

Forum:[Hack Forums](#)

Thread: [\[TUT\] SQL Injection from BurpSuite with SQLmap Burp Plugin \[/TUT\]](#)

CalebBucker - October 17, 2012, 9:26 am

[img]<http://www.unixwiz.net/images/sqlinjection.jpg>[/img]

INTRODUCTION:

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Many times when performing audit of a website, it is always advisable to place an intermediate proxy to know and have full control of the requests sent and received, for it to use Burp Suite.

It is also known that in these audits, better known vulnerability that can occur is the SQL Injection.

For this case, in this post brings a completely free plugin developed by ggdaniel that will help us use the Burp Suite sqlmap from an easy and effective.

¿WHAT IS SQLMAP?

SQLMAP is an open source penetration testing tool that helps in automating the process of detecting and exploiting SQL injection vulnerabilities and taking full access over the database servers.

¿WHAT IS SQLMAP PLUG-IN?

When we audit a web application, we normally configure an intermediate proxy to have more control over the request and response parameters.

SQLMAP plug-in is an add-on feature that we can configure to the burp through which we can redirect a URL or a request directly to the SQLMAP with a single mouse click.

¿HOW TO CHARGE THE PLUGIN SUITE BURP?

Very easy, the first thing we have to do is download the plugin from the following link: <http://code.google.com/p/gason/downloads/list> recommend downloading (burpplugins-0.9.3.zip), then decompress files and place them in the same folder where this Burp Suite (Pentest - web - burpsuite)

Next, run the command to run Burp Suite along with respective plugin.

Linux:

```
- java -classpath burpplugins.jar:burpsuite_v1.4.01.jar burp.StartBurp
```

Windows:

```
- java -classpath burpsuite_v1.4.01.jar;burpplugins.jar burp.StartBurp
```

CONFIGURING THE PROXY:

Firefox:

- Edit - Preferences - Advanced - Network - Settings - Manual Proxy Configuration

Google Chrome:

- Settings - Show Advanced Options - Network - Change Proxy Settings - Connections - LAN Settings

The proxy configuration is necessary for this method because we need the browser to send requests to the Burp Suite

¿HOW DO WE USE THE PLUGIN?

Once you have executed the next to Burp Suite Plugin is very easy to use it, simply right click on the request parameters which you can appreciate the "Send to sqlmap" as shown in the following image:

[img]<http://imageshack.us/a/img846/9759/67700130.png>[/img]

If we click on that option will open a new window (sqlmap wrapper) that will configure sqlmap.

[img]<http://imageshack.us/a/img854/9093/68075536.png>[/img]

It shows the overview of the configuration features in the "Target" specifies the URL you're testing (usually filled by default as it has previously sent the request parameters).

We specify the method in which the domain is accessible (GET/POST), then in the "bin-path" seek the location and load the file sqlmap sqlmap.py

In "Custom Options" you can select the options you execute the tool, for example we can list the database users, passwords, roles, privileges, databases, etc.. Default is set to "Auto" which means that the tool tried to list all the options listed.

Sqlmap Once configured, click on "Run" to open a new tab with the execution of the configuration, as shown in the following image:

[img]<http://imageshack.us/a/img812/3240/77723773.png>[/img]

One can see that the website is vulnerable, so it is accessible database.

Now we will try to list all the tables in the database "intranet", for it set the sqlmap wrapper with "Enumerate database tables" which returns the following results:

[img]<http://imageshack.us/a/img35/7629/50831189.png>[/img]

Then we list the table "dbo.BusquedaWeb" for its columns, select the option for it "Enumerate database tables and columns" returning the following result:

[img]<http://imageshack.us/a/img705/6294/69630536.png>[/img]

As we already have the data of the database, tables and columns, we will give Dump to get the final results, we will use the option "Dump DBMS database" getting the latest results as shown in the

following image:

[img]http://imageshack.us/a/img526/4857/14350533.png[/img]

After obtaining the data we "want" can save the contents of the information obtained, to select it in the "Save to file" which will be saved in a text file.

[img]http://imageshack.us/a/img812/1451/13418383.png[/img]

You see, audit a website from BurpSuite with this plugin is very comfortable and efficient, which helps us a lot in this process so tedious that usually the Penetration Test.

I hope they can.

Greetings. ?

Hooded Robin - *October 17, 2012, 10:41 am*

Thanks for sharing this, its a cool plugin. I previously just logged proxy traffic from Burp to file and then import/analyse with sqlmap. This saves a bit of time though.

Jae? - *October 17, 2012, 12:05 pm*

Great tutorial, really goes into detail. I can honestly say I've never used burp due to laziness.

chronical - *October 17, 2012, 12:05 pm*

Thank for this burp tutorial release