sqlmap frequently asked questions (FAQ)

Bernardo Damele A. G. and Miroslav Stampar

July 14, 2012 (**DRAFT**)

Abstract

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Contents

1 Frequently Asked Questions

1.1 What is sqlmap?

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

1.2 How do I execute sqlmap?

If you are running on a Unix/Linux system type the following command from a terminal:

```
python sqlmap.py -h
```

If you are running on a Windows system type the following command from a terminal:

```
C:\Python27\python.exe sqlmap.py -h
```

Where `C:\Python27` is the path where you installed Python >= **2.6**.

1.3 Can I integrate sqlmap with a security tool I am developing?

Yes. sqlmap is released under the terms of the GPLv2, which means that any derivative work must be distributed without further restrictions on the rights granted by the GPL itself.

1.4 Will you support other database management systems?

Yes. There are plans to support also Informix and Ingres at some point of time.

1.5 How can I occasionally contribute?

All help is greatly appreciated. First of all download the tool, make sure you are running the latest development version from the Subversion repository, read the user's manual carefully, have fun with it during your penetration tests. If you find bugs or have ideas for possible improvements, feel free to get in touch on the mailing list. Many people have contributed in different ways to the sqlmap development. **You** can be the next!

1.6 Can I actively contribute in the long-term development?

Yes, we are looking for people who can write some clean Python code, are up to do security research, know about web application security, database assessment and takeover, software refactoring and are motivated to join the development team. If this sounds interesting to you, get in touch!

1.7 How can I support the development?

If you think that sqlmap is a great tool, it really played well during your penetration tests, or you simply like it, you, or your boss, can donate some money to the developers via PayPal.

1.8 Can you hack a site for me?

No.

1.9 When sqlmap will switch to the Python 3?

Currently there is no pressure on Python projects to switch to the new version of Python interpreter, as the process of switching, especially on larger projects can be cumbersome (due to the few backward incompatibilities). The switch will take place eventually, but currently it's a very low priority task.

1.10 What does "WARNING unknown charset '...'" mean?

sqlmap needs to properly decode page content to be able to properly detect and deal with internationalized characters. In some cases web developers are doing mistakes when declaring used web page charset (e.g. `iso_8859` instead of standardized name `iso-8859`), which can cause problems. As a failsafe mechanism we've incorporated heuristic detection engine chardet, so in most cases sqlmap will deal with this kind of problems automatically. Nevertheless, you are strongly advised to report us back those typographic "mistakes" so we could handle them manually inside the code.

Question(s): #1 #2 #3

1.11 How to use sqlmap with `mod_rewrite` enabled?

Just put * to the place where sqlmap should check for injections in URI itself. In example: `./sqlmap.py -u "www.site.com/id1/1*/id2/2"` sqlmap will try to inject the payloads just at that place marked with * character.

Question(s): #1 #2 #3

1.12 Why is sqlmap not able to get password hashes in some cases?

You most probably don't have enough permissions for querying on a system table containing password hashes.

Question(s): #1

1.13 What is `--text-only` switch?

Switch `--text-only` is used for removing non-textual data (tags, javascripts, styles,...) from the retrieved page content to further improve detection capabilities.

Question(s): #1

1.14 I am getting "CRITICAL connection timed" while I am able to browse

the site normally?

There are few IDSes that filter out all sqlmap requests based on default User-Agent HTTP header used (e.g. `"User-agent:  sqlmap/1.0-dev"`). To prevent this kind of situations you are advised to use switch `--random-agent`. If you are getting those kind of messages for all targets then you most probably need to properly set up your proxy settings (switches `--proxy` and/or `--ignore-proxy`)

Question(s): #1

1.15 Is it possible to use `"INSERT/UPDATE"` SQL commands via `--sql-query`

and/or `--sql-shell`?

It is possible to use those commands, but only if the stacked injection is supported by the vulnerable target. In vast majority of cases affected DBMSes by these kind of attacks are Microsoft SQL Server and PostgreSQL.

Question(s): #1

1.16 I am getting `"finally: SyntaxError: invalid syntax"` when trying to run sqlmap?

You are most probably using outdated version of Python. sqlmap is generally supported by Python versions in range 2.5, 2.6 and 2.7, while you are strongly advised to use versions 2.6 and 2.7.

Question(s): #1

1.17 sqlmap is not able to detect/exploit injection while other commercial tools are?

In most of those kind of cases blatant error message detection is used by commercial tools making some “false positive” claims. You have to be aware that DBMS error message doesn’t mean that the affected web application is vulnerable to SQL injection attacks. sqlmap goes several steps further and never claims an injection point without making through tests if it can be exploited at the first place.

Question(s): #1