Ethical Hacking and Countermeasures
Mole Cheat Sheet

EC-Council
Building A Culture Of Security

Mole

Source: https://sourceforge.net

It is a command-line interface SQL Injection exploitation tool. It can detect the injection on the site and exploit it, only if a vulnerable URL and a valid string are provided. Mole can be used to exploit both union-based and blind boolean-based injections and supports MySQL, SQL Server, and Oracle databases.

Syntax

```
./mole.py [PARAMS]
```

Options

`-u <URL>`	URL that contains an SQLi vulnerability
`-n <NEEDLE>`	String printed on good queries
`-t <n>`	THREADS: The number of threads to run. Default is 4
`-p <PARAM>`	Sets the GET vulnerable param

Mole Commands

Command	Description
`Clear` `Syntax: clear`	Clears the screen
`columns` `Syntax: columns <database> <table>`	Displays the columns of a table from a given database and table
`cookie` `Syntax: cookie <cookie>`	Obtains or sets a cookie to be sent in each HTTP request's headers
`dbinfo` `Syntax: dbinfo`	Displays database information
`delay` `Syntax: delay <delay>`	Gets or sets the delay (in seconds) between requests
`encoding` `Syntax: encoding <encoding>`	Gets or sets the encoding use to decode the response received.
`exit` `Syntax: exit`	Quit the application
`export` `Syntax: export <format> <file>`	Exports the current mole configuration and the dumped schema's structures \
`fetch` `Syntax: fetch schemas|tables <SCHEMA>`	Recursively fetches the structure of all schemas or just of the SCHEMA if used with tables
`find_tables` `Syntax: find_tables <SCHEMA> <TABLE1> [<TABLE2>, ...]`	Bruteforce to determine if the TABLES given as parameters are part of the SCHEMA
`find_tables_like` `Syntax: find_tables_like <SCHEMA> <FILTER>`	Issue a query to extract all
`find_users_table` `Syntax: find_users_table <SCHEMA>`	Bruteforce to find tables in SCHEMA that match common names for tables where usernames are stored
`headers` `Syntax: headers <set|del> <HEADER> [VALUE]`	Sets or removes the given HTTP header
`htmlfilter` `Syntax: htmlfilter <add|del> <FILTER> [ARGS]`	Adds or removes an HTML filter
`import` `Syntax: import <TYPE> [<ARG1>, ...]`	Obtains a previously exported mole configuration and dumped schema's structures
`injectable_field` `Syntax: njectable_field (GET | POST) <INJECTABLE_FIELD>`	Sets or gets the field of the query which will be used to print the information retrieved when using a union technique
`method` `Syntax: method (GET|POST <param_post> ) [injectable_field]`	Sets the method of the request to GET or POST
`mode` `Syntax: mode <union|blind>`	Sets the SQL Injection exploitation method
`needle` `Syntax: needle [NEEDLE]`	Gets or sets the NEEDLE
`output` `Syntax: output <pretty|plain>`	Sets the output style
`prefix` `Syntax: prefix [PREFIX]`	Gets or sets the prefix for each request
`qfilter` `Syntax: qfilter <add|config|del> <FILTER> [ARGS]`	Add or configure or remove query filters
`query` `Syntax: query <SCHEMAgt; <TABLE> COLUMN1[,COLUMN2[,COLUMN3[...]]] [where COND]`	Perform a query to fetch every column given
`readfile` `Syntax: readfile <FILE>`	Read the FILE from the remote server and print it
`recursive` `Syntax: recursive (schemas|tables <SCHEMA>)`	Recursively fetches the structure of all schemas or just of the SCHEMA if used with tables
`schemas` `Syntax: schemas`	Retrieves the schema of the database
`suffix` `Syntax: suffix [SUFFIX]`	Gets or sets the suffix for each request
`tables` `Syntax: tables <database>`	Show the table from a given database
`url` `Syntax: url [URL [PARAM]]`	Gets or sets the URL
`usage` `Syntax: usage <COMMAND>`	Print the usage for the command COMMAND
`verbose` `Syntax: verbose <on|off>`	Sets the verbose mode on and off, each request's parameters will be printed out
`vulnerable_param` `Syntax: <GET|POST|Cookie> VULNERABLE_PARAM`	Sets or gets the type and name of the vulnerable parameter to be exploited by The Mole
`auth` `Syntax: <basic> <USERNAME:PASSWORD>`	Sets or gets the authentication information used by The Mole in each request
`follow_redirects` `Syntax: <on|off>`	Sets or gets the follow redirect flag. If enabled, The Mole will follow HTTP redirects received from the server
`usercreds`	Fetches the credentials for the DBMS. Usually requires administrator privileges on the database
`requestsender` `Syntax: <httpsender|headsender>`	Gets or sets the request sending mechanism
`responsefilter` `Syntax: <add|del|config> <FILTER> [ARGS]`	Adds or removes or configures a response filter
`requestfilter` `Syntax: <add|del|config> <FILTER> [ARGS]`	Add or configure or remove a request filter