

# sqlmap

```
$ python sqlmap.py -u "http://target/vuln.php?id=1" --batch
```



{1.0-dev-4512258}

<http://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[\*] starting at 15:02:07

```
[15:02:07] [INFO] testing connection to the target URL  
[15:02:07] [INFO] heuristics detected web page charset 'ascii'  
[15:02:07] [INFO] testing if the target URL is stable. This can take a couple of seconds  
[15:02:08] [INFO] target URL is stable  
[15:02:08] [INFO] testing if GET parameter 'id' is dynamic  
[15:02:08] [INFO] confirming that GET parameter 'id' is dynamic  
[15:02:08] [INFO] GET parameter 'id' is dynamic  
[15:02:08] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

## More information

<https://sqlmap.org/>