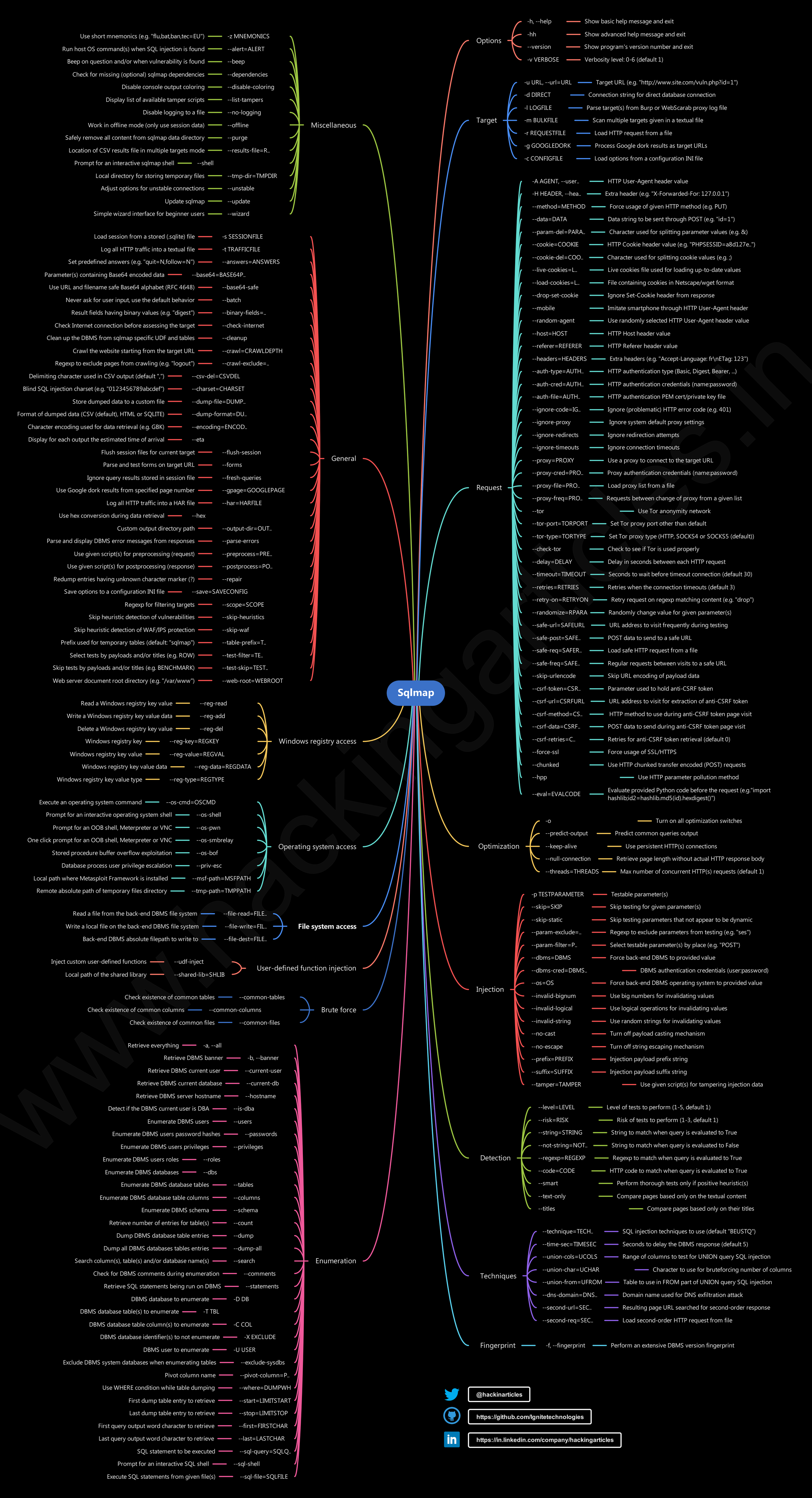
Sqlmap
Options
-h, --help
Show basic help message and exit
-hh
Show advanced help message and exit
--version
Show program's version number and exit
-v VERBOSE
Verbosity level: 0-6 (default 1)
Target
-u URL, --url=URL
Target URL (e.g. "http://www.site.com/vuln.php?id=1")
-d DIRECT
Connection string for direct database connection
-l LOGFILE
Parse target(s) from Burp or WebScarab proxy log file
-m BULKFILE
Scan multiple targets given in a textual file
-r REQUESTFILE
Load HTTP request from a file
-g GOOGLEDORK
Process Google dork results as target URLs
-c CONFIGFILE
Load options from a configuration INI file
Request
-A AGENT, --user..
HTTP User-Agent header value
-H HEADER, --hea..
Extra header (e.g. "X-Forwarded-For: 127.0.0.1")
--method=METHOD
Force usage of given HTTP method (e.g. PUT)
--data=DATA
Data string to be sent through POST (e.g. "id=1")
--param-del=PARA..
Character used for splitting parameter values (e.g. &)
--cookie=COOKIE
HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
--cookie-del=COO..
Character used for splitting cookie values (e.g. ;)
--live-cookies=L..
Live cookies file used for loading up-to-date values
--load-cookies=L..
File containing cookies in Netscape/wget format
--drop-set-cookie
Ignore Set-Cookie header from response
--mobile
Imitate smartphone through HTTP User-Agent header
--random-agent
Use randomly selected HTTP User-Agent header value
--host=HOST
HTTP Host header value
--referer=REFERER
HTTP Referer header value
--headers=HEADERS
Extra headers (e.g. "Accept-Language: fr\nETag: 123")
--auth-type=AUTH..
HTTP authentication type (Basic, Digest, Bearer, ...)
--auth-cred=AUTH..
HTTP authentication credentials (name:password)
--auth-file=AUTH..
HTTP authentication PEM cert/private key file
--ignore-code=IG..
Ignore (problematic) HTTP error code (e.g. 401)
--ignore-proxy
Ignore system default proxy settings
--ignore-redirects
Ignore redirection attempts
--ignore-timeouts
Ignore connection timeouts
--proxy=PROXY
Use a proxy to connect to the target URL
--proxy-cred=PRO..
Proxy authentication credentials (name:password)
--proxy-file=PRO..
Load proxy list from a file
--proxy-freq=PRO..
Requests between change of proxy from a given list
--tor
Use Tor anonymity network
--tor-port=TORPORT
Set Tor proxy port other than default
--tor-type=TORTYPE
Set Tor proxy type (HTTP, SOCKS4 or SOCKS5 (default))
--check-tor
Check to see if Tor is used properly
--delay=DELAY
Delay in seconds between each HTTP request
--timeout=TIMEOUT
Seconds to wait before timeout connection (default 30)
--retries=RETRIES
Retries when the connection timeouts (default 3)
--retry-on=RETRYON
Retry request on regexp matching content (e.g. "drop")
--randomize=RPARA
Randomly change value for given parameter(s)
--safe-url=SAFEURL
URL address to visit frequently during testing
--safe-post=SAFE..
POST data to send to a safe URL
--safe-req=SAFER..
Load safe HTTP request from a file
--safe-freq=SAFE..
Regular requests between visits to a safe URL
--skip-urlencode
Skip URL encoding of payload data
--csrf-token=CSR..
Parameter used to hold anti-CSRF token
--csrf-url=CSRFURL
URL address to visit for extraction of anti-CSRF token
--csrf-method=CS..
HTTP method to use during anti-CSRF token page visit
--csrf-data=CSRF..
POST data to send during anti-CSRF token page visit
--csrf-retries=C..
Retries for anti-CSRF token retrieval (default 0)
--force-ssl
Force usage of SSL/HTTPS
--chunked
Use HTTP chunked transfer encoded (POST) requests
--hpp
Use HTTP parameter pollution method
--eval=EVALCODE
Evaluate provided Python code before the request (e.g."import hashlib;id2=hashlib.md5(id).hexdigest()")
Optimization
-o
Turn on all optimization switches
--predict-output
Predict common queries output
--keep-alive
Use persistent HTTP(s) connections
--null-connection
Retrieve page length without actual HTTP response body
--threads=THREADS
Max number of concurrent HTTP(s) requests (default 1)
Injection
-p TESTPARAMETER
Testable parameter(s)
--skip=SKIP
Skip testing for given parameter(s)
--skip-static
Skip testing parameters that not appear to be dynamic
--param-exclude=..
Regexp to exclude parameters from testing (e.g. "ses")
--param-filter=P..
Select testable parameter(s) by place (e.g. "POST")
--dbms=DBMS
Force back-end DBMS to provided value
--dbms-cred=DBMS..
DBMS authentication credentials (user:password)
--os=OS
Force back-end DBMS operating system to provided value
--invalid-bignum
Use big numbers for invalidating values
--invalid-logical
Use logical operations for invalidating values
--invalid-string
Use random strings for invalidating values
--no-cast
Turn off payload casting mechanism
--no-escape
Turn off string escaping mechanism
--prefix=PREFIX
Injection payload prefix string
--suffix=SUFFIX
Injection payload suffix string
--tamper=TAMPER
Use given script(s) for tampering injection data
Detection
--level=LEVEL
Level of tests to perform (1-5, default 1)
--risk=RISK
Risk of tests to perform (1-3, default 1)
--string=STRING
String to match when query is evaluated to True
--not-string=NOT..
String to match when query is evaluated to False
--regexp=REGEXP
Regexp to match when query is evaluated to True
--code=CODE
HTTP code to match when query is evaluated to True
--smart
Perform thorough tests only if positive heuristic(s)
--text-only
Compare pages based only on the textual content
--titles
Compare pages based only on their titles
Techniques
--technique=TECH..
SQL injection techniques to use (default "BEUSTQ")
--time-sec=TIMESEC
Seconds to delay the DBMS response (default 5)
--union-cols=UCOLS
Range of columns to test for UNION query SQL injection
--union-char=UCHAR
Character to use for bruteforcing number of columns
--union-from=UFROM
Table to use in FROM part of UNION query SQL injection
--dns-domain=DNS..
Domain name used for DNS exfiltration attack
--second-url=SEC..
Resulting page URL searched for second-order response
--second-req=SEC..
Load second-order HTTP request from file
Fingerprint
-f, --fingerprint
Perform an extensive DBMS version fingerprint
Miscellaneous
-z MNEMONICS
Use short mnemonics (e.g. "flu,bat,ban,tec=EU")
--alert=ALERT
Run host OS command(s) when SQL injection is found
--beep
Beep on question and/or when vulnerability is found
--dependencies
Check for missing (optional) sqlmap dependencies
--disable-coloring
Disable console output coloring
--list-tampers
Display list of available tamper scripts
--no-logging
Disable logging to a file
--offline
Work in offline mode (only use session data)
--purge
Safely remove all content from sqlmap data directory
--results-file=R..
Location of CSV results file in multiple targets mode
--shell
Prompt for an interactive sqlmap shell
--tmp-dir=TMPDIR
Local directory for storing temporary files
--unstable
Adjust options for unstable connections
--update
Update sqlmap
--wizard
Simple wizard interface for beginner users
General
-s SESSIONFILE
Load session from a stored (.sqlite) file
-t TRAFFICFILE
Log all HTTP traffic into a textual file
--answers=ANSWERS
Set predefined answers (e.g. "quit=N,follow=N")
--base64=BASE64P..
Parameter(s) containing Base64 encoded data
--base64-safe
Use URL and filename safe Base64 alphabet (RFC 4648)
--batch
Never ask for user input, use the default behavior
--binary-fields=..
Result fields having binary values (e.g. "digest")
--check-internet
Check Internet connection before assessing the target
--cleanup
Clean up the DBMS from sqlmap specific UDF and tables
--crawl=CRAWLDEPTH
Crawl the website starting from the target URL
--crawl-exclude=..
Regexp to exclude pages from crawling (e.g. "logout")
--csv-del=CSVDEL
Delimiting character used in CSV output (default ",")
--charset=CHARSET
Blind SQL injection charset (e.g. "0123456789abcdef")
--dump-file=DUMP..
Store dumped data to a custom file
--dump-format=DU..
Format of dumped data (CSV (default), HTML or SQLITE)
--encoding=ENCOD..
Character encoding used for data retrieval (e.g. GBK)
--eta
Display for each output the estimated time of arrival
--flush-session
Flush session files for current target
--forms
Parse and test forms on target URL
--fresh-queries
Ignore query results stored in session file
--gpage=GOOGLEPAGE
Use Google dork results from specified page number
--har=HARFILE
Log all HTTP traffic into a HAR file
--hex
Use hex conversion during data retrieval
--output-dir=OUT..
Custom output directory path
--parse-errors
Parse and display DBMS error messages from responses
--preprocess=PRE..
Use given script(s) for preprocessing (request)
--postprocess=PO..
Use given script(s) for postprocessing (response)
--repair
Redump entries having unknown character marker (?)
--save=SAVECONFIG
Save options to a configuration INI file
--scope=SCOPE
Regexp for filtering targets
--skip-heuristics
Skip heuristic detection of vulnerabilities
--skip-waf
Skip heuristic detection of WAF/IPS protection
--table-prefix=T..
Prefix used for temporary tables (default: "sqlmap")
--test-filter=TE..
Select tests by payloads and/or titles (e.g. ROW)
--test-skip=TEST..
Skip tests by payloads and/or titles (e.g. BENCHMARK)
--web-root=WEBROOT
Web server document root directory (e.g. "/var/www")
Windows registry access
--reg-read
Read a Windows registry key value
--reg-add
Write a Windows registry key value data
--reg-del
Delete a Windows registry key value
--reg-key=REGKEY
Windows registry key
--reg-value=REGVAL
Windows registry key value
--reg-data=REGDATA
Windows registry key value data
--reg-type=REGTYPE
Windows registry key value type
Operating system access
--os-cmd=OSCMD
Execute an operating system command
--os-shell
Prompt for an interactive operating system shell
--os-pwn
Prompt for an OOB shell, Meterpreter or VNC
--os-smbrelay
One click prompt for an OOB shell, Meterpreter or VNC
--os-bof
Stored procedure buffer overflow exploitation
--priv-esc
Database process user privilege escalation
--msf-path=MSFPATH
Local path where Metasploit Framework is installed
--tmp-path=TMPPATH
Remote absolute path of temporary files directory
File system access
--file-read=FILE..
Read a file from the back-end DBMS file system
--file-write=FIL..
Write a local file on the back-end DBMS file system
--file-dest=FILE..
Back-end DBMS absolute filepath to write to
User-defined function injection
--udf-inject
Inject custom user-defined functions
--shared-lib=SHLIB
Local path of the shared library
Brute force
--common-tables
Check existence of common tables
--common-columns
Check existence of common columns
--common-files
Check existence of common files
Enumeration
-a, --all
Retrieve everything
-b, --banner
Retrieve DBMS banner
--current-user
Retrieve DBMS current user
--current-db
Retrieve DBMS current database
--hostname
Retrieve DBMS server hostname
--is-dba
Detect if the DBMS current user is DBA
--users
Enumerate DBMS users
--passwords
Enumerate DBMS users password hashes
--privileges
Enumerate DBMS users privileges
--roles
Enumerate DBMS users roles
--dbs
Enumerate DBMS databases
--tables
Enumerate DBMS database tables
--columns
Enumerate DBMS database table columns
--schema
Enumerate DBMS schema
--count
Retrieve number of entries for table(s)
--dump
Dump DBMS database table entries
--dump-all
Dump all DBMS databases tables entries
--search
Search column(s), table(s) and/or database name(s)
--comments
Check for DBMS comments during enumeration
--statements
Retrieve SQL statements being run on DBMS
-D DB
DBMS database to enumerate
-T TBL
DBMS database table(s) to enumerate
-C COL
DBMS database table column(s) to enumerate
-X EXCLUDE
DBMS database identifier(s) to not enumerate
-U USER
DBMS user to enumerate
--exclude-sysdbs
Exclude DBMS system databases when enumerating tables
--pivot-column=P..
Pivot column name
--where=DUMPWH
Use WHERE condition while table dumping
--start=LIMITSTART
First dump table entry to retrieve
--stop=LIMITSTOP
Last dump table entry to retrieve
--first=FIRSTCHAR
First query output word character to retrieve
--last=LASTCHAR
Last query output word character to retrieve
--sql-query=SQLQ..
SQL statement to be executed
--sql-shell
Prompt for an interactive SQL shell
--sql-file=SQLFILE
Execute SQL statements from given file(s)
@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles