CveSearch

Paul Tikken

Oct 02, 2020

CVESEARCH

GETTING STARTED

The CveSearch project is. . . .

1.1 Dependencies

The following system packages are required by reaper. See installing on how to install them.

- redis
- mongodb

CVESEARCH

2.1 CveSearch Main

class CveSearch.main.**CveSearch**(*mongodb_connection_details={}*)

> Bases: `object`

> Main class for CveSearch package

> **__init__**(*mongodb_connection_details={}*)
>> Initialize self. See help(type(self)) for accurate signature.

> **__repr__**()
>> String representation of object

> **capec_by_cwe_id**(*cwe_id*)
>> Method to retrieve capecs related to a specific CWE ID

>>> **Parameters** **cwe_id** – String representing the CWE id; e.g. '15'

>>> **Returns** List with Capecs

>>> **Return type** list

> **cve_by_id**(*cve_id*)
>> Method to retrieve a single CVE from the database by it's CVE ID number

>>> **Parameters** **cve_id** (*str*) – String representing the CVE id; e.g. CVE-2020-0001

>>> **Returns** CVE object

>>> **Return type** Cves

> **cves_for_cpe**(*cpe_string*, *vuln_prod_search=False*)
>> Method for retrieving Cves that match a single CPE string. By default the search will be made matching the configuration fields of the cves documents.

>>> **Parameters**

>>> - **cpe_string** (*str*) – CPE string: e.g. 'cpe:2.3:o:microsoft:windows_7::*sp1*:::::*'
>>> - **vuln_prod_search** (*bool*) – Search for matching products instead of configurations

>>> **Returns** List with Cves

>>> **Return type** list

> **property get_db_content_stats**
>> Property returning the stats from the database. Stats consist of the time last modified and the document count per cvedb store in the database.

>>> **Returns** Statistics

>>> **Return type** dict

get_multi_store_entries(**queries*)

    Method to perform *multiple* queries on *a single* or *multiple* collections in the mongodb and return the results.

        Parameters queries (`list`) – A list of tuples which contains the entry_type and the dict_filter. Choices for entry_type: - capec; - cpe; - cwe; - via4; - cves; dict_filter is a dictionary representing a filter according to pymongo documentation. example: get_multi_store_entries([("CWE", {"id": "78"}), ("cves", {"id": "CVE-2019-19178"})])

        Returns Queried results in a single list

        Return type list

get_single_store_entries(*query*)

    Method to perform a query on a *single* collection in the mongodb and return the results.

        Parameters query (`tuple`) – Tuple which contains the entry_type and the dict_filter in a tuple. Choices for entry_type: - capec; - cpe; - cwe; - via4; - cves; dict_filter is a dictionary representing a filter according to pymongo documentation. example: get_single_store_entries(("CWE", {"id": "78"}))

        Returns list with queried results

        Return type list

get_single_store_entry(*entry_type*, *dict_filter={}*)

    Method to perform a query on a *single* collection in the mongodb and return a *single* result.

        Parameters

            • **entry_type** (`str`) – Which specific store are you querying? Choices are: - capec; - cpe; - cwe; - via4; - cves;

            • **dict_filter** (`dict`) – Dictionary representing a filter according to pymongo documentation

        Returns Objectified result from the query

        Return type object

property version

    Property returning current version

THREE

INDICES AND TABLES

- genindex
- modindex
- search

PYTHON MODULE INDEX

C

CveSearch.main,

Symbols

C

G

M

V