

BULK SQL Injection Test on Burp Requests

Author: Milad Khoshdel

Email: miladkhoshdel@gmail.com

Contents

INTRODUCTION.....	3
What is QL Injection Attack	3
What is SQLMap.....	3
What is Burp Suite Scanner	4
Exporting Packets from Burp Suite	4
Installing Burp-to-SQLMap Script	6
Running Burp-To-SQLMap Script	7
Refrences	8

INTRODUCTION

As you know, SQL Injection is a security vulnerability with critical severity. If you are a hacker you know it as well that it takes a lot of times to find a sql injection vulnerability on a target. It will be worse if you are a penetration tester. You must check this vulnerability on all of target URLs by intercepting packets using Burp Suit or other tools and in big Portals it's not easy.

I have good news for hackers and pen testers. I made it easier by my new python script. The only thing you should do, is exporting your packets as a burp suit state file. The rest of steps will done by my script. I called me script "Burp-TO-SQLMap" and I will explain the test process from the beginning.

What is SQL Injection Attack

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

What is SQLMap

Sqlmap is an open source software that is used to detect and exploit database vulnerabilities and provides options for injecting malicious codes into them. It is a penetration testing tool that automates the process of detecting and exploiting SQL injection flaws providing its user interface in the terminal. The software is run at the command line and is available to download for different operating systems: Linux distributions, Windows and Mac OS operating systems.

In addition to mapping and detecting vulnerabilities, the software enables access to the database, editing and deleting data, and viewing data in tables such as users, passwords, backups, phone numbers, e-mail addresses, credit cards and other confidential and sensitive information.

Sqlmap has full support for multiple DBMSs, including MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird and SAP MaxDB And full support for all injection techniques: Boolean, Error, Stack, Time, Union.

What is Burp Suite Scanner

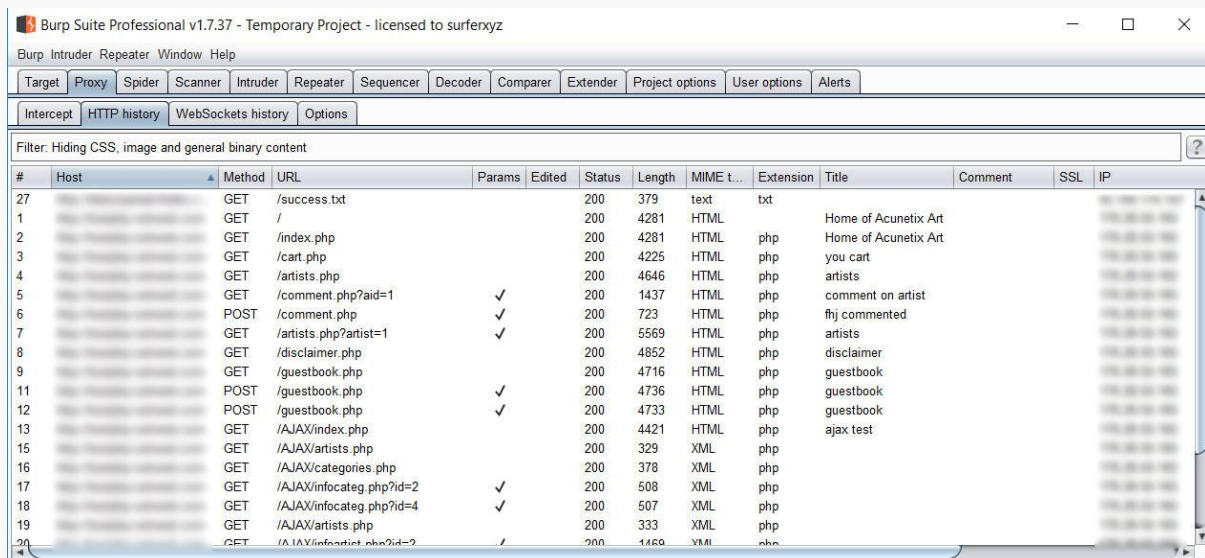
Burp or Burp Suite is a graphical tool for testing Web application security. The tool is written in Java and developed by PortSwigger Security. It was developed to provide a comprehensive solution for web application security checks. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a spider, a repeater, a decoder, a comparer, an extender and a sequencer.

Exporting Packets from Burp Suite

First of all you should open your Burp Suite application and browse your target URLs. Remember that you should set your browser proxy on Burp Suite. Burp will Crawl Your Target Automatically and save all of packets in HTTP history Tab.

Click on **Proxy > HTTP history** to see your Burp Suite Packet history.

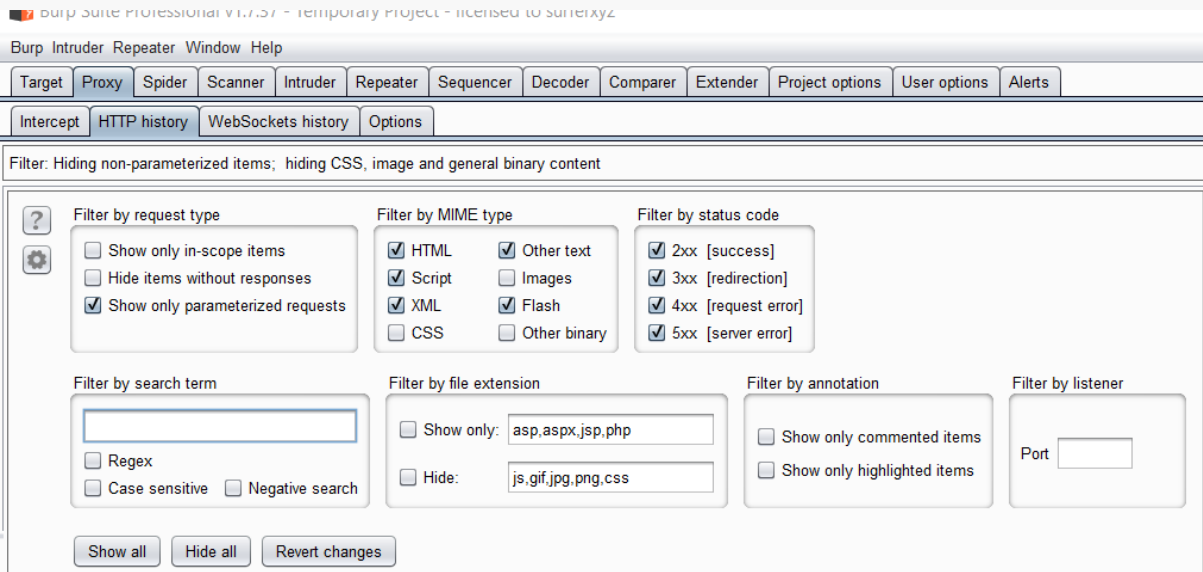
Note: if you browse other websites during the test process, you should click on HOST header column to set order on that. So you will have all of your target packets in one place.



#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP
27		GET	/success.txt			200	379	text	txt				
1		GET	/			200	4281	HTML		Home of Acunetix Art			
2		GET	/index.php			200	4281	HTML	php	Home of Acunetix Art			
3		GET	/cart.php			200	4225	HTML	php	you cart			
4		GET	/artists.php			200	4646	HTML	php	artists			
5		GET	/comment.php?aid=1		✓	200	1437	HTML	php	comment on artist			
6		POST	/comment.php		✓	200	723	HTML	php	fbj commented			
7		GET	/artists.php?artist=1		✓	200	5569	HTML	php	artists			
8		GET	/disclaimer.php			200	4852	HTML	php	disclaimer			
9		GET	/guestbook.php			200	4716	HTML	php	guestbook			
11		POST	/guestbook.php		✓	200	4736	HTML	php	guestbook			
12		POST	/guestbook.php		✓	200	4733	HTML	php	guestbook			
13		GET	/AJAX/index.php			200	4421	HTML	php	ajax test			
15		GET	/AJAX/artists.php			200	329	XML	php				
16		GET	/AJAX/categories.php			200	378	XML	php				
17		GET	/AJAX/infocateg.php?id=2		✓	200	508	XML	php				
18		GET	/AJAX/infocateg.php?id=4		✓	200	507	XML	php				
19		GET	/AJAX/artists.php			200	333	XML	php				
20		GET	/AJAX/infocateg.php?id=2		✓	200	1469	XML	php				

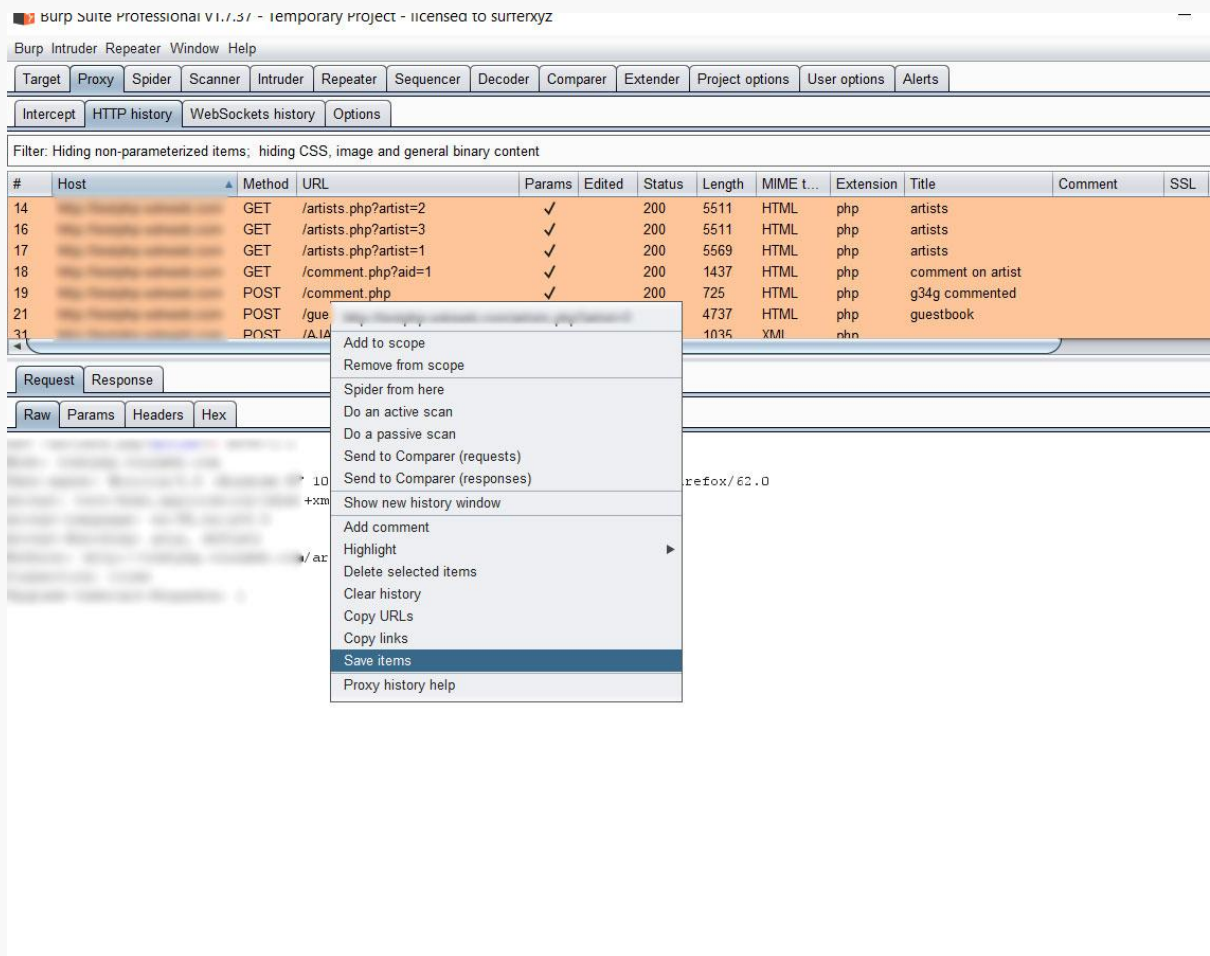
Based on out explanation in INTRODUCTION, Burp-TO-SQLMap script performs SQL Injection test using SQLMAP and SQLMap needs URLs with valid Parameters (POST/GET). So you should only select parametrized requests. Fortunately, this is easy and you can filter parametrized packets with just two clicks.

Click On **Filter** Section and select **Show only parametrized requests**.

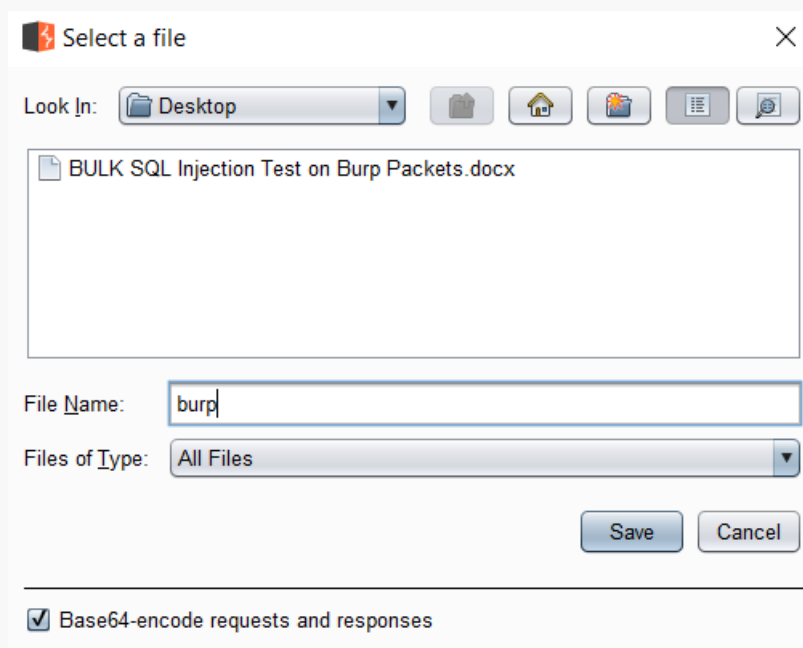


As you see Now we only have parametrized requests.

Select all of your target packets for performing SQL Injection Test. Right Click and Click on **Save items**.



In the new windows, uncheck **Base64-encode requests and responses**. Choose a name for your burp state file and save it. Now its done and you only need to run script, give this file as input and get the vulnerability result in output.



Installing Burp-to-SQLMap Script

You can use Burp-to-SQLMap script on windows platform. But we have some plan for extend it to work on Linux and mac.

- 1) Download and Install python 2.7 (you can download it from bellow URL)
 - <https://www.python.org/download/releases/2.7/>
- 2) Download and install java SE from bellow URL.
 - <http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>
- 3) Download and install latest version of Burp Suite from bellow URL.
 - <https://portswigger.net/burp/communitydownload>
- 4) Download and Install sql map. (you can download it from sqlmap website)
 - <http://sqlmap.org/>
- 5) Download Burp-To-SQLMap script from Github.
 - <https://github.com/Miladkhoshdel/burp-to-sqlmap>

Running Burp-To-SQLMap Script

Run Script with bellow command.

```
C:\> python burp-to-sqlmap.py -f burp -o result -s D:\Apps\SQLMAP
```

Note:

- ❖ -f Input File (Burp State File)
- ❖ -o Output Directory
- ❖ -s SQLMap Path

Script will extract all of GET/POST request and save each request in separate file in output directory. After that script will run sqlmap and test request files one by one and print the result. For vulnerable requests it print **URL is not Vulnerable** and for other URLs it print **URL is not Vulnerable**.

Also it will print the complete sqlmap output for each request in a separate file beside the request file in output directory.

```
C:\Users\Tester\PycharmProjects\burp-to-sqlmap>python burp-to-sqlmap.py -f burp -o result -s D:\Apps\SQLMAP

#####
#                                                                    #
#   _____   _____   _____   _____   _____   #
#  /   _  _  \  /   _  _  \  /   _  _  \  /   _  _  \  /   _  _  \ #
# /   /  /  \ /   /  /  \ /   /  /  \ /   /  /  \ /   /  /  \ /   #
# \   \  \  / \   \  \  / \   \  \  / \   \  \  / \   \  \  / \   #
#  \___/  \_/  \___/  \_/  \___/  \_/  \___/  \_/  \___/  \_/  \___#
#                                                                    #
#   Created By: Milad Khoshdel    Blog: https://blog.regex.com #
#                                                                    #
#                                                                    #
#####

[+] Exporting Packets ...
[-] Packet 1 Exported.
[-] Packet 2 Exported.
[-] Packet 3 Exported.
[-] Packet 4 Exported.
[-] Packet 5 Exported.
[-] Packet 6 Exported.
[-] Packet 7 Exported.

7 Packets Exported Successfully.

[+] Testing SQL Injection on packets ... (Based on your network connection Test can take up to 5 minutes.)
[-] Performing SQL Injection on packet number 1. Please Wait ...
- URL is Vulnerable.
- Output saved in result\testresult1.txt

[-] Performing SQL Injection on packet number 2. Please Wait ...
- URL is Vulnerable.
- Output saved in result\testresult2.txt

[-] Performing SQL Injection on packet number 3. Please Wait ...
- URL is Vulnerable.
- Output saved in result\testresult3.txt

[-] Performing SQL Injection on packet number 4. Please Wait ...
- URL is not Vulnerable.
- Output saved in result\testresult4.txt

[-] Performing SQL Injection on packet number 5. Please Wait ...
```

Also if you open your Output directory, you can see list of requests and result file. You can use it for your exploit evidence or POC.

References

1. https://www.owasp.org/index.php/SQL_Injection
2. https://en.wikipedia.org/wiki/SQL_injection
3. https://en.wikipedia.org/wiki/Burp_suite
4. <https://en.wikipedia.org/wiki/Sqlmap>