Projectเพิ่มความสามารถในการตรวจจับช่องโหว่ของ SQL Injection

1.การใช้ Pattern Matching เพื่อตรวจจับคำสั่ง SQL ที่อาจเป็นอันตราย: คุณสามารถใช้ Regular Expressions (regex) เพื่อตรวจหาคำสั่ง SQL ที่พบได้บ่อย เช่น SELECT, INSERT, UPDATE, DELETE หรือคำสั่ง WHERE ภายในโค้ด โดยตรวจสอบว่ามีการส่งผ่าน input ที่ไม่ได้รับการป้องกันเข้าสู่คำสั่งเหล่านี้หรือไม่ ซึ่งอาจนำไปสู่ SQL Injection

ตัวอย่างโค้ด:

```
sql_patterns = [
    r'\bSELECT\b.*\bFROM\b',
    r'\bINSERT\b.*\bINTO\b',
    r'\bUPDATE\b.*\bSET\b',
    r'\bDELETE\b.*\bFROM\b',
    r'\bWHERE\b.*=.*'
]
def detect_sql_injection(code):
    for pattern in sql_patterns:
        if re.search(pattern, code, re.IGNORECASE):
            print(f"พบความเป็นไปได้ของ SQL Injection: {pattern}")
```

2.ตรวจสอบการใช้ Parameter Binding: แนะนำให้เพิ่มการตรวจสอบการใช้ Parameter Binding ใน SQL Queries ซึ่งเป็นวิธีหนึ่งในการป้องกัน SQL Injection โดยการตรวจหาโค้ดที่ใช้การเชื่อมต่อข้อความด้วยวิธีที่ไม่ปลอดภัย เช่นการใช้ + หรือ .format() เพื่อประกอบคำสั่ง SQL

ตัวอย่างโค้ด:

```
def check_for_unsafe_concatenation(sql_code):
    if "" in sql_code or """ in sql_code:
        print("พบการเชื่อมต่อข้อความที่ไม่ปลอดภัย")
```

3.ปรับปรุงการสแกน JavaScript: ถ้า JavaScript ถูกใช้ในการสร้างคำสั่ง SQL ฝั่งไคลเอนต์ (เช่นผ่าน WebSQL หรือไลบรารี SQL อื่นๆ) เครื่องมือนี้ควรจะสามารถสแกนหาช่องโหว่ในกรณีนี้ได้ โดยการเพิ่มฟังก์ชันที่ตรวจจับการใช้คำสั่ง SQL ใน JavaScript

4.การใช้ OpenAI เพื่อวิเคราะห์คำสั่ง SQL: เนื่องจากโค้ดมีการเชื่อมต่อกับ OpenAI API คุณสามารถใช้ API นี้เพื่อตรวจสอบและวิเคราะห์คำสั่ง SQL และพิจารณาว่าคำสั่งเหล่านั้นมีความเสี่ยงต่อ SQL Injection หรือไม่

ตัวอย่างโค้ด:

```
def use_openai_for_sql_detection(sql_code):
    response = openai.Completion.create(
        engine="text-davinci-003",
        prompt=f"วิเคราะห์คำสั่ง SQL นี้ว่ามีความเสี่ยงต่อการถูกโจมตี SQL Injection หรือไม่: {sql_code}",
        max_tokens=100
    )
    print(response.choices[0].text.strip())
```

สรุป:

คุณสามารถเพิ่มฟังก์ชันในการตรวจจับช่องโหว่ SQL ได้โดยการใช้ Regular Expressions เพื่อค้นหาคำสั่ง SQL ที่น่าสงสัย การตรวจสอบการใช้ Parameter Binding และการวิเคราะห์คำสั่ง SQL โดยใช้ OpenAI API ซึ่งจะช่วยให้เครื่องมือนี้มีความสามารถในการตรวจจับ SQL Injection ที่ดีขึ้น