Code Alpha Project

Task:- 3

Task Assigned :- Secure Coding Review

Name :- Ratnesh Sharma

Email :- ratneshsh0978@gmail.com

I'll use a straightforward web application created with the Flask framework and the Python programming language as an example. We'll check the code for security flaws and offer suggestions for safe coding techniques. I'll assume you know the basics of Python and Flask for the sake of this example.

Web Application Overview:

Let's look at a simple Flask web application that enables comment submission from users. Users can enter their comments into the application's form, and those comments are subsequently shown on a webpage.

```
# app.py

from flask import Flask, render_template, request

app = Flask(__name__)

comments = []

@app.route('/')
def index():
    return render_template('index.html', comments=comments)

@app.route('/submit', methods=['POST'])
def submit():
    comment = request.form.get('comment')
    comments.append(comment)
    return redirect('/')

if __name__ == '__main__':
    app.run(debug=True)
```

Security Review:-

1. **SQL Injection**
   - **SQL injection is not a direct concern because the current code does not communicate with a database. To avoid SQL injection, it's crucial to use parameterized queries or an ORM (Object-Relational Mapping) if the application eventually uses a database.**
2. **Cross-Site Scripting (XSS):-**
   - **User input is rendered directly in the template by the current code, which can result in XSS vulnerabilities. When rendering user input in HTML, always escape it to avoid script injection attacks. The safe filter is provided by Flask, but the Markup class is a better option for escape.**

```
from flask import Markup

# In the template
{{ user_input|safe }}
```

3. **Cross-Site Request Forgery (CSRF):-**
   - **Forms are protected from CSRF by Flask-WTF. Use the Flask-WTF extension for form handling and make sure it is installed.**

```
from flask_wtf import FlaskForm
from wtforms import StringField, SubmitField

class CommentForm(FlaskForm):
    comment = StringField('Comment')
    submit = SubmitField('Submit')
```