Vuln Live List

중부대학교 정보보안SW융합전공

김두형, 김성준, 은정욱, 박형준

2022.12.16

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

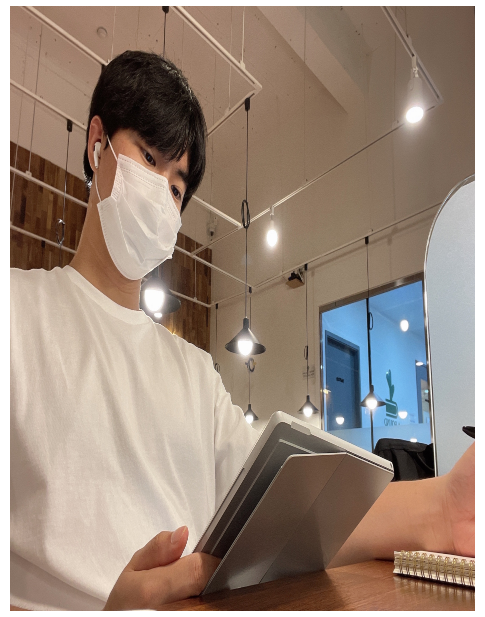
Index

- 팀원 소개
- 프로젝트 개요
- Crawler
- NLTK
- Web
- 개선점

팀원 소개

김두형

- 팀장
- Web Service



박형준

- CVE Crawler Develop

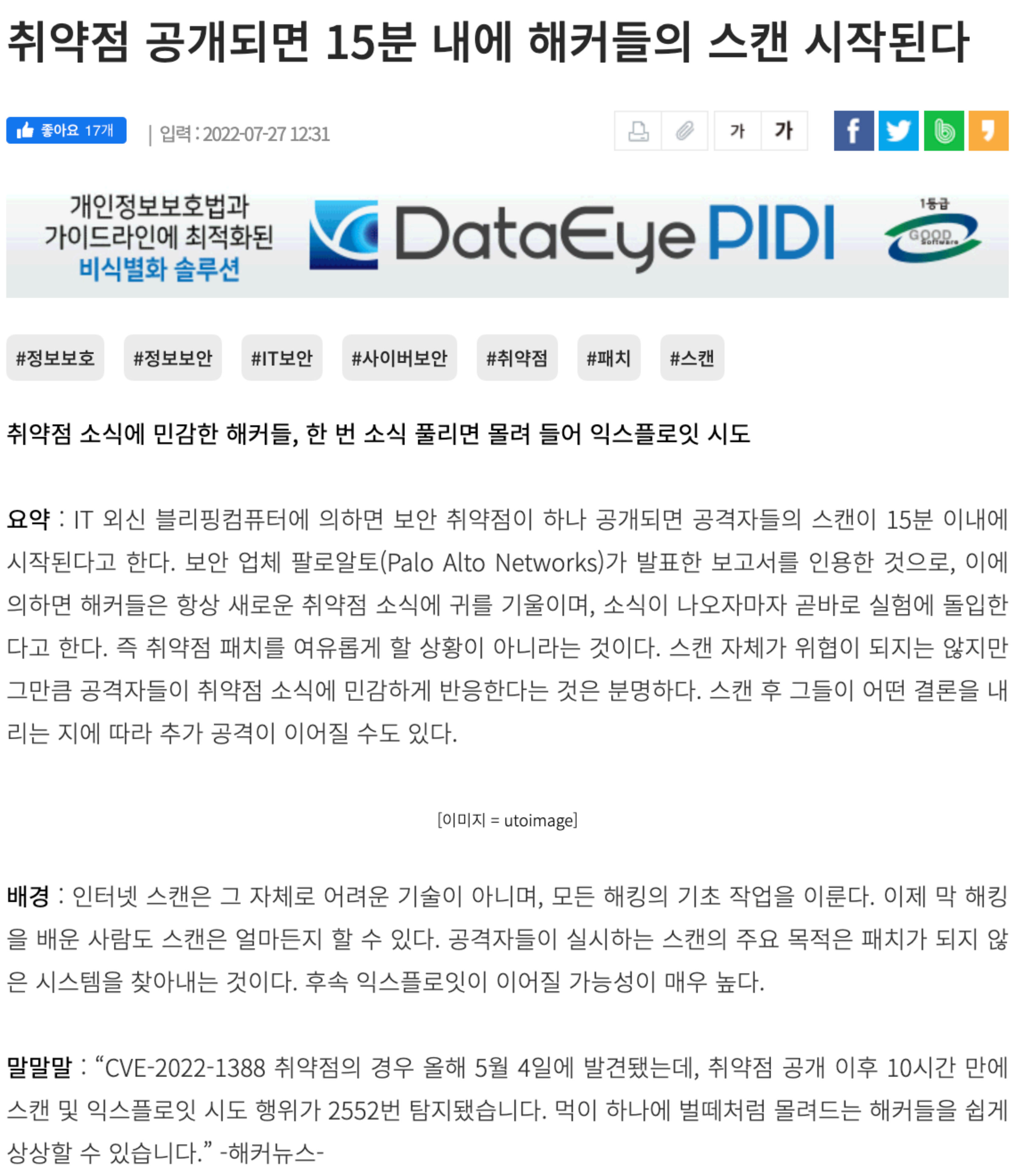
은정욱

- NLP

김성준

- CVE Crawler Develop
- ElasticSearch DB

프로젝트 개요



취약점 공개되면 15분 내에 해커들의 스캔 시작된다

좋아요 17개 | 입력 : 2022-07-27 12:31

가 가

#정보보호 #정보보안 #IT보안 #사이버보안 #취약점 #패치 #스캔

취약점 소식에 민감한 해커들, 한 번 소식 풀리면 몰려 들어 익스플로잇 시도

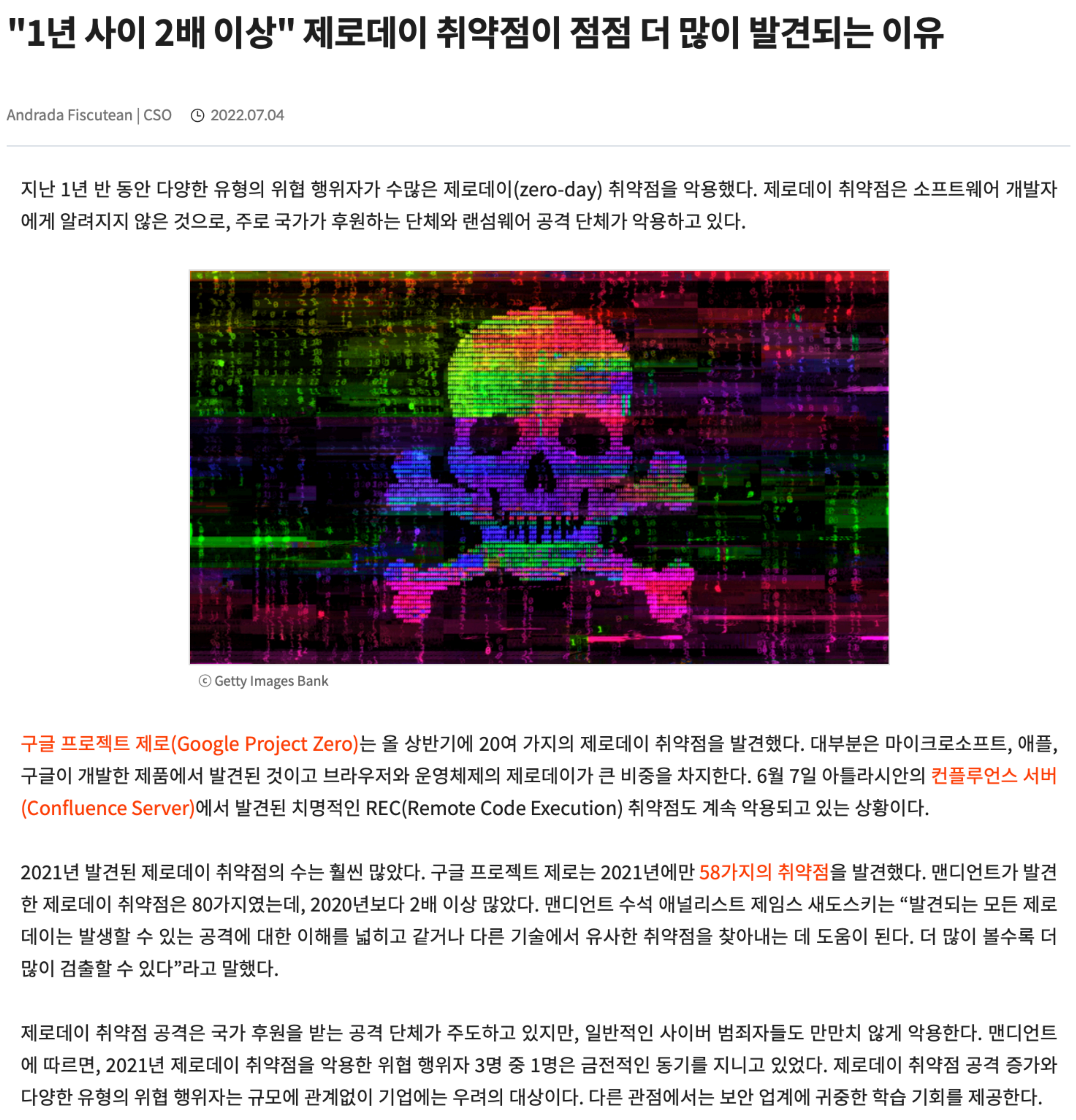
요약 : IT 외신 블리핑컴퓨터에 의하면 보안 취약점이 하나 공개되면 공격자들의 스캔이 15분 이내에 시작된다고 한다. 보안 업체 팔로알토(Palo Alto Networks)가 발표한 보고서를 인용한 것으로, 이에 의하면 해커들은 항상 새로운 취약점 소식에 귀를 기울이며, 소식이 나오자마자 곧바로 실험에 돌입한다고 한다. 즉 취약점 패치를 여유롭게 할 상황이 아니라는 것이다. 스캔 자체가 위협이 되지는 않지만 그만큼 공격자들이 취약점 소식에 민감하게 반응한다는 것은 분명하다. 스캔 후 그들이 어떤 결론을 내리는 지에 따라 추가 공격이 이어질 수도 있다.

[이미지 = utoimage]

배경 : 인터넷 스캔은 그 자체로 어려운 기술이 아니며, 모든 해킹의 기초 작업을 이룬다. 이제 막 해킹을 배운 사람도 스캔은 얼마든지 할 수 있다. 공격자들이 실시하는 스캔의 주요 목적은 패치가 되지 않은 시스템을 찾아내는 것이다. 후속 익스플로잇이 이어질 가능성이 매우 높다.

말말말 : "CVE-2022-1388 취약점의 경우 올해 5월 4일에 발견됐는데, 취약점 공개 이후 10시간 만에 스캔 및 익스플로잇 시도 행위가 2552번 탐지됐습니다. 먹이 하나에 벌떼처럼 몰려드는 해커들을 쉽게 상상할 수 있습니다." -해커뉴스-

https://www.boannews.com/media/view.asp?idx=108674&kind=1&search=title&find=%C3%EB%BE%E0%C1%A1



"1년 사이 2배 이상" 제로데이 취약점이 점점 더 많이 발견되는 이유

Andrada Fiscutean | CSO 2022.07.04

지난 1년 반 동안 다양한 유형의 위협 행위자가 수많은 제로데이(zero-day) 취약점을 악용했다. 제로데이 취약점은 소프트웨어 개발자에게 알려지지 않은 것으로, 주로 국가가 후원하는 단체와 랜섬웨어 공격 단체가 악용하고 있다.

ⓒ Getty Images Bank

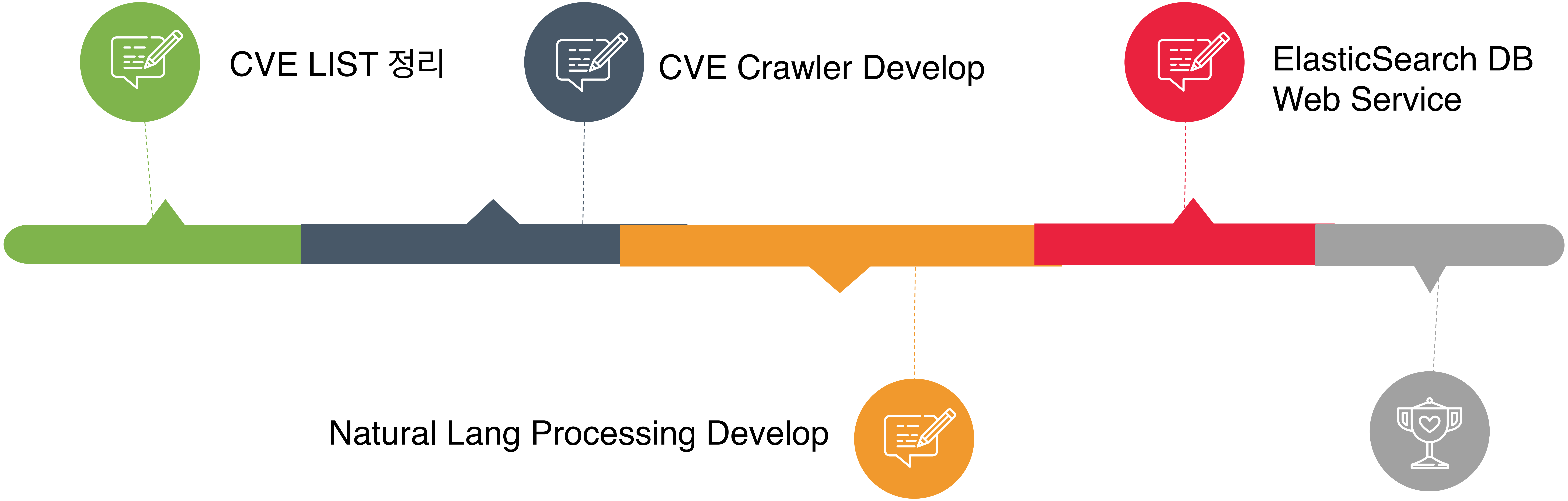
구글 프로젝트 제로(Google Project Zero)는 올 상반기에 20여 가지의 제로데이 취약점을 발견했다. 대부분은 마이크로소프트, 애플, 구글이 개발한 제품에서 발견된 것이고 브라우저와 운영체제의 제로데이가 큰 비중을 차지한다. 6월 7일 아틀라시안의 컨플루언스 서버(Confluence Server)에서 발견된 치명적인 REC(Remote Code Execution) 취약점도 계속 악용되고 있는 상황이다.

2021년 발견된 제로데이 취약점의 수는 훨씬 많았다. 구글 프로젝트 제로는 2021년에만 58가지의 취약점을 발견했다. 맨디언트가 발견한 제로데이 취약점은 80가지였는데, 2020년보다 2배 이상 많았다. 맨디언트 수석 애널리스트 제임스 새도스키는 "발견되는 모든 제로데이는 발생할 수 있는 공격에 대한 이해를 넓히고 같거나 다른 기술에서 유사한 취약점을 찾아내는 데 도움이 된다. 더 많이 볼수록 더 많이 검출할 수 있다"라고 말했다.

제로데이 취약점 공격은 국가 후원을 받는 공격 단체가 주도하고 있지만, 일반적인 사이버 범죄자들도 만만치 않게 악용한다. 맨디언트에 따르면, 2021년 제로데이 취약점을 악용한 위협 행위자 3명 중 1명은 금전적인 동기를 지니고 있었다. 제로데이 취약점 공격 증가와 다양한 유형의 위협 행위자는 규모에 관계없이 기업에는 우려의 대상이다. 다른 관점에서는 보안 업계에 귀중한 학습 기회를 제공한다.

https://www.itworld.co.kr/topnews/243019

프로젝트



CVE LIST 정리

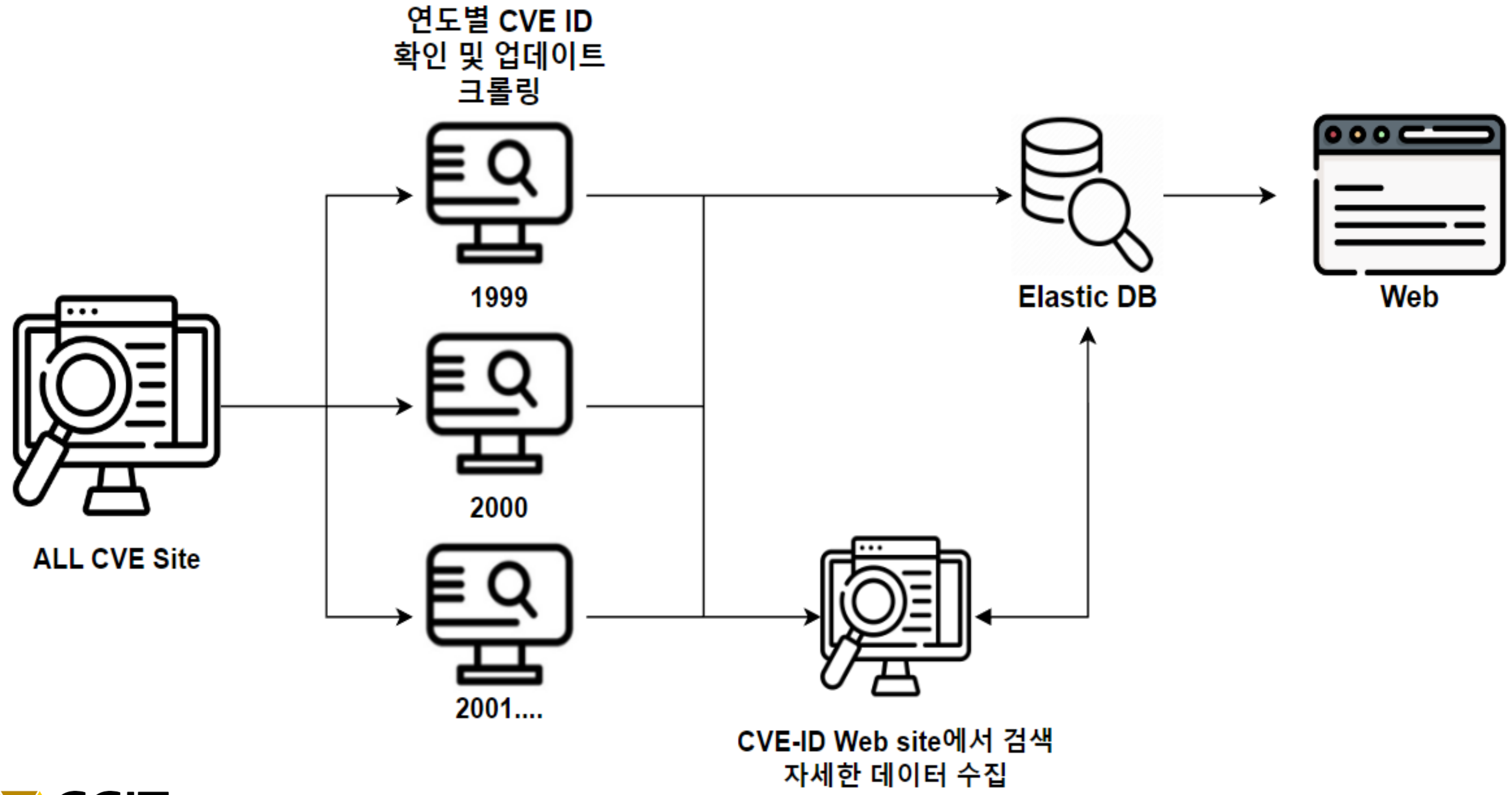
CVE Crawler Develop

ElasticSearch DB
Web Service

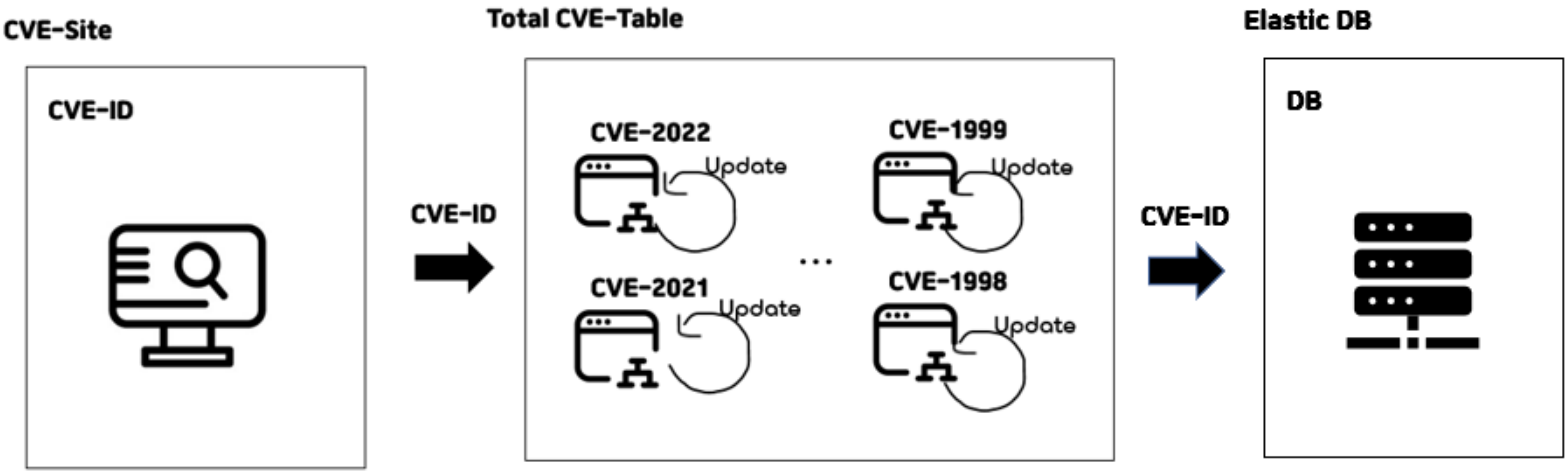
Natural Lang Processing Develop

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

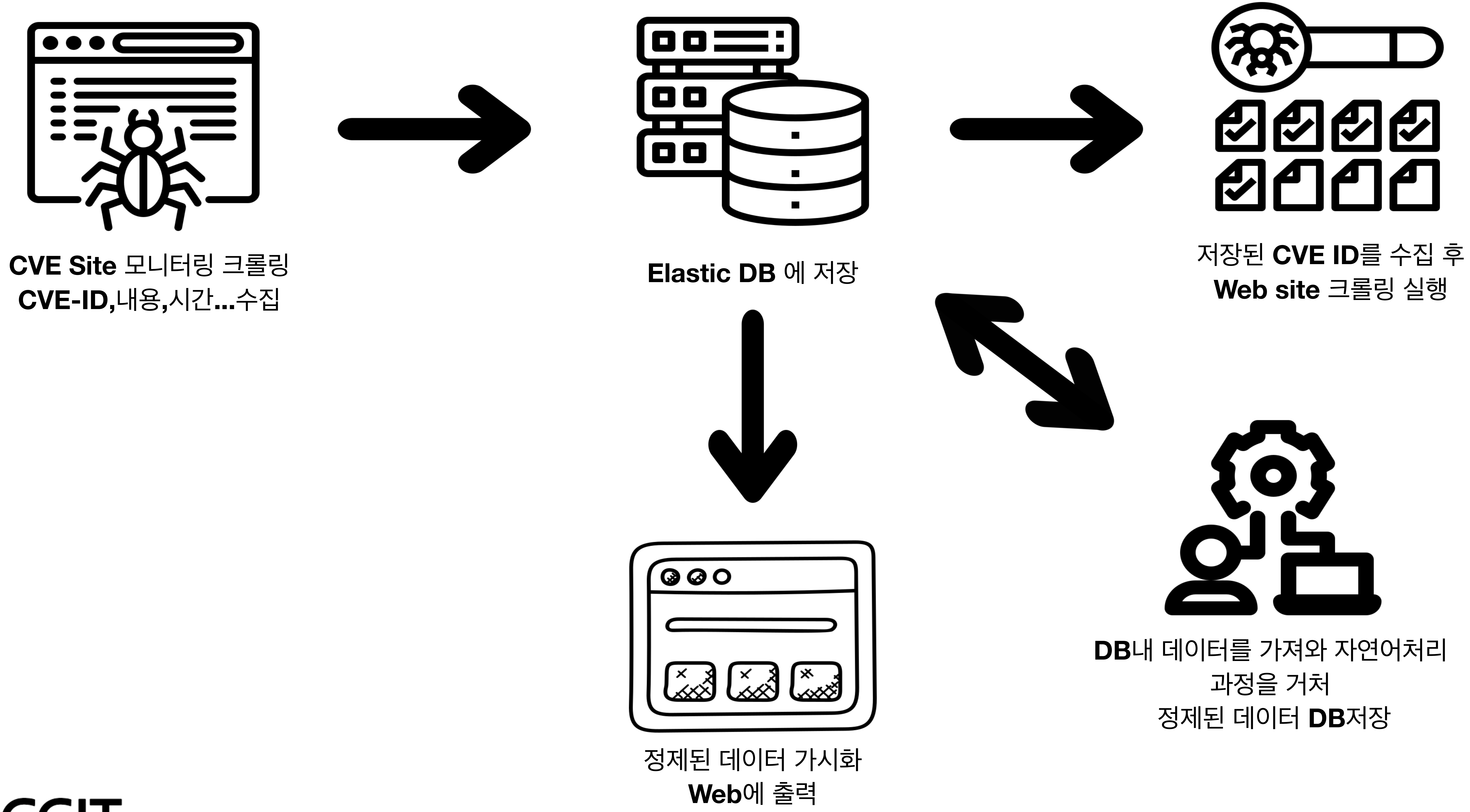
Crawler


연도별 CVE ID
확인 및 업데이트
크롤링
1999
2000
2001....
ALL CVE Site
Elastic DB
Web
CVE-ID Web site에서 검색
자세한 데이터 수집

Crawler 구상



CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY



CVE Site 모니터링 크롤링
CVE-ID,내용**,**시간**...**수집

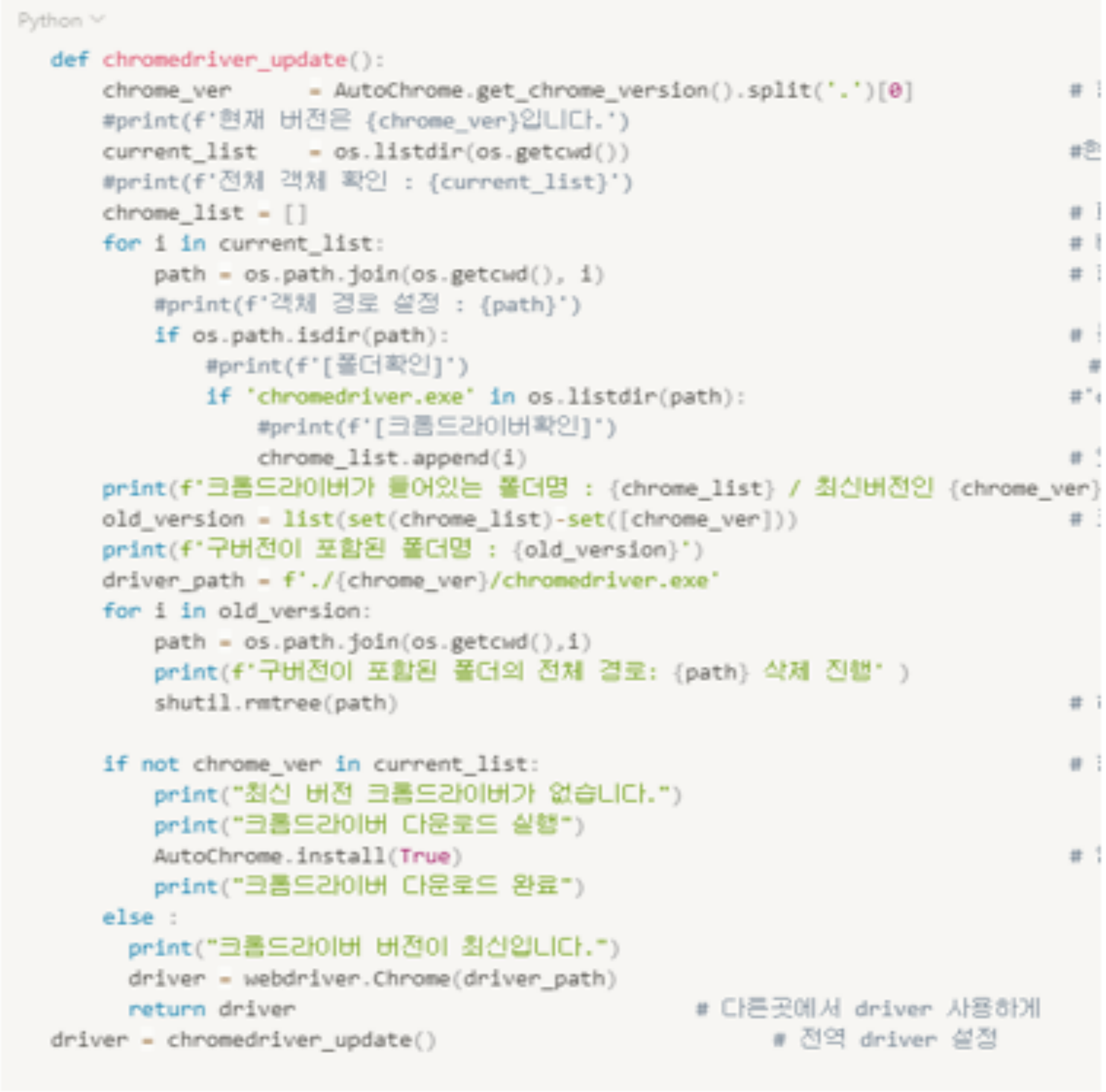
Elastic DB 에 저장

저장된 **CVE ID**를 수집 후
Web site 크롤링 실행

DB내 데이터를 가져와 자연어처리
과정을 거처
정제된 데이터 **DB**저장

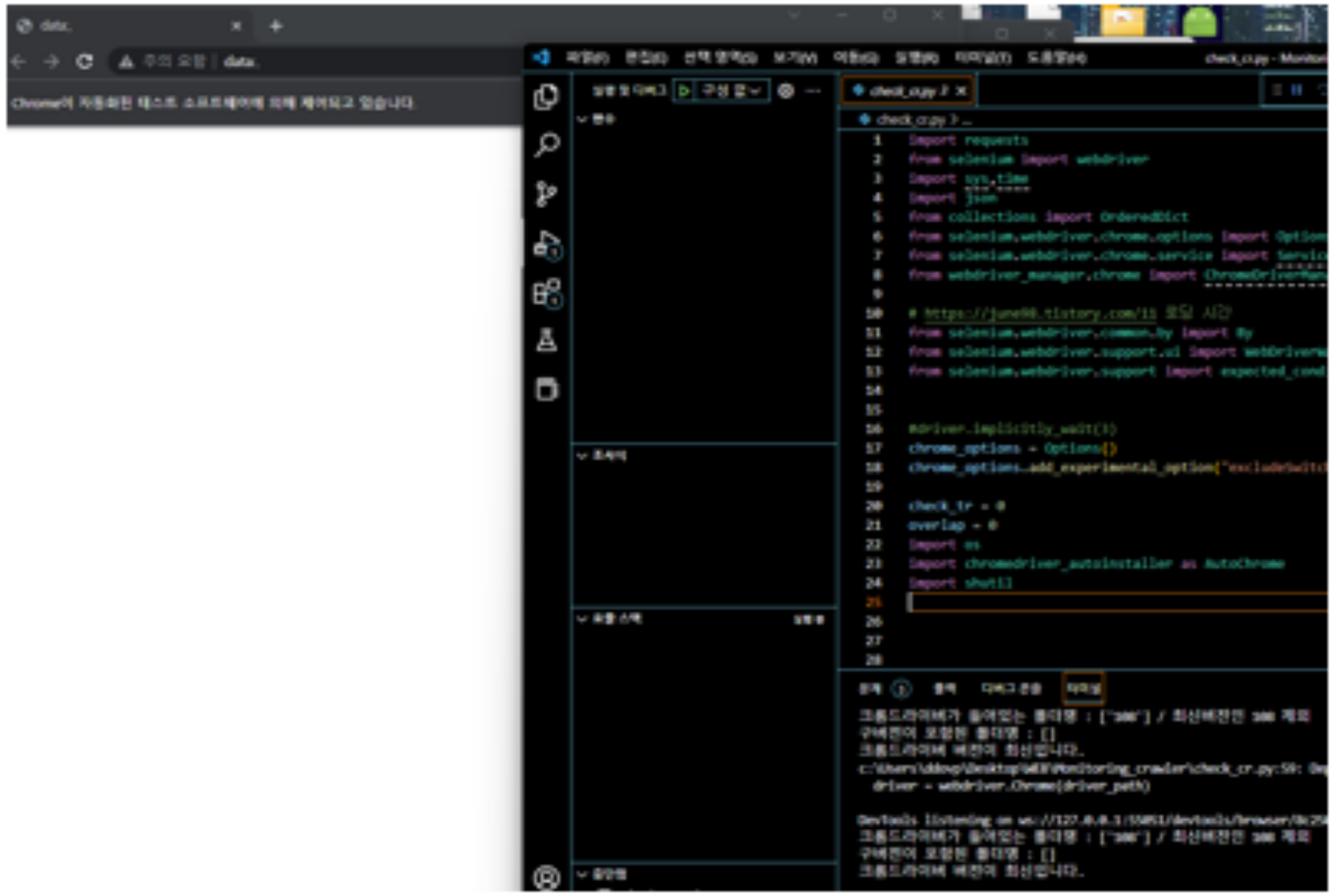
정제된 데이터 가시화
Web에 출력

CVE-Site Crawler



```python
def chromedriver_update():
    chrome_ver       = AutoChrome.get_chrome_version().split('.')[0]            # 
    #print(f'현재 버전은 {chrome_ver}입니다.')
    current_list     = os.listdir(os.getcwd())                                  #한
    #print(f'전체 객체 확인 : {current_list}')
    chrome_list = []                                                            # 
    for i in current_list:                                                      # 
        path = os.path.join(os.getcwd(), i)                                     # 
        #print(f'객체 경로 설정 : {path}')
        if os.path.isdir(path):                                                 # 
            #print(f'[폴더확인]')                                                  #
            if 'chromedriver.exe' in os.listdir(path):                          #"
                #print(f'[크롬드라이버확인]')
                chrome_list.append(i)                                           # 
    print(f'크롬드라이버가 들어있는 폴더명 : {chrome_list} / 최신버전인 {chrome_ver}
    old_version = list(set(chrome_list)-set([chrome_ver]))                      # 
    print(f'구버전이 포함된 폴더명 : {old_version}')
    driver_path = f'./{chrome_ver}/chromedriver.exe'
    for i in old_version:
        path = os.path.join(os.getcwd(),i)
        print(f'구버전이 포함된 폴더의 전체 경로: {path} 삭제 진행' )
        shutil.rmtree(path)                                                     # 

    if not chrome_ver in current_list:                                          # 
        print("최신 버전 크롬드라이버가 없습니다.")
        print("크롬드라이버 다운로드 실행")
        AutoChrome.install(True)                                                # 
        print("크롬드라이버 다운로드 완료")
    else :
      print("크롬드라이버 버전이 최신입니다.")
      driver = webdriver.Chrome(driver_path)
      return driver                                     # 다른곳에서 driver 사용하게
driver = chromedriver_update()                               # 전역 driver 설정
```

현재 크롬 버전을 확인하여 최신 크롬드라이버로 업데이트 하고 구버전 크롬드라이버는 자동 삭제



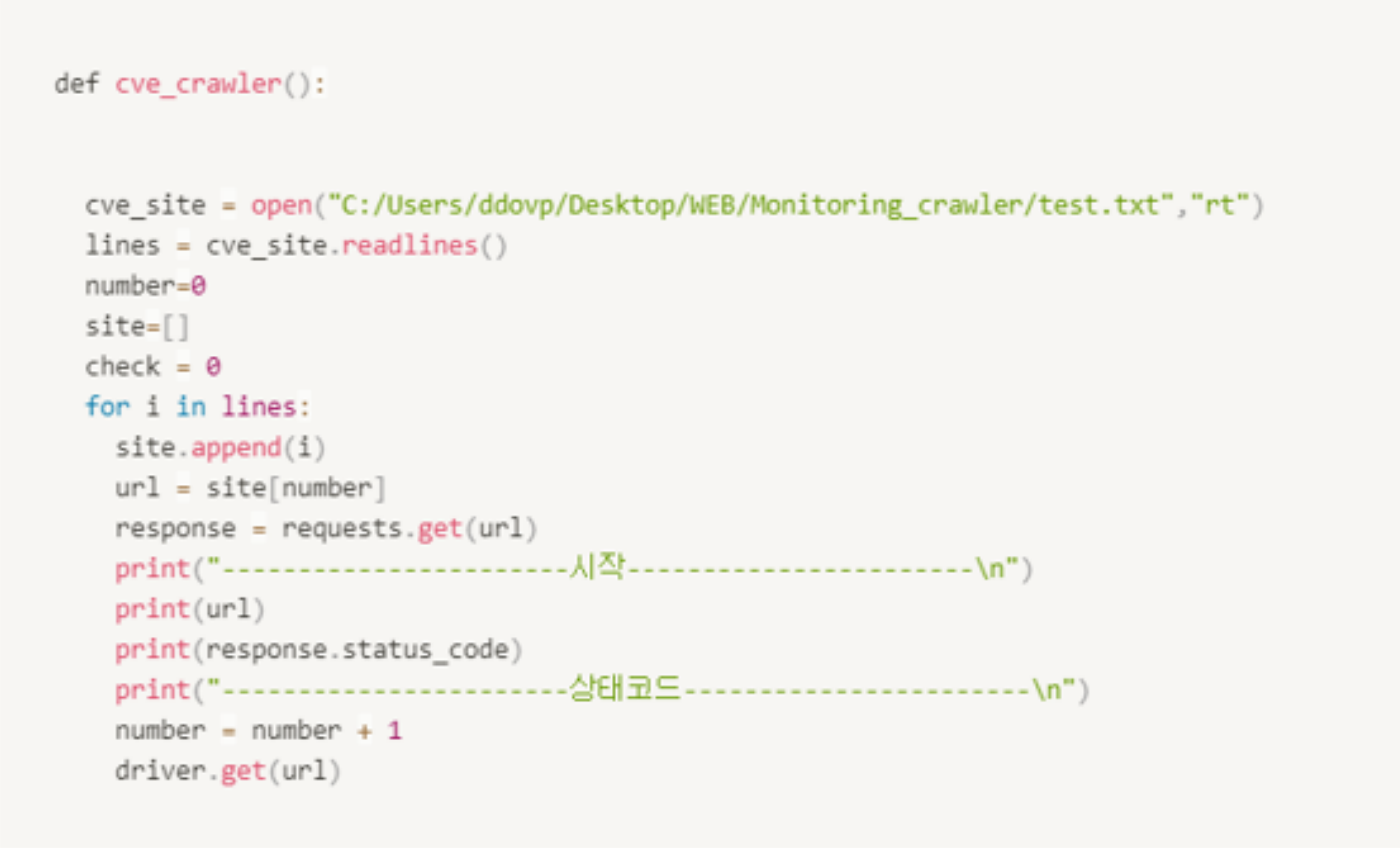
data:
Chrome이 자동화된 테스트 소프트웨어에 의해 제어되고 있습니다.
check_cr.py
문제
출력
디버그 콘솔
터미널

```python
import requests
from selenium import webdriver
import sys,time
import json
from collections import OrderedDict
from selenium.webdriver.chrome.options import Option
from selenium.webdriver.chrome.service import Servic
from webdriver_manager.chrome import ChromeDriverMan

# https://june00.tistory.com/11 로딩 시간
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWa
from selenium.webdriver.support import expected_cond


#driver.implicitly_wait(3)
chrome_options = Options()
chrome_options.add_experimental_option("excludeSwitc

check_tr = 0
overlap = 0
import os
import chromedriver_autoinstaller as AutoChrome
import shutil
```

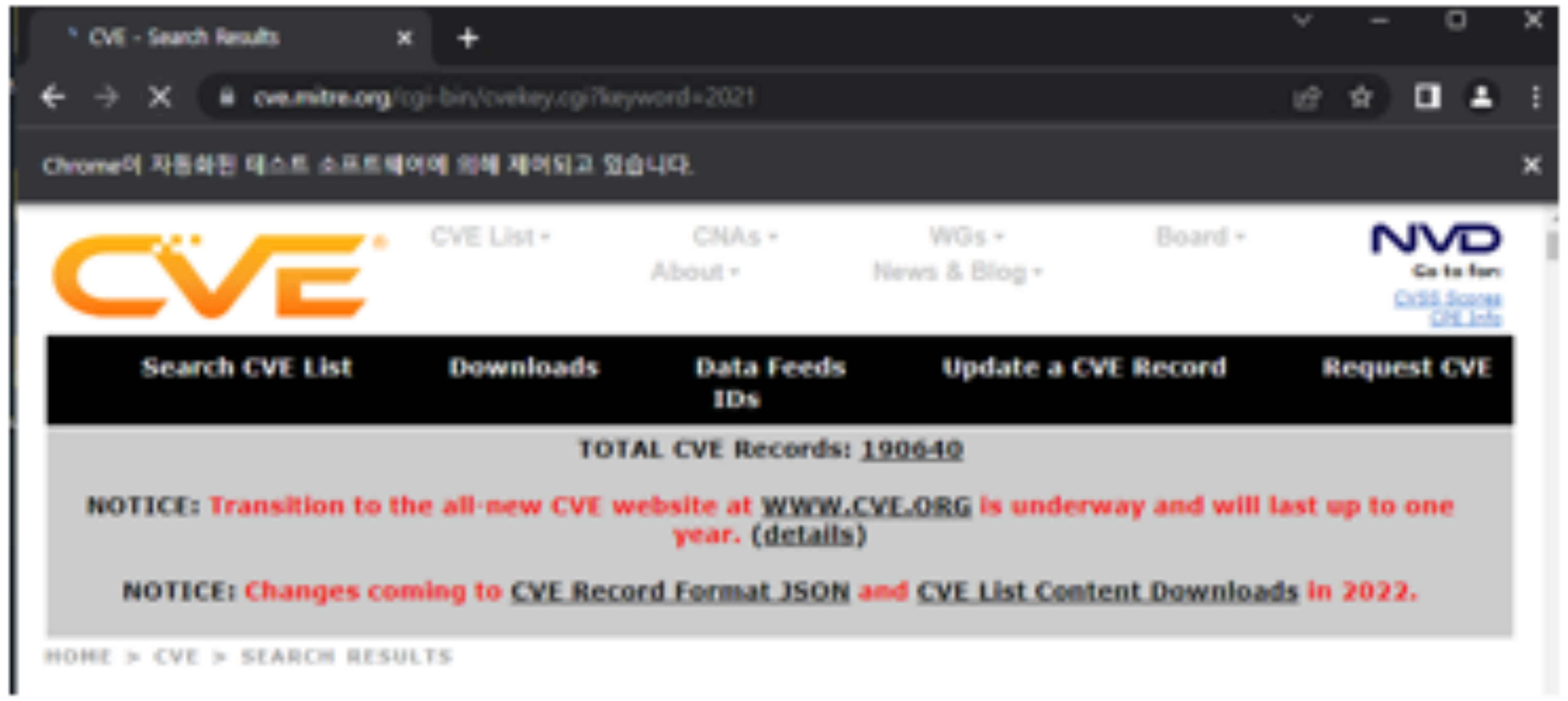
```
크롬드라이버가 들어있는 폴더명 : ['108'] / 최신버전인 108 제외
구버전이 포함된 폴더명 : []
크롬드라이버 버전이 최신입니다.
c:\Users\[illegible]\Desktop\[illegible]\Monitoring_crawler\check_cr.py:59: De
  driver = webdriver.Chrome(driver_path)

DevTools listening on ws://127.0.0.1:[illegible]/devtools/browser/[illegible]
크롬드라이버가 들어있는 폴더명 : ['108'] / 최신버전인 108 제외
구버전이 포함된 폴더명 : []
크롬드라이버 버전이 최신입니다.
```

CVE-Site Crawler

CVE-URL을 TXT파일에 저장후 순차적으로 접속



```
def cve_crawler():


  cve_site = open("C:/Users/ddovp/Desktop/WEB/Monitoring_crawler/test.txt","rt")
  lines = cve_site.readlines()
  number=0
  site=[]
  check = 0
  for i in lines:
    site.append(i)
    url = site[number]
    response = requests.get(url)
    print("----------------------시작----------------------\n")
    print(url)
    print(response.status_code)
    print("----------------------상태코드----------------------\n")
    number = number + 1
    driver.get(url)
```

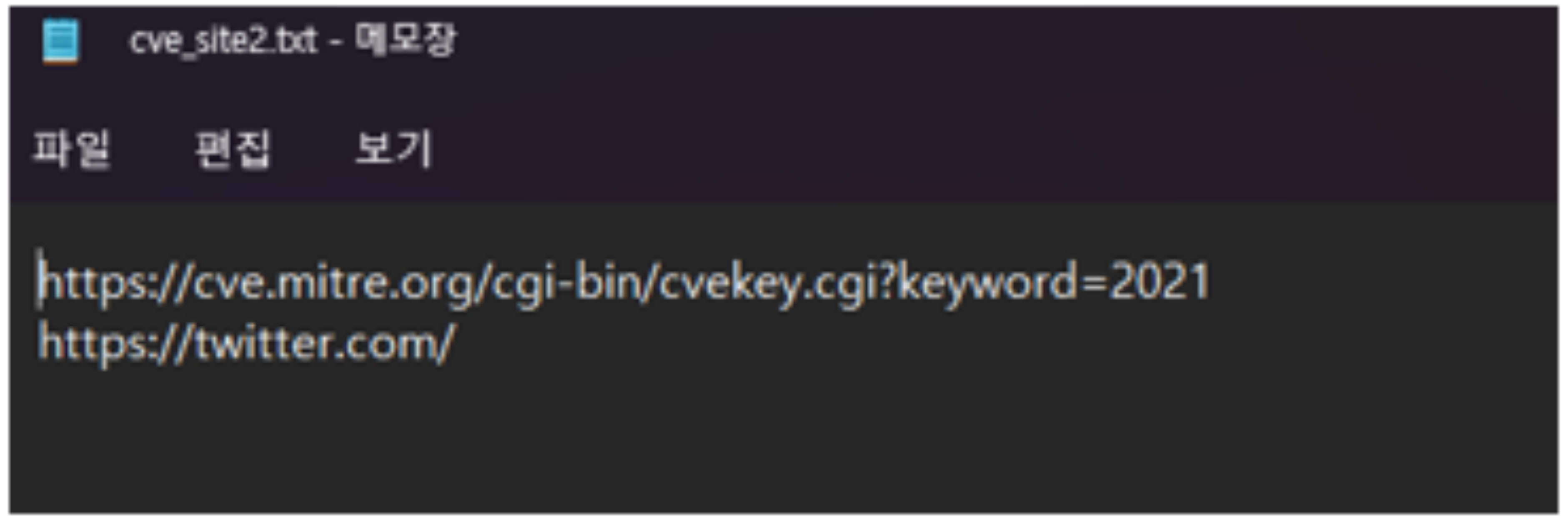


Chrome이 자동화된 테스트 소프트웨어에 의해 제어되고 있습니다.

TOTAL CVE Records: 190640

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

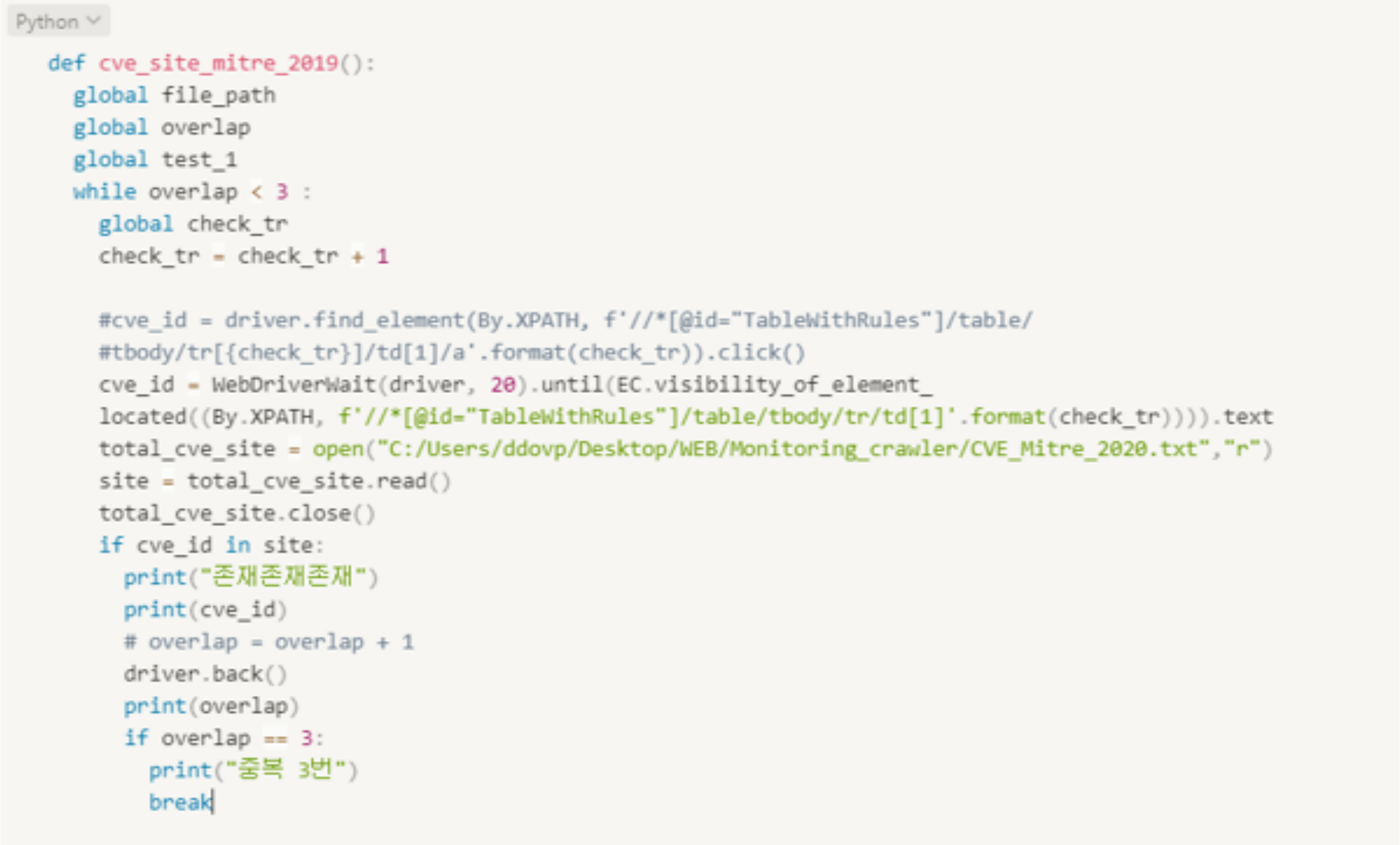
NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.



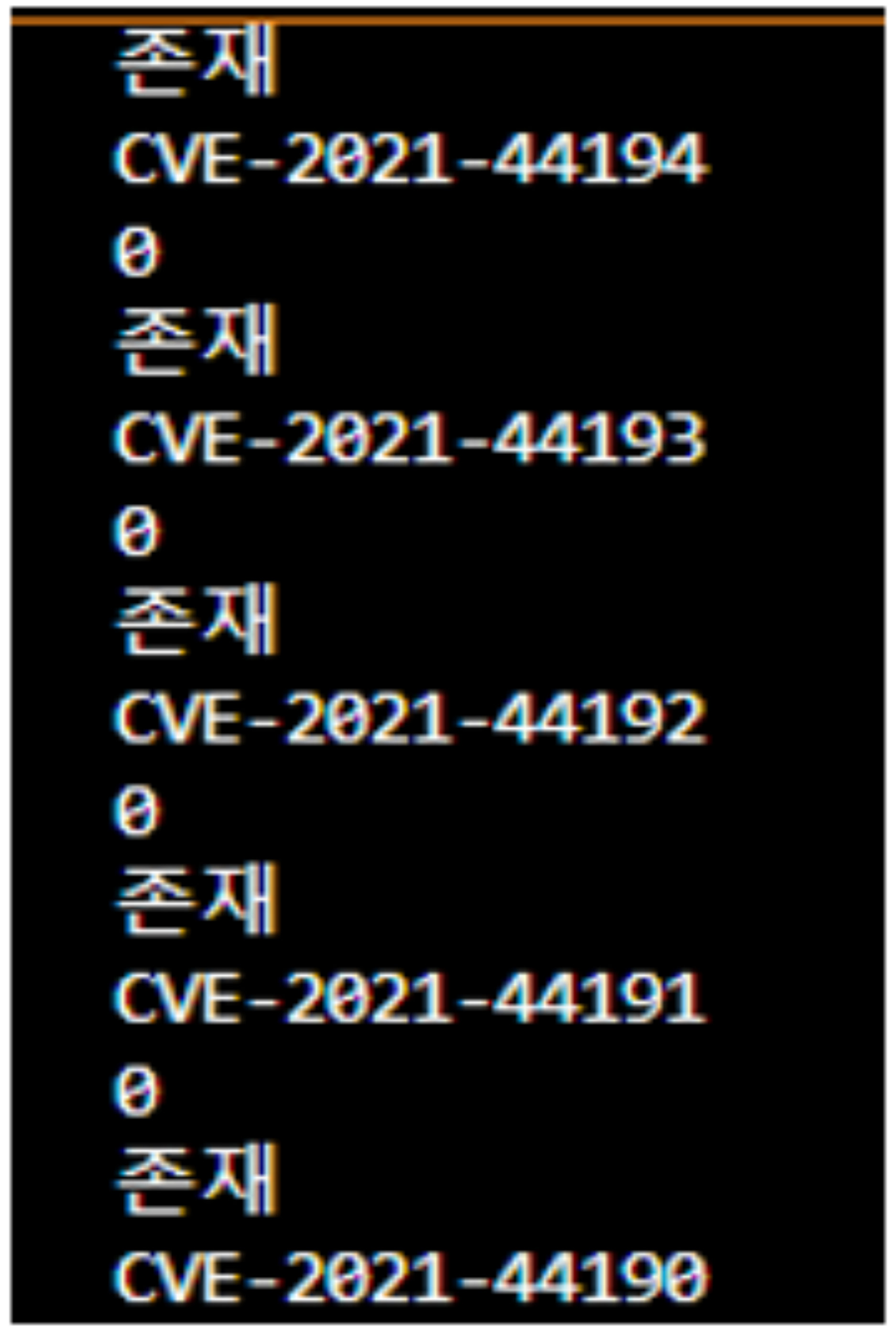
```
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=2021
https://twitter.com/
```

CVE-Site Crawler

CVE 리스트 중복 예외처리

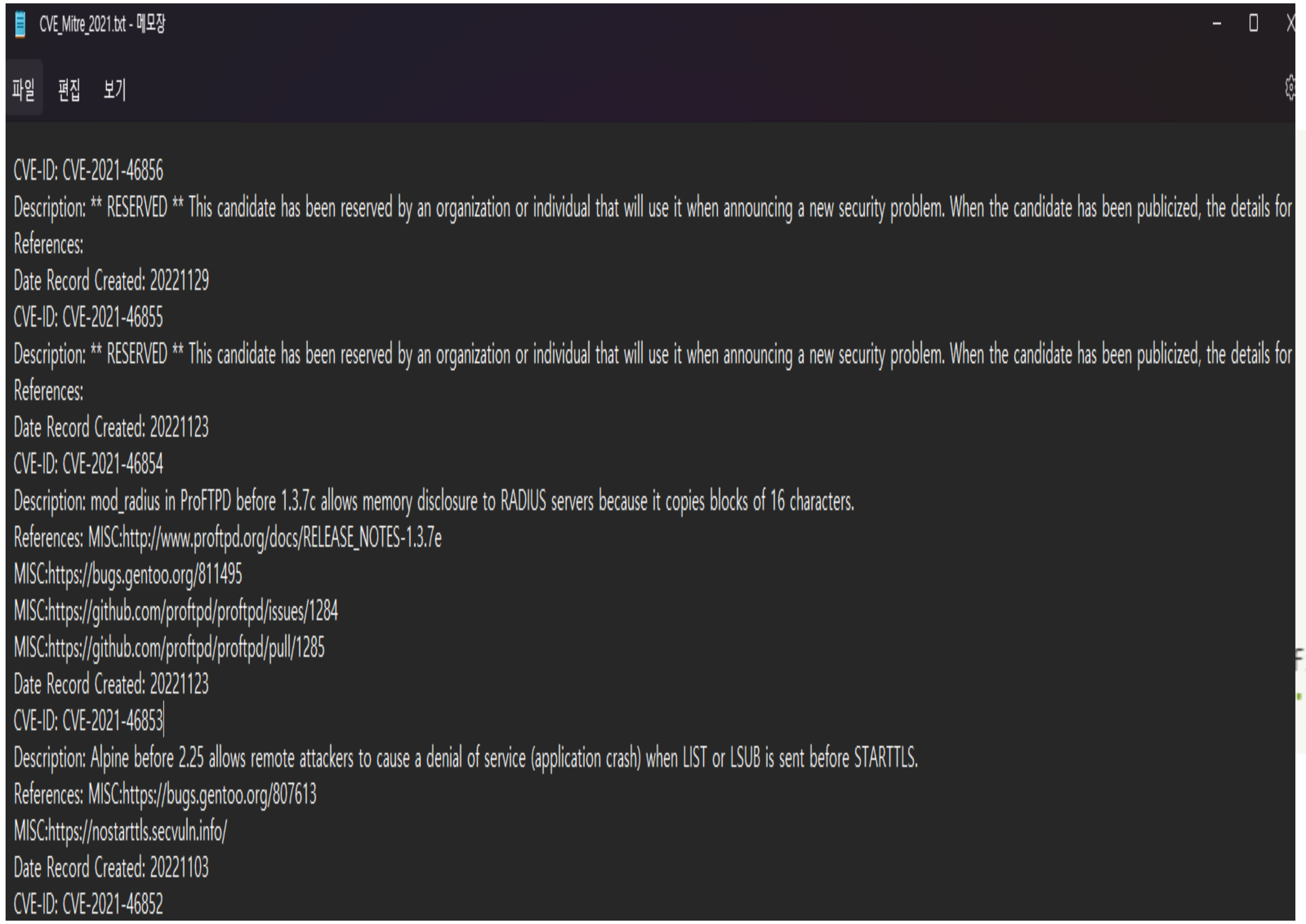


```python
def cve_site_mitre_2019():
  global file_path
  global overlap
  global test_1
  while overlap < 3 :
    global check_tr
    check_tr = check_tr + 1

    #cve_id = driver.find_element(By.XPATH, f'//*[@id="TableWithRules"]/table/
    #tbody/tr[{check_tr}]/td[1]/a'.format(check_tr)).click()
    cve_id = WebDriverWait(driver, 20).until(EC.visibility_of_element_
    located((By.XPATH, f'//*[@id="TableWithRules"]/table/tbody/tr/td[1]'.format(check_tr)))).text
    total_cve_site = open("C:/Users/ddovp/Desktop/WEB/Monitoring_crawler/CVE_Mitre_2020.txt","r")
    site = total_cve_site.read()
    total_cve_site.close()
    if cve_id in site:
      print("존재존재존재")
      print(cve_id)
      # overlap = overlap + 1
      driver.back()
      print(overlap)
      if overlap == 3:
        print("중복 3번")
        break
```



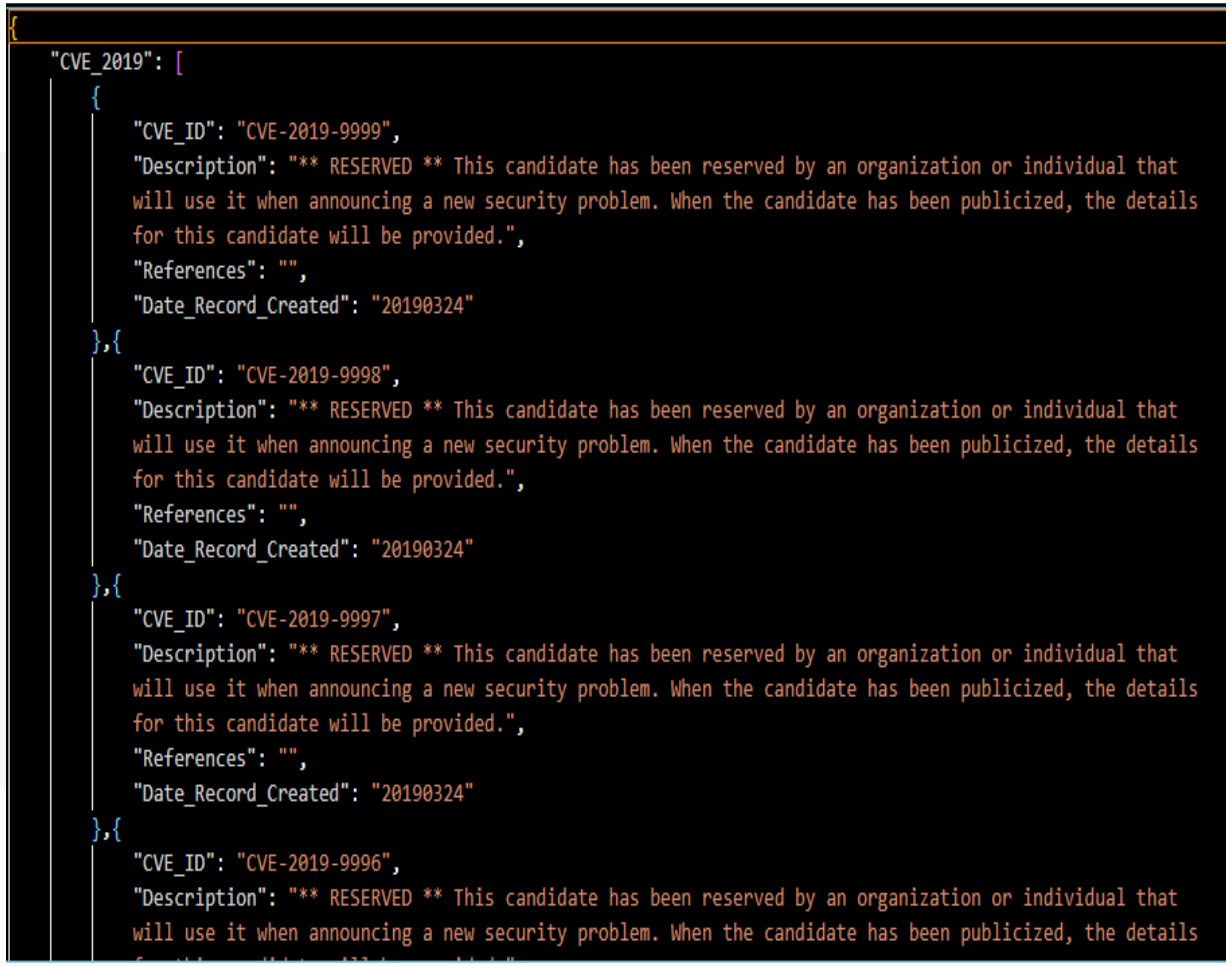
```
존재
CVE-2021-44194
0
존재
CVE-2021-44193
0
존재
CVE-2021-44192
0
존재
CVE-2021-44191
0
존재
CVE-2021-44190
```

CVE-Site Crawler



```
CVE-ID: CVE-2021-46856
Description: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for
References:
Date Record Created: 20221129
CVE-ID: CVE-2021-46855
Description: ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for
References:
Date Record Created: 20221123
CVE-ID: CVE-2021-46854
Description: mod_radius in ProFTPD before 1.3.7c allows memory disclosure to RADIUS servers because it copies blocks of 16 characters.
References: MISC:http://www.proftpd.org/docs/RELEASE_NOTES-1.3.7e
MISC:https://bugs.gentoo.org/811495
MISC:https://github.com/proftpd/proftpd/issues/1284
MISC:https://github.com/proftpd/proftpd/pull/1285
Date Record Created: 20221123
CVE-ID: CVE-2021-46853
Description: Alpine before 2.25 allows remote attackers to cause a denial of service (application crash) when LIST or LSUB is sent before STARTTLS.
References: MISC:https://bugs.gentoo.org/807613
MISC:https://nostarttls.secvuln.info/
Date Record Created: 20221103
CVE-ID: CVE-2021-46852
```

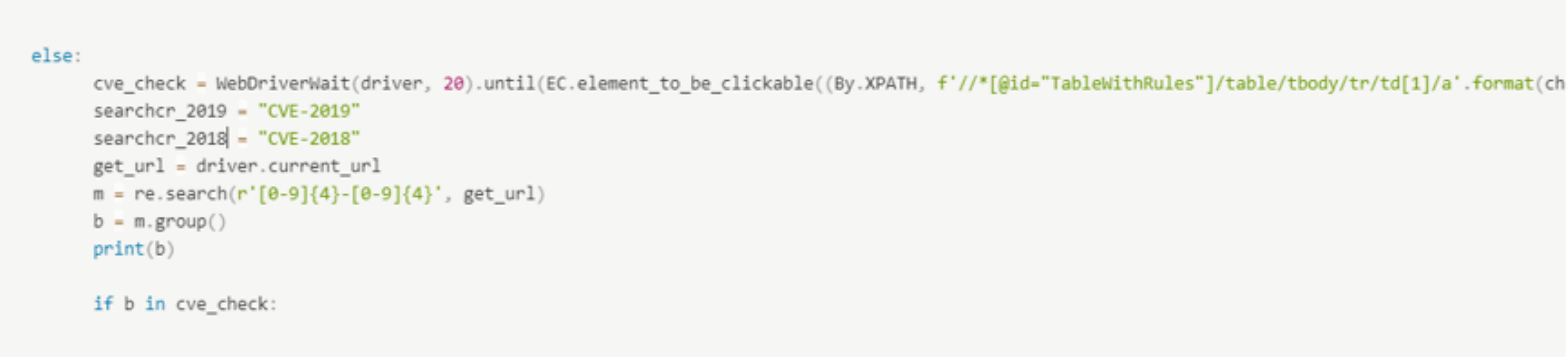
```
file:
')
```



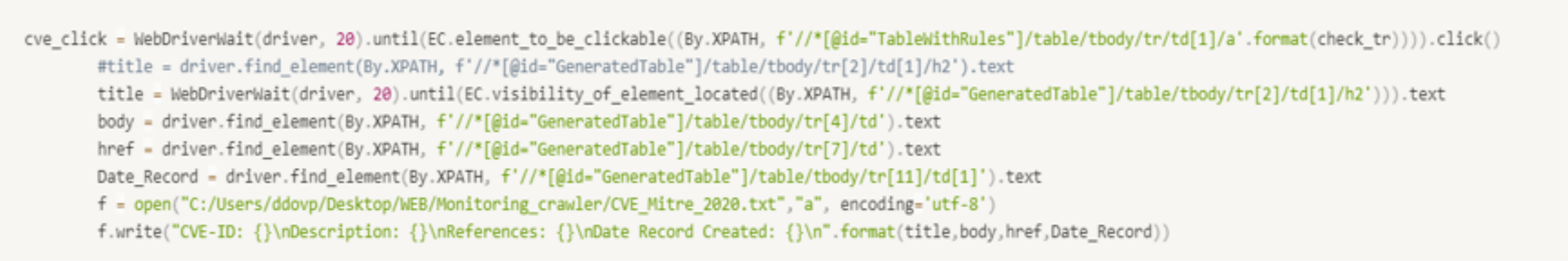
```
{
    "CVE_2019": [
        {
            "CVE_ID": "CVE-2019-9999",
            "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
            will use it when announcing a new security problem. When the candidate has been publicized, the details
            for this candidate will be provided.",
            "References": "",
            "Date_Record_Created": "20190324"
        },{
            "CVE_ID": "CVE-2019-9998",
            "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
            will use it when announcing a new security problem. When the candidate has been publicized, the details
            for this candidate will be provided.",
            "References": "",
            "Date_Record_Created": "20190324"
        },{
            "CVE_ID": "CVE-2019-9997",
            "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
            will use it when announcing a new security problem. When the candidate has been publicized, the details
            for this candidate will be provided.",
            "References": "",
            "Date_Record_Created": "20190324"
        },{
            "CVE_ID": "CVE-2019-9996",
            "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
            will use it when announcing a new security problem. When the candidate has been publicized, the details
```

CVE-Site Crawler

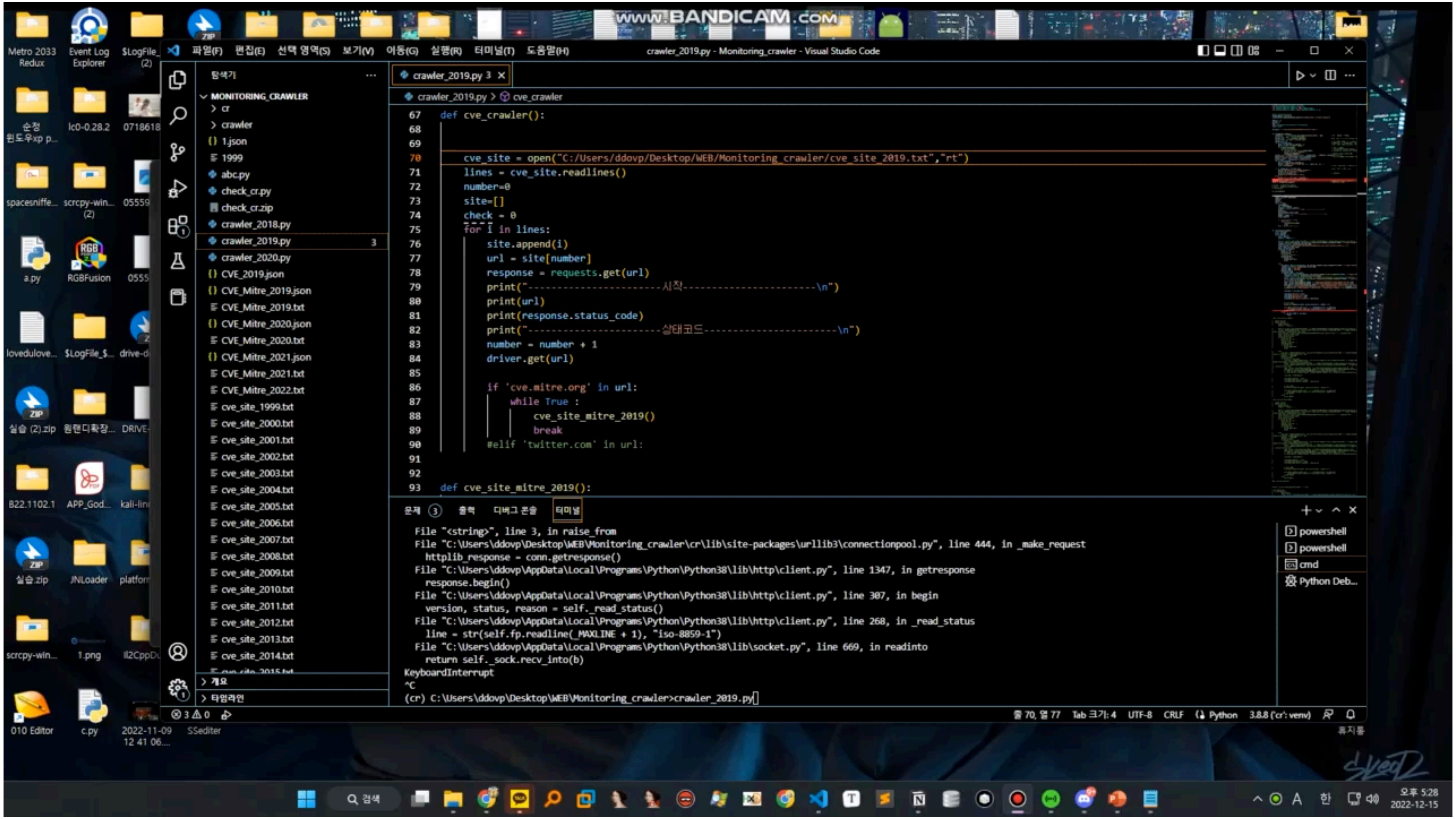
CVE-ID 예외처리와 메인 크롤러



```
else:
    cve_check = WebDriverWait(driver, 20).until(EC.element_to_be_clickable((By.XPATH, f'//*[@id="TableWithRules"]/table/tbody/tr/td[1]/a'.format(ch
    searchcr_2019 = "CVE-2019"
    searchcr_2018 = "CVE-2018"
    get_url = driver.current_url
    m = re.search(r'[0-9]{4}-[0-9]{4}', get_url)
    b = m.group()
    print(b)

    if b in cve_check:
```



```
cve_click = WebDriverWait(driver, 20).until(EC.element_to_be_clickable((By.XPATH, f'//*[@id="TableWithRules"]/table/tbody/tr/td[1]/a'.format(check_tr)))).click()
        #title = driver.find_element(By.XPATH, f'//*[@id="GeneratedTable"]/table/tbody/tr[2]/td[1]/h2').text
        title = WebDriverWait(driver, 20).until(EC.visibility_of_element_located((By.XPATH, f'//*[@id="GeneratedTable"]/table/tbody/tr[2]/td[1]/h2'))).text
        body = driver.find_element(By.XPATH, f'//*[@id="GeneratedTable"]/table/tbody/tr[4]/td').text
        href = driver.find_element(By.XPATH, f'//*[@id="GeneratedTable"]/table/tbody/tr[7]/td').text
        Date_Record = driver.find_element(By.XPATH, f'//*[@id="GeneratedTable"]/table/tbody/tr[11]/td[1]').text
        f = open("C:/Users/ddovp/Desktop/WEB/Monitoring_crawler/CVE_Mitre_2020.txt","a", encoding='utf-8')
        f.write("CVE-ID: {}\nDescription: {}\nReferences: {}\nDate Record Created: {}\n".format(title,body,href,Date_Record))
```

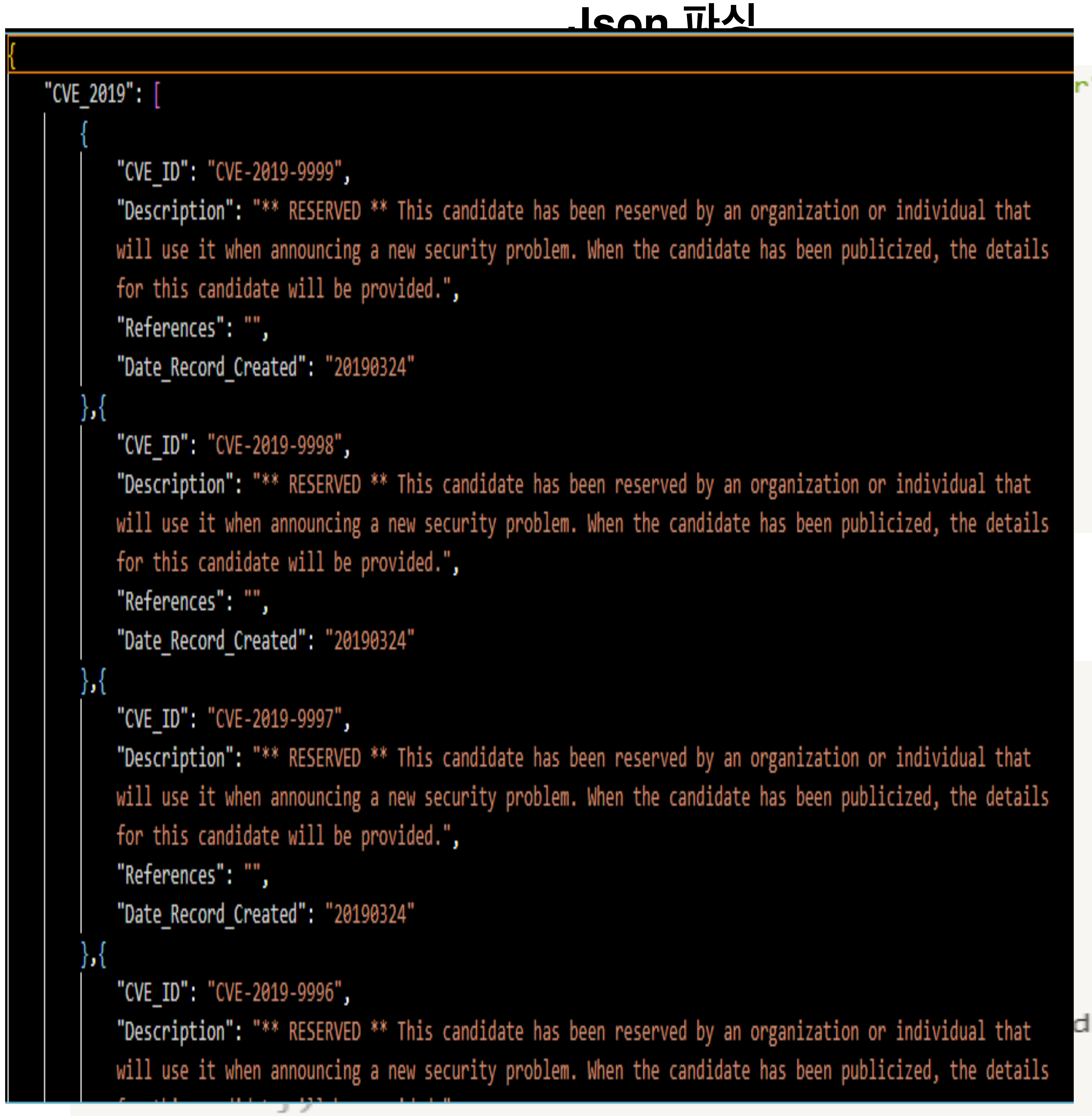


```python
def cve_crawler():


    cve_site = open("C:/Users/ddovp/Desktop/WEB/Monitoring_crawler/cve_site_2019.txt","rt")
    lines = cve_site.readlines()
    number=0
    site=[]
    check = 0
    for i in lines:
        site.append(i)
        url = site[number]
        response = requests.get(url)
        print("---------------------시작---------------------\n")
        print(url)
        print(response.status_code)
        print("---------------------상태코드---------------------\n")
        number = number + 1
        driver.get(url)

        if 'cve.mitre.org' in url:
            while True :
                cve_site_mitre_2019()
                break
        #elif 'twitter.com' in url:


def cve_site_mitre_2019():
```

```
  File "<string>", line 3, in raise_from
  File "C:\Users\ddovp\Desktop\WEB\Monitoring_crawler\cr\lib\site-packages\urllib3\connectionpool.py", line 444, in _make_request
    httplib_response = conn.getresponse()
  File "C:\Users\ddovp\AppData\Local\Programs\Python\Python38\lib\http\client.py", line 1347, in getresponse
    response.begin()
  File "C:\Users\ddovp\AppData\Local\Programs\Python\Python38\lib\http\client.py", line 307, in begin
    version, status, reason = self._read_status()
  File "C:\Users\ddovp\AppData\Local\Programs\Python\Python38\lib\http\client.py", line 268, in _read_status
    line = str(self.fp.readline(_MAXLINE + 1), "iso-8859-1")
  File "C:\Users\ddovp\AppData\Local\Programs\Python\Python38\lib\socket.py", line 669, in readinto
    return self._sock.recv_into(b)
KeyboardInterrupt
^C
(cr) C:\Users\ddovp\Desktop\WEB\Monitoring_crawler>crawler_2019.py
```

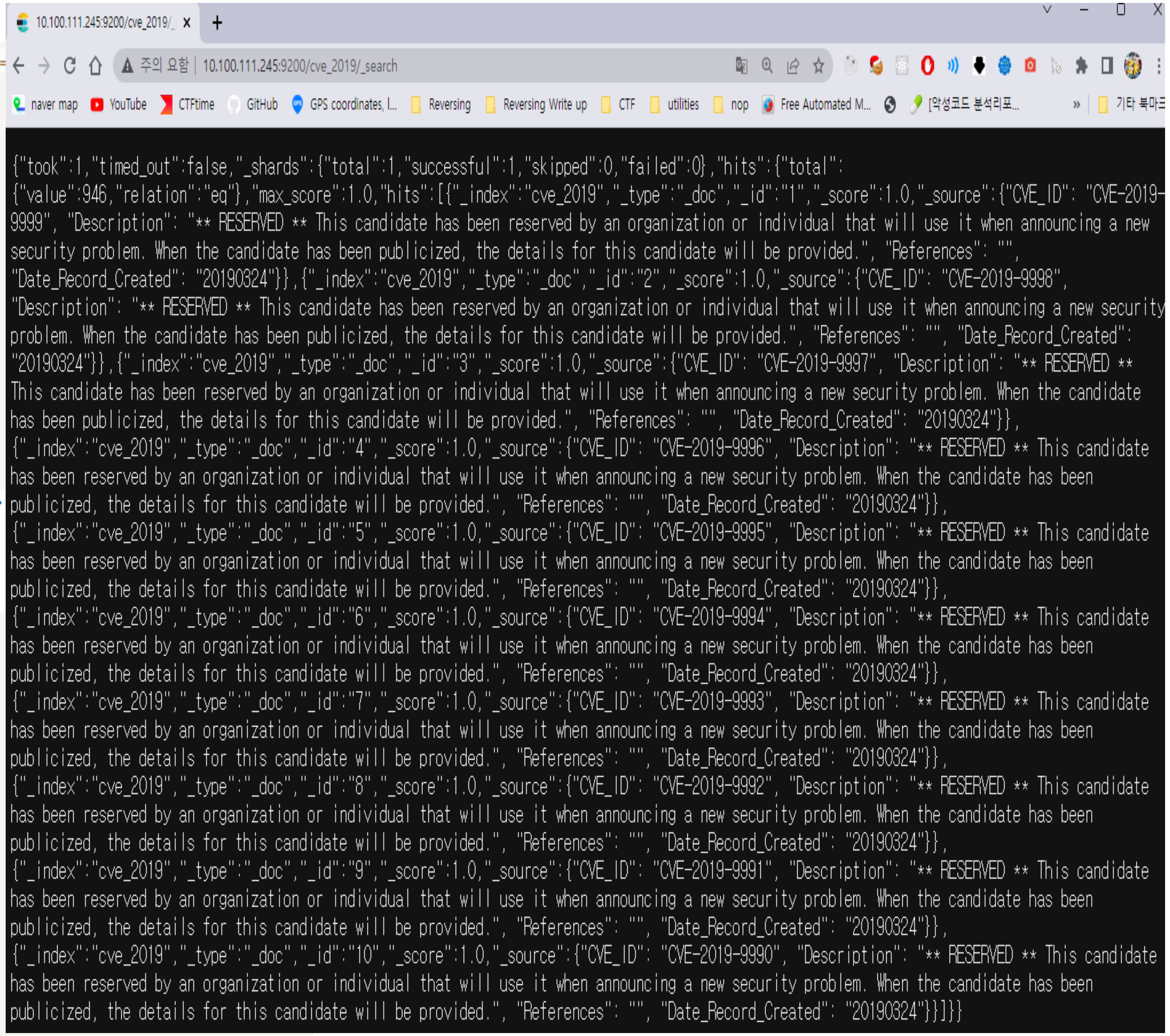
Crawler Result DB_Connection

Json 파싱

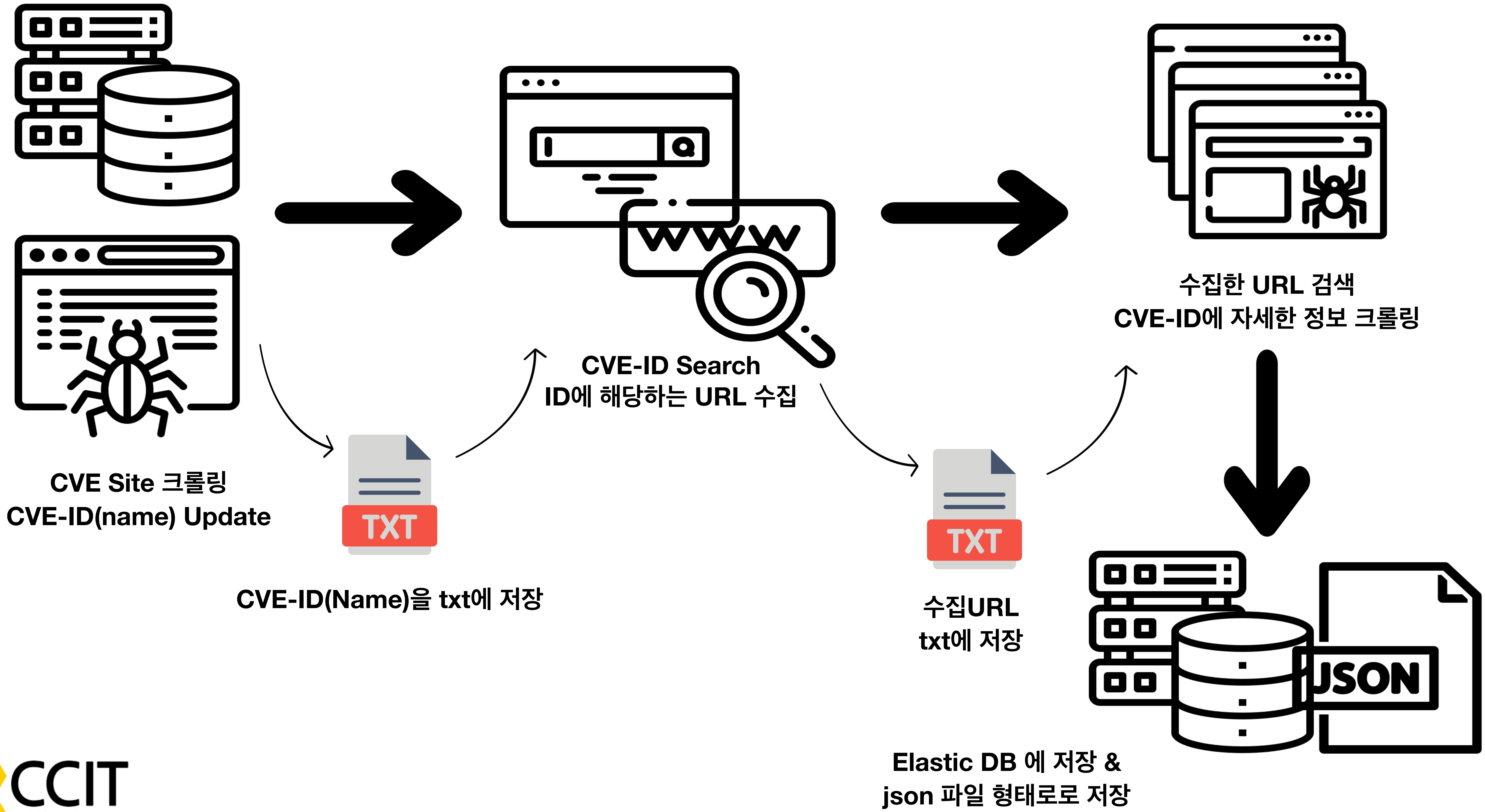


```
{
  "CVE_2019": [
    {
      "CVE_ID": "CVE-2019-9999",
      "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
      will use it when announcing a new security problem. When the candidate has been publicized, the details
      for this candidate will be provided.",
      "References": "",
      "Date_Record_Created": "20190324"
    },{
      "CVE_ID": "CVE-2019-9998",
      "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
      will use it when announcing a new security problem. When the candidate has been publicized, the details
      for this candidate will be provided.",
      "References": "",
      "Date_Record_Created": "20190324"
    },{
      "CVE_ID": "CVE-2019-9997",
      "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
      will use it when announcing a new security problem. When the candidate has been publicized, the details
      for this candidate will be provided.",
      "References": "",
      "Date_Record_Created": "20190324"
    },{
      "CVE_ID": "CVE-2019-9996",
      "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that
      will use it when announcing a new security problem. When the candidate has been publicized, the details
```

```
r" , encoding=

d

    helpers.bulk(es, docs)
```



```
{"took":1,"timed_out":false,"_shards":{"total":1,"successful":1,"skipped":0,"failed":0},"hits":{"total":
{"value":946,"relation":"eq"},"max_score":1.0,"hits":[{"_index":"cve_2019","_type":"_doc","_id":"1","_score":1.0,"_source":{"CVE_ID": "CVE-2019-
9999", "Description": "** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new
security problem. When the candidate has been publicized, the details for this candidate will be provided.", "References": "",
"Date_Record_Created": "20190324"}},{"_index":"cve_2019","_type":"_doc","_id":"2","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9998",
"Description": "** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security
problem. When the candidate has been publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created":
"20190324"}},{"_index":"cve_2019","_type":"_doc","_id":"3","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9997", "Description": "** RESERVED **
This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate
has been publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}},
{"_index":"cve_2019","_type":"_doc","_id":"4","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9996", "Description": "** RESERVED ** This candidate
has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}},
{"_index":"cve_2019","_type":"_doc","_id":"5","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9995", "Description": "** RESERVED ** This candidate
has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}},
{"_index":"cve_2019","_type":"_doc","_id":"6","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9994", "Description": "** RESERVED ** This candidate
has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}},
{"_index":"cve_2019","_type":"_doc","_id":"7","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9993", "Description": "** RESERVED ** This candidate
has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}},
{"_index":"cve_2019","_type":"_doc","_id":"8","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9992", "Description": "** RESERVED ** This candidate
has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}},
{"_index":"cve_2019","_type":"_doc","_id":"9","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9991", "Description": "** RESERVED ** This candidate
has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}},
{"_index":"cve_2019","_type":"_doc","_id":"10","_score":1.0,"_source":{"CVE_ID": "CVE-2019-9990", "Description": "** RESERVED ** This candidate
has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been
publicized, the details for this candidate will be provided.", "References": "", "Date_Record_Created": "20190324"}}]}}
```



CVE Site 크롤링
CVE-ID(name) Update

CVE-ID(Name)을 txt에 저장

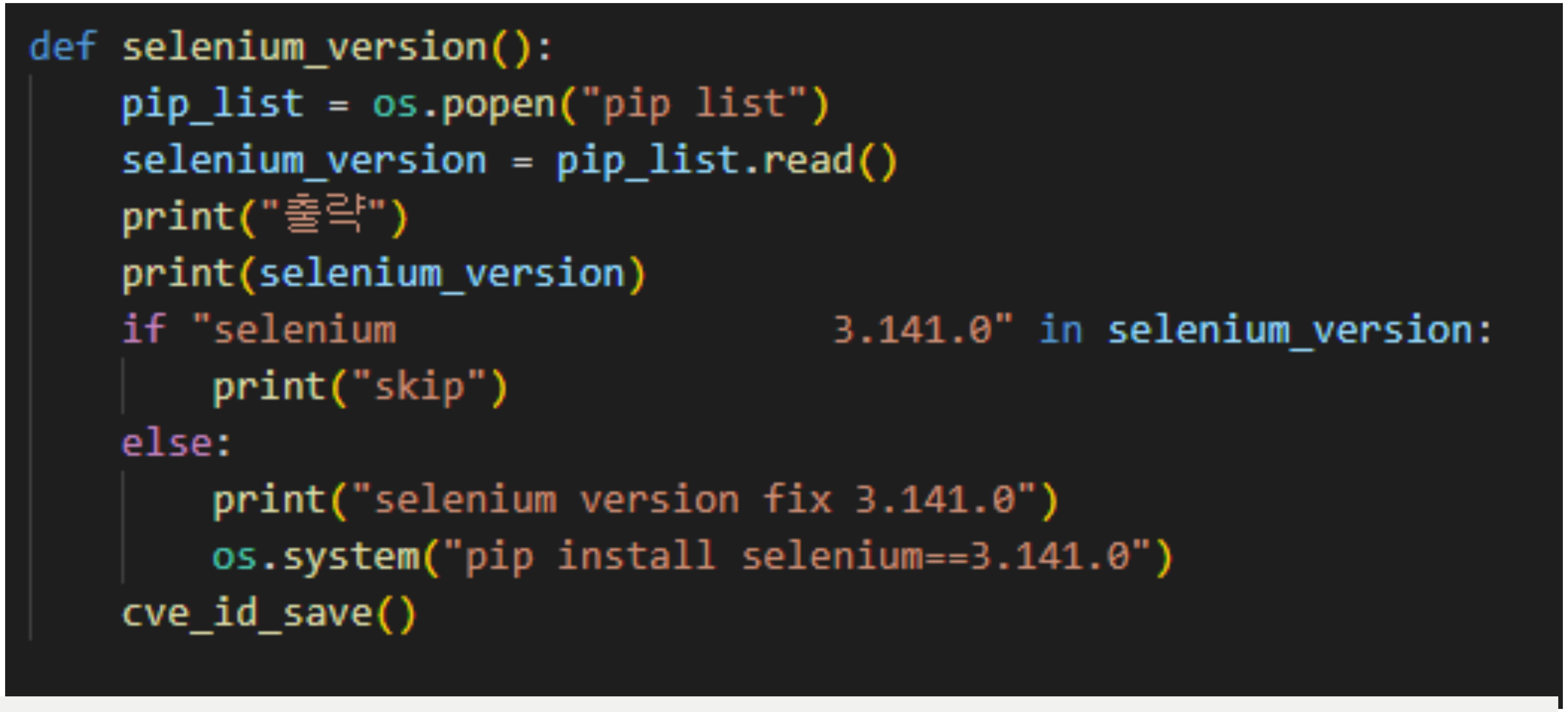
CVE-ID Search
ID에 해당하는 URL 수집

수집URL
txt에 저장

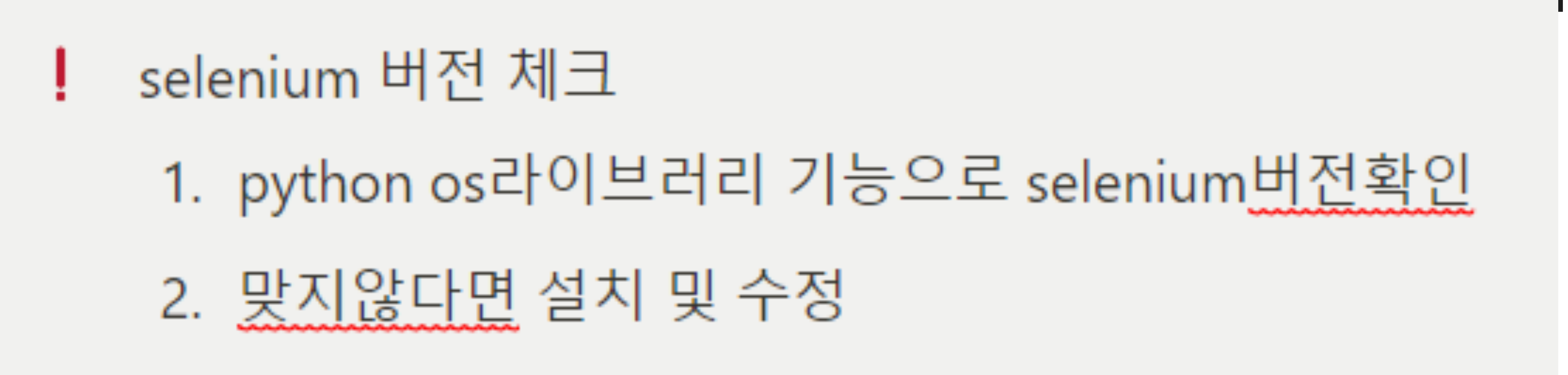
수집한 URL 검색
CVE-ID에 자세한 정보 크롤링

Elastic DB 에 저장 &
json 파일 형태로 저장

CVE Site 크롤링
CVE-ID(name) Update



```
def selenium_version():
    pip_list = os.popen("pip list")
    selenium_version = pip_list.read()
    print("출략")
    print(selenium_version)
    if "selenium                   3.141.0" in selenium_version:
        print("skip")
    else:
        print("selenium version fix 3.141.0")
        os.system("pip install selenium==3.141.0")
    cve_id_save()
```

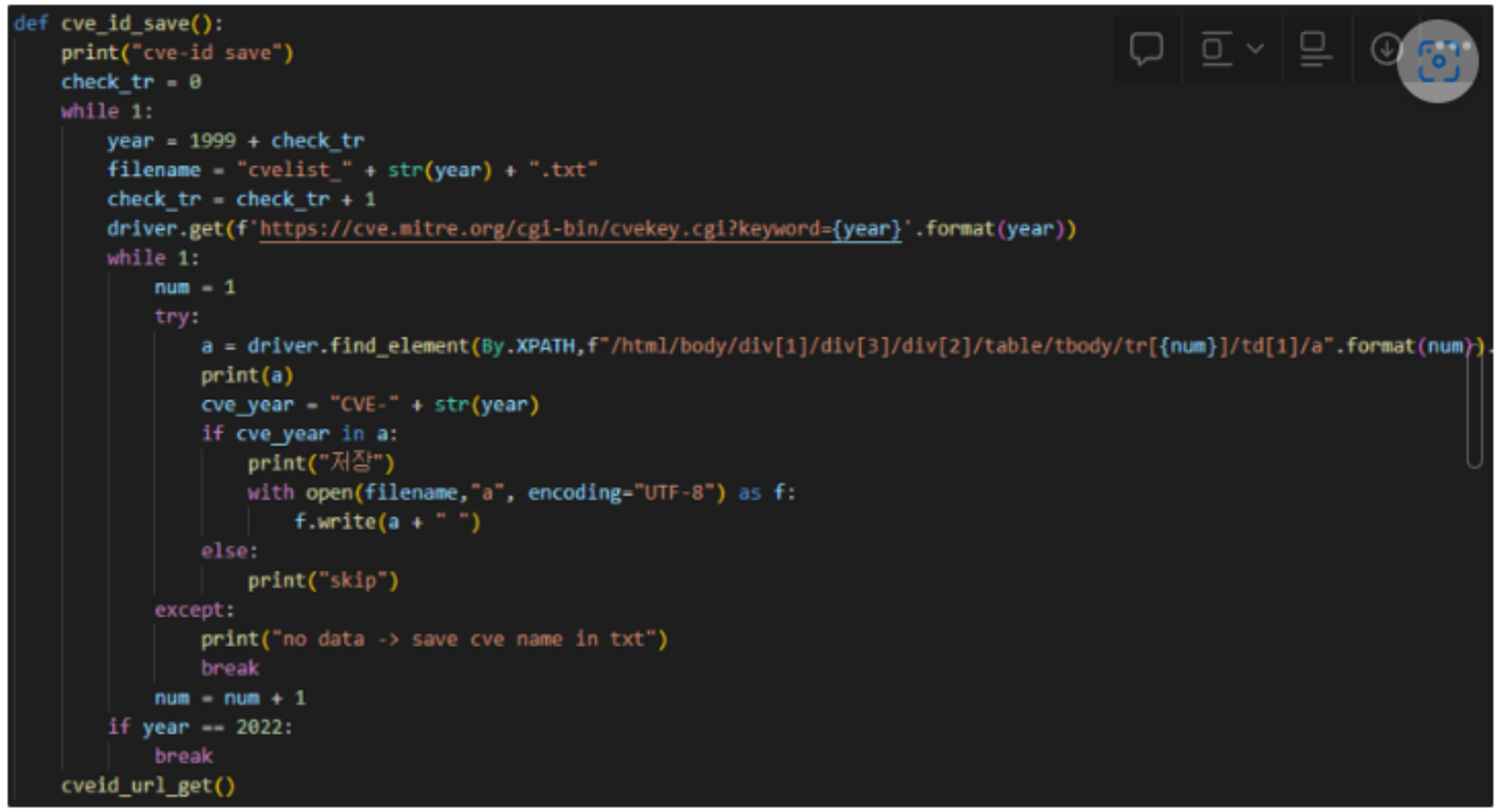


! selenium 버전 체크

1. python os라이브러리 기능으로 selenium버전확인
2. 맞지않다면 설치 및 수정

CVE-ID(Name) 업데이트

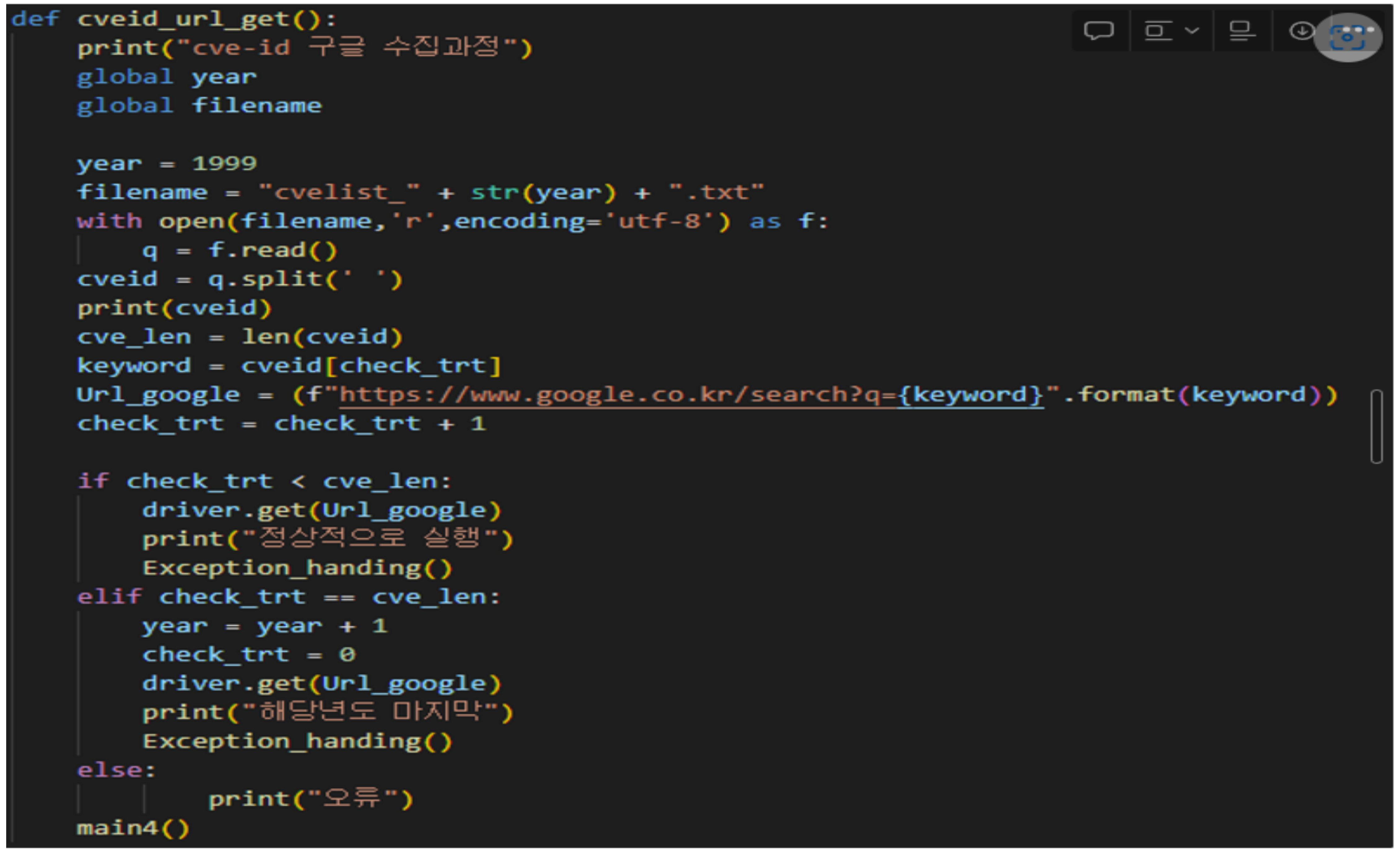
CVE Site 크롤링
CVE-ID(name) Update



```python
def cve_id_save():
    print("cve-id save")
    check_tr = 0
    while 1:
        year = 1999 + check_tr
        filename = "cvelist_" + str(year) + ".txt"
        check_tr = check_tr + 1
        driver.get(f'https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword={year}'.format(year))
        while 1:
            num = 1
            try:
                a = driver.find_element(By.XPATH,f"/html/body/div[1]/div[3]/div[2]/table/tbody/tr[{num}]/td[1]/a".format(num))
                print(a)
                cve_year = "CVE-" + str(year)
                if cve_year in a:
                    print("저장")
                    with open(filename,"a", encoding="UTF-8") as f:
                        f.write(a + " ")
                else:
                    print("skip")
            except:
                print("no data -> save cve name in txt")
                break
            num = num + 1
        if year == 2022:
            break
    cveid_url_get()
```

! CVE-ID 가져오는 코드

1. cve.mitre.org 사이트에서 1999년도 검색
2. CVE-ID 크롤링
3. TXT File에 CVE-ID 년도별로 저장
4. 2022년까지 반복



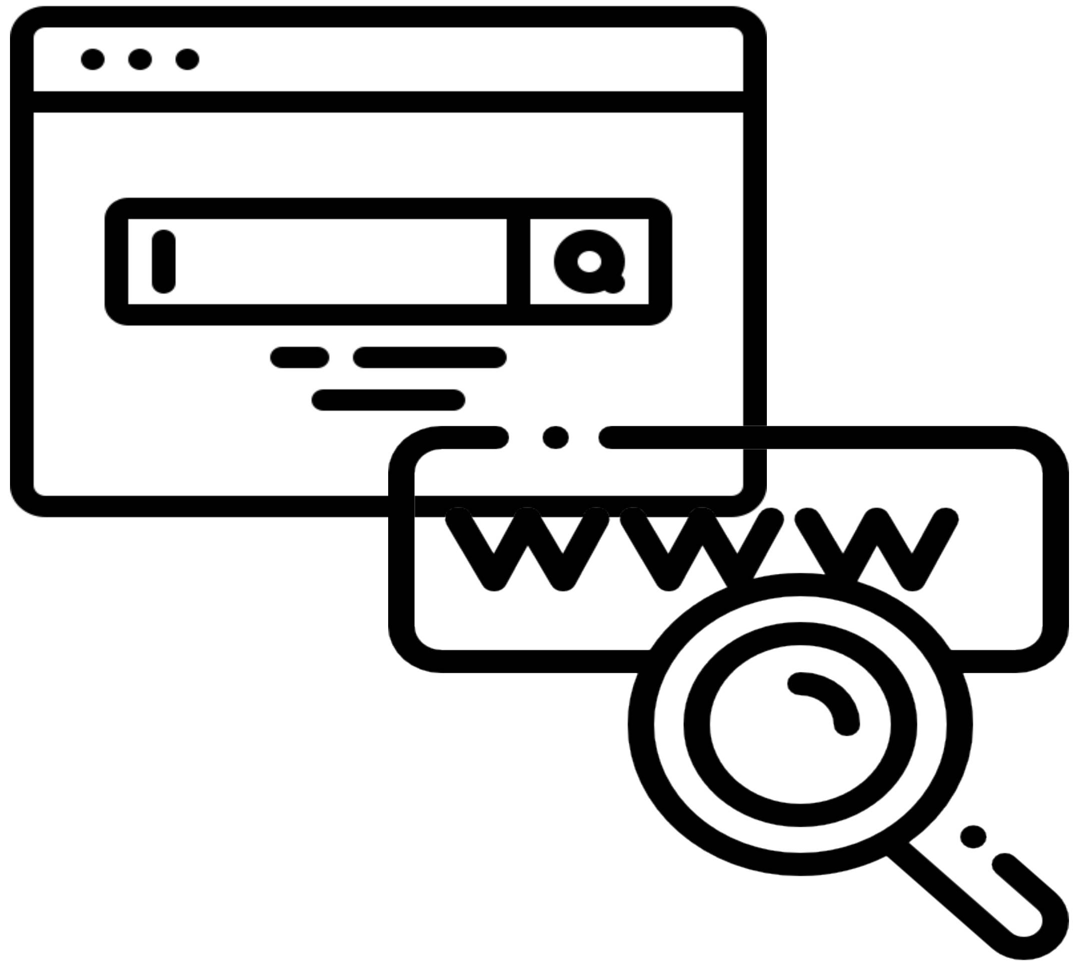
```python
def cveid_url_get():
    print("cve-id 구글 수집과정")
    global year
    global filename

    year = 1999
    filename = "cvelist_" + str(year) + ".txt"
    with open(filename,'r',encoding='utf-8') as f:
        q = f.read()
    cveid = q.split(' ')
    print(cveid)
    cve_len = len(cveid)
    keyword = cveid[check_trt]
    Url_google = (f"https://www.google.co.kr/search?q={keyword}".format(keyword))
    check_trt = check_trt + 1

    if check_trt < cve_len:
        driver.get(Url_google)
        print("정상적으로 실행")
        Exception_handing()
    elif check_trt == cve_len:
        year = year + 1
        check_trt = 0
        driver.get(Url_google)
        print("해당년도 마지막")
        Exception_handing()
    else:
            print("오류")
    main4()
```

! TXT에 있는 CVE-ID 검색 코드

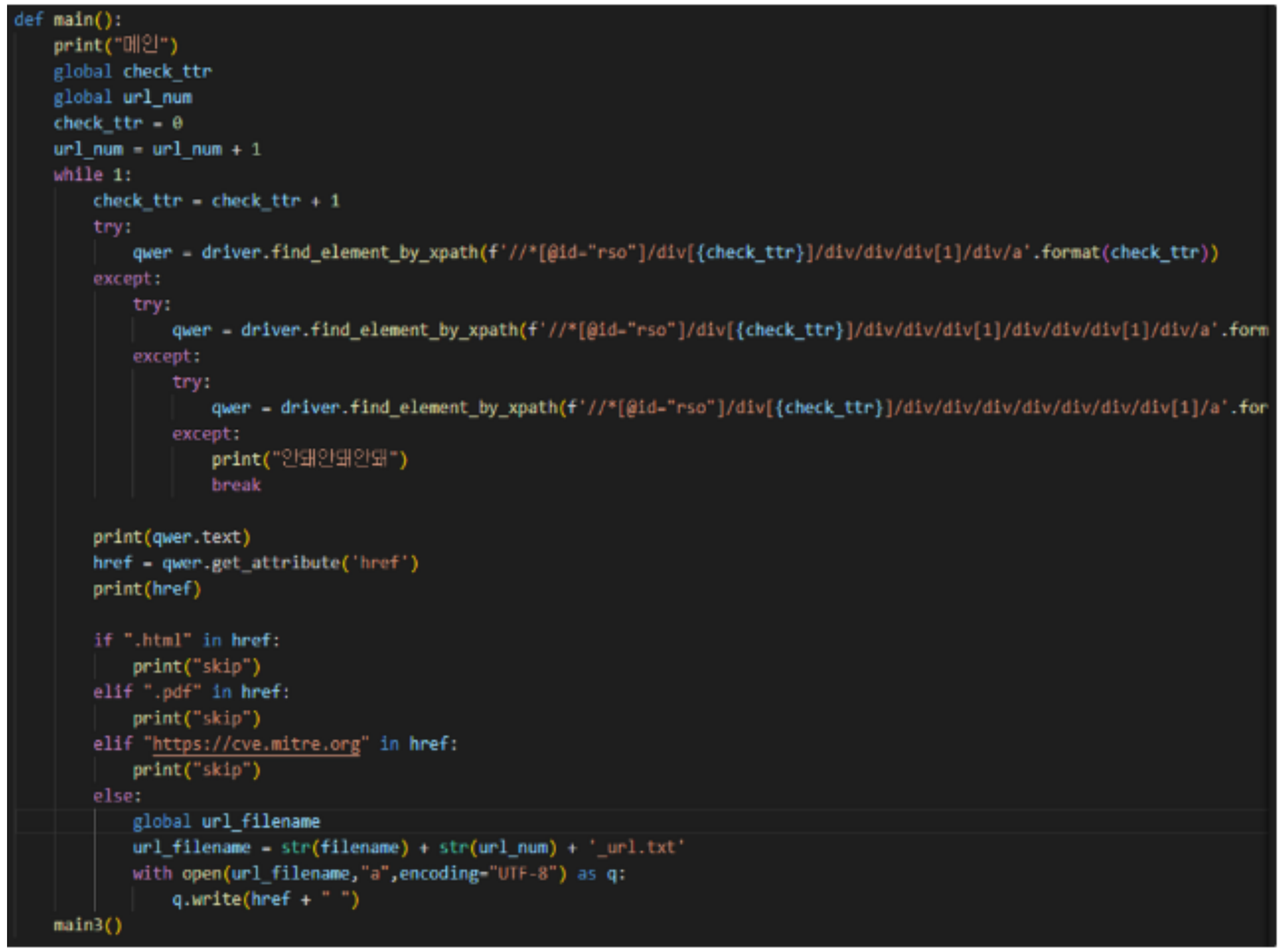
1. 연도별로 되어있는 TXT파일 열기
2. 파일내 CVE-ID를 리스트형태로 변수에 저장
3. 리스트 순서대로 구글에 검색
4. 다음 함수로 이동

- 만약 파일 id갯수랑 반복횟수가 같다면 다음년도로 세팅

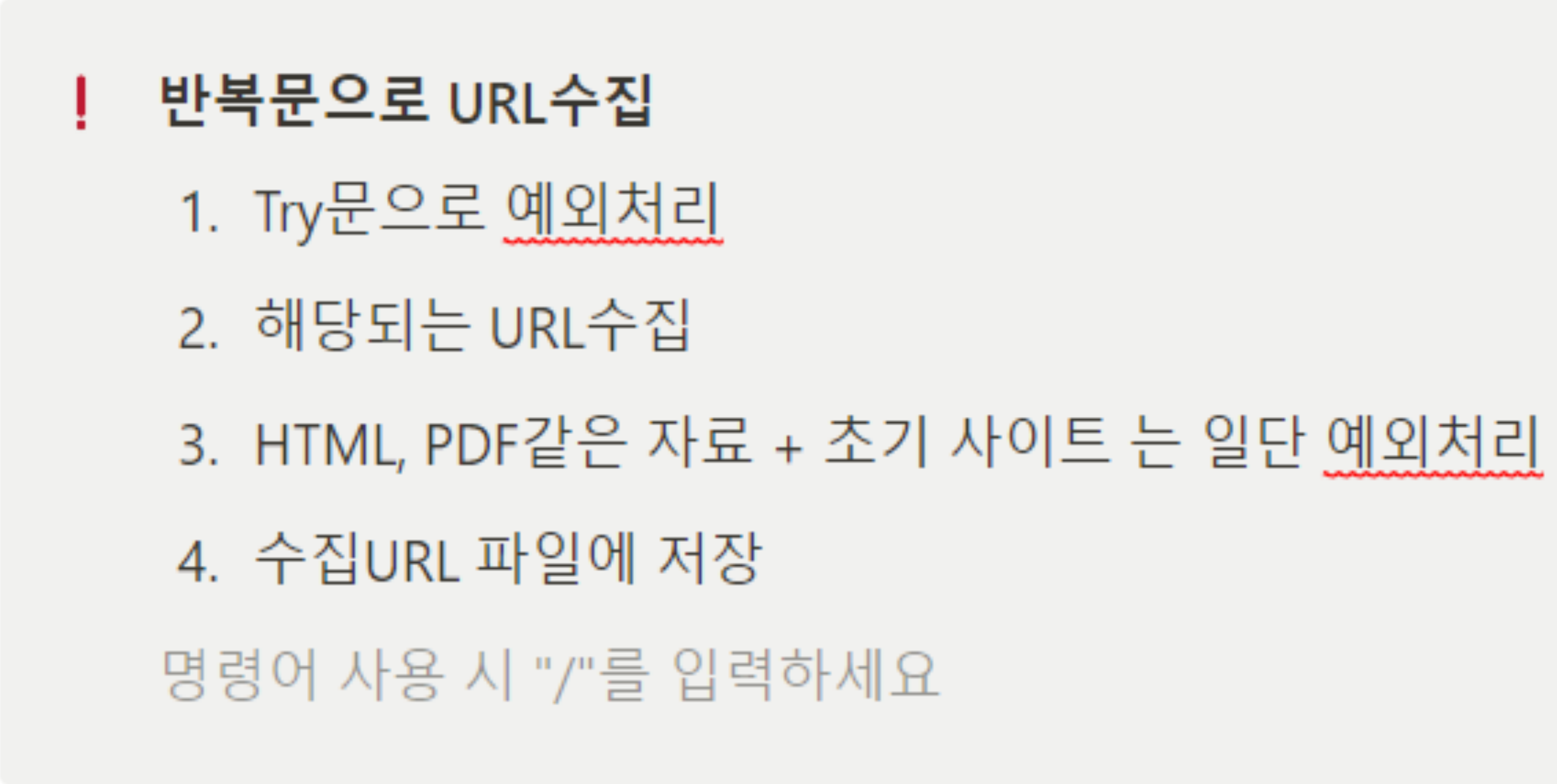
수집한 CVE-ID URL수집



CVE-ID Search
ID에 해당하는 URL 수집



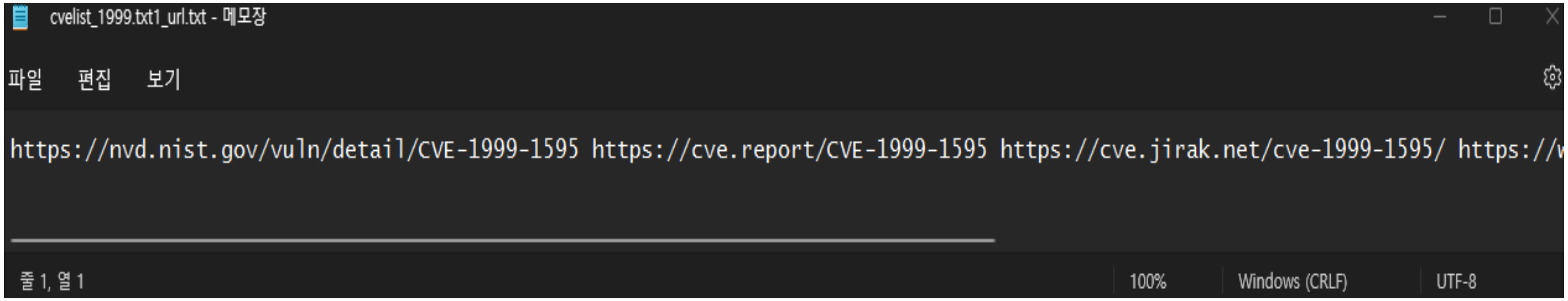
```
def main():
    print("메인")
    global check_ttr
    global url_num
    check_ttr = 0
    url_num = url_num + 1
    while 1:
        check_ttr = check_ttr + 1
        try:
            qwer = driver.find_element_by_xpath(f'//*[@id="rso"]/div[{check_ttr}]/div/div/div[1]/div/a'.format(check_ttr))
        except:
            try:
                qwer = driver.find_element_by_xpath(f'//*[@id="rso"]/div[{check_ttr}]/div/div/div[1]/div/div/div[1]/div/a'.form
            except:
                try:
                    qwer = driver.find_element_by_xpath(f'//*[@id="rso"]/div[{check_ttr}]/div/div/div/div/div/div/div[1]/a'.for
                except:
                    print("안돼안돼안돼")
                    break

        print(qwer.text)
        href = qwer.get_attribute('href')
        print(href)

        if ".html" in href:
            print("skip")
        elif ".pdf" in href:
            print("skip")
        elif "https://cve.mitre.org" in href:
            print("skip")
        else:
            global url_filename
            url_filename = str(filename) + str(url_num) + '_url.txt'
            with open(url_filename,"a",encoding="UTF-8") as q:
                q.write(href + " ")
    main3()
```



! 반복문으로 URL수집

1. Try문으로 예외처리
2. 해당되는 URL수집
3. HTML, PDF같은 자료 + 초기 사이트 는 일단 예외처리
4. 수집URL 파일에 저장

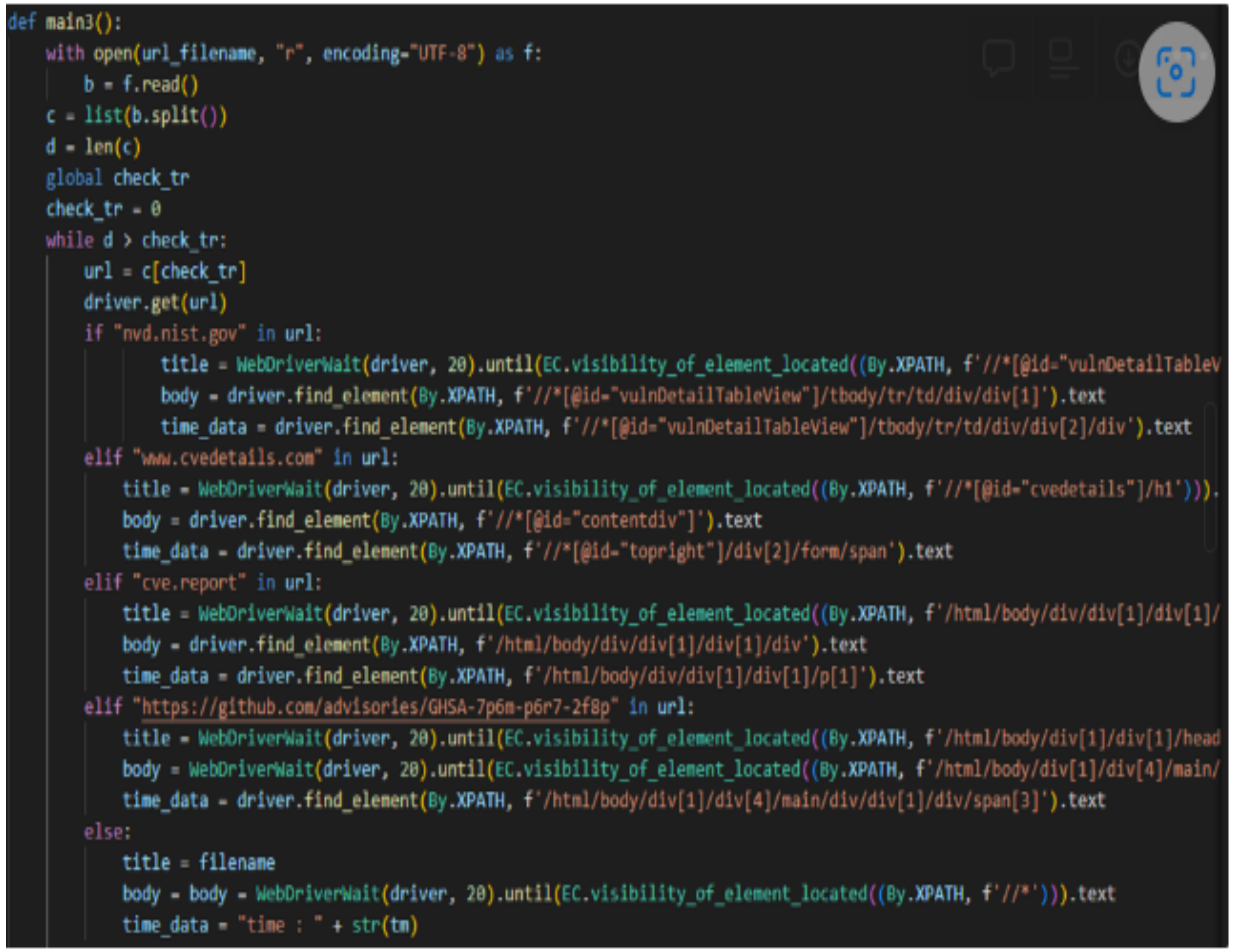
명령어 사용 시 "/"를 입력하세요



```
https://nvd.nist.gov/vuln/detail/CVE-1999-1595 https://cve.report/CVE-1999-1595 https://cve.jirak.net/cve-1999-1595/ https://w
```

수집된 URL 사이트 이동 데이터 수집

수집한 URL 검색
CVE-ID에 자세한 정보 크롤링

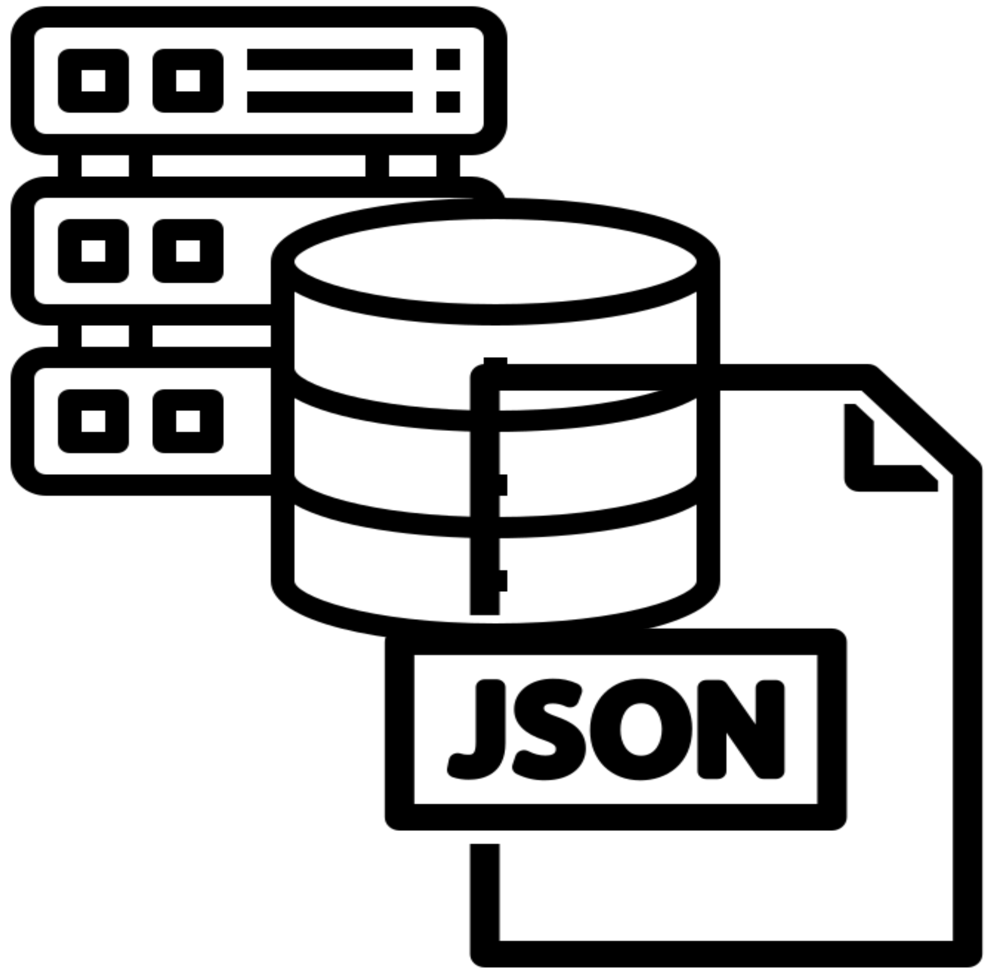


```
def main3():
    with open(url_filename, "r", encoding="UTF-8") as f:
        b = f.read()
    c = list(b.split())
    d = len(c)
    global check_tr
    check_tr = 0
    while d > check_tr:
        url = c[check_tr]
        driver.get(url)
        if "nvd.nist.gov" in url:
                title = WebDriverWait(driver, 20).until(EC.visibility_of_element_located((By.XPATH, f'//*[@id="vulnDetailTableV
                body = driver.find_element(By.XPATH, f'//*[@id="vulnDetailTableView"]/tbody/tr/td/div/div[1]').text
                time_data = driver.find_element(By.XPATH, f'//*[@id="vulnDetailTableView"]/tbody/tr/td/div/div[2]/div').text
        elif "www.cvedetails.com" in url:
            title = WebDriverWait(driver, 20).until(EC.visibility_of_element_located((By.XPATH, f'//*[@id="cvedetails"]/h1'))).
            body = driver.find_element(By.XPATH, f'//*[@id="contentdiv"]').text
            time_data = driver.find_element(By.XPATH, f'//*[@id="topright"]/div[2]/form/span').text
        elif "cve.report" in url:
            title = WebDriverWait(driver, 20).until(EC.visibility_of_element_located((By.XPATH, f'/html/body/div/div[1]/div[1]/
            body = driver.find_element(By.XPATH, f'/html/body/div/div[1]/div[1]/div').text
            time_data = driver.find_element(By.XPATH, f'/html/body/div/div[1]/div[1]/p[1]').text
        elif "https://github.com/advisories/GHSA-7p6m-p6r7-2f8p" in url:
            title = WebDriverWait(driver, 20).until(EC.visibility_of_element_located((By.XPATH, f'/html/body/div[1]/div[1]/head
            body = WebDriverWait(driver, 20).until(EC.visibility_of_element_located((By.XPATH, f'/html/body/div[1]/div[4]/main/
            time_data = driver.find_element(By.XPATH, f'/html/body/div[1]/div[4]/main/div/div[1]/div/span[3]').text
        else:
            title = filename
            body = body = WebDriverWait(driver, 20).until(EC.visibility_of_element_located((By.XPATH, f'//*'))).text
            time_data = "time : " + str(tm)
```

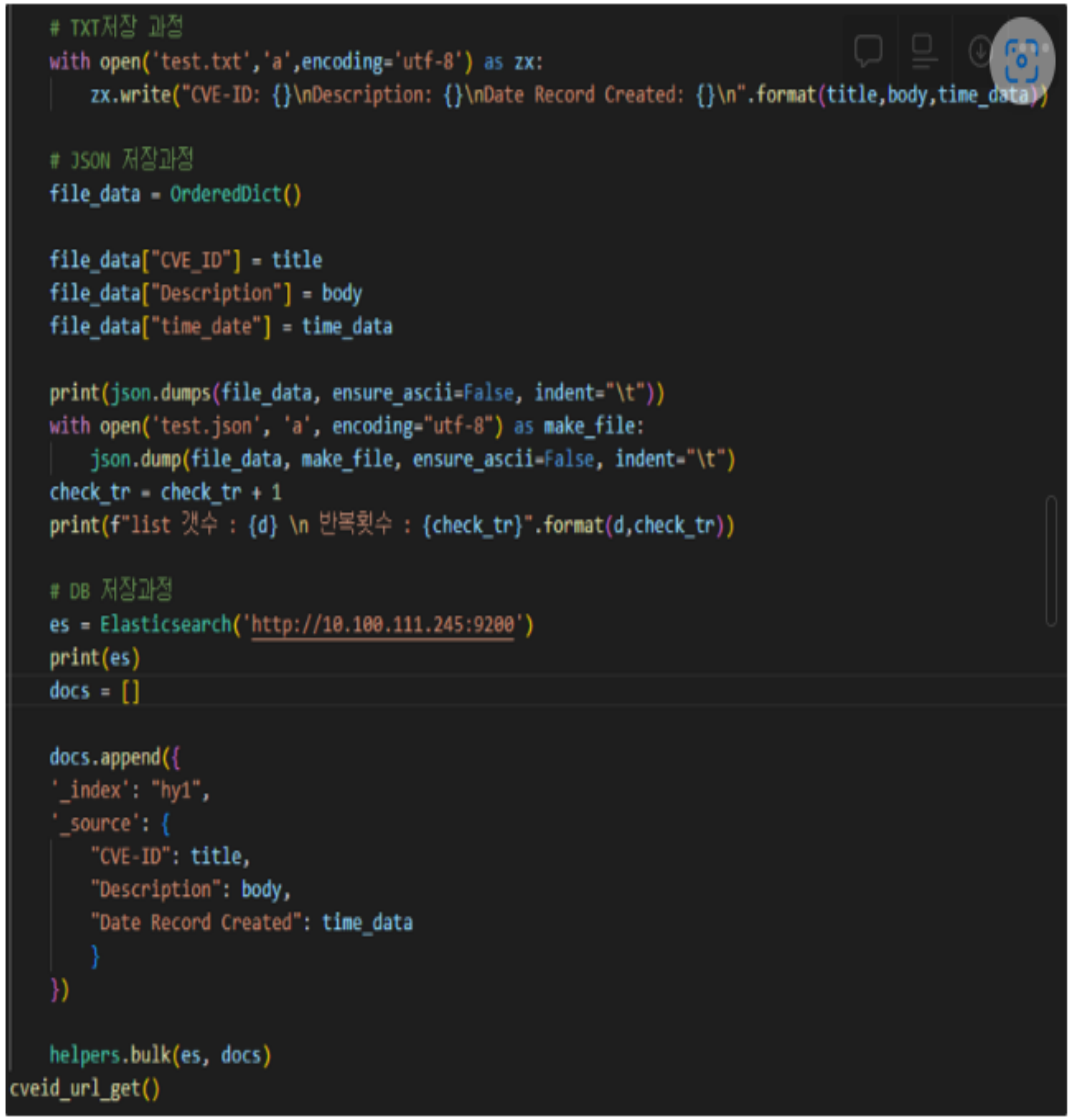
❗ 수집된 URL 이동후 데이터 수집

1. 수집된 URL 리스트 형태로 반환 및 순서대로 접속
2. 특정 사이트 형식 체계화
3. 그외 다른사이트는 모든 데이터 가져오는 방식

TXT, DB, JSON 저장



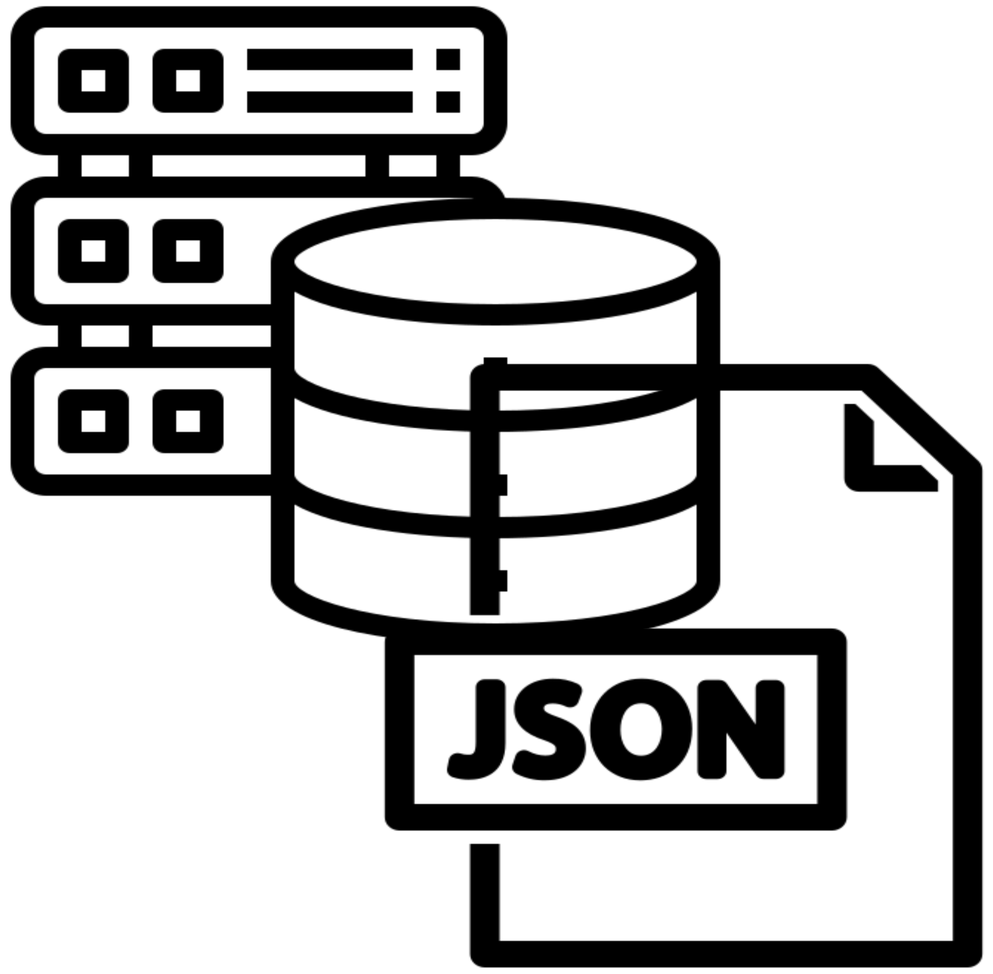
Elastic DB 에 저장 &
json 파일 형태로로 저장



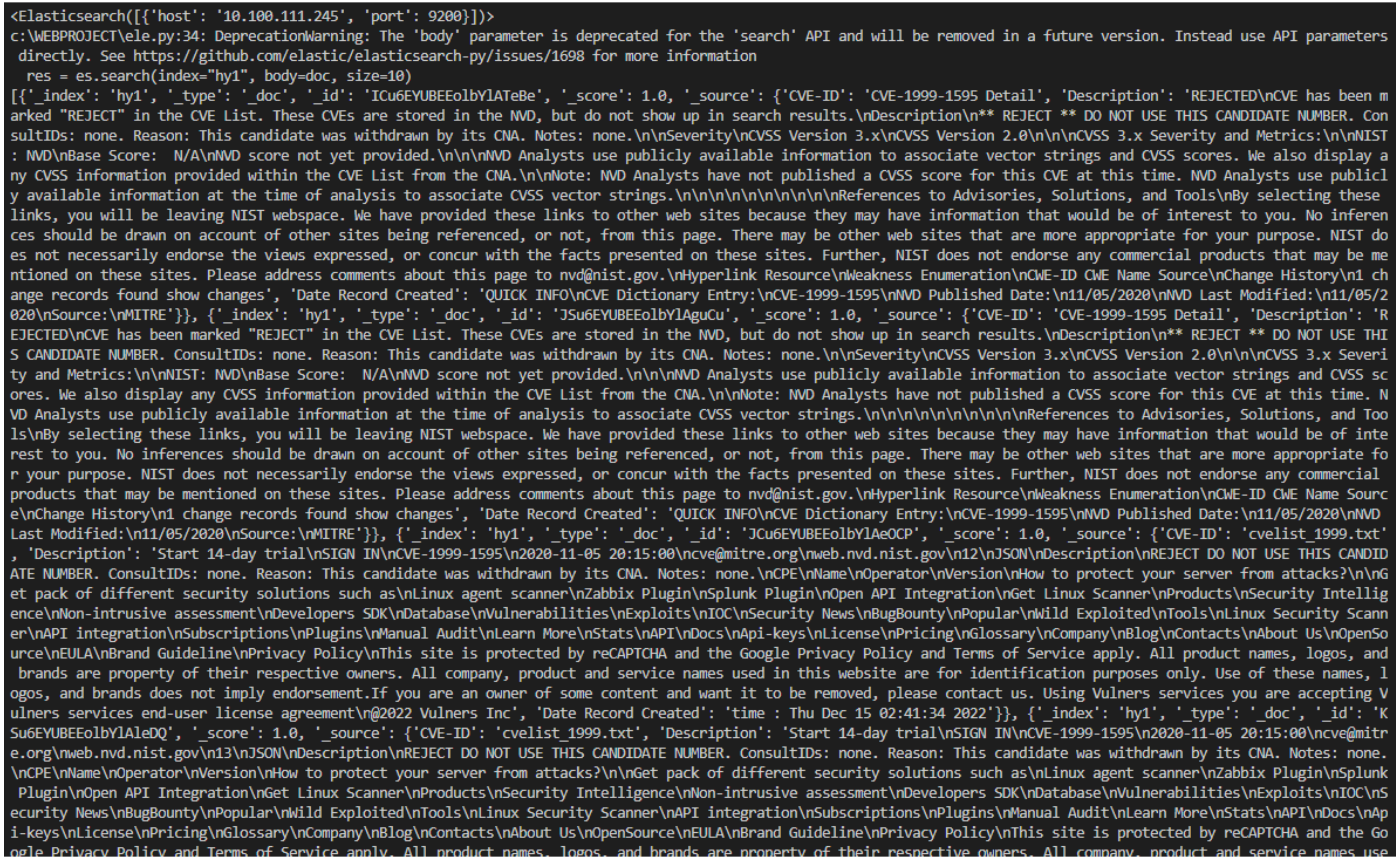
```
    # TXT저장 과정
    with open('test.txt','a',encoding='utf-8') as zx:
        zx.write("CVE-ID: {}\nDescription: {}\nDate Record Created: {}\n".format(title,body,time_data))

    # JSON 저장과정
    file_data = OrderedDict()

    file_data["CVE_ID"] = title
    file_data["Description"] = body
    file_data["time_date"] = time_data

    print(json.dumps(file_data, ensure_ascii=False, indent="\t"))
    with open('test.json', 'a', encoding="utf-8") as make_file:
        json.dump(file_data, make_file, ensure_ascii=False, indent="\t")
    check_tr = check_tr + 1
    print(f"list 갯수 : {d} \n 반복횟수 : {check_tr}".format(d,check_tr))

    # DB 저장과정
    es = Elasticsearch('http://10.100.111.245:9200')
    print(es)
    docs = []

    docs.append({
    '_index': "hy1",
    '_source': {
        "CVE-ID": title,
        "Description": body,
        "Date Record Created": time_data
        }
    })

    helpers.bulk(es, docs)
cveid_url_get()
```

! **데이터 저장과정**

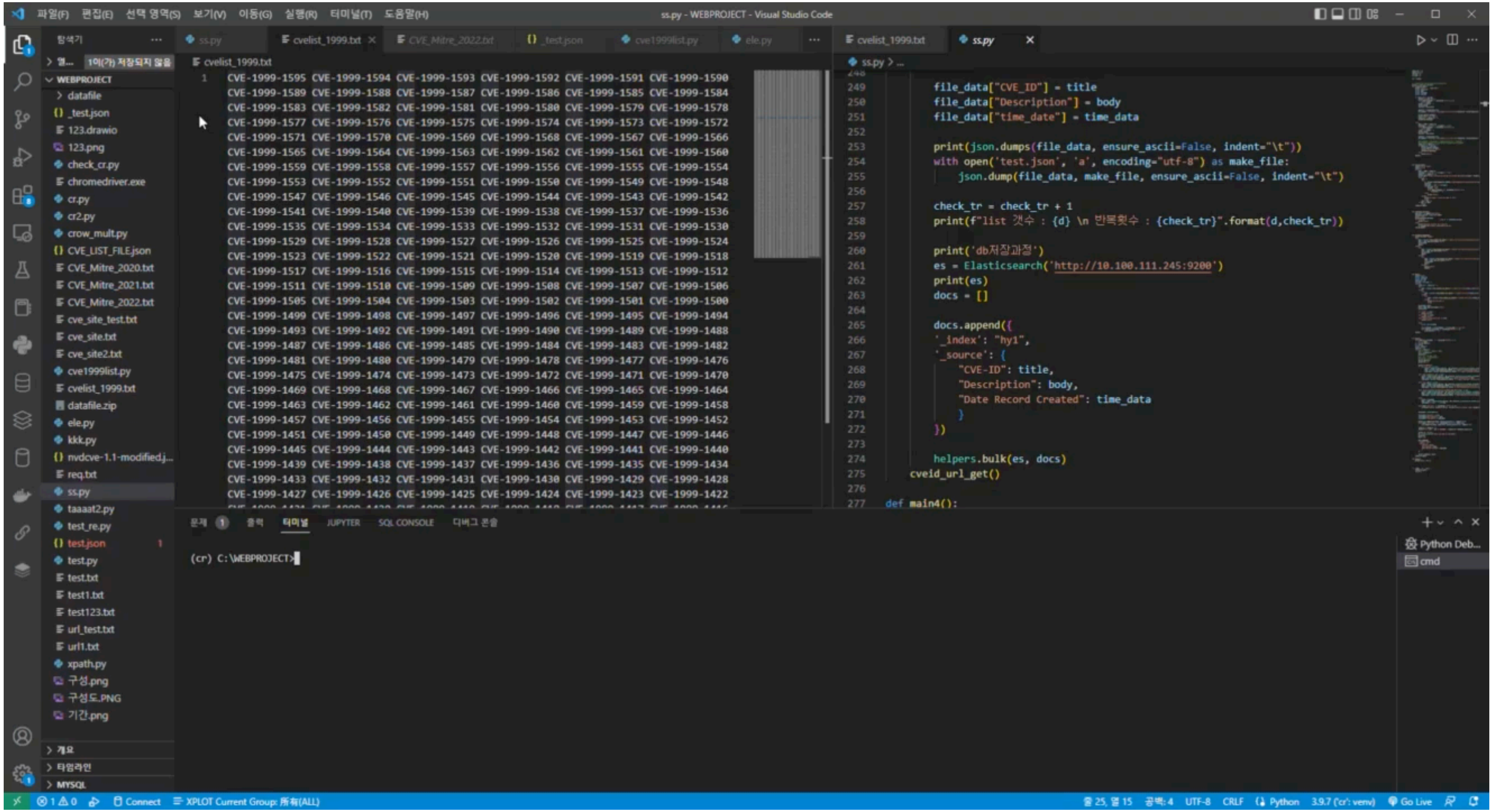
1. TXT로 형태를 갖춰서 저장
2. JSON으로 저장
3. Elasticsearch 연결
4. json형태로 만들고 index, cve-id, description, date record created 등과같은 형태를 만들어 저장



Elastic DB 에 저장 &
json 파일 형태로로 저장



```
<Elasticsearch([{'host': '10.100.111.245', 'port': 9200}])>
c:\WEBPROJECT\ele.py:34: DeprecationWarning: The 'body' parameter is deprecated for the 'search' API and will be removed in a future version. Instead use API parameters
 directly. See https://github.com/elastic/elasticsearch-py/issues/1698 for more information
  res = es.search(index="hy1", body=doc, size=10)
[{'_index': 'hy1', '_type': '_doc', '_id': 'ICu6EYUBEEolbYlATeBe', '_score': 1.0, '_source': {'CVE-ID': 'CVE-1999-1595 Detail', 'Description': 'REJECTED\nCVE has been m
arked "REJECT" in the CVE List. These CVEs are stored in the NVD, but do not show up in search results.\nDescription\n** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Con
sultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none.\n\nSeverity\nCVSS Version 3.x\nCVSS Version 2.0\n\n\nCVSS 3.x Severity and Metrics:\n\nNIST
: NVD\nBase Score:  N/A\nNVD score not yet provided.\n\n\nNVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display a
ny CVSS information provided within the CVE List from the CNA.\n\nNote: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicl
y available information at the time of analysis to associate CVSS vector strings.\n\n\n\n\n\n\n\n\n\nReferences to Advisories, Solutions, and Tools\nBy selecting these
links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferen
ces should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST do
es not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be me
ntioned on these sites. Please address comments about this page to nvd@nist.gov.\nHyperlink Resource\nWeakness Enumeration\nCWE-ID CWE Name Source\nChange History\n1 ch
ange records found show changes', 'Date Record Created': 'QUICK INFO\nCVE Dictionary Entry:\nCVE-1999-1595\nNVD Published Date:\n11/05/2020\nNVD Last Modified:\n11/05/2
020\nSource:\nMITRE'}}, {'_index': 'hy1', '_type': '_doc', '_id': 'JSu6EYUBEEolbYlAguCu', '_score': 1.0, '_source': {'CVE-ID': 'CVE-1999-1595 Detail', 'Description': 'R
EJECTED\nCVE has been marked "REJECT" in the CVE List. These CVEs are stored in the NVD, but do not show up in search results.\nDescription\n** REJECT ** DO NOT USE THI
S CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none.\n\nSeverity\nCVSS Version 3.x\nCVSS Version 2.0\n\n\nCVSS 3.x Severi
ty and Metrics:\n\nNIST: NVD\nBase Score:  N/A\nNVD score not yet provided.\n\n\nNVD Analysts use publicly available information to associate vector strings and CVSS sc
ores. We also display any CVSS information provided within the CVE List from the CNA.\n\nNote: NVD Analysts have not published a CVSS score for this CVE at this time. N
VD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.\n\n\n\n\n\n\n\n\n\nReferences to Advisories, Solutions, and Too
ls\nBy selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of inte
rest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate fo
r your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial
products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.\nHyperlink Resource\nWeakness Enumeration\nCWE-ID CWE Name Sourc
e\nChange History\n1 change records found show changes', 'Date Record Created': 'QUICK INFO\nCVE Dictionary Entry:\nCVE-1999-1595\nNVD Published Date:\n11/05/2020\nNVD
Last Modified:\n11/05/2020\nSource:\nMITRE'}}, {'_index': 'hy1', '_type': '_doc', '_id': 'JCu6EYUBEEolbYlAeOCP', '_score': 1.0, '_source': {'CVE-ID': 'cvelist_1999.txt'
, 'Description': 'Start 14-day trial\nSIGN IN\nCVE-1999-1595\n2020-11-05 20:15:00\ncve@mitre.org\nweb.nvd.nist.gov\n12\nJSON\nDescription\nREJECT DO NOT USE THIS CANDID
ATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none.\nCPE\nName\nOperator\nVersion\nHow to protect your server from attacks?\n\nG
et pack of different security solutions such as\nLinux agent scanner\nZabbix Plugin\nSplunk Plugin\nOpen API Integration\nGet Linux Scanner\nProducts\nSecurity Intellig
ence\nNon-intrusive assessment\nDevelopers SDK\nDatabase\nVulnerabilities\nExploits\nIOC\nSecurity News\nBugBounty\nPopular\nWild Exploited\nTools\nLinux Security Scann
er\nAPI integration\nSubscriptions\nPlugins\nManual Audit\nLearn More\nStats\nAPI\nDocs\nApi-keys\nLicense\nPricing\nGlossary\nCompany\nBlog\nContacts\nAbout Us\nOpenSo
urce\nEULA\nBrand Guideline\nPrivacy Policy\nThis site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply. All product names, logos, and
 brands are property of their respective owners. All company, product and service names used in this website are for identification purposes only. Use of these names, l
ogos, and brands does not imply endorsement.If you are an owner of some content and want it to be removed, please contact us. Using Vulners services you are accepting V
ulners services end-user license agreement\n@2022 Vulners Inc', 'Date Record Created': 'time : Thu Dec 15 02:41:34 2022'}}, {'_index': 'hy1', '_type': '_doc', '_id': 'K
Su6EYUBEEolbYlAleDQ', '_score': 1.0, '_source': {'CVE-ID': 'cvelist_1999.txt', 'Description': 'Start 14-day trial\nSIGN IN\nCVE-1999-1595\n2020-11-05 20:15:00\ncve@mitr
e.org\nweb.nvd.nist.gov\n13\nJSON\nDescription\nREJECT DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none.
\nCPE\nName\nOperator\nVersion\nHow to protect your server from attacks?\n\nGet pack of different security solutions such as\nLinux agent scanner\nZabbix Plugin\nSplunk
 Plugin\nOpen API Integration\nGet Linux Scanner\nProducts\nSecurity Intelligence\nNon-intrusive assessment\nDevelopers SDK\nDatabase\nVulnerabilities\nExploits\nIOC\nS
ecurity News\nBugBounty\nPopular\nWild Exploited\nTools\nLinux Security Scanner\nAPI integration\nSubscriptions\nPlugins\nManual Audit\nLearn More\nStats\nAPI\nDocs\nAp
i-keys\nLicense\nPricing\nGlossary\nCompany\nBlog\nContacts\nAbout Us\nOpenSource\nEULA\nBrand Guideline\nPrivacy Policy\nThis site is protected by reCAPTCHA and the Go
ogle Privacy Policy and Terms of Service apply. All product names, logos, and brands are property of their respective owners. All company, product and service names use
```



cvelist_1999.txt

```
CVE-1999-1595 CVE-1999-1594 CVE-1999-1593 CVE-1999-1592 CVE-1999-1591 CVE-1999-1590
CVE-1999-1589 CVE-1999-1588 CVE-1999-1587 CVE-1999-1586 CVE-1999-1585 CVE-1999-1584
CVE-1999-1583 CVE-1999-1582 CVE-1999-1581 CVE-1999-1580 CVE-1999-1579 CVE-1999-1578
CVE-1999-1577 CVE-1999-1576 CVE-1999-1575 CVE-1999-1574 CVE-1999-1573 CVE-1999-1572
CVE-1999-1571 CVE-1999-1570 CVE-1999-1569 CVE-1999-1568 CVE-1999-1567 CVE-1999-1566
CVE-1999-1565 CVE-1999-1564 CVE-1999-1563 CVE-1999-1562 CVE-1999-1561 CVE-1999-1560
CVE-1999-1559 CVE-1999-1558 CVE-1999-1557 CVE-1999-1556 CVE-1999-1555 CVE-1999-1554
CVE-1999-1553 CVE-1999-1552 CVE-1999-1551 CVE-1999-1550 CVE-1999-1549 CVE-1999-1548
CVE-1999-1547 CVE-1999-1546 CVE-1999-1545 CVE-1999-1544 CVE-1999-1543 CVE-1999-1542
CVE-1999-1541 CVE-1999-1540 CVE-1999-1539 CVE-1999-1538 CVE-1999-1537 CVE-1999-1536
CVE-1999-1535 CVE-1999-1534 CVE-1999-1533 CVE-1999-1532 CVE-1999-1531 CVE-1999-1530
CVE-1999-1529 CVE-1999-1528 CVE-1999-1527 CVE-1999-1526 CVE-1999-1525 CVE-1999-1524
CVE-1999-1523 CVE-1999-1522 CVE-1999-1521 CVE-1999-1520 CVE-1999-1519 CVE-1999-1518
CVE-1999-1517 CVE-1999-1516 CVE-1999-1515 CVE-1999-1514 CVE-1999-1513 CVE-1999-1512
CVE-1999-1511 CVE-1999-1510 CVE-1999-1509 CVE-1999-1508 CVE-1999-1507 CVE-1999-1506
CVE-1999-1505 CVE-1999-1504 CVE-1999-1503 CVE-1999-1502 CVE-1999-1501 CVE-1999-1500
CVE-1999-1499 CVE-1999-1498 CVE-1999-1497 CVE-1999-1496 CVE-1999-1495 CVE-1999-1494
CVE-1999-1493 CVE-1999-1492 CVE-1999-1491 CVE-1999-1490 CVE-1999-1489 CVE-1999-1488
CVE-1999-1487 CVE-1999-1486 CVE-1999-1485 CVE-1999-1484 CVE-1999-1483 CVE-1999-1482
CVE-1999-1481 CVE-1999-1480 CVE-1999-1479 CVE-1999-1478 CVE-1999-1477 CVE-1999-1476
CVE-1999-1475 CVE-1999-1474 CVE-1999-1473 CVE-1999-1472 CVE-1999-1471 CVE-1999-1470
CVE-1999-1469 CVE-1999-1468 CVE-1999-1467 CVE-1999-1466 CVE-1999-1465 CVE-1999-1464
CVE-1999-1463 CVE-1999-1462 CVE-1999-1461 CVE-1999-1460 CVE-1999-1459 CVE-1999-1458
CVE-1999-1457 CVE-1999-1456 CVE-1999-1455 CVE-1999-1454 CVE-1999-1453 CVE-1999-1452
CVE-1999-1451 CVE-1999-1450 CVE-1999-1449 CVE-1999-1448 CVE-1999-1447 CVE-1999-1446
CVE-1999-1445 CVE-1999-1444 CVE-1999-1443 CVE-1999-1442 CVE-1999-1441 CVE-1999-1440
CVE-1999-1439 CVE-1999-1438 CVE-1999-1437 CVE-1999-1436 CVE-1999-1435 CVE-1999-1434
CVE-1999-1433 CVE-1999-1432 CVE-1999-1431 CVE-1999-1430 CVE-1999-1429 CVE-1999-1428
CVE-1999-1427 CVE-1999-1426 CVE-1999-1425 CVE-1999-1424 CVE-1999-1423 CVE-1999-1422
```

ss.py

```python
        file_data["CVE_ID"] = title
        file_data["Description"] = body
        file_data["time_date"] = time_data

        print(json.dumps(file_data, ensure_ascii=False, indent="\t"))
        with open('test.json', 'a', encoding="utf-8") as make_file:
            json.dump(file_data, make_file, ensure_ascii=False, indent="\t")

        check_tr = check_tr + 1
        print(f"list 갯수 : {d} \n 반복횟수 : {check_tr}".format(d,check_tr))

        print('db저장과정')
        es = Elasticsearch('http://10.100.111.245:9200')
        print(es)
        docs = []

        docs.append({
        '_index': "hy1",
        '_source': {
            "CVE-ID": title,
            "Description": body,
            "Date Record Created": time_data
            }
        })

        helpers.bulk(es, docs)
    cveid_url_get()

def main4():
```

```
(cr) C:\WEBPROJECT>
```

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

자연어 처리

개발 환경

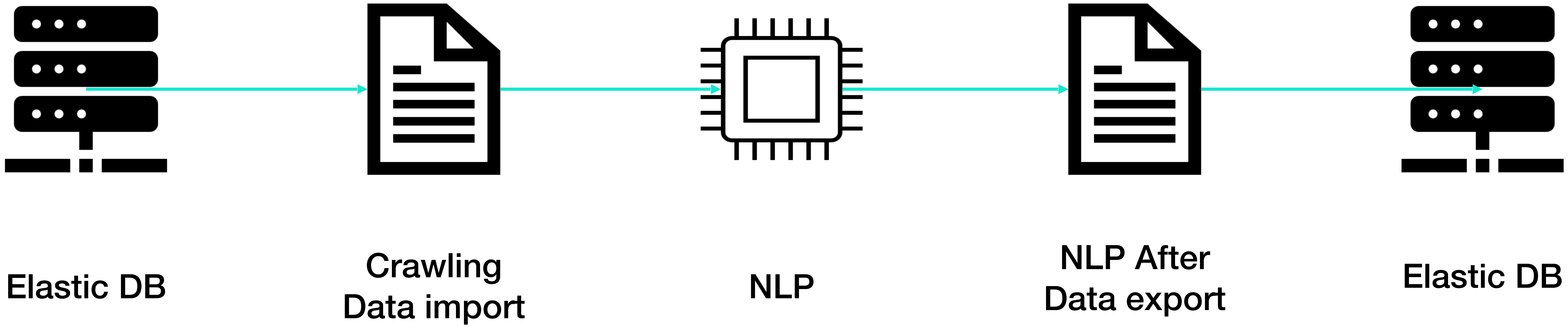
VS Code

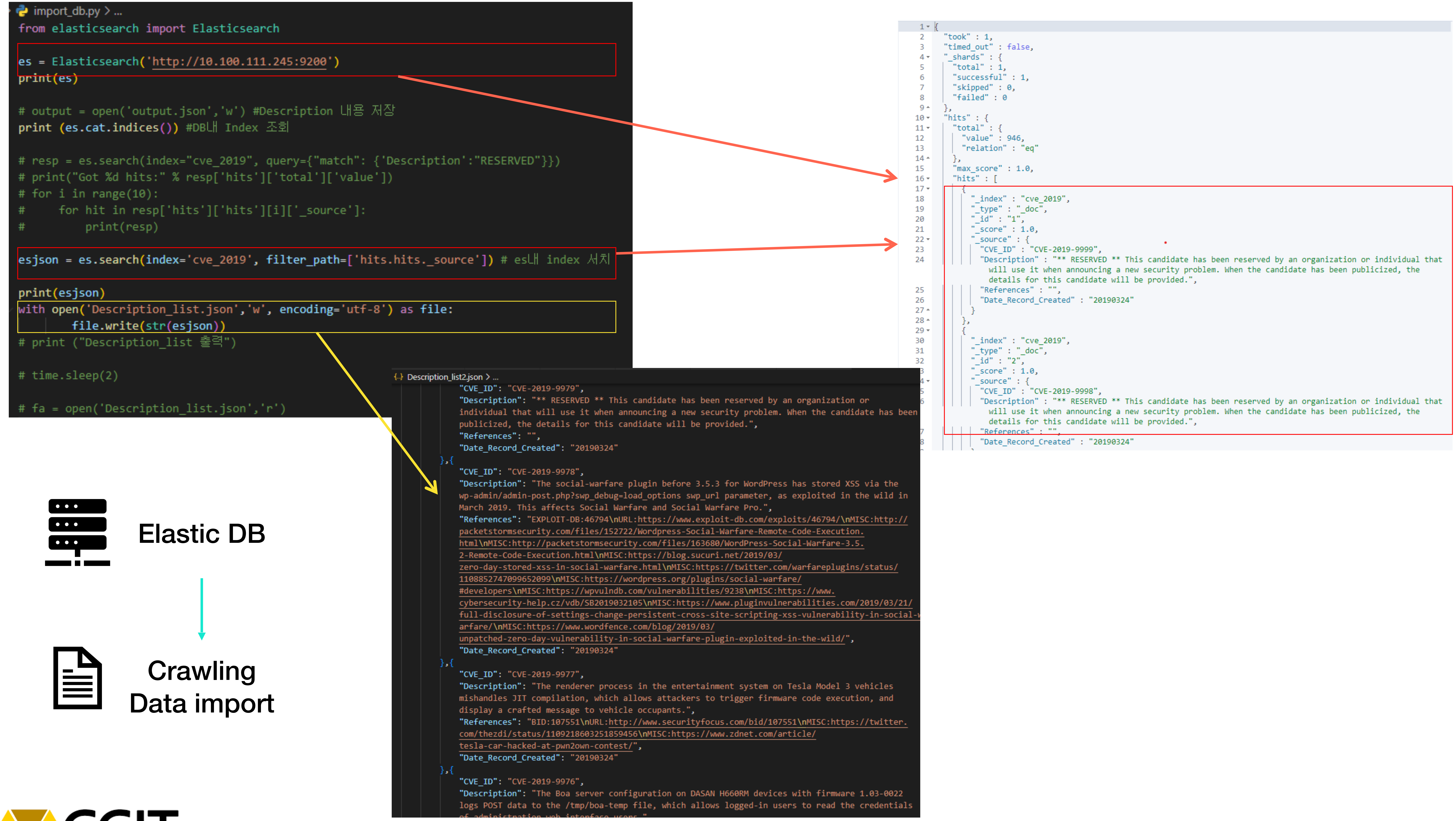
NLTK

Pandas

Elasticsearch

작동 구조


Elastic DB
Crawling
Data import
NLP
NLP After
Data export
Elastic DB

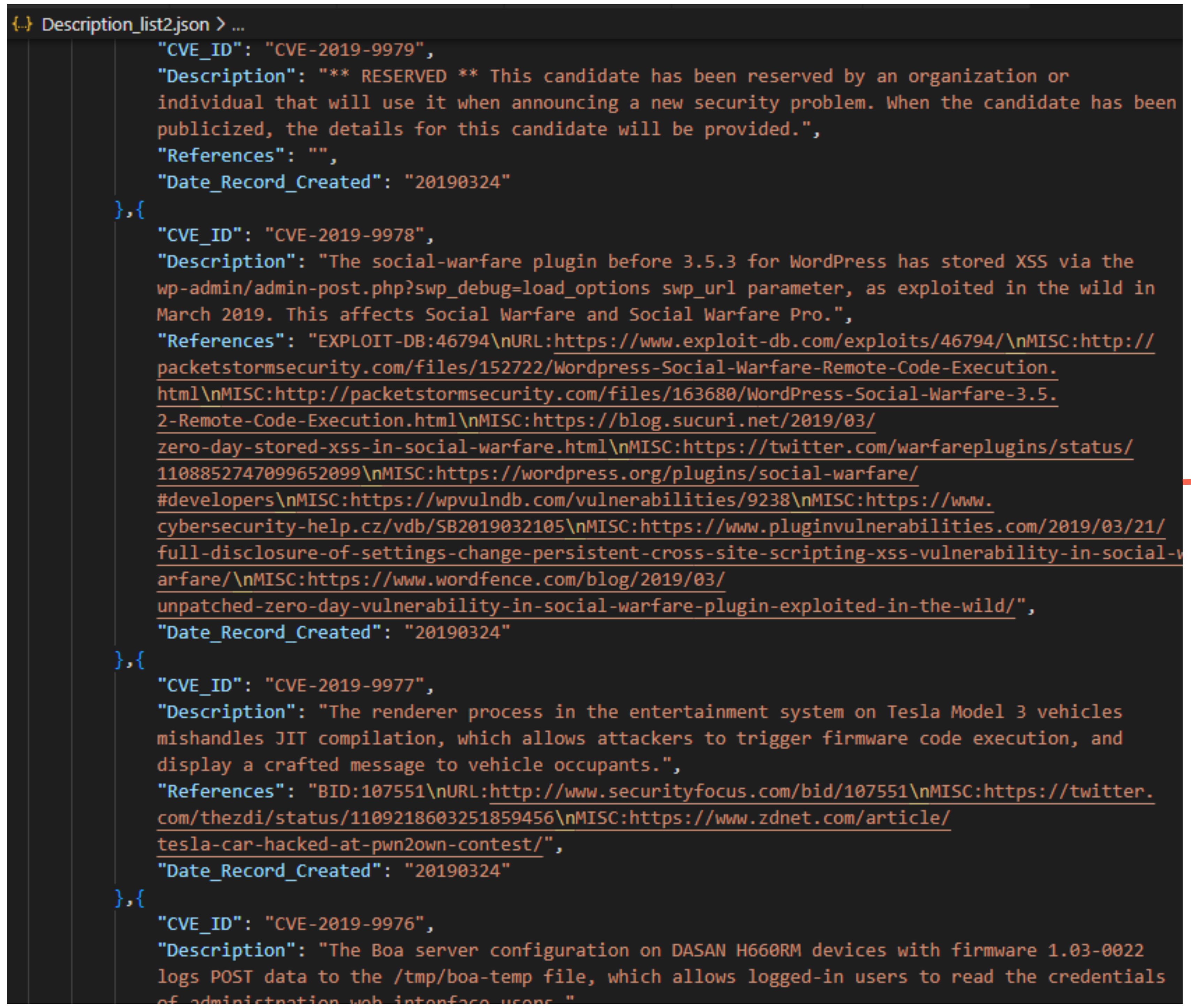


```python
from elasticsearch import Elasticsearch

es = Elasticsearch('http://10.100.111.245:9200')
print(es)

# output = open('output.json','w') #Description 내용 저장
print (es.cat.indices()) #DB내 Index 조회

# resp = es.search(index="cve_2019", query={"match": {'Description':"RESERVED"}})
# print("Got %d hits:" % resp['hits']['total']['value'])
# for i in range(10):
#     for hit in resp['hits']['hits'][i]['_source']:
#         print(resp)

esjson = es.search(index='cve_2019', filter_path=['hits.hits._source']) # es내 index 서치

print(esjson)
with open('Description_list.json','w', encoding='utf-8') as file:
        file.write(str(esjson))
# print ("Description_list 출력")

# time.sleep(2)

# fa = open('Description_list.json','r')
```

```json
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 946,
      "relation" : "eq"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "cve_2019",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 1.0,
        "_source" : {
          "CVE_ID" : "CVE-2019-9999",
          "Description" : "** RESERVED ** This candidate has been reserved by an organization or individual that
            will use it when announcing a new security problem. When the candidate has been publicized, the
            details for this candidate will be provided.",
          "References" : "",
          "Date_Record_Created" : "20190324"
        }
      },
      {
        "_index" : "cve_2019",
        "_type" : "_doc",
        "_id" : "2",
        "_score" : 1.0,
        "_source" : {
          "CVE_ID" : "CVE-2019-9998",
          "Description" : "** RESERVED ** This candidate has been reserved by an organization or individual that
            will use it when announcing a new security problem. When the candidate has been publicized, the
            details for this candidate will be provided.",
          "References" : "",
          "Date_Record_Created" : "20190324"
```

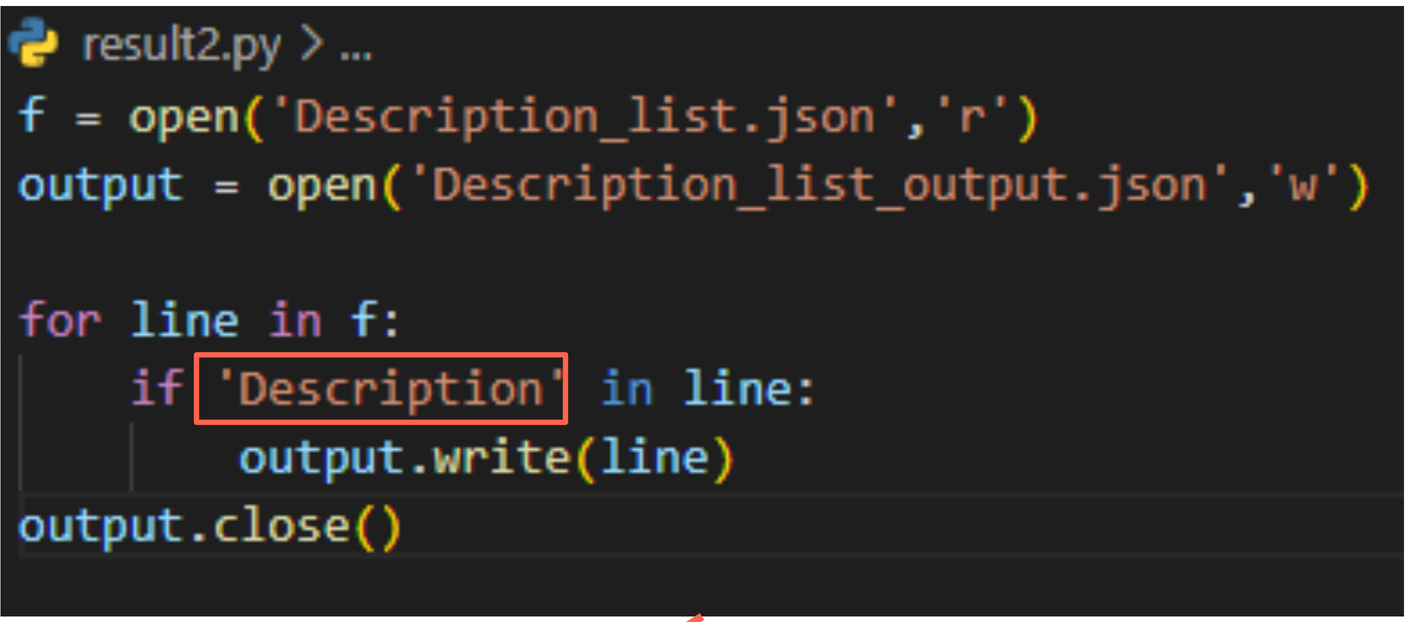
```json
          "CVE_ID": "CVE-2019-9979",
          "Description": "** RESERVED ** This candidate has been reserved by an organization or
          individual that will use it when announcing a new security problem. When the candidate has been
          publicized, the details for this candidate will be provided.",
          "References": "",
          "Date_Record_Created": "20190324"
        },{
          "CVE_ID": "CVE-2019-9978",
          "Description": "The social-warfare plugin before 3.5.3 for WordPress has stored XSS via the
          wp-admin/admin-post.php?swp_debug=load_options swp_url parameter, as exploited in the wild in
          March 2019. This affects Social Warfare and Social Warfare Pro.",
          "References": "EXPLOIT-DB:46794\nURL:https://www.exploit-db.com/exploits/46794/\nMISC:http://
          packetstormsecurity.com/files/152722/Wordpress-Social-Warfare-Remote-Code-Execution.
          html\nMISC:http://packetstormsecurity.com/files/163680/WordPress-Social-Warfare-3.5.
          2-Remote-Code-Execution.html\nMISC:https://blog.sucuri.net/2019/03/
          zero-day-stored-xss-in-social-warfare.html\nMISC:https://twitter.com/warfareplugins/status/
          1108852747099652099\nMISC:https://wordpress.org/plugins/social-warfare/
          #developers\nMISC:https://wpvulndb.com/vulnerabilities/9238\nMISC:https://www.
          cybersecurity-help.cz/vdb/SB2019032105\nMISC:https://www.pluginvulnerabilities.com/2019/03/21/
          full-disclosure-of-settings-change-persistent-cross-site-scripting-xss-vulnerability-in-social-w
          arfare/\nMISC:https://www.wordfence.com/blog/2019/03/
          unpatched-zero-day-vulnerability-in-social-warfare-plugin-exploited-in-the-wild/",
          "Date_Record_Created": "20190324"
        },{
          "CVE_ID": "CVE-2019-9977",
          "Description": "The renderer process in the entertainment system on Tesla Model 3 vehicles
          mishandles JIT compilation, which allows attackers to trigger firmware code execution, and
          display a crafted message to vehicle occupants.",
          "References": "BID:107551\nURL:http://www.securityfocus.com/bid/107551\nMISC:https://twitter.
          com/thezdi/status/1109218603251859456\nMISC:https://www.zdnet.com/article/
          tesla-car-hacked-at-pwn2own-contest/",
          "Date_Record_Created": "20190324"
        },{
          "CVE_ID": "CVE-2019-9976",
          "Description": "The Boa server configuration on DASAN H660RM devices with firmware 1.03-0022
          logs POST data to the /tmp/boa-temp file, which allows logged-in users to read the credentials
          of administration web interface users.",
```

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY



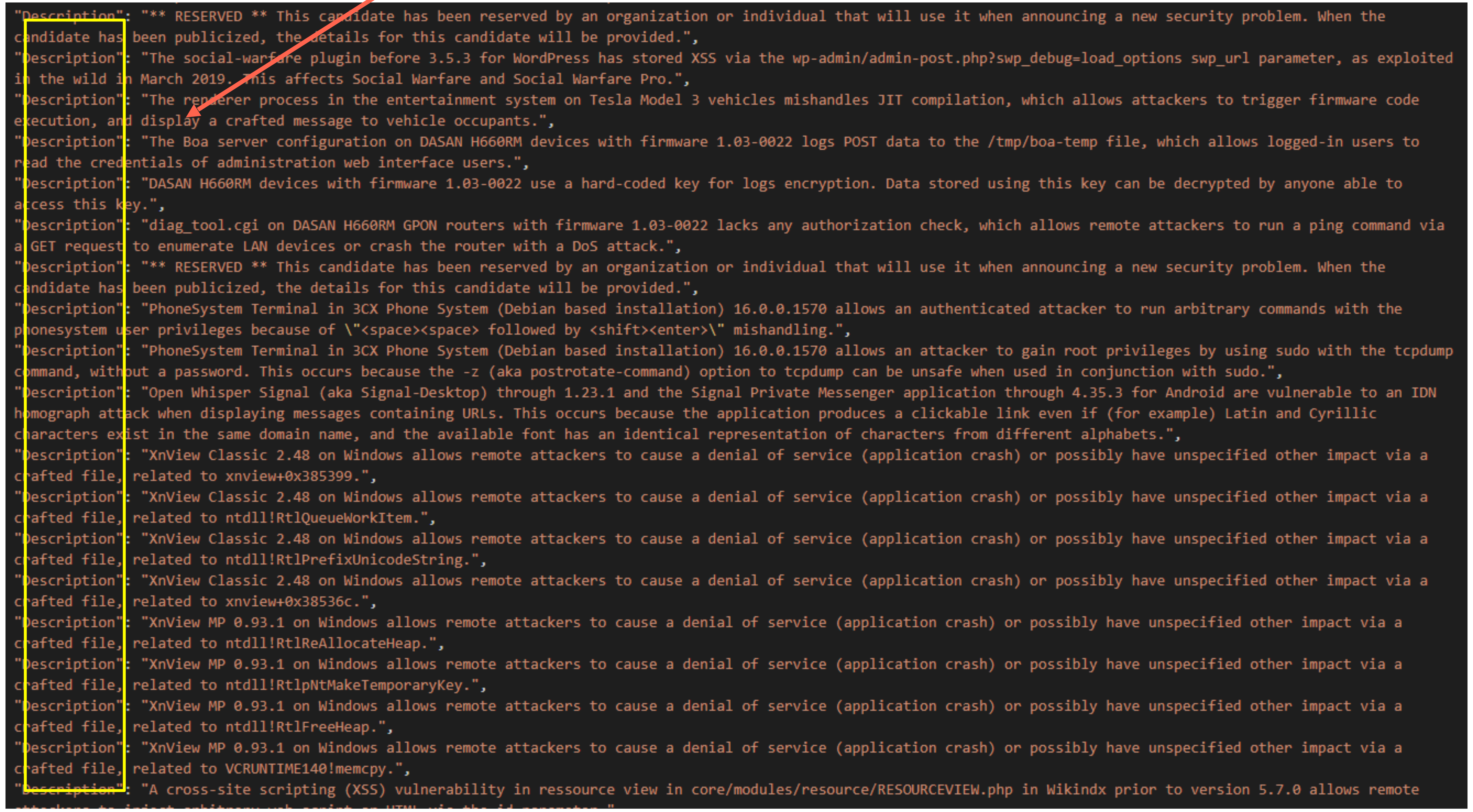
Description_list2.json > ...

```
            "CVE_ID": "CVE-2019-9979",
            "Description": "** RESERVED ** This candidate has been reserved by an organization or
            individual that will use it when announcing a new security problem. When the candidate has been
            publicized, the details for this candidate will be provided.",
            "References": "",
            "Date_Record_Created": "20190324"
        },{
            "CVE_ID": "CVE-2019-9978",
            "Description": "The social-warfare plugin before 3.5.3 for WordPress has stored XSS via the
            wp-admin/admin-post.php?swp_debug=load_options swp_url parameter, as exploited in the wild in
            March 2019. This affects Social Warfare and Social Warfare Pro.",
            "References": "EXPLOIT-DB:46794\nURL:https://www.exploit-db.com/exploits/46794/\nMISC:http://
            packetstormsecurity.com/files/152722/Wordpress-Social-Warfare-Remote-Code-Execution.
            html\nMISC:http://packetstormsecurity.com/files/163680/WordPress-Social-Warfare-3.5.
            2-Remote-Code-Execution.html\nMISC:https://blog.sucuri.net/2019/03/
            zero-day-stored-xss-in-social-warfare.html\nMISC:https://twitter.com/warfareplugins/status/
            1108852747099652099\nMISC:https://wordpress.org/plugins/social-warfare/
            #developers\nMISC:https://wpvulndb.com/vulnerabilities/9238\nMISC:https://www.
            cybersecurity-help.cz/vdb/SB2019032105\nMISC:https://www.pluginvulnerabilities.com/2019/03/21/
            full-disclosure-of-settings-change-persistent-cross-site-scripting-xss-vulnerability-in-social-w
            arfare/\nMISC:https://www.wordfence.com/blog/2019/03/
            unpatched-zero-day-vulnerability-in-social-warfare-plugin-exploited-in-the-wild/",
            "Date_Record_Created": "20190324"
        },{
            "CVE_ID": "CVE-2019-9977",
            "Description": "The renderer process in the entertainment system on Tesla Model 3 vehicles
            mishandles JIT compilation, which allows attackers to trigger firmware code execution, and
            display a crafted message to vehicle occupants.",
            "References": "BID:107551\nURL:http://www.securityfocus.com/bid/107551\nMISC:https://twitter.
            com/thezdi/status/1109218603251859456\nMISC:https://www.zdnet.com/article/
            tesla-car-hacked-at-pwn2own-contest/",
            "Date_Record_Created": "20190324"
        },{
            "CVE_ID": "CVE-2019-9976",
            "Description": "The Boa server configuration on DASAN H660RM devices with firmware 1.03-0022
            logs POST data to the /tmp/boa-temp file, which allows logged-in users to read the credentials
            of administration web interface users.",
```



result2.py > ...

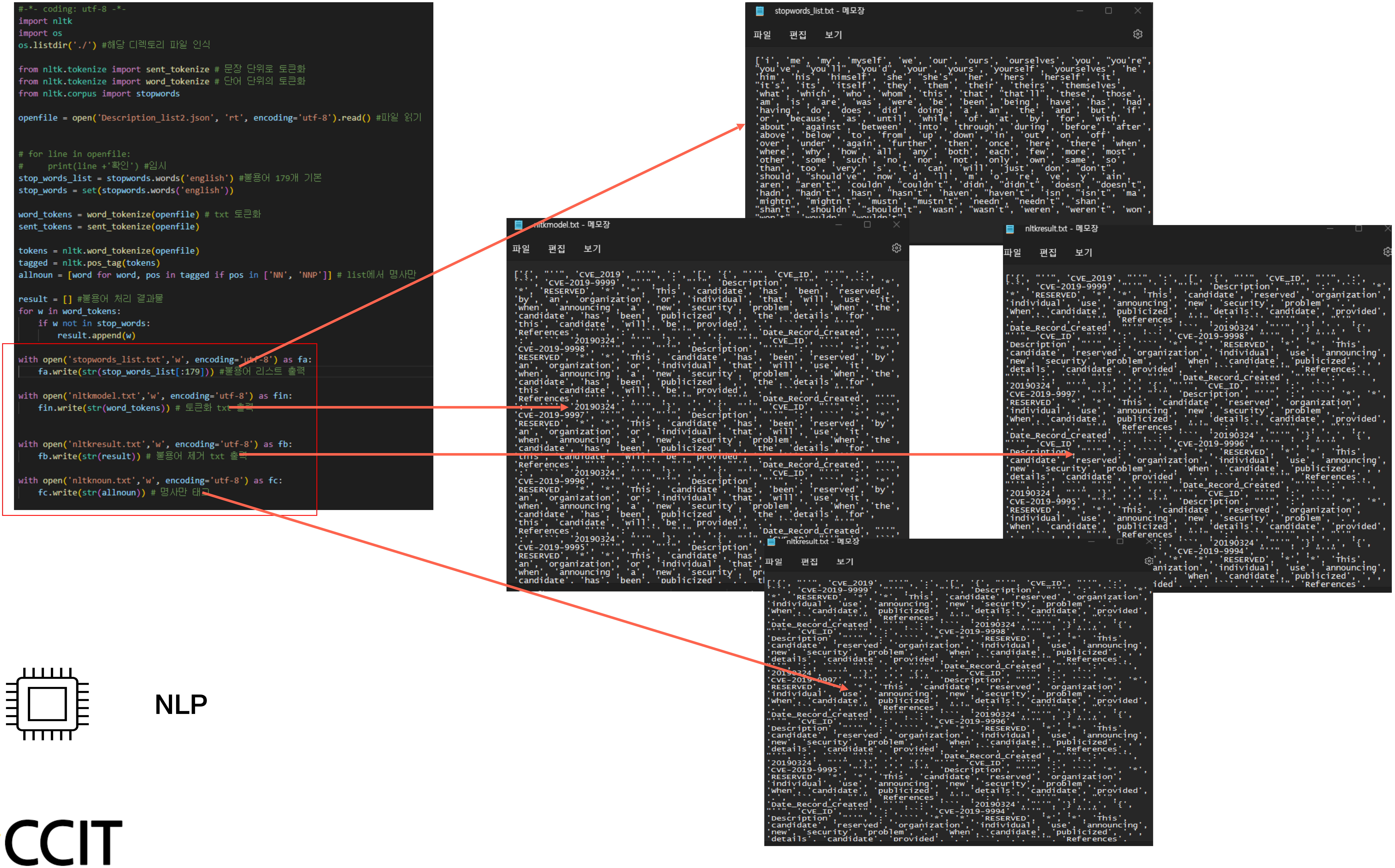
```python
f = open('Description_list.json','r')
output = open('Description_list_output.json','w')

for line in f:
    if 'Description' in line:
        output.write(line)
output.close()
```



```
"Description": "** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the
candidate has been publicized, the details for this candidate will be provided.",
"Description": "The social-warfare plugin before 3.5.3 for WordPress has stored XSS via the wp-admin/admin-post.php?swp_debug=load_options swp_url parameter, as exploited
in the wild in March 2019. This affects Social Warfare and Social Warfare Pro.",
"Description": "The renderer process in the entertainment system on Tesla Model 3 vehicles mishandles JIT compilation, which allows attackers to trigger firmware code
execution, and display a crafted message to vehicle occupants.",
"Description": "The Boa server configuration on DASAN H660RM devices with firmware 1.03-0022 logs POST data to the /tmp/boa-temp file, which allows logged-in users to
read the credentials of administration web interface users.",
"Description": "DASAN H660RM devices with firmware 1.03-0022 use a hard-coded key for logs encryption. Data stored using this key can be decrypted by anyone able to
access this key.",
"Description": "diag_tool.cgi on DASAN H660RM GPON routers with firmware 1.03-0022 lacks any authorization check, which allows remote attackers to run a ping command via
a GET request to enumerate LAN devices or crash the router with a DoS attack.",
"Description": "** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the
candidate has been publicized, the details for this candidate will be provided.",
"Description": "PhoneSystem Terminal in 3CX Phone System (Debian based installation) 16.0.0.1570 allows an authenticated attacker to run arbitrary commands with the
phonesystem user privileges because of \"<space><space> followed by <shift><enter>\" mishandling.",
"Description": "PhoneSystem Terminal in 3CX Phone System (Debian based installation) 16.0.0.1570 allows an attacker to gain root privileges by using sudo with the tcpdump
command, without a password. This occurs because the -z (aka postrotate-command) option to tcpdump can be unsafe when used in conjunction with sudo.",
"Description": "Open Whisper Signal (aka Signal-Desktop) through 1.23.1 and the Signal Private Messenger application through 4.35.3 for Android are vulnerable to an IDN
homograph attack when displaying messages containing URLs. This occurs because the application produces a clickable link even if (for example) Latin and Cyrillic
characters exist in the same domain name, and the available font has an identical representation of characters from different alphabets.",
"Description": "XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to xnview+0x385399.",
"Description": "XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to ntdll!RtlQueueWorkItem.",
"Description": "XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to ntdll!RtlPrefixUnicodeString.",
"Description": "XnView Classic 2.48 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to xnview+0x38536c.",
"Description": "XnView MP 0.93.1 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to ntdll!RtlReAllocateHeap.",
"Description": "XnView MP 0.93.1 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to ntdll!RtlpNtMakeTemporaryKey.",
"Description": "XnView MP 0.93.1 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to ntdll!RtlFreeHeap.",
"Description": "XnView MP 0.93.1 on Windows allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a
crafted file, related to VCRUNTIME140!memcpy.",
"Description": "A cross-site scripting (XSS) vulnerability in ressource view in core/modules/resource/RESOURCEVIEW.php in Wikindx prior to version 5.7.0 allows remote
attackers to inject arbitrary web script or HTML via the id parameter.",
```

Crawling
Data import

NLP



```python
#-*- coding: utf-8 -*-
import nltk
import os
os.listdir('./') #해당 디렉토리 파일 인식

from nltk.tokenize import sent_tokenize # 문장 단위로 토큰화
from nltk.tokenize import word_tokenize # 단어 단위의 토큰화
from nltk.corpus import stopwords

openfile = open('Description_list2.json', 'rt', encoding='utf-8').read() #파일 읽기


# for line in openfile:
#     print(line +'확인') #임시
stop_words_list = stopwords.words('english') #불용어 179개 기본
stop_words = set(stopwords.words('english'))

word_tokens = word_tokenize(openfile) # txt 토큰화
sent_tokens = sent_tokenize(openfile)

tokens = nltk.word_tokenize(openfile)
tagged = nltk.pos_tag(tokens)
allnoun = [word for word, pos in tagged if pos in ['NN', 'NNP']] # list에서 명사만

result = [] #불용어 처리 결과물
for w in word_tokens:
    if w not in stop_words:
        result.append(w)

with open('stopwords_list.txt','w', encoding='utf-8') as fa:
    fa.write(str(stop_words_list[:179])) #불용어 리스트 출력

with open('nltkmodel.txt','w', encoding='utf-8') as fin:
    fin.write(str(word_tokens)) # 토큰화 txt 출력


with open('nltkresult.txt','w', encoding='utf-8') as fb:
    fb.write(str(result)) # 불용어 제거 txt 출력

with open('nltknoun.txt','w', encoding='utf-8') as fc:
    fc.write(str(allnoun)) # 명사만 태그
```

stopwords_list.txt - 메모장

```
['i', 'me', 'my', 'myself', 'we', 'our', 'ours', 'ourselves', 'you', "you're",
"you've", "you'll", "you'd", 'your', 'yours', 'yourself', 'yourselves', 'he',
'him', 'his', 'himself', 'she', "she's", 'her', 'hers', 'herself', 'it',
"it's", 'its', 'itself', 'they', 'them', 'their', 'theirs', 'themselves',
'what', 'which', 'who', 'whom', 'this', 'that', "that'll", 'these', 'those',
'am', 'is', 'are', 'was', 'were', 'be', 'been', 'being', 'have', 'has', 'had',
'having', 'do', 'does', 'did', 'doing', 'a', 'an', 'the', 'and', 'but', 'if',
'or', 'because', 'as', 'until', 'while', 'of', 'at', 'by', 'for', 'with',
'about', 'against', 'between', 'into', 'through', 'during', 'before', 'after',
'above', 'below', 'to', 'from', 'up', 'down', 'in', 'out', 'on', 'off',
'over', 'under', 'again', 'further', 'then', 'once', 'here', 'there', 'when',
'where', 'why', 'how', 'all', 'any', 'both', 'each', 'few', 'more', 'most',
'other', 'some', 'such', 'no', 'nor', 'not', 'only', 'own', 'same', 'so',
'than', 'too', 'very', 's', 't', 'can', 'will', 'just', 'don', "don't",
'should', "should've", 'now', 'd', 'll', 'm', 'o', 're', 've', 'y', 'ain',
'aren', "aren't", 'couldn', "couldn't", 'didn', "didn't", 'doesn', "doesn't",
'hadn', "hadn't", 'hasn', "hasn't", 'haven', "haven't", 'isn', "isn't", 'ma',
'mightn', "mightn't", 'mustn', "mustn't", 'needn', "needn't", 'shan',
"shan't", 'shouldn', "shouldn't", 'wasn', "wasn't", 'weren', "weren't", 'won',
"won't", 'wouldn', "wouldn't"]
```

nltkmodel.txt - 메모장

```
['{', "''", 'CVE_2019', "''", ':', '[', '{', "''", 'CVE_ID', "''", ':',
'``', 'CVE-2019-9999', "''", ',', "''", 'Description', "''", ':', '``', '*',
'*', 'RESERVED', '*', '*', 'This', 'candidate', 'has', 'been', 'reserved',
'by', 'an', 'organization', 'or', 'individual', 'that', 'will', 'use', 'it',
'when', 'announcing', 'a', 'new', 'security', 'problem', '.', 'When', 'the',
'candidate', 'has', 'been', 'publicized', ',', 'the', 'details', 'for',
'this', 'candidate', 'will', 'be', 'provided', '.', '``', ',', "''",
'References', "''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''",
':', '``', '20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9998', "''", ',', "''", 'Description', "''", ':', '``', '*', '*',
'RESERVED', '*', '*', 'This', 'candidate', 'has', 'been', 'reserved', 'by',
'an', 'organization', 'or', 'individual', 'that', 'will', 'use', 'it',
'when', 'announcing', 'a', 'new', 'security', 'problem', '.', 'When', 'the',
'candidate', 'has', 'been', 'publicized', ',', 'the', 'details', 'for',
'this', 'candidate', 'will', 'be', 'provided', '.', '``', ',', "''",
'References', "''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''",
':', '``', '20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9997', "''", ',', "''", 'Description', "''", ':', '``', '*', '*',
'RESERVED', '*', '*', 'This', 'candidate', 'has', 'been', 'reserved', 'by',
'an', 'organization', 'or', 'individual', 'that', 'will', 'use', 'it',
'when', 'announcing', 'a', 'new', 'security', 'problem', '.', 'When', 'the',
'candidate', 'has', 'been', 'publicized', ',', 'the', 'details', 'for',
'this', 'candidate', 'will', 'be', 'provided', '.', '``', ',', "''",
'References', "''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''",
':', '``', '20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9996', "''", ',', "''", 'Description', "''", ':', '``', '*', '*',
'RESERVED', '*', '*', 'This', 'candidate', 'has', 'been', 'reserved', 'by',
'an', 'organization', 'or', 'individual', 'that', 'will', 'use', 'it',
'when', 'announcing', 'a', 'new', 'security', 'problem', '.', 'When', 'the',
'candidate', 'has', 'been', 'publicized', ',', 'the', 'details', 'for',
'this', 'candidate', 'will', 'be', 'provided', '.', '``', ',', "''",
'References', "''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''",
':', '``', '20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9995', "''", ',', "''", 'Description',
'RESERVED', '*', '*', 'This', 'candidate', 'has',
'an', 'organization', 'or', 'individual', 'that',
'when', 'announcing', 'a', 'new', 'security', 'pr
'candidate', 'has', 'been', 'publicized', ',', 't
```

nltkresult.txt - 메모장

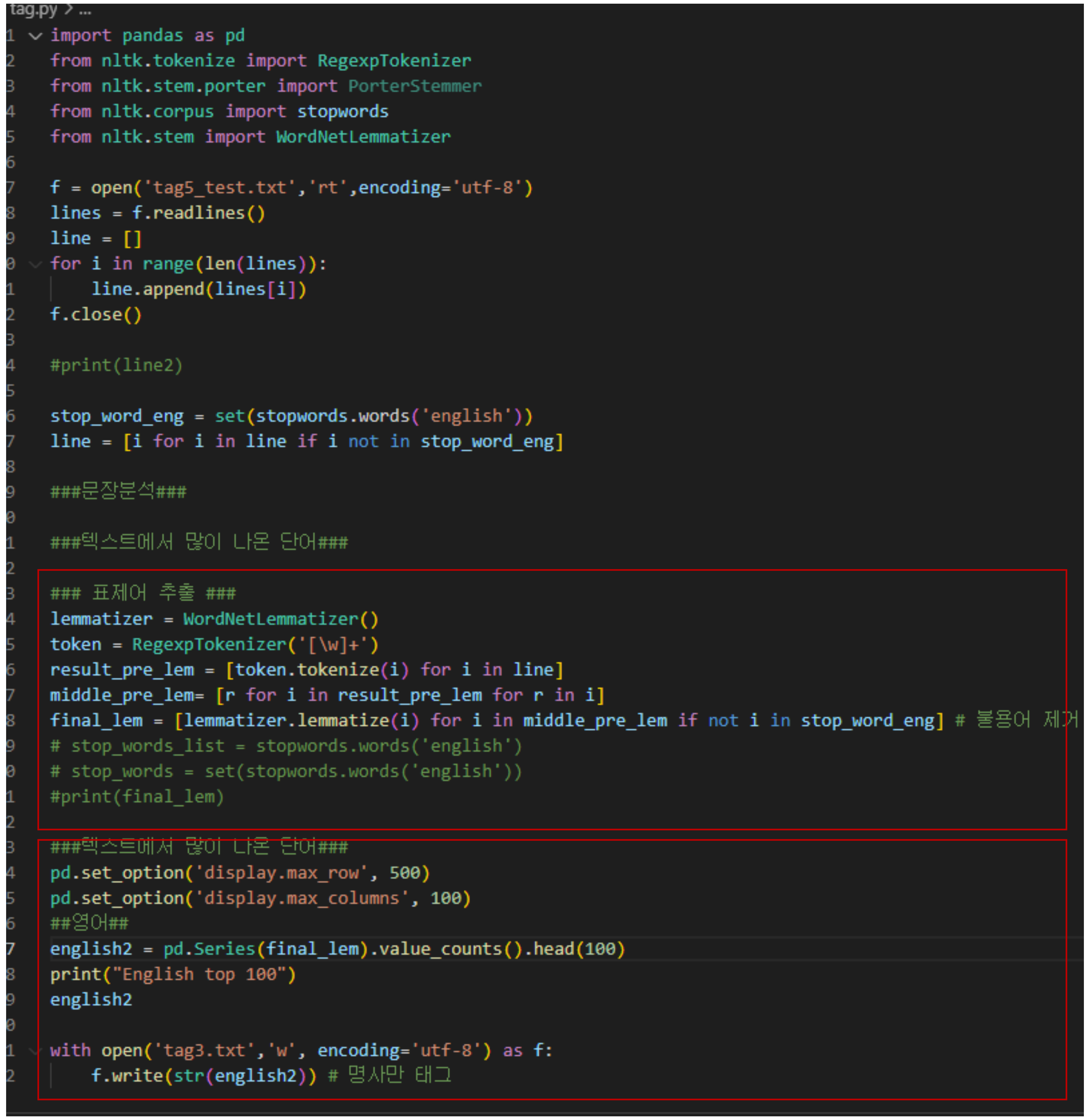
```
['{', "''", 'CVE_2019', "''", ':', '[', '{', "''", 'CVE_ID', "''", ':',
'``', 'CVE-2019-9999', "''", ',', "''", 'Description', "''", ':', '``', '*',
'*', 'RESERVED', '*', '*', 'This', 'candidate', 'reserved', 'organization',
'individual', 'use', 'announcing', 'new', 'security', 'problem', '.',
'When', 'candidate', 'publicized', ',', 'details', 'candidate', 'provided',
'.', '``', ',', "''", 'References', "''", ':', '``', "''", ',', "''",
'Date_Record_Created', "''", ':', '``', '20190324', "''", '}', ',', '{',
"''", 'CVE_ID', "''", ':', '``', 'CVE-2019-9998', "''", ',', "''",
'Description', "''", ':', '``', '*', '*', 'RESERVED', '*', '*', 'This',
'candidate', 'reserved', 'organization', 'individual', 'use', 'announcing',
'new', 'security', 'problem', '.', 'When', 'candidate', 'publicized', ',',
'details', 'candidate', 'provided', '.', '``', ',', "''", 'References',
"''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''", ':', '``',
'20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9997', "''", ',', "''", 'Description', "''", ':', '``', '*', '*',
'RESERVED', '*', '*', 'This', 'candidate', 'reserved', 'organization',
'individual', 'use', 'announcing', 'new', 'security', 'problem', '.',
'When', 'candidate', 'publicized', ',', 'details', 'candidate', 'provided',
'.', '``', ',', "''", 'References', "''", ':', '``', "''", ',', "''",
'Date_Record_Created', "''", ':', '``', '20190324', "''", '}', ',', '{',
"''", 'CVE_ID', "''", ':', '``', 'CVE-2019-9996', "''", ',', "''",
'Description', "''", ':', '``', '*', '*', 'RESERVED', '*', '*', 'This',
'candidate', 'reserved', 'organization', 'individual', 'use', 'announcing',
'new', 'security', 'problem', '.', 'When', 'candidate', 'publicized', ',',
'details', 'candidate', 'provided', '.', '``', ',', "''", 'References',
"''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''", ':', '``',
'20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9995', "''", ',', "''", 'Description', "''", ':', '``', '*', '*',
'RESERVED', '*', '*', 'This', 'candidate', 'reserved', 'organization',
'individual', 'use', 'announcing', 'new', 'security', 'problem', '.',
'When', 'candidate', 'publicized', ',', 'details', 'candidate', 'provided',
'.', '``', ',', "''", 'References', "''", ':', '``', "''", ',', "''",
'Date_Record_Created', "''", ':', '``', '20190324', "''", '}', ',', '{',
"''", 'CVE_ID', "''", ':', '``', 'CVE-2019-9994', "''", ',', "''",
'Description', "''", ':', '``', '*', '*', 'RESERVED', '*', '*', 'This',
'candidate', 'reserved', 'organization', 'individual', 'use', 'announcing',
'new', 'security', 'problem', '.', 'When', 'candidate', 'publicized', ',',
'details', 'candidate', 'provided', '.', '``', ',', "''", 'References',
```

nltkresult.txt - 메모장

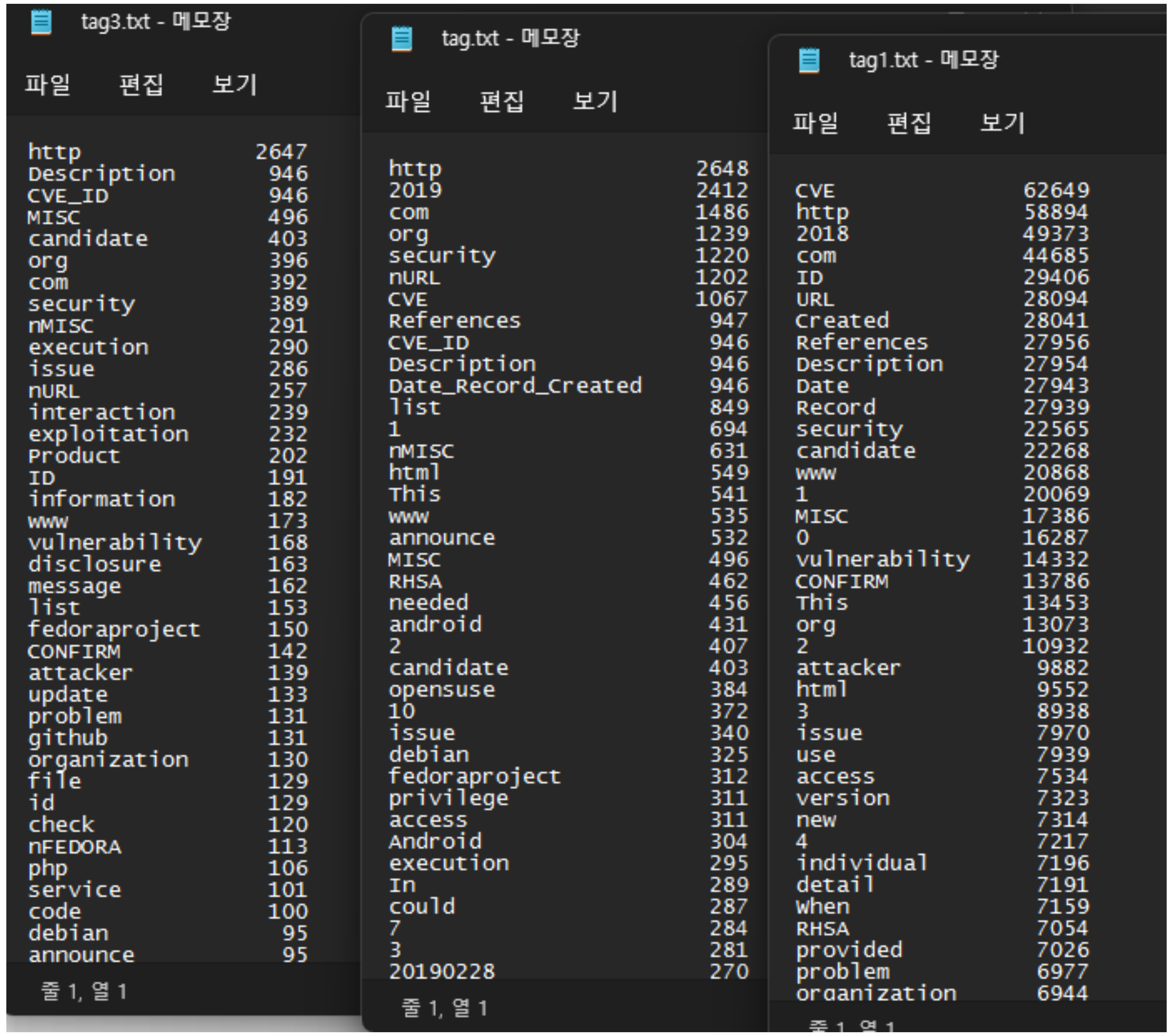
```
['{', "''", 'CVE_2019', "''", ':', '[', '{', "''", 'CVE_ID', "''", ':',
'``', 'CVE-2019-9999', "''", ',', "''", 'Description', "''", ':', '``', '*',
'*', 'RESERVED', '*', '*', 'This', 'candidate', 'reserved', 'organization',
'individual', 'use', 'announcing', 'new', 'security', 'problem', '.',
'When', 'candidate', 'publicized', ',', 'details', 'candidate', 'provided',
'.', '``', ',', "''", 'References', "''", ':', '``', "''", ',', "''",
'Date_Record_Created', "''", ':', '``', '20190324', "''", '}', ',', '{',
"''", 'CVE_ID', "''", ':', '``', 'CVE-2019-9998', "''", ',', "''",
'Description', "''", ':', '``', '*', '*', 'RESERVED', '*', '*', 'This',
'candidate', 'reserved', 'organization', 'individual', 'use', 'announcing',
'new', 'security', 'problem', '.', 'When', 'candidate', 'publicized', ',',
'details', 'candidate', 'provided', '.', '``', ',', "''", 'References',
"''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''", ':', '``',
'20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9997', "''", ',', "''", 'Description', "''", ':', '``', '*', '*',
'RESERVED', '*', '*', 'This', 'candidate', 'reserved', 'organization',
'individual', 'use', 'announcing', 'new', 'security', 'problem', '.',
'When', 'candidate', 'publicized', ',', 'details', 'candidate', 'provided',
'.', '``', ',', "''", 'References', "''", ':', '``', "''", ',', "''",
'Date_Record_Created', "''", ':', '``', '20190324', "''", '}', ',', '{',
"''", 'CVE_ID', "''", ':', '``', 'CVE-2019-9996', "''", ',', "''",
'Description', "''", ':', '``', '*', '*', 'RESERVED', '*', '*', 'This',
'candidate', 'reserved', 'organization', 'individual', 'use', 'announcing',
'new', 'security', 'problem', '.', 'When', 'candidate', 'publicized', ',',
'details', 'candidate', 'provided', '.', '``', ',', "''", 'References',
"''", ':', '``', "''", ',', "''", 'Date_Record_Created', "''", ':', '``',
'20190324', "''", '}', ',', '{', "''", 'CVE_ID', "''", ':', '``',
'CVE-2019-9995', "''", ',', "''", 'Description', "''", ':', '``', '*', '*',
'RESERVED', '*', '*', 'This', 'candidate', 'reserved', 'organization',
'individual', 'use', 'announcing', 'new', 'security', 'problem', '.',
'When', 'candidate', 'publicized', ',', 'details', 'candidate', 'provided',
'.', '``', ',', "''", 'References', "''", ':', '``', "''", ',', "''",
'Date_Record_Created', "''", ':', '``', '20190324', "''", '}', ',', '{',
"''", 'CVE_ID', "''", ':', '``', 'CVE-2019-9994', "''", ',', "''",
'Description', "''", ':', '``', '*', '*', 'RESERVED', '*', '*', 'This',
'candidate', 'reserved', 'organization', 'individual', 'use', 'announcing',
'new', 'security', 'problem', '.', 'When', 'candidate', 'publicized', ',',
'details', 'candidate', 'provided', '.', '``', ',', "''", 'References',
```

NLP

CULTURE CONTENTS &
INFORMATION TECHNOLOGY



```python
import pandas as pd
from nltk.tokenize import RegexpTokenizer
from nltk.stem.porter import PorterStemmer
from nltk.corpus import stopwords
from nltk.stem import WordNetLemmatizer

f = open('tag5_test.txt','rt',encoding='utf-8')
lines = f.readlines()
line = []
for i in range(len(lines)):
    line.append(lines[i])
f.close()

#print(line2)

stop_word_eng = set(stopwords.words('english'))
line = [i for i in line if i not in stop_word_eng]

###문장분석###

###텍스트에서 많이 나온 단어###

### 표제어 추출 ###
lemmatizer = WordNetLemmatizer()
token = RegexpTokenizer('[\w]+')
result_pre_lem = [token.tokenize(i) for i in line]
middle_pre_lem= [r for i in result_pre_lem for r in i]
final_lem = [lemmatizer.lemmatize(i) for i in middle_pre_lem if not i in stop_word_eng] # 불용어 제거
# stop_words_list = stopwords.words('english')
# stop_words = set(stopwords.words('english'))
#print(final_lem)

###텍스트에서 많이 나온 단어###
pd.set_option('display.max_row', 500)
pd.set_option('display.max_columns', 100)
##영어##
english2 = pd.Series(final_lem).value_counts().head(100)
print("English top 100")
english2

with open('tag3.txt','w', encoding='utf-8') as f:
    f.write(str(english2)) # 명사만 태그
```



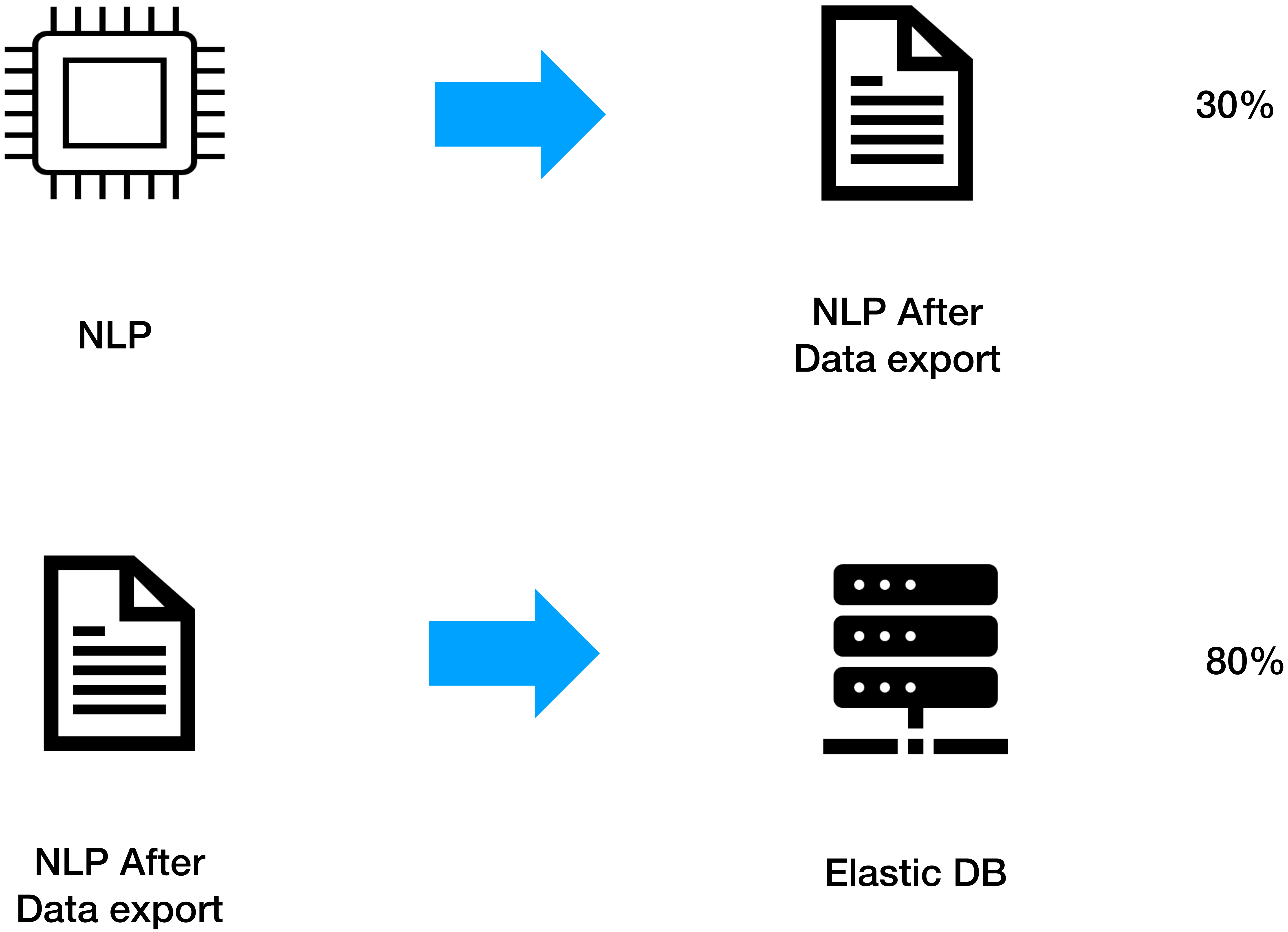
```
http              2647
Description        946
CVE_ID             946
MISC               496
candidate          403
org                396
com                392
security           389
nMISC              291
execution          290
issue              286
nURL               257
interaction        239
exploitation       232
Product            202
ID                 191
information        182
www                173
vulnerability      168
disclosure         163
message            162
list               153
fedoraproject      150
CONFIRM            142
attacker           139
update             133
problem            131
github             131
organization       130
file               129
id                 129
check              120
nFEDORA            113
php                106
service            101
code               100
debian              95
announce            95
```

```
http                     2648
2019                     2412
com                      1486
org                      1239
security                 1220
nURL                     1202
CVE                      1067
References                947
CVE_ID                    946
Description               946
Date_Record_Created       946
list                      849
1                         694
nMISC                     631
html                      549
This                      541
www                       535
announce                  532
MISC                      496
RHSA                      462
needed                    456
android                   431
2                         407
candidate                 403
opensuse                  384
10                        372
issue                     340
debian                    325
fedoraproject             312
privilege                 311
access                    311
Android                   304
execution                 295
In                        289
could                     287
7                         284
3                         281
20190228                  270
```

```
CVE              62649
http             58894
2018             49373
com              44685
ID               29406
URL              28094
Created          28041
References       27956
Description      27954
Date             27943
Record           27939
security         22565
candidate        22268
www              20868
1                20069
MISC             17386
0                16287
vulnerability    14332
CONFIRM          13786
This             13453
org              13073
2                10932
attacker          9882
html              9552
3                 8938
issue             7970
use               7939
access            7534
version           7323
new               7314
4                 7217
individual        7196
detail            7191
When              7159
RHSA              7054
provided          7026
problem           6977
organization      6944
```

NLP

추가 진행 사항



NLP

NLP After
Data export

30%

NLP After
Data export

Elastic DB

80%

Web

개발 환경

VS Code

Node.JS + Express

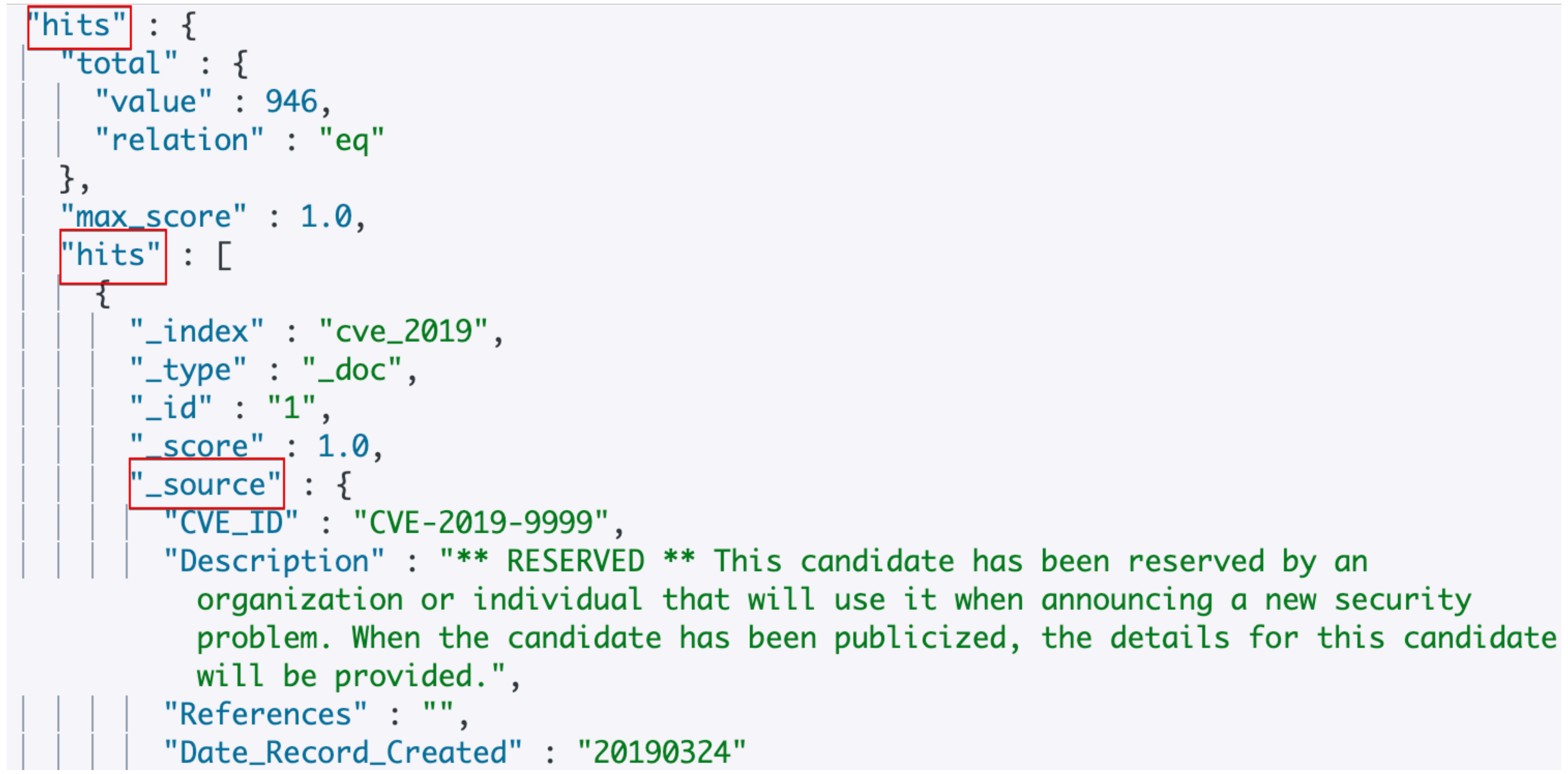
Elasticsearch

Mysql

Source Structure

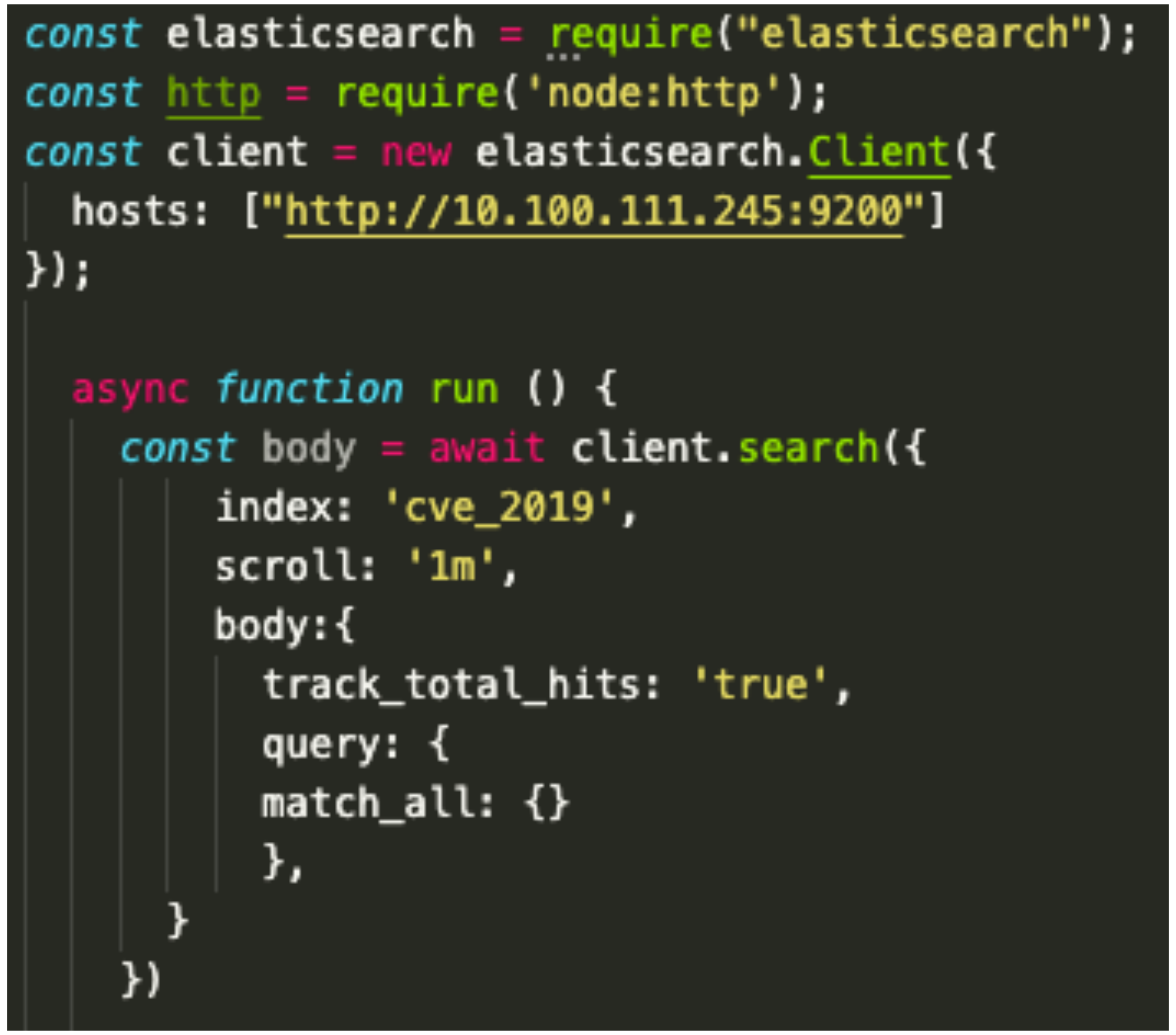
- Asset: css, fonts, image, js, scss
- CVE_Json_open: elastic search에서 client.search/get data 출력
- Login-router: 로그인/ 회원가입
- Views: 웹 페이지(ejs, html)
- app.js

CVE_Json_open



```
"hits" : {
  "total" : {
    "value" : 946,
    "relation" : "eq"
  },
  "max_score" : 1.0,
  "hits" : [
    {
      "_index" : "cve_2019",
      "_type" : "_doc",
      "_id" : "1",
      "_score" : 1.0,
      "_source" : {
        "CVE_ID" : "CVE-2019-9999",
        "Description" : "** RESERVED ** This candidate has been reserved by an
          organization or individual that will use it when announcing a new security
          problem. When the candidate has been publicized, the details for this candidate
          will be provided.",
        "References" : "",
        "Date_Record_Created" : "20190324"
```

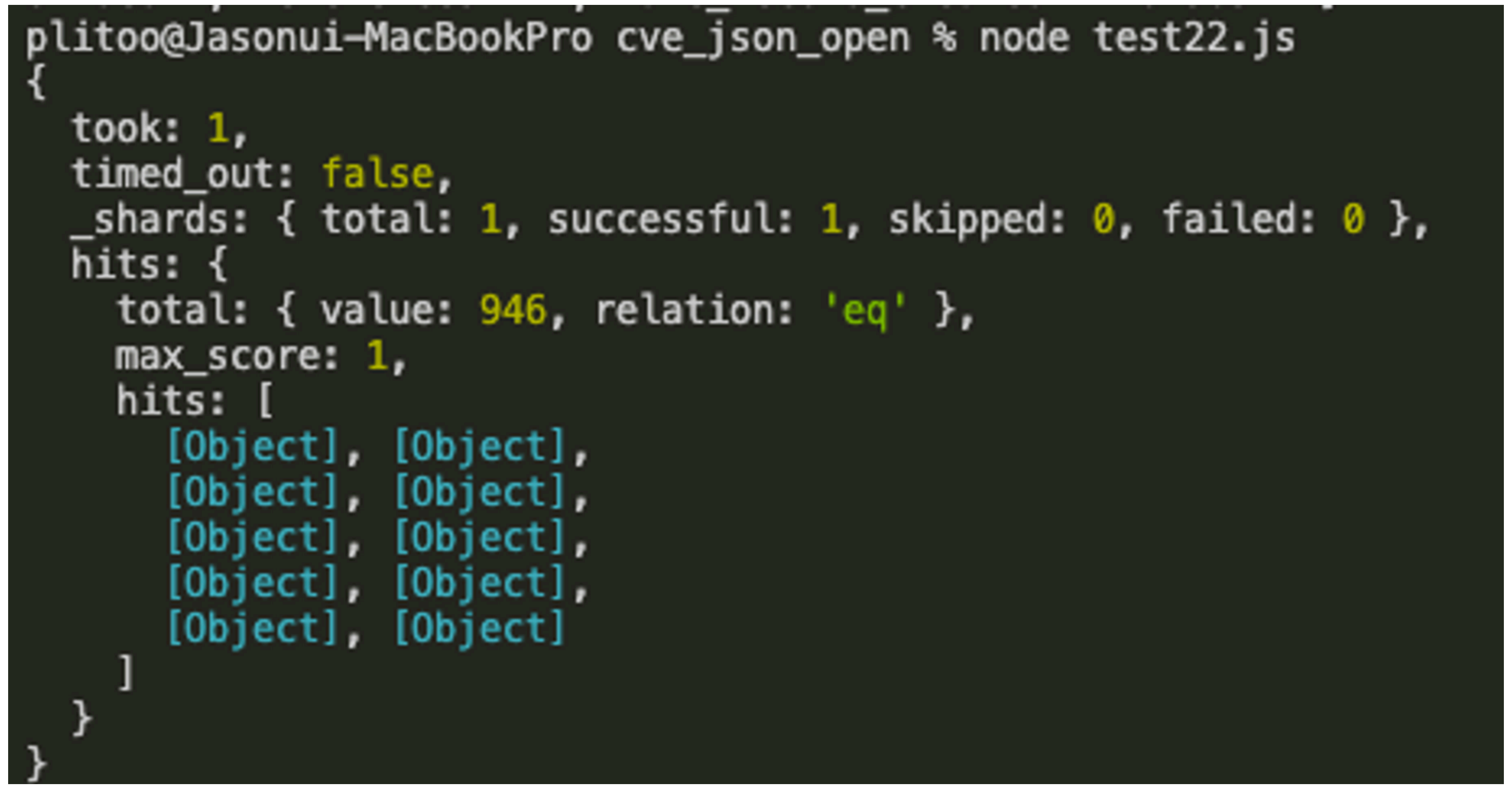
Get cve_2019/_search 구조



```
const elasticsearch = require("elasticsearch");
const http = require('node:http');
const client = new elasticsearch.Client({
  hosts: ["http://10.100.111.245:9200"]
});

  async function run () {
    const body = await client.search({
        index: 'cve_2019',
        scroll: '1m',
        body:{
          track_total_hits: 'true',
          query: {
          match_all: {}
          },
        }
    })
```

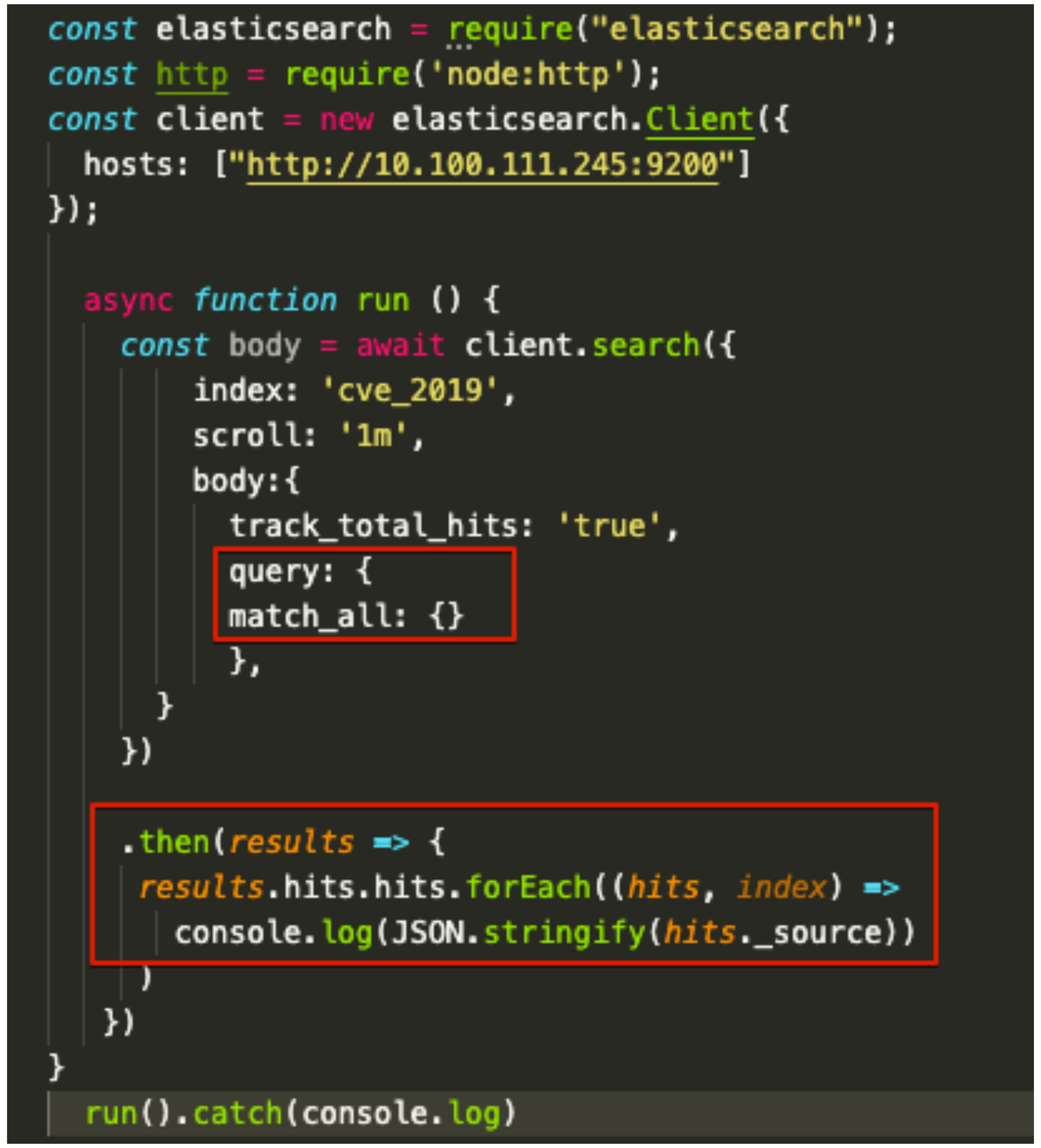
해당 query

CVE_Json_open



```
plitoo@Jasonui-MacBookPro cve_json_open % node test22.js
{
  took: 1,
  timed_out: false,
  _shards: { total: 1, successful: 1, skipped: 0, failed: 0 },
  hits: {
    total: { value: 946, relation: 'eq' },
    max_score: 1,
    hits: [
      [Object], [Object],
      [Object], [Object],
      [Object], [Object],
      [Object], [Object],
      [Object], [Object]
    ]
  }
}
```

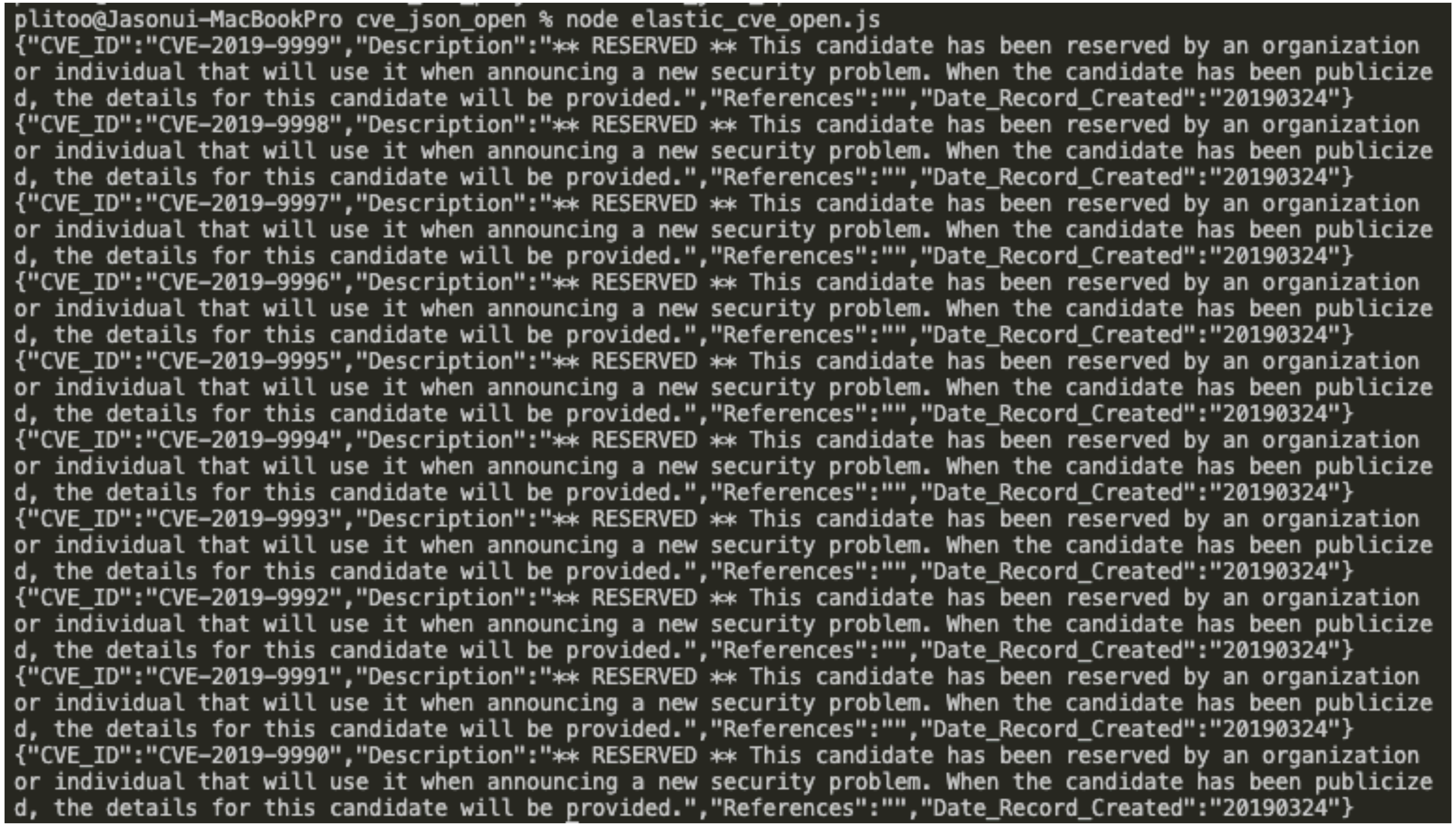
query에 대한 출력 값



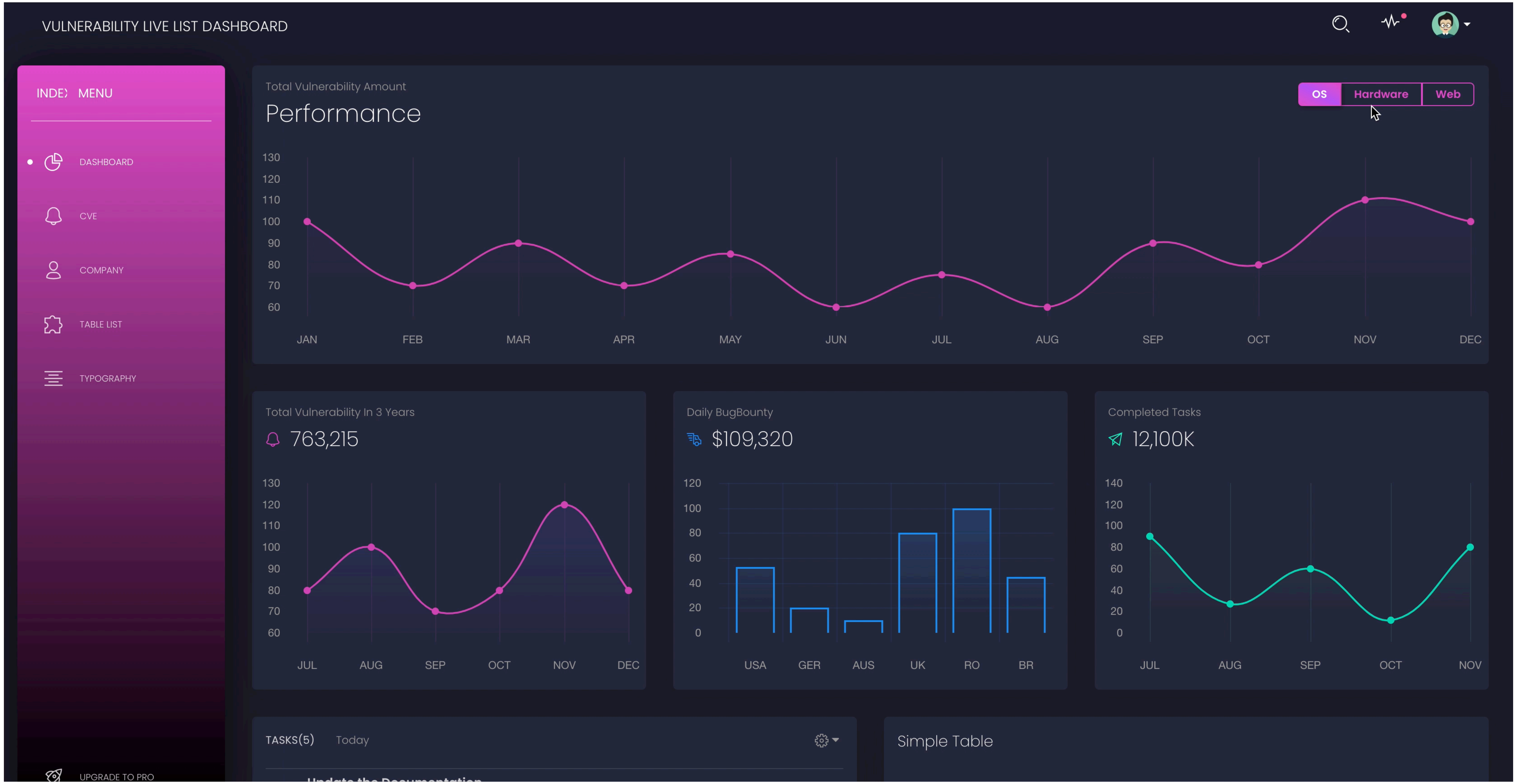
```
const elasticsearch = require("elasticsearch");
const http = require('node:http');
const client = new elasticsearch.Client({
  hosts: ["http://10.100.111.245:9200"]
});

  async function run () {
    const body = await client.search({
        index: 'cve_2019',
        scroll: '1m',
        body:{
          track_total_hits: 'true',
          query: {
          match_all: {}
          },
        }
    })

    .then(results => {
     results.hits.hits.forEach((hits, index) =>
       console.log(JSON.stringify(hits._source))
    )
   })
}
  run().catch(console.log)
```

해당 query

CVE_Json_open



```
plitoo@Jasonui-MacBookPro cve_json_open % node elastic_cve_open.js
{"CVE_ID":"CVE-2019-9999","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9998","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9997","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9996","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9995","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9994","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9993","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9992","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9991","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
{"CVE_ID":"CVE-2019-9990","Description":"** RESERVED ** This candidate has been reserved by an organization
or individual that will use it when announcing a new security problem. When the candidate has been publicize
d, the details for this candidate will be provided.","References":"","Date_Record_Created":"20190324"}
```



VULNERABILITY LIVE LIST DASHBOARD

Total Vulnerability Amount

Performance

Total Vulnerability In 3 Years

763,215

Daily BugBounty

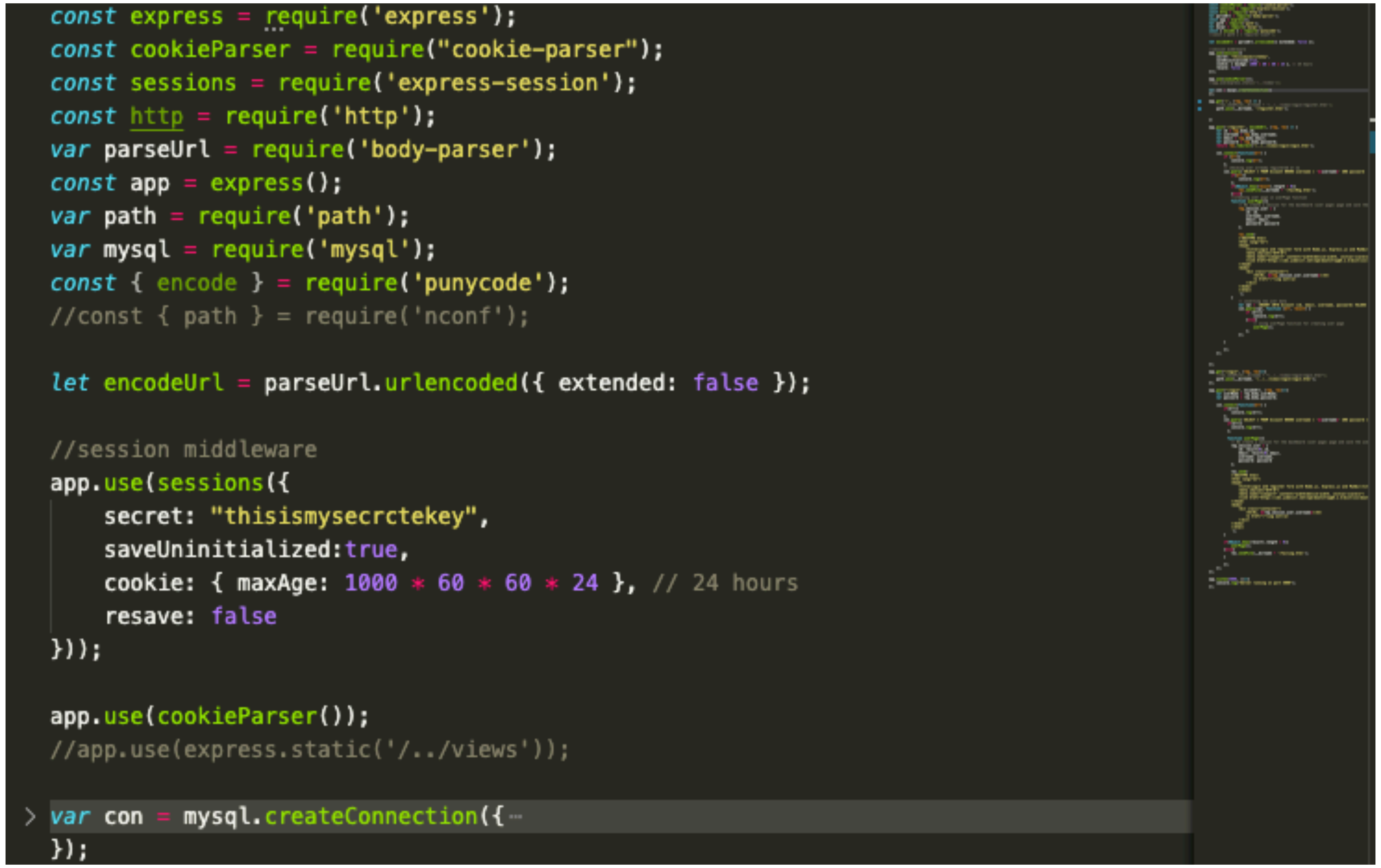
$109,320

Completed Tasks

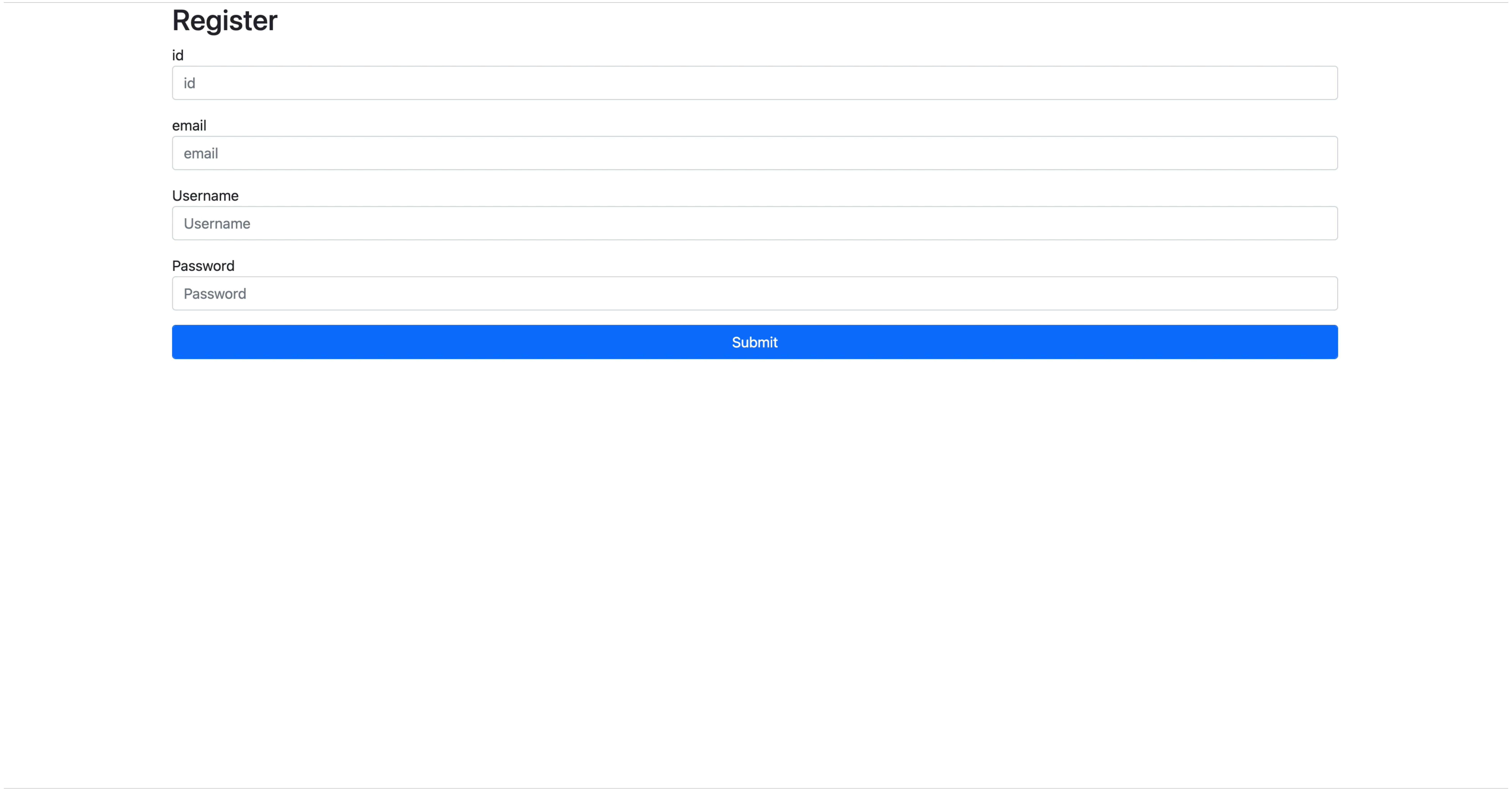
12,100K

Simple Table

Login-router



```
const express = require('express');
const cookieParser = require("cookie-parser");
const sessions = require('express-session');
const http = require('http');
var parseUrl = require('body-parser');
const app = express();
var path = require('path');
var mysql = require('mysql');
const { encode } = require('punycode');
//const { path } = require('nconf');

let encodeUrl = parseUrl.urlencoded({ extended: false });

//session middleware
app.use(sessions({
    secret: "thisismysecrctekey",
    saveUninitialized:true,
    cookie: { maxAge: 1000 * 60 * 60 * 24 }, // 24 hours
    resave: false
}));

app.use(cookieParser());
//app.use(express.static('/../views'));

var con = mysql.createConnection({⋯
});
```



Register

id

id

email

email

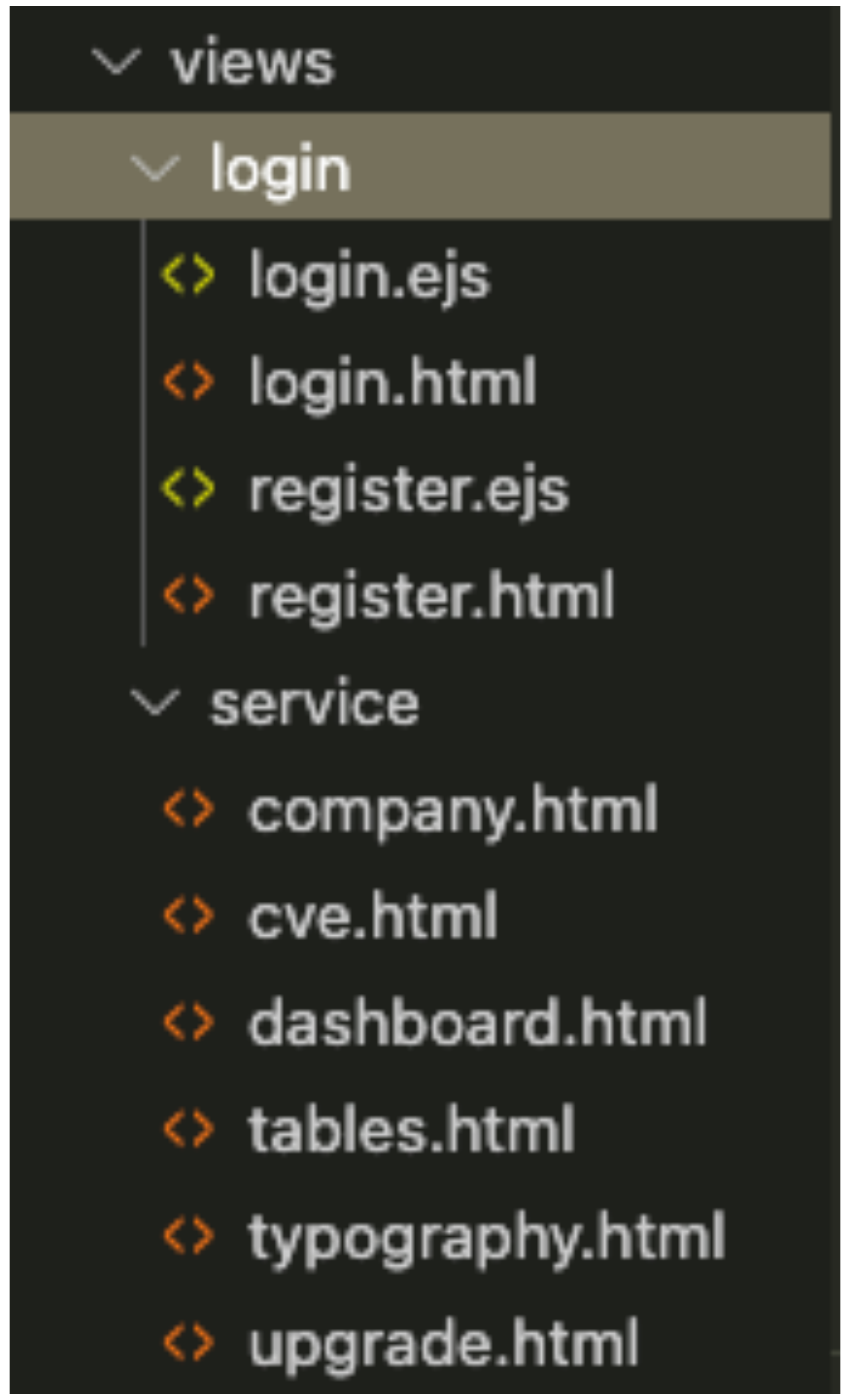
Username

Username

Password

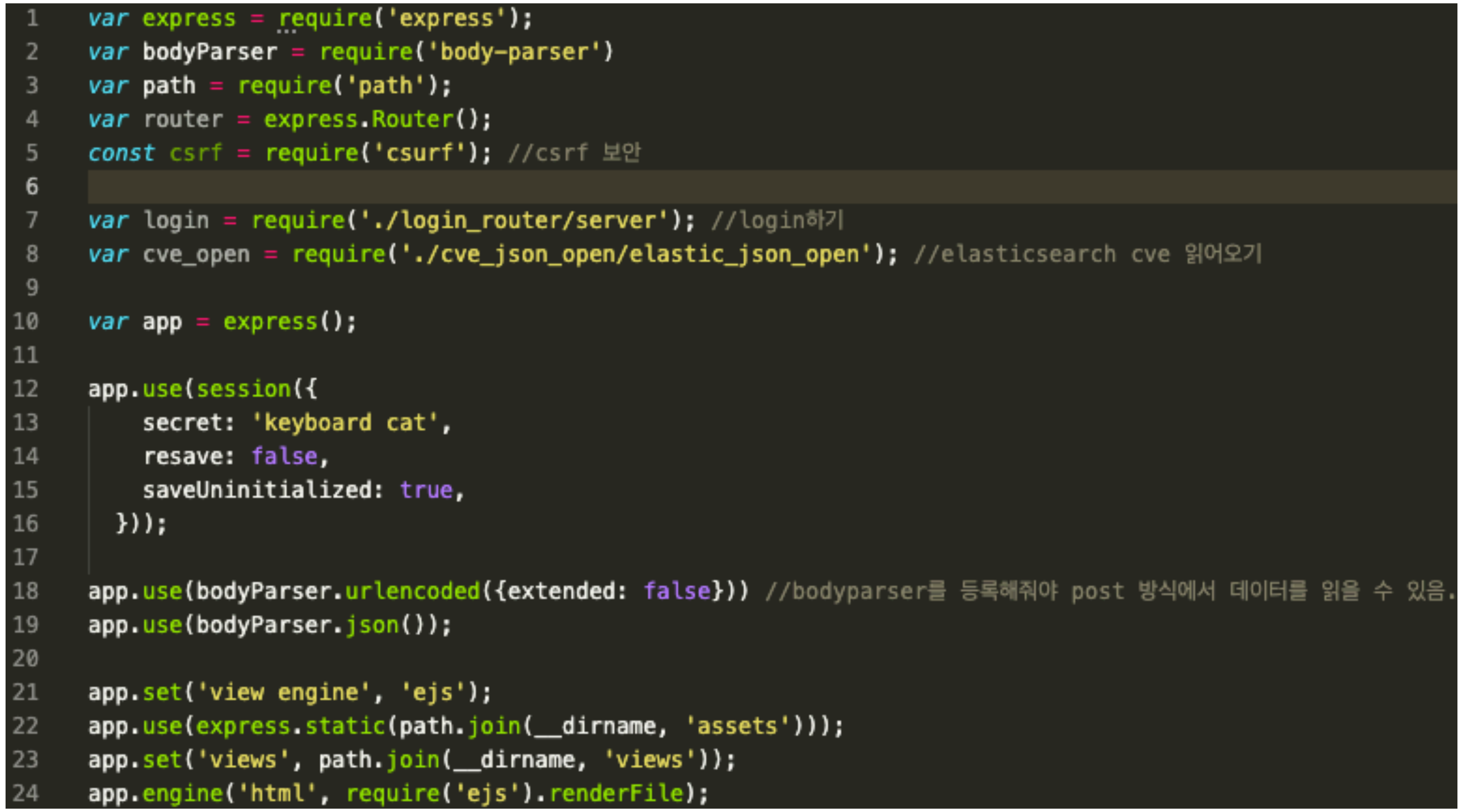
Password

Views & app.js



```
views
  login
    login.ejs
    login.html
    register.ejs
    register.html
  service
    company.html
    cve.html
    dashboard.html
    tables.html
    typography.html
    upgrade.html
```

<% value %>



```
var express = require('express');
var bodyParser = require('body-parser')
var path = require('path');
var router = express.Router();
const csrf = require('csurf'); //csrf 보안

var login = require('./login_router/server'); //login하기
var cve_open = require('./cve_json_open/elastic_json_open'); //elasticsearch cve 읽어오기

var app = express();

app.use(session({
    secret: 'keyboard cat',
    resave: false,
    saveUninitialized: true,
  }));

app.use(bodyParser.urlencoded({extended: false})) //bodyparser를 등록해줘야 post 방식에서 데이터를 읽을 수 있음.
app.use(bodyParser.json());

app.set('view engine', 'ejs');
app.use(express.static(path.join(__dirname, 'assets')));
app.set('views', path.join(__dirname, 'views'));
app.engine('html', require('ejs').renderFile);
```

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

추가 진행

- Pagenation, Tag
- 알림 서비스

“QnA”