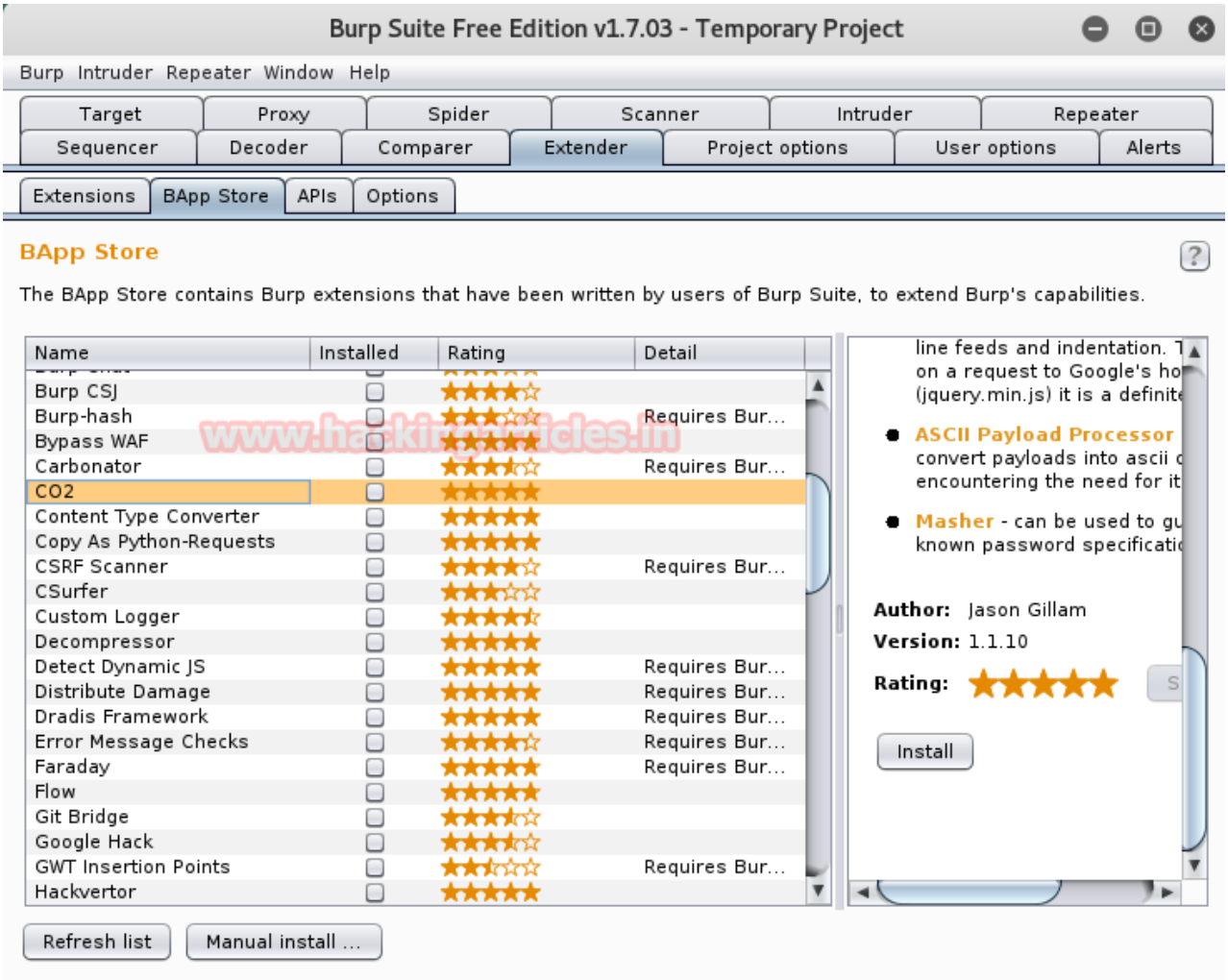
Sql Injection Exploitation with Sqlmap and Burp Suite (Burp CO2 Plugin)

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.

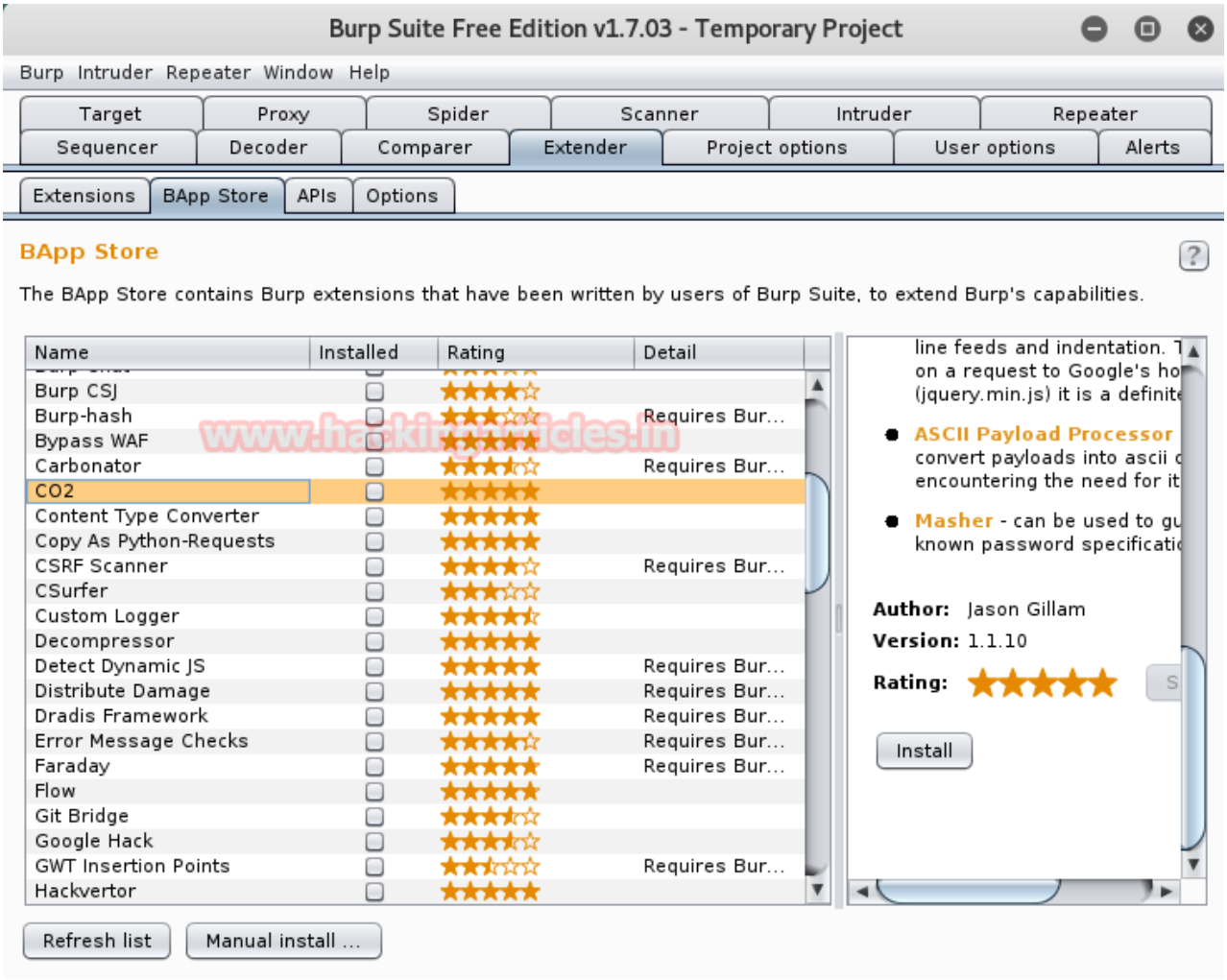
For more details read from here **burpco2.com**

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

Installing Burp CO2 Extension

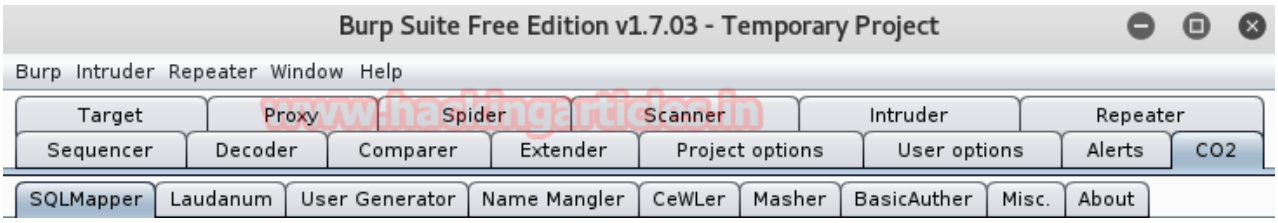
Start burp suit and click on **Extender** tag then **click** on **BApp store** which contains burp extensions to extend burp's capabilities.

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 **SQLMappe**r tool.



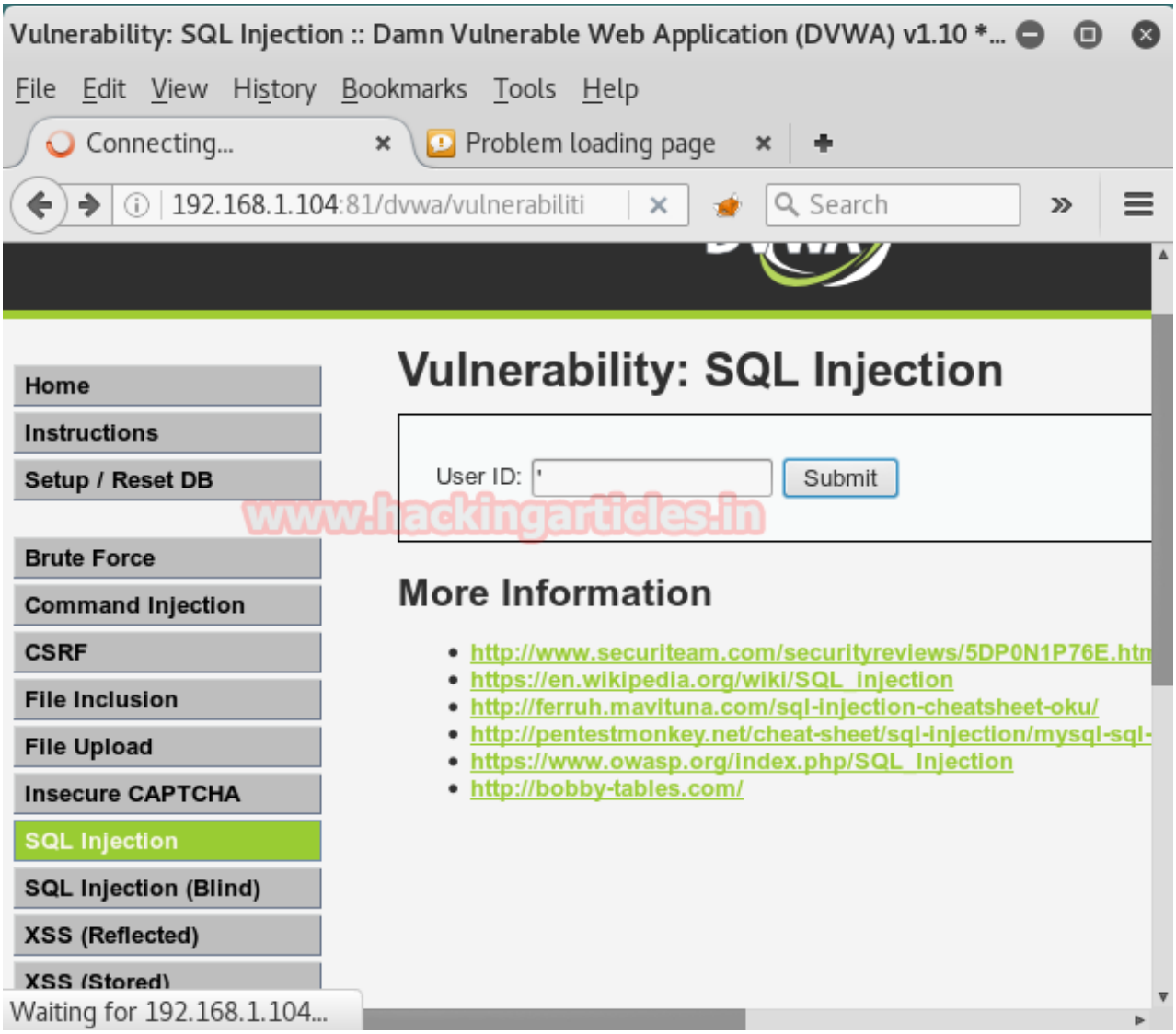
Now open the DVWA in your pc and log in with following credentials:

Username – admin

Password – password

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

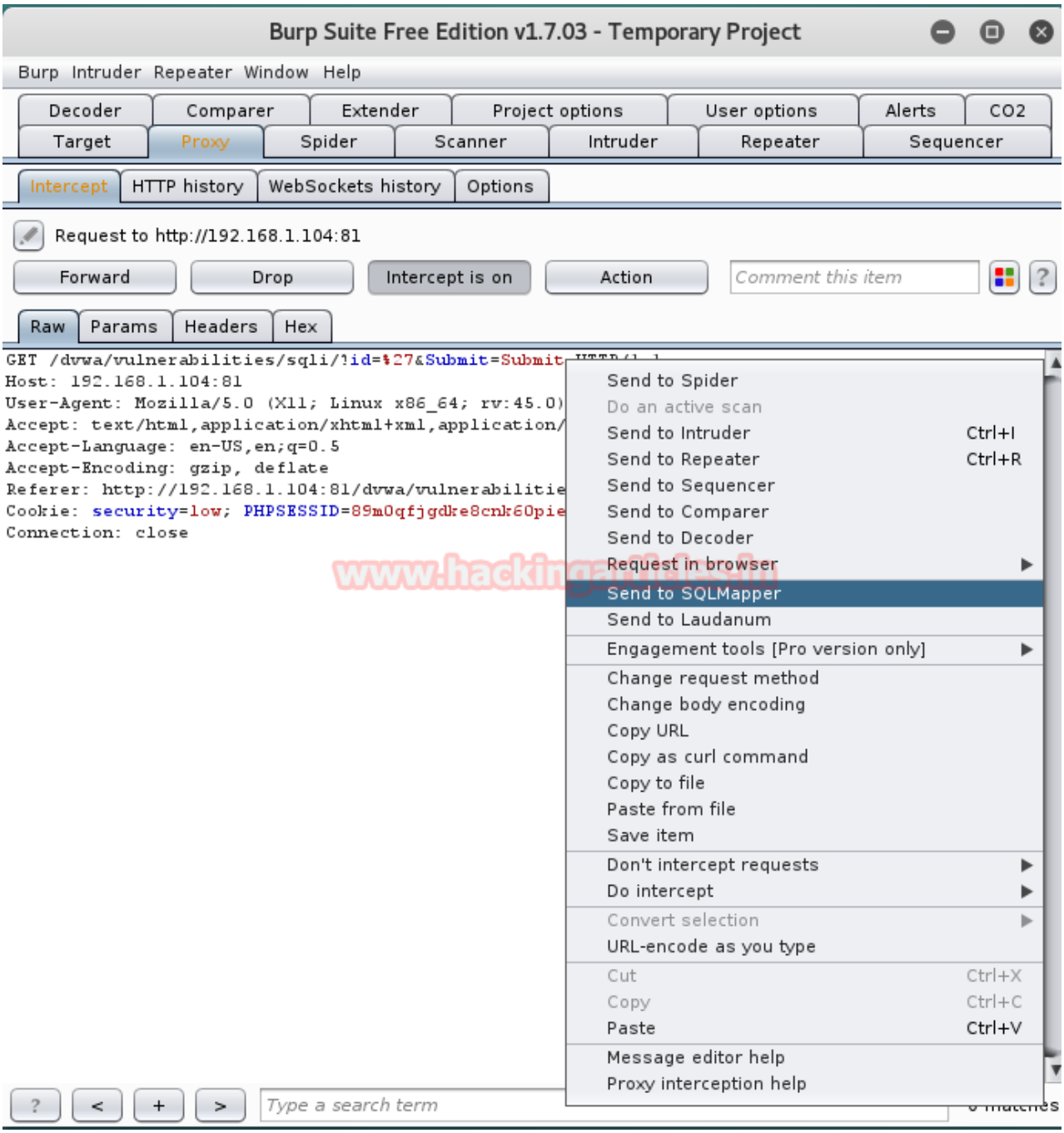
From the list of vulnerability select **SQL Injection** for your attack. Type **user ID: '**in the text box. Don't click on submit button without setting browser proxy. Set your browser proxy to make burp suite work properly.



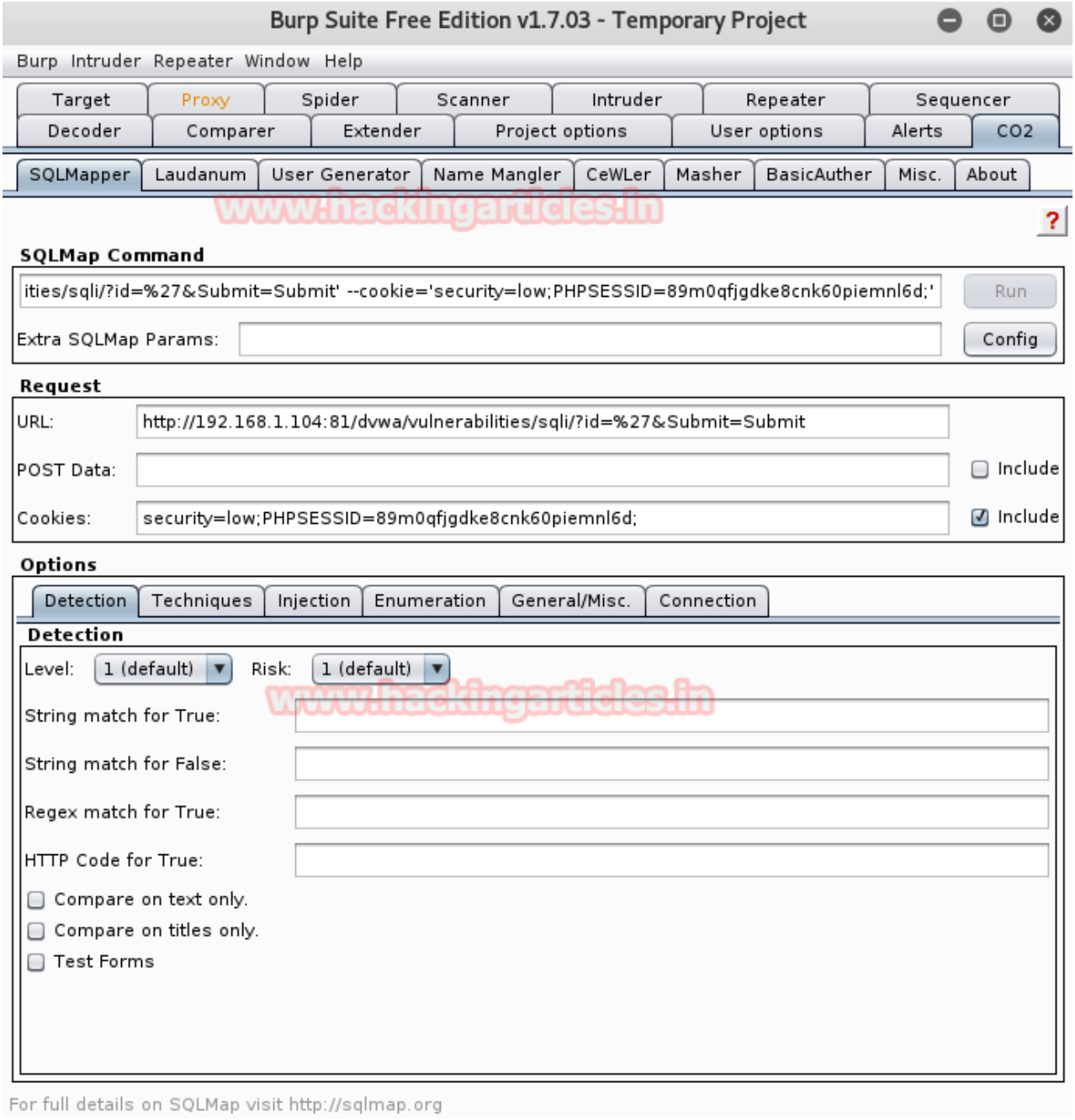
Intercepting the Request with Burp Proxy

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**.

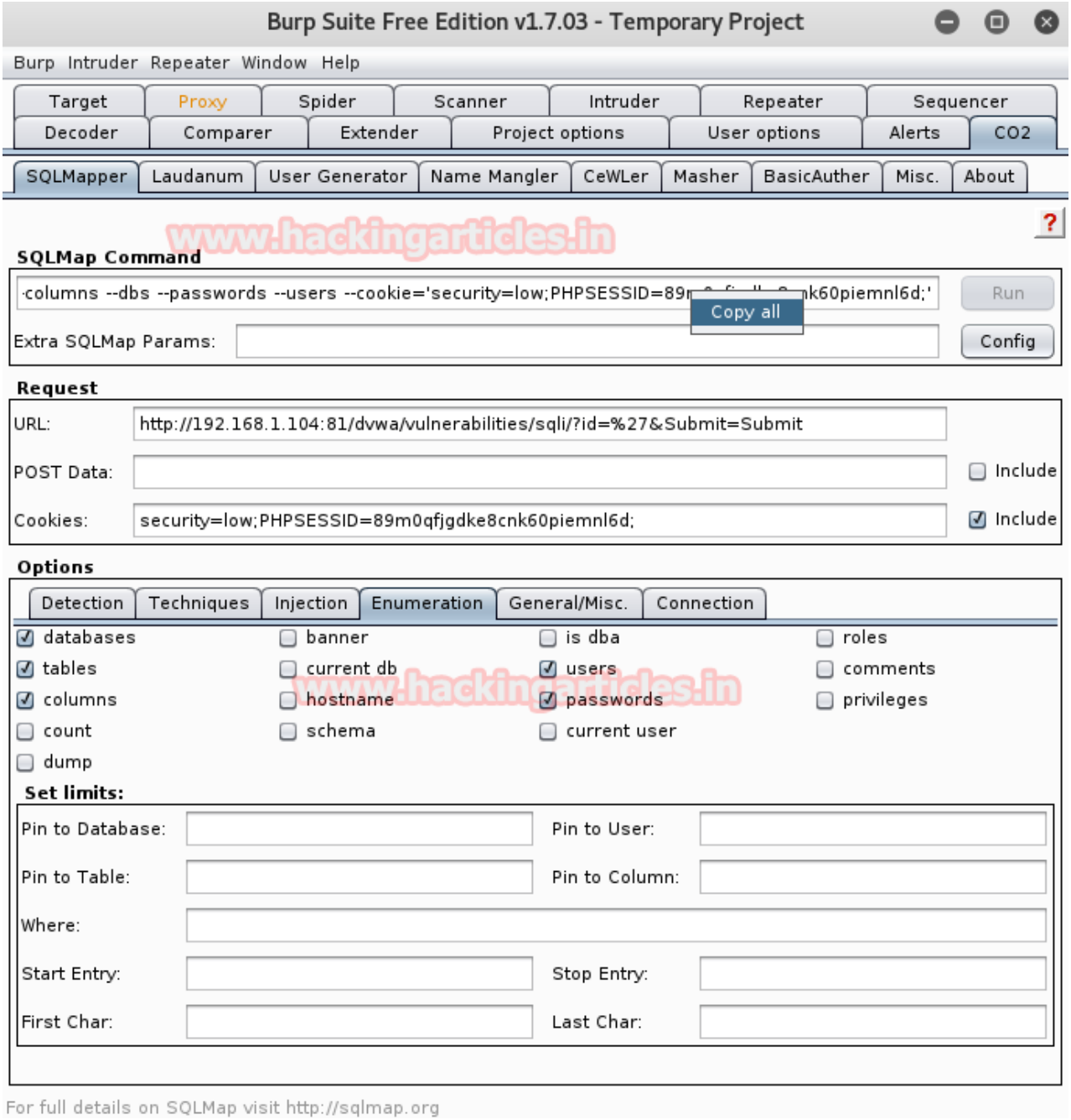


When the fetched data will be sent to SQL mapper it will automatically itself generates **sqlmap command** using referrer and cookie.

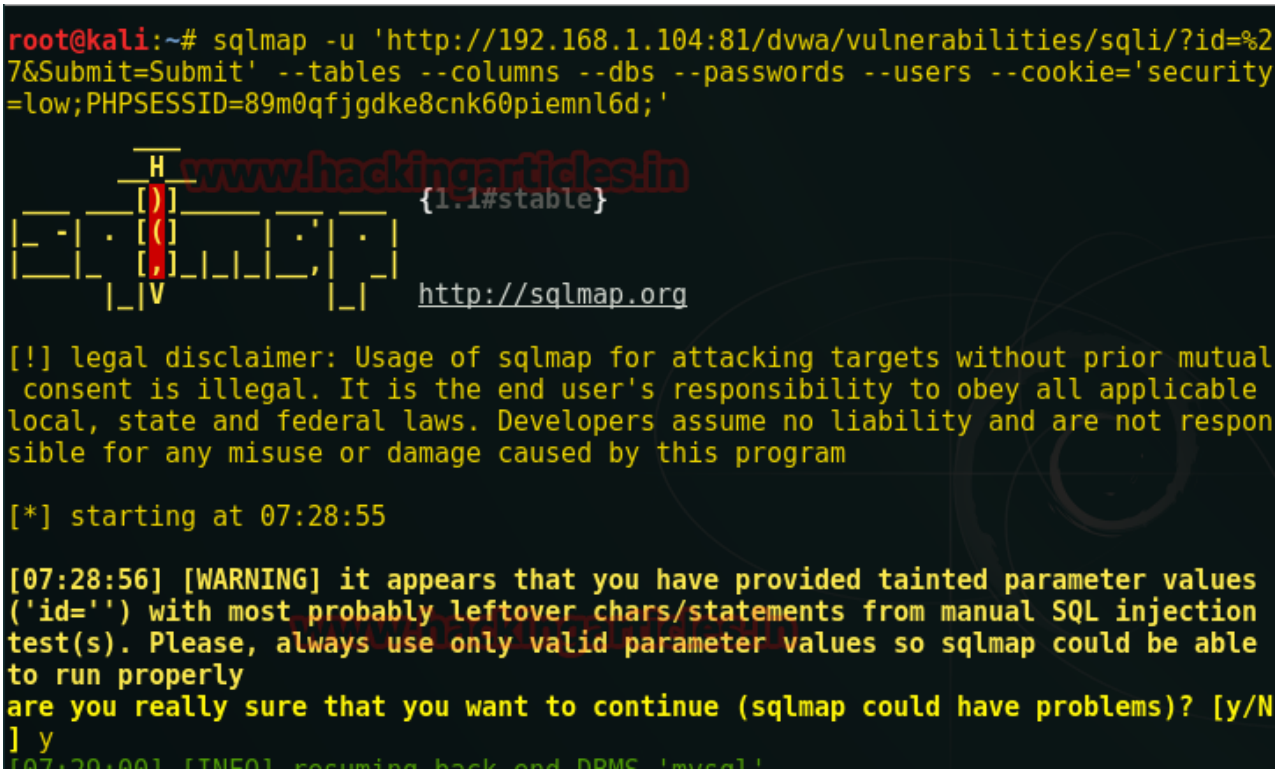


Here you can see **the options** box at the end of burp suite frame. Now **click** on **enumeration** tag and select the checkboxes for **database, tables, columns, users, and passwords**.

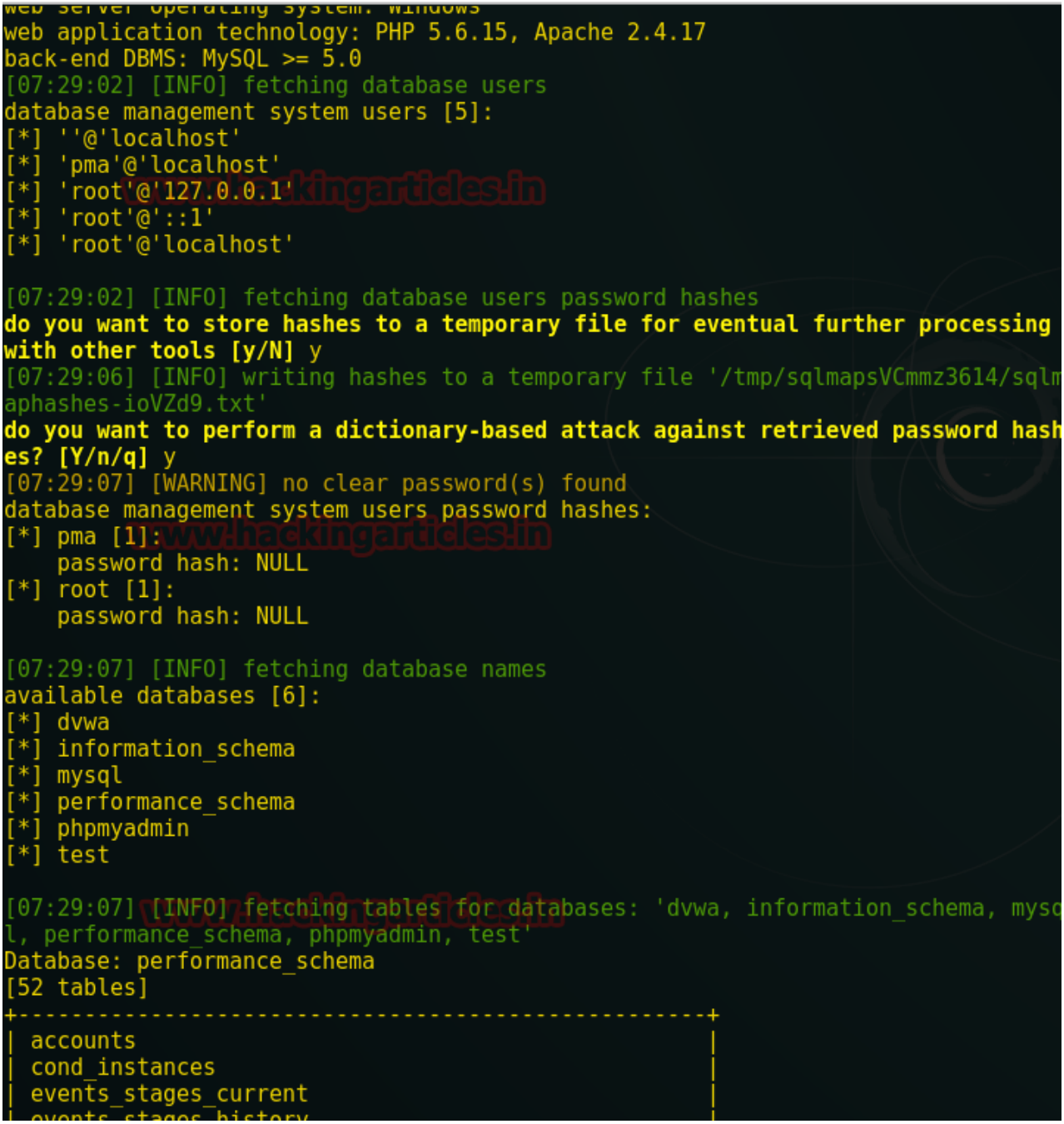
Now copy the **sqlmap command** from the text field and run this command manually on terminal using **sqlmap**.



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.



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.



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**