INDEX

ABOUT NEMESIS

This script is designed to fetch vulnerability information from the National Vulnerability Database (NVD). Users can specify various query parameters through command-line arguments to search for vulnerabilities by CVE ID, keyword, CPE name, CWE ID, and more. The script can filter results based on CVSS v2 and v3 severity levels and allows users to save the output in either JSON or TXT format. It handles API key management, URL encoding, API request handling, and parsing and formatting of the fetched data for user-friendly output.

API REQUIERMENTS

The script requires an API key to function correctly, as it needs to authenticate requests made to the NVD API. Without an API key, the script will not be able to fetch any data from the NVD. Visit the following link to get an API:

https://nvd.nist.gov/developers/request-an-api-key

Users can configure the API key in three different ways:
1. **File**: Users can store their API key in the api-key.yaml file. The script will read this file to retrieve the API key if it is not provided elsewhere.

2. **Command line**: Users can use the *-a* or *--api* flag to specify the API key as a command line argument.

3. **Environment variable**: Users can set environment variable API_KEY along with the key value. The script will use this if the API key is not provided through the previous 2 methods.

CONFIGURING API KEY AS ENVIRONMENT VARIABLE

Windows

Execute the following command in cmd and restart your terminal:

```
setx API_KEY “Your API key”
```

Linux

Open the shell configuration file. For *bash* it is usually *~/.profile* , *~/.bashrc* , *~/.bash_profile.*

```
vim ~/.profile
```

Add the following command at the end of the file

```
export API_KEY=”your api key”
```

Save and close it and apply the changes

```
source ~/.profile
```

INSTALLATION

- Clone the repository

```
git clone https://github.com/RIZZZIOM/nemesis.git
```

- Move into the directory

```
cd nemesis
```

- Install requirements

```
pip install -r requirements.txt
```

FEATURES

- **Fetch Vulnerability Information**

Retrieve detailed information about a vulnerability from the National Vulnerability Database (NVD) based on various query parameters passed on by the user.

- **Query Parameters**

CVE ID	Search vulnerabilities using specific CVE IDs.
Keyword	Search vulnerabilities using specific keywords.
CPE Name	Search vulnerabilities using Common Platform Enumeration (CPE) names.
CWE ID	Search vulnerabilities using Common Weakness Enumeration (CWE) IDs.
Results Per Page	Specify the maximum number of vulnerabilities returned in a single response.
Start Index	Display vulnerabilities starting from a specified index.
CVSS v3 Severity	Filter results based on the CVSS v3 severity levels (LOW, MEDIUM, HIGH, CRITICAL).
CVSS v2 Severity	Filter results based on the CVSS v2 severity levels (LOW, MEDIUM, HIGH).

- **API Key Configuration**

Command Line Argument	Provide the API key directly via the **-a** or **--api** argument.
YAML File	Store the API key in an **api-key.yaml** file, which the script will read.
Environment Variable	Set the API key using the **API_KEY** environment variable.

• **Output Formats**

TXT File	Save the output in a human-readable text format.
JSON File	Save the output in a structured JSON format.

• **Command Line Interface**
User-friendly CLI for specifying query parameters and configuring output options.

• **Cross Platform**
Works on Windows and Linux.

LIBRARIES

- **ARGPARSE:** To parse command-line arguments.
This library is used to define and handle various command-line arguments that the user can provide to customize the script's behavior. It allows users to specify query parameters, output formats, and API keys through a user-friendly interface.

- ***SYS***: To interact with the Python interpreter.
This library is used to exit the script when necessary, particularly when required arguments are missing or when an error occurs. It provides a way to handle script termination cleanly.

- ***OS***: To interact with the operating system.
This library is used to check for the existence of files (like api-key.yaml) and to read environment variables (such as API_KEY). It enables the script to dynamically adapt to the environment it's running in.

- **PLATFORM**: To access underlying platform data.

This library is used to determine the operating system (e.g., Windows, Linux) to manage platform-specific behavior, particularly for reading environment variables.

- **URLLIB.PARSE.QUOTE**: To handle URL encoding.
This function is used to URL-encode query parameters, ensuring that special characters in service names and versions are correctly formatted for API requests.

- **REQUESTS**: To make HTTP requests.
This library is used to send HTTP GET requests to the NVD API. It handles the network communication required to fetch vulnerability information based on the provided query parameters.

- **JSON**: To handle JSON data.
This library is used to parse JSON responses from the NVD API and to format the output data as JSON when saving to a file. It enables the script to work with structured data efficiently.

- **YAML**: To handle YAML files.
This library is used to read the api-key.yaml file, allowing the script to retrieve the API key if it is not provided through the command line or environment variables. It provides a convenient way to manage configuration settings.

FUNCTIONS

GET_SERVICE

The *get_service* function parses command-line arguments to customize how the script fetches vulnerability information from the NVD. It defines various options for search parameters, result limits, severity filters, and output formats. The function ensures that necessary arguments are provided, validates them, and then returns a dictionary of these arguments for use in the script.

CPE2TOCPE3

The *cpe2tocpe3* function converts a Common Platform Enumeration (CPE) name from version 2.2 format to version 2.3 format. If the provided CPE name is already in version 2.3 format, it returns the original name. If the CPE name format is invalid, it raises an error.

ENCODE_SERVICE

The *encode_service* function URL-encodes certain values in a dictionary of command-line arguments to prepare them for API requests. It handles special characters, converts CPE names to version 2.3, and ensures CVE IDs are in the correct format.

QUERY_URL

The *query_url* function constructs a URL for querying the National Vulnerability Database (NVD) API based on URL-encoded argument names and values.

FETCH_RESPONSE

The *fetch_response* function sends a query URL to the National Vulnerability Database (NVD) API and retrieves the JSON response.

CLEAN_UP

The *clean_up* function processes raw JSON responses from the NVD API and extracts relevant information into a more usable format.

MAKE_TFILE

The *make_tfile* function creates a text file and appends the parsed vulnerability information into it.

MAKE_JFILE

The *make_jfile* function creates a JSON file and appends the parsed vulnerability information into it.

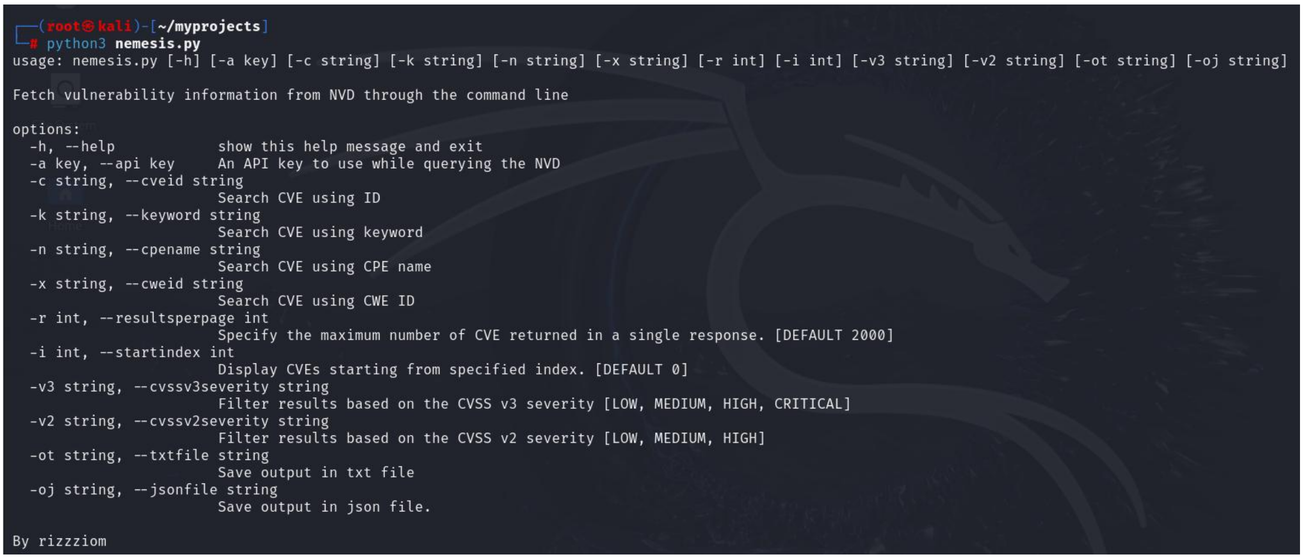
MAIN

The main function orchestrates the script's overall execution, managing input, processing, and output of vulnerability information.

USAGE

HELP MENU

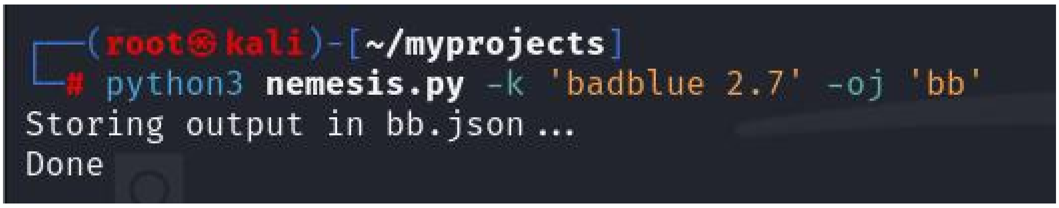
To see the help menu and get a brief description of all available arguments, use the *-h* or *--help* flag.



```
┌──(root㉿kali)-[~/myprojects]
└─# python3 nemesis.py
usage: nemesis.py [-h] [-a key] [-c string] [-k string] [-n string] [-x string] [-r int] [-i int] [-v3 string] [-v2 string] [-ot string] [-oj string]

Fetch vulnerability information from NVD through the command line

options:
  -h, --help            show this help message and exit
  -a key, --api key     An API key to use while querying the NVD
  -c string, --cveid string
                        Search CVE using ID
  -k string, --keyword string
                        Search CVE using keyword
  -n string, --cpename string
                        Search CVE using CPE name
  -x string, --cweid string
                        Search CVE using CWE ID
  -r int, --resultsperpage int
                        Specify the maximum number of CVE returned in a single response. [DEFAULT 2000]
  -i int, --startindex int
                        Display CVEs starting from specified index. [DEFAULT 0]
  -v3 string, --cvssv3severity string
                        Filter results based on the CVSS v3 severity [LOW, MEDIUM, HIGH, CRITICAL]
  -v2 string, --cvssv2severity string
                        Filter results based on the CVSS v2 severity [LOW, MEDIUM, HIGH]
  -ot string, --txtfile string
                        Save output in txt file
  -oj string, --jsonfile string
                        Save output in json file.

By rizzziom
```

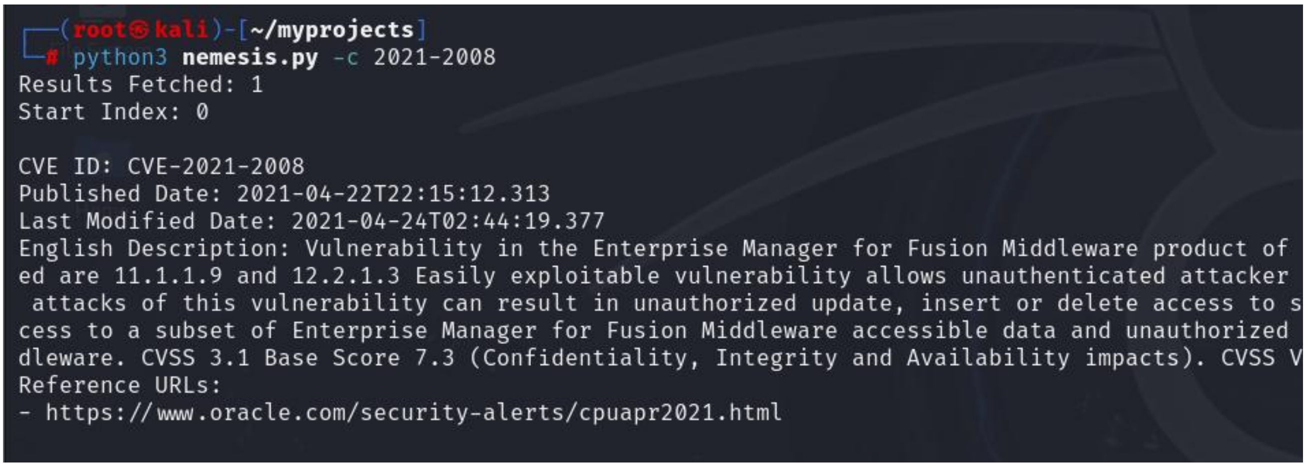
EXAMPLE COMMANDS

- Finding vulnerabilities using keyword and storing the information in a json file.



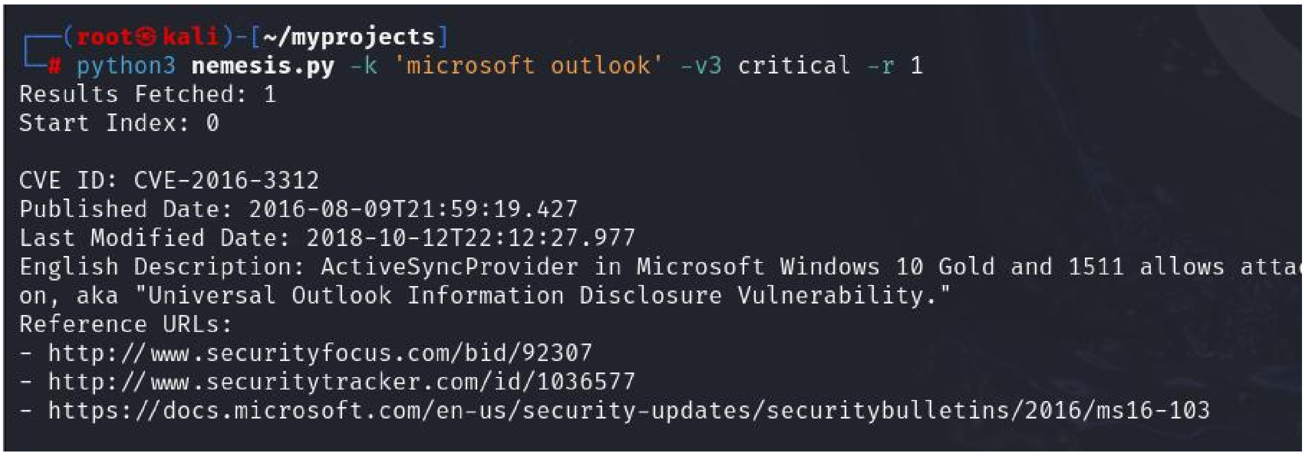
```
┌──(root㉿kali)-[~/myprojects]
└─# python3 nemesis.py -k 'badblue 2.7' -oj 'bb'
Storing output in bb.json ...
Done
```

- Finding vulnerability using CVE ID.



```
┌──(root㉿kali)-[~/myprojects]
└─# python3 nemesis.py -c 2021-2008
Results Fetched: 1
Start Index: 0

CVE ID: CVE-2021-2008
Published Date: 2021-04-22T22:15:12.313
Last Modified Date: 2021-04-24T02:44:19.377
English Description: Vulnerability in the Enterprise Manager for Fusion Middleware product of
ed are 11.1.1.9 and 12.2.1.3 Easily exploitable vulnerability allows unauthenticated attacker
 attacks of this vulnerability can result in unauthorized update, insert or delete access to s
cess to a subset of Enterprise Manager for Fusion Middleware accessible data and unauthorized
dleware. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS V
Reference URLs:
- https://www.oracle.com/security-alerts/cpuapr2021.html
```

- Filtering results based on severity of the vulnerability.



```
┌──(root㉿kali)-[~/myprojects]
└─# python3 nemesis.py -k 'microsoft outlook' -v3 critical -r 1
Results Fetched: 1
Start Index: 0

CVE ID: CVE-2016-3312
Published Date: 2016-08-09T21:59:19.427
Last Modified Date: 2018-10-12T22:12:27.977
English Description: ActiveSyncProvider in Microsoft Windows 10 Gold and 1511 allows atta
on, aka "Universal Outlook Information Disclosure Vulnerability."
Reference URLs:
- http://www.securityfocus.com/bid/92307
- http://www.securitytracker.com/id/1036577
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-103
```