CodTech Internship - Task 2 Report

Intern Name: Prajin S

College: Adithya Institute of Technology

Program: B.Tech IT - 3rd Year

Internship Organization: CodTech

Task Number: Task 2

Task Title: Web Application Vulnerability Scanner using Python

Objective:

To develop a Python-based tool that scans web applications and identifies common vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS).

Technologies Used:

- Python 3.x
- requests
- BeautifulSoup
- HTML parsing
- Command Line Interface (CLI)

Task Description:

The tool accepts a target URL, extracts all forms using BeautifulSoup, and tests each with predefined payloads for SQLi and XSS. It analyzes responses to detect if the application reflects the payloads, which may indicate a vulnerability.

Scanner Features:

- Detects and tests all forms on a given webpage
- Sends both GET and POST requests
- Tests with known SQLi and XSS payloads

- Provides simple CLI output with vulnerability status

Sample Output:

[+] Detected 2 forms on http://testphp.vulnweb.com

[*] Testing form #1 at /search.php

[!] Potential SQL Injection vulnerability detected

[-] No XSS vulnerability detected

Outcome:

The tool successfully demonstrated basic scanning functionality and detected potentially vulnerable forms using simple payloads.

Conclusion:

This task enhanced my understanding of web security, form parsing, and Python-based automation. It provided practical insights into identifying input-based vulnerabilities in web applications.

Submitted By: Prajin S, CodTech Intern - Task 2