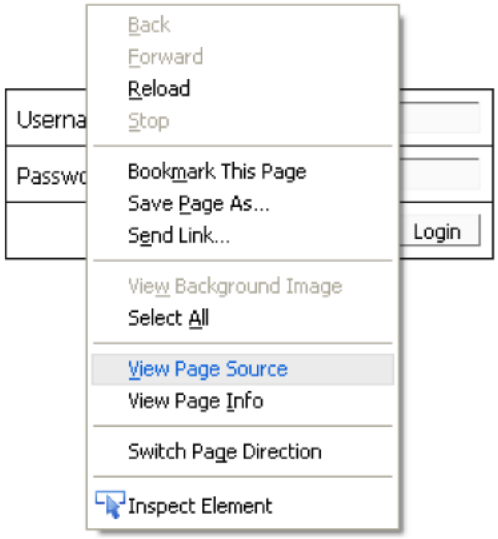
Method is the http method that Havij uses to send injection to target. All links in html pages use GET method and most of forms use POST method. GET method is selected by default. If you found injection in a form, you should use POST method.

Injecting into Forms (POST Method)

For example if you saw the following form in a page and you would like to inject into it with Havij, follow these steps:



1- Select POST method
2- View the source code of the page.



3- Look for <form> tag in the page source code.

```
<body>
<div align="center">
  <center>
  <table border="0" cellpadding="0" cellspacing="0" style="border-collapse: coll
    <tr>
      <td width="100%">
      <div align="center">
        <center>
        <form method=post action="login.php">
        <table border="1" cellpadding="6" cellspacing="0" style="border-collapse
          <tr>
            <td width="50%">Username:</td>
            <td width="50%"><input type="text" name="name" size="20"></td>
          </tr>
          <tr>
            <td width="50%">Password:</td>
            <td width="50%"><input type="password" name="pass" size="20"></td>
          </tr>
          <tr>
            <td width="100%" colspan="2">
            <p align="right"><input type=submit name=submit value="Login"></td>
          </tr>
        </table>
        </form>


        </center>
      </div>
      </td>
```

4- Enter the action value (login.php) after the URL like this:

http://site.com/login.php

5- In Post Data field enter the input parameters in the following format:

pass=&submit=Login&name=whatever

Important: the last parameter (name) will be injected. If you would like to inject into 'pass' parameter, you can write it and the end or define it as below:

pass=%Inject_Here%&submit=Login&name=whatever

6- Click on 'Analyze' to start injection.

Settings

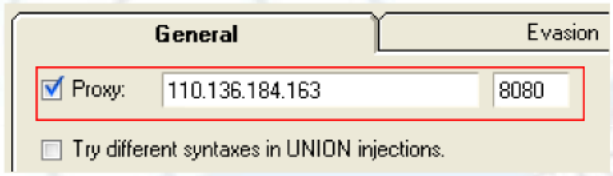
By using 'Settings' from the top menu you can change some settings of Havij.

Important: for settings to take effect after analyze and while doing injections, you should click on 'Apply' button in 'Settings' window otherwise new settings will take effect with clicking on 'Analyze'.

Basic Settings

Using Proxy

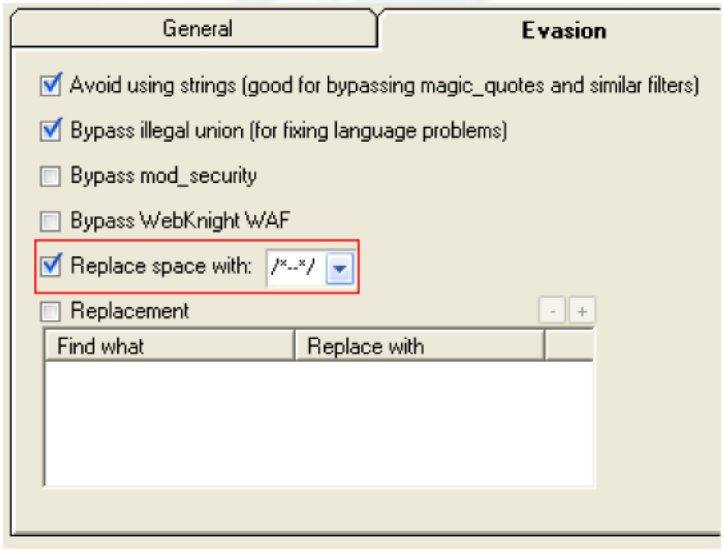
For hiding your IP while injecting a target you can use proxy. In settings window check 'Proxy' checkbox and enter your proxy server address and port.



Replacing Space character

For bypassing some filters that block injection requests you can replace space character with +,/**/,... . This won't change the injection result but can bypass weak filters.

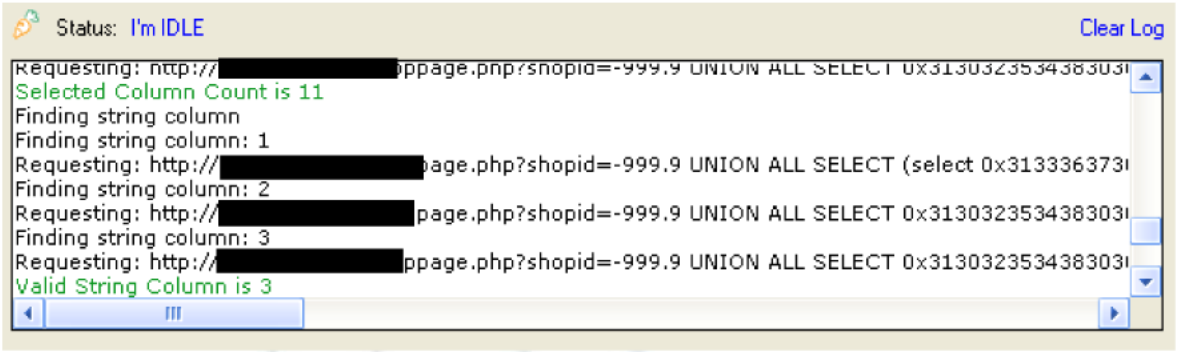
To do this click on 'Replace space with' on 'Evasion' tab of settings to check it and select or enter what you want to be replaced with space character in injections.



Showing Injections

Havij can display all injection that it does and you can open them in your browser to see the result.

Click on 'Show Requests' in settings window to check it. All injections will be shown in log window.



Injecting URL rewrite pages

Sometimes you can see URLs without any input parameter. In this URLs input parameters are set using URL rewrite option (if exists). You define injection point using %Inject_Here% tag in your target. For example if you had a URL like this:

http://somewhere.com/news/1077/index.html

And 1077 is the vulnerable variable, you should enter the following URL as target:

http://somewhere.com/news/%Inject_Here%/index.html

Important: %Inject_Here% is case sensitive

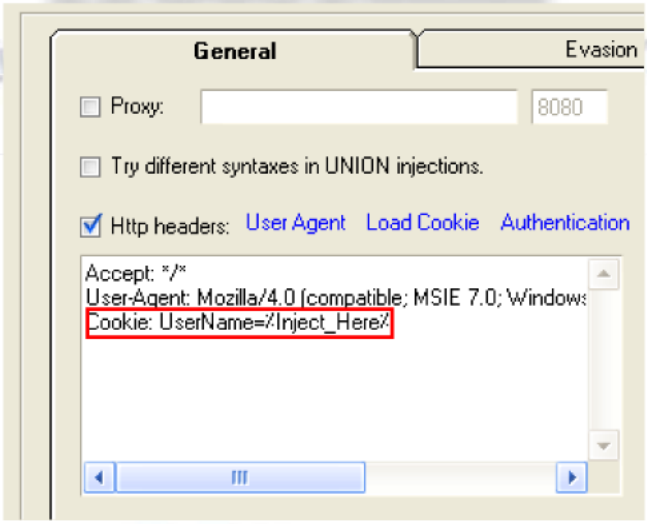
In case of using the %Inject_Here% the default injection value that will be used is 1 if you need to use the exact value, you can change it in the settings.

Injecting into Cookie, User-Agent, etc

If SQL Injection vulnerability exists in cookie, user-agent, referrer or any other http headers you can automate scanning and exploitation of it by Havij.

For example if there's a sql injection in a cookie parameter named 'UserName' add the following line to the 'Additional http headers' in the settings:

Cookie: UserName=%Inject_Here%



It's same for other headers like referrer or User-Agent.

In case of using the %Inject_Here% the default injection value that will be used is 1 if you need to use the exact value, you can change it in the settings.

Advanced Settings

Authentication is needed for injection!

In some cases you need to login into site to access the vulnerable web page. Havij can inject these kinds of targets too.

Havij supports for three type of authentications: 1- Http Basic authentication 2- Http Digest authentication 3- Http form authentication

Http Basic authentication

If the target uses Basic authentication, Havij will detect it and ask you for username and password.

Just enter your username and password and click ok.
You can do this manually by clicking on 'Authentication' in settings.

Http Digest authentication

This is same as Basic authentication

Http form authentication

This is when you have to login through a form in website

Just follow these steps for authentication:

1- Enter vulnerable web page address as 'Target'.
2- Go to settings and check 'Additional http headers' checkbox and click on 'Load Cookie'.
3- In new window you can see the web page as you see it in your browser (IE), now login into the site.
4- Click 'Add'.

5- Click on 'Analyze' to start injection.

Defining character set to use in blind injections

In blind injections Havij finds each character of data by binary trial and error method. Characters range that Havij uses can be changed. In settings set your character ascii range as 'Blind injection character ascii set'

Changing Headers

All injections that Havij does are sent using http protocol. This protocol has a lot of headers that you can set them manually for example one of common headers is User-Agent that indicates user browsers.

In settings click on 'Additional http headers' to check it and enter any header you want.

To set the 'User-Agent' click on it and select one from the menu.

Time Out

This options in 'General' tab of settings defines maximum time in milliseconds that Havij spends for sending and receiving a request.

Default Injection Value

When you use %Inject_Here% to define the injection point, you can use this option to specify the default value. For example if you found that the following URL is vulnerable:

http://site.com/index.html/id/1324

And injec on point is 1324, you replace it with %Inject_Here% as follow:

http://site.com/index.html/id/%Inject_Here%

To specify 1312 as default injec on value enter it in 'Default injection value' in 'General' tab of settings.

Avoid using strings

If this option is checked Havij will encode all string (literals between quotation marks) automatically. This can bypass filters like 'magic_quotes'. It's recommended to use this option.

Bypass illegal union

This option is for solving different table languages problem in injections with union method. It's recommended to use this option.

Try different syntaxes in union injections

If this option is checked, Havij will try to find columns count with different syntaxes (normal and with parentheses) in union injections.

Follow redirections

If this option is checked, Havij will search for injection result in redirected page (if server redirects to another page).

Column count

You can set minimum and maximum number of selected columns that Havij tries to find in union injections.

Do not find columns count in MsSQL with error

If this option is checked, Havij won't try to find columns count when database server and injection method is Microsoft SQL Server with error based method. It's recommended to use this option.

Bypass mod_security

This is for bypassing mod_security web application firewall and similar firewalls. This option will be used automatically by Havij, you can also set it manually.

Bypass WebKnight WAF

This is for bypassing AQTRONIX WebKnight web application firewall and similar firewalls. This option will be used automatically by Havij, you can also set it manually.

Custom Replacement

In some targets you need to replace a keyword with something else in injections to avoid detection and filtering. In these cases you can use Replacement option. For example if you like to change 'select' with 'SeLeCt' in all injections, click on Replacement checkbox on 'Evasion' tab of settings and then click the '+' button and enter your replacement as follow:

select::SeLeCt

This will finds all 'select' and replaces them with 'SeLeCt'

Time based method delay

This option defines milliseconds delay for time based injection methods. If it is set to 'Auto' Havij will automatically use the best suitable delay.

Blind table prefix

If you know the prefix of the target's tables you can set it on 'Blind' tab of settings. So in blind injections Havij will ignore the table's prefix and finds the table name.

Blind column prefix

If you know the prefix of the target's columns you can set it on 'Blind' tab of settings. So in blind injections Havij will ignore the column's prefix and finds the column name.

Table list for blind guessing

You can set a list of table names to use when Havij can't extract the table names and should try guessing method. The default list is included in Havij's installation directory you can specify your custom list in 'Blind' tab of Settings.

Column list for blind guessing

You can set a list of column names to use when Havij can't extract the column names and should try guessing method. The default list is included in Havij's installation directory you can specify your custom list in 'Blind' tab of Settings.