Cyber Security Tool
SQL Injection Scan by Python

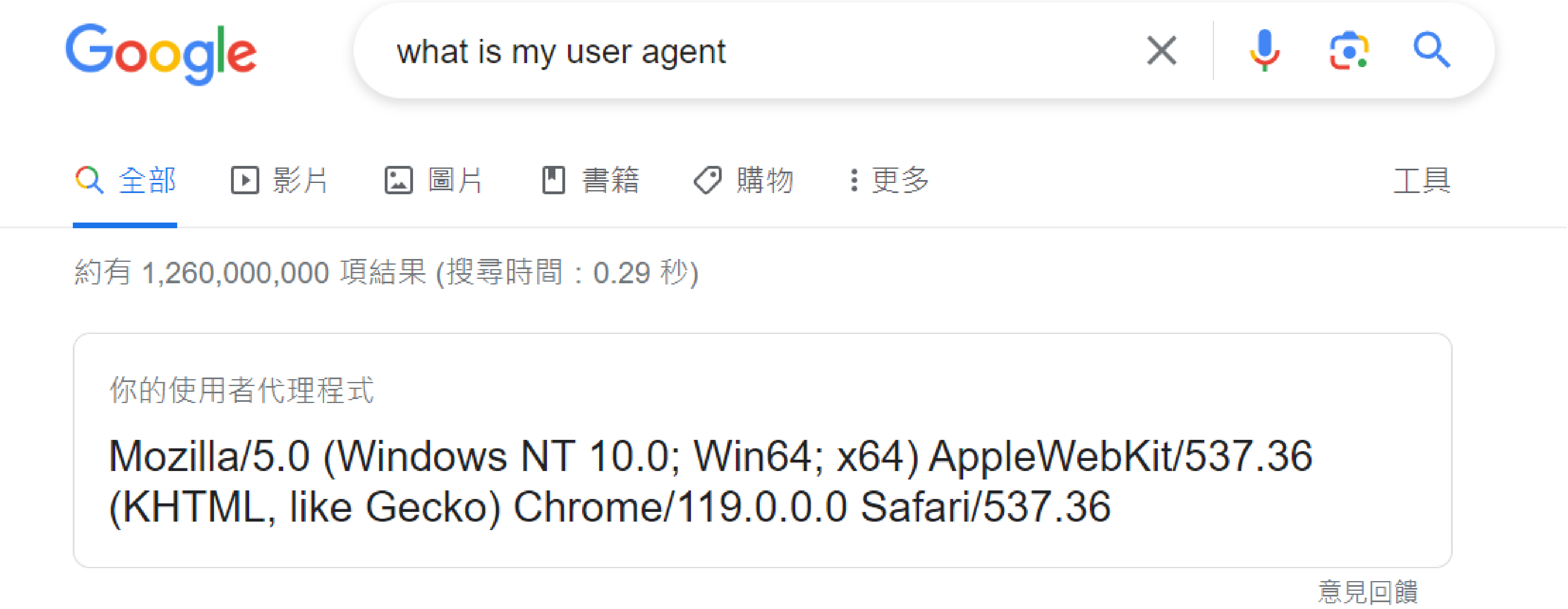
郭益華

GitHub

Flow

1	get_forms()	偵測網站中所有的表單
2	form_details()	獲取表單中的詳細資訊
3	vulnerable()	錯誤回傳
4	sql_injection_scan()	SQL注入偵測

查詢自己的 user agent

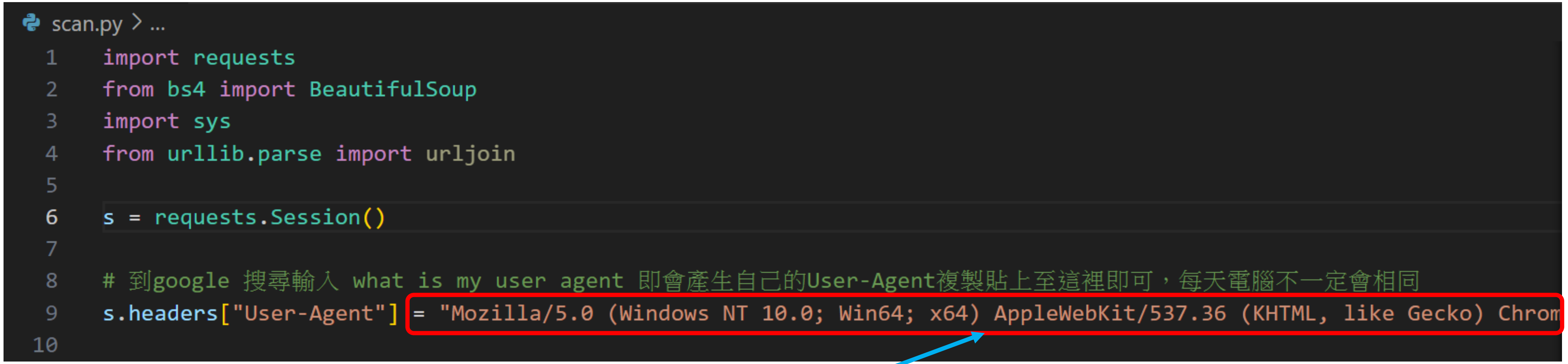


約有 1,260,000,000 項結果 (搜尋時間：0.29 秒)

你的使用者代理程式

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36

設定 user agent



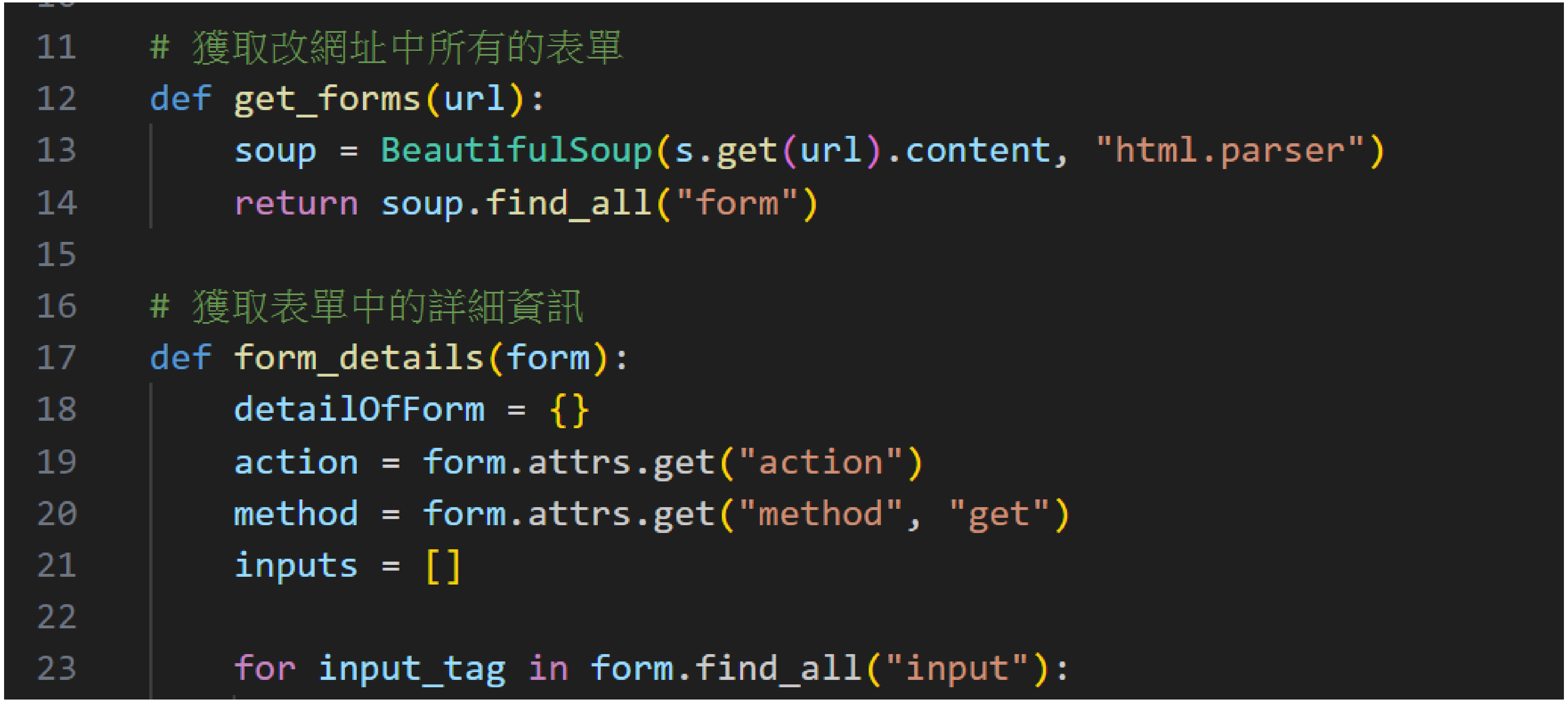
scan.py > ...

```python
import requests
from bs4 import BeautifulSoup
import sys
from urllib.parse import urljoin

s = requests.Session()

# 到google 搜尋輸入 what is my user agent 即會產生自己的User-Agent複製貼上至這裡即可，每天電腦不一定會相同
s.headers["User-Agent"] = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
```

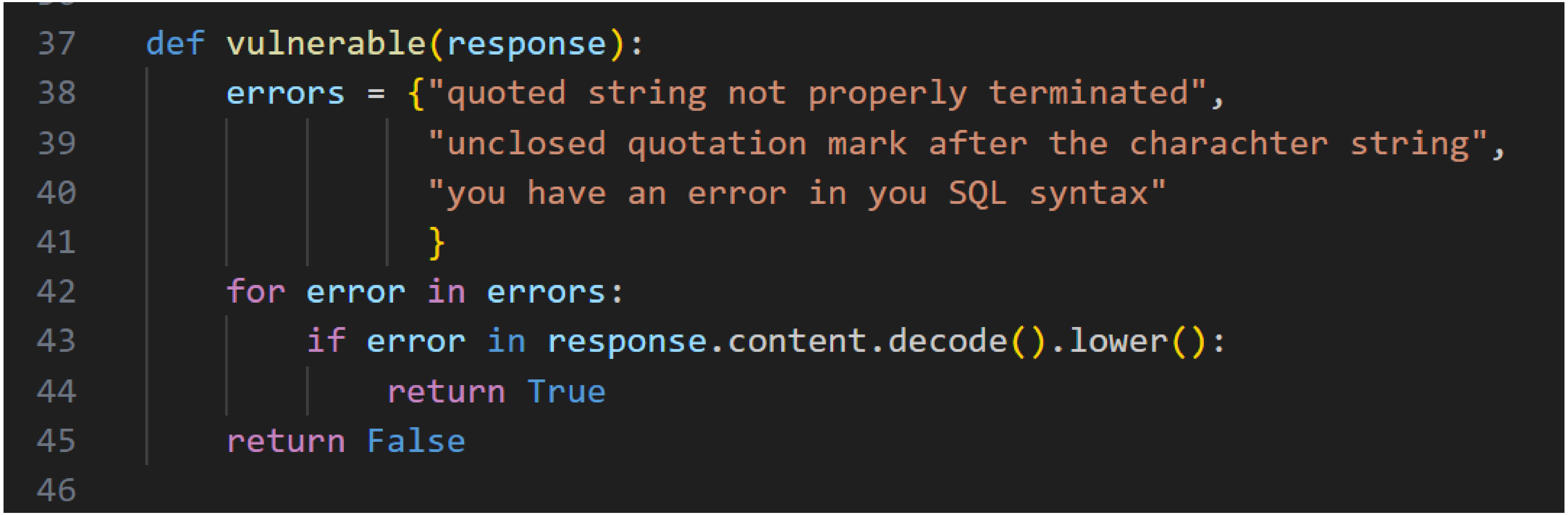
User agent 複製貼上



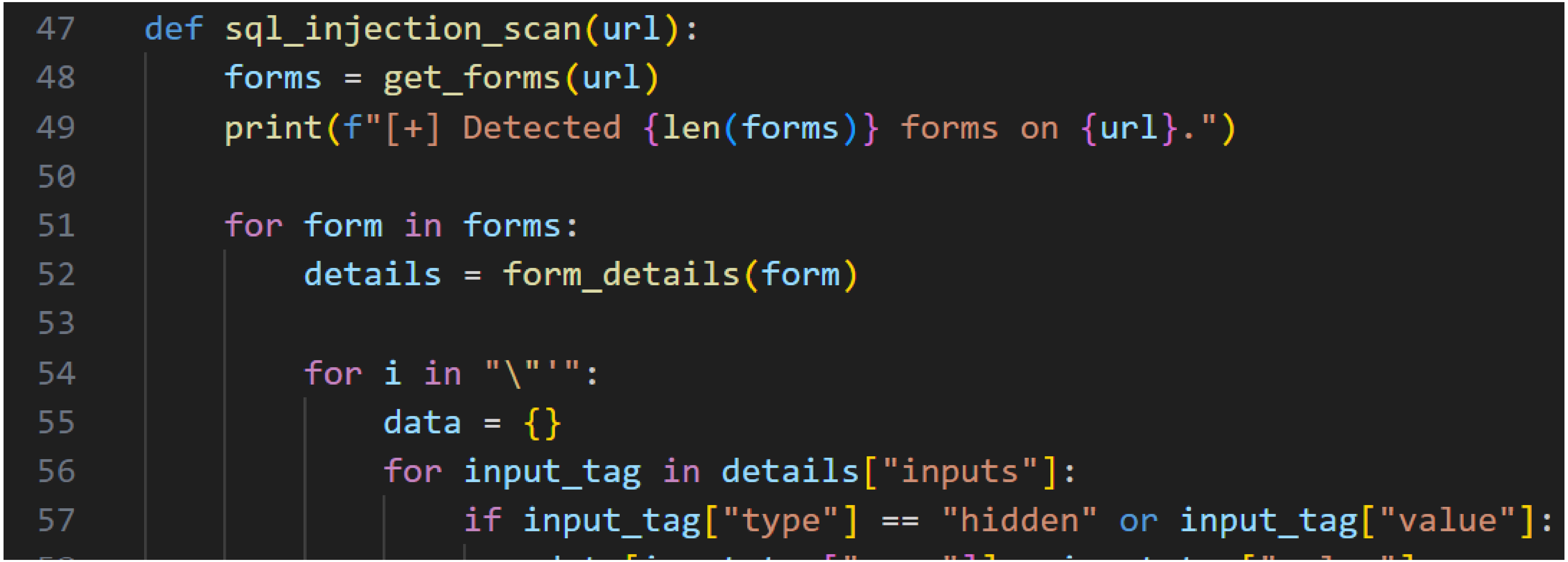
```python
# 獲取改網址中所有的表單
def get_forms(url):
    soup = BeautifulSoup(s.get(url).content, "html.parser")
    return soup.find_all("form")

# 獲取表單中的詳細資訊
def form_details(form):
    detailOfForm = {}
    action = form.attrs.get("action")
    method = form.attrs.get("method", "get")
    inputs = []

    for input_tag in form.find_all("input"):
```



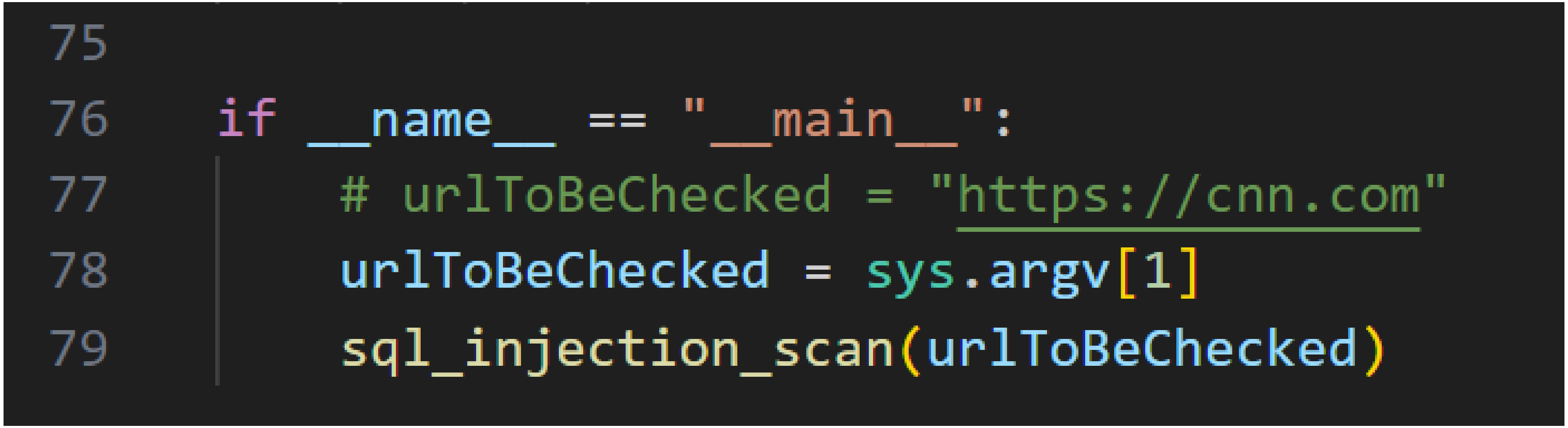
```python
def vulnerable(response):
    errors = {"quoted string not properly terminated",
              "unclosed quotation mark after the charachter string",
              "you have an error in you SQL syntax"
              }
    for error in errors:
        if error in response.content.decode().lower():
            return True
    return False
```



```python
def sql_injection_scan(url):
    forms = get_forms(url)
    print(f"[+] Detected {len(forms)} forms on {url}.")

    for form in forms:
        details = form_details(form)

        for i in "\"'":
            data = {}
            for input_tag in details["inputs"]:
                if input_tag["type"] == "hidden" or input_tag["value"]:
```



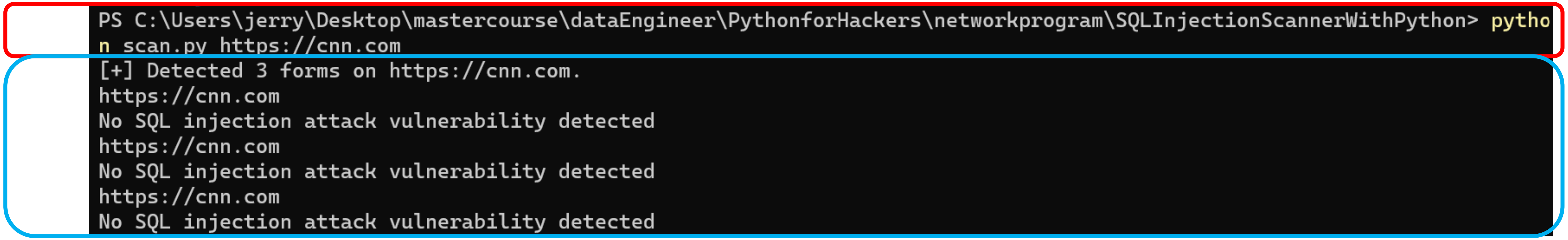
```python

if __name__ == "__main__":
    # urlToBeChecked = "https://cnn.com"
    urlToBeChecked = sys.argv[1]
    sql_injection_scan(urlToBeChecked)
```

Test

以 cnn.com 測試

使用方式:
python scan.py [url]
Ex: python scan.py https://cnn.com



```
PS C:\Users\jerry\Desktop\mastercourse\dataEngineer\PythonforHackers\networkprogram\SQLInjectionScannerWithPython> pytho
n scan.py https://cnn.com
[+] Detected 3 forms on https://cnn.com.
https://cnn.com
No SQL injection attack vulnerability detected
https://cnn.com
No SQL injection attack vulnerability detected
https://cnn.com
No SQL injection attack vulnerability detected
```

偵測到該網站有三個表單，SQL注入掃描後都沒有SQL注入攻擊的弱點

End