SHADOWFORM : Vulnerable Forms & Input Attack Tester

Developer: D Shaun Angel

For: OffSecDiary Red Team Internship

Problem Statement: Web applications commonly fail due to insecure input handling. Attackers exploit form fields to inject SQL queries, execute scripts (XSS), or bypass authentication. ShadowForm automates this process by scanning forms and testing them with pre-defined payloads.

1. Objective

ShadowForm is an automated web form vulnerability scanner designed to detect insecure input fields on websites. It acts like a mini version of Burp Suite Intruder by:

- Crawling webpages
- Detecting all forms + inputs
- Injecting payloads
- Checking for:
    - SQL Injection
    - XSS (Reflected)
    - Authentication bypass
    - Basic IDOR behaviour

This tool performs **non-destructive testing** only.

2. Architecture

Modules

1. **Web Crawler**

- Recursively visits internal links
- Avoids duplicates
- Collects pages containing forms

2. **Form Extractor**
   - Detects `<form>`, `<input>`, `<textarea>`, `<select>`
   - Captures method + action + field names
3. **Payload Engine**
   - SQL injection payload list
   - XSS payload list
   - Authentication bypass payloads
4. **Request Maker**
   - Submits payloads via GET or POST
   - Captures HTML response & status codes
5. **Vulnerability Detector**
   - Identifies SQL error messages
   - Detects reflected XSS (payload returned in response)
6. **Report Generator**
   - Lists vulnerable pages
   - Shows exact payload
   - Severity classification

3. How to Run

pip install requests beautifulsoup4

python shadowform.py

(enter the target url when prompted in this demo - http://testphp.vulnweb.com)

4. Output Format

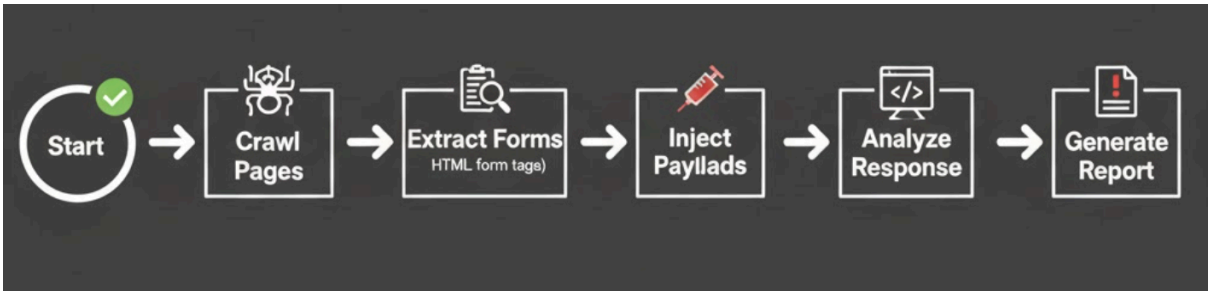
The tool generates a console report showing:

- Page URL
- Form action
- Vulnerability name
- Working payload

5. Working Principle

ShadowForm follows five stages:

1. Crawling
2. Form Discovery
3. Payload Injection
4. Response Analysis
5. Vulnerability Reporting



Each form is fuzzed with multiple payloads that mimic real-world attacks.

6. Features

- SQL Injection detection
- XSS reflection detection
- Authentication bypass attempts

- Basic IDOR pattern probing
- Recursive crawling
- Full form parameter fuzzing

7. Tools & Libraries

- Python 3
- Requests
- BeautifulSoup
- urllib

8. Results

ShadowForm produces a structured vulnerability report listing:

- Affected pages
- Form action method
- Payload that succeeded
- Type of vulnerability detected

This makes the tool practical for preliminary recon during Red Team engagements.

9. Conclusion

ShadowForm proves that lightweight scanners can rapidly identify unsafe inputs and assist security analysts. With further enhancements such as multi-threading, CSRF token handling, and headless browser support, the project can evolve into a full-fledged vulnerability auditing framework.

10.Demo

Screen Recording 2025-12-01 at 4.54.47 PM.mov