**Source code**

import requests

from bs4 import BeautifulSoup

# Function to check for SQL Injection vulnerability

def check\_sql\_injection(url):

sql\_payloads = ["'", '"', "' OR '1'='1", '" OR "1"="1']

vulnerable = False

for payload in sql\_payloads:

full\_url = f"{url}{payload}"

response = requests.get(full\_url)

if "error" in response.text.lower() or "sql" in response.text.lower():

vulnerable = True

print(f"Possible SQL Injection vulnerability detected with payload: {payload}")

return vulnerable

# Function to check for XSS vulnerability

def check\_xss(url):

xss\_payloads = ["<script>alert('XSS')</script>", '"><script>alert(1)</script>']

vulnerable = False

for payload in xss\_payloads:

full\_url = f"{url}{payload}"

response = requests.get(full\_url)

if payload in response.text:

vulnerable = True

print(f"Possible XSS vulnerability detected with payload: {payload}")

return vulnerable

# Function to parse forms and check for vulnerabilities

def scan\_forms(url):

response = requests.get(url)

soup = BeautifulSoup(response.text, 'html.parser')

forms = soup.find\_all('form')

for form in forms:

action = form.get('action')

method = form.get('method', 'get').lower()

inputs = form.find\_all('input')

form\_data = {}

for input in inputs:

input\_name = input.get('name')

input\_value = input.get('value', 'test')

form\_data[input\_name] = input\_value

if method == 'post':

response = requests.post(url + action, data=form\_data)

else:

response = requests.get(url + action, params=form\_data)

# Check for vulnerabilities in the form response

if "error" in response.text.lower() or "sql" in response.text.lower():

print(f"Possible SQL Injection vulnerability detected in form action: {action}")

if "<script>alert('XSS')</script>" in response.text:

print(f"Possible XSS vulnerability detected in form action: {action}")

# Main function to start the scan

def start\_scan(url):

print(f"Scanning URL: {url}")

if check\_sql\_injection(url):

print("SQL Injection vulnerability detected!")

else:

print("No SQL Injection vulnerability detected.")

if check\_xss(url):

print("XSS vulnerability detected!")

else:

print("No XSS vulnerability detected.")

scan\_forms(url)

print("Scan completed.")

# Example usage

if \_name\_ == "\_main\_":

target\_url = "http://example.com"

start\_scan(target\_url)

import requests

def check\_sql\_injection(url):

sql\_payload = "' OR '1'='1"

target\_url = f"{url}{sql\_payload}"

try:

response = requests.get(target\_url)

if "syntax error" in response.text or "mysql" in response.text:

return True

return False

except requests.exceptions.RequestException:

return False

def check\_xss(url):

xss\_payload = "<script>alert('XSS')</script>"

target\_url = f"{url}{xss\_payload}"

try:

response = requests.get(target\_url)

if xss\_payload in response.text:

return True

return False

except requests.exceptions.RequestException:

return False

from flask import Flask, render\_template, request

from scanner import check\_sql\_injection, check\_xss

app = Flask(\_name\_)

@app.route('/')

def index():

return render\_template('index.html')

@app.route('/scan', methods=['POST'])

def scan():

url = request.form['url']

results = {

'sql\_injection': check\_sql\_injection(url),

'xss': check\_xss(url),

}

return render\_template('results.html', url=url, results=results)

if \_name\_ == '\_main\_':

app.run(debug=True)

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Scan Results</title>

</head>

<body>

<h1>Scan Results for {{ url }}</h1>

<ul>

<li>SQL Injection: {{ 'Vulnerable' if results['sql\_injection'] else 'Not Vulnerable' }}</li>

<li>XSS: {{ 'Vulnerable' if results['xss'] else 'Not Vulnerable' }}</li>

</ul>

<a href="/">Scan another URL</a>

</body>

</html>

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Vulnerability Scanner</title>

</head>

<body>

<h1>Lightweight Vulnerability Scanner</h1>

<form action="/scan" method="POST">

<label for="url">Enter URL:</label>

<input type="text" id="url" name="url" required>

<button type="submit">Scan</button>

</form>

</body>

</html>