DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNIVERSITY COLLEGE OF ENGINEERING

BHARATHIDASAN INSTITUTE OF TECHNOLOGY CAMPUS

ANNA UNIVERSITY

TIRUCHIRAPPALLI – 620 024

CCS374 - WEB APPLICATION SECURUTY LABORATORY

NAME :

REGISTER NUMBER :

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNIVERSITY COLLEGE OF ENGINEERING

BHARATHIDASAN INSTITUTE OF TECHNOLOGY CAMPUS

ANNA UNIVERSITY

TIRUCHIRAPPALLI – 620 024

Bonafide Certificate

This is to certify that Mr. /Ms. _____ bearing the Register No: _____ have satisfactorily completed the course of practical examination of **CCS374 - WEB APPLICATION SECURUTY LABORATORY** for **SIXTH** semester, **B.E COMPUTER SCIENCE AND ENGINEERING** during the academic year 2023-2024

Faculty in Charge **Head of the Department**

Submitted for the practical examination held on _____.

Internal Examiner **External Examiner**

INDEX

S.NO	DATE	DESCRIPTION	PAGE NO	SIGNATURE
1		Install wireshark and explore the various protocols a) Analyze the difference between HTTP vs HTTPS.		
		b) Analyze the various security mechanisms embedded with different protocols.		
2		Identification of the vulnerabilities using OWASP ZAP tool		
3		Create simple REST API using Python & Perform HTTP Requests		
4		Installation of Burp Suite to Perform Vulnerabilities Testing		
5		Attacking a Website Using Social Engineering Method		

Exp no : 1A	Analyze the difference between HTTP vs HTTPS
Date :	

Aim :

To Analyze the difference between HTTP vs HTTPS.

Algorithm:

Step 1: Start
Step 2: Install wireshark.
Step 3: Start wireshark
Step 4: Analyze the difference between HTTP vs HTTPS
Step 5: View Server Output
Step 6: Stop

Procedure:

To install Wireshark on Windows, follow these steps:

1. Download Wireshark:

- Go to the Wireshark download page: https://www.wireshark.org/download.html

- Select the appropriate installer for your Windows version (32-bit or 64-bit).

2. Run the Installer:

- Once the download is complete, run the installer (e.g., `Wireshark-win64-x.y.z.exe` for 64-bit).

- If prompted by User Account Control (UAC), click "Yes" to allow the installer to make changes to your device.

3. Select Components:

- In the Wireshark Setup wizard, select the components you want to install. The default selection is usually sufficient for most users.

- Click "Next" to proceed.

4. Choose Install Location:

- Choose the destination folder where Wireshark will be installed or use the default location.

- Click "Next" to continue.

5. Install WinPcap/Npcap:

- During the installation, you may be prompted to install WinPcap (legacy) or Npcap (newer version). These are required for capturing live network traffic.

- Choose whether to install WinPcap or Npcap (Npcap is recommended for Windows 7 and later).

- Click "Next" to proceed with the installation of the selected driver.

6. Select Additional Tasks:

- Choose whether to create desktop icons and add Wireshark shortcuts to the start menu.

- Click "Install" to begin the installation process.

7. Complete Installation:

- Wait for the installation to complete. Once finished, click "Next" and then "Finish" to exit the setup wizard.

8. Run Wireshark:

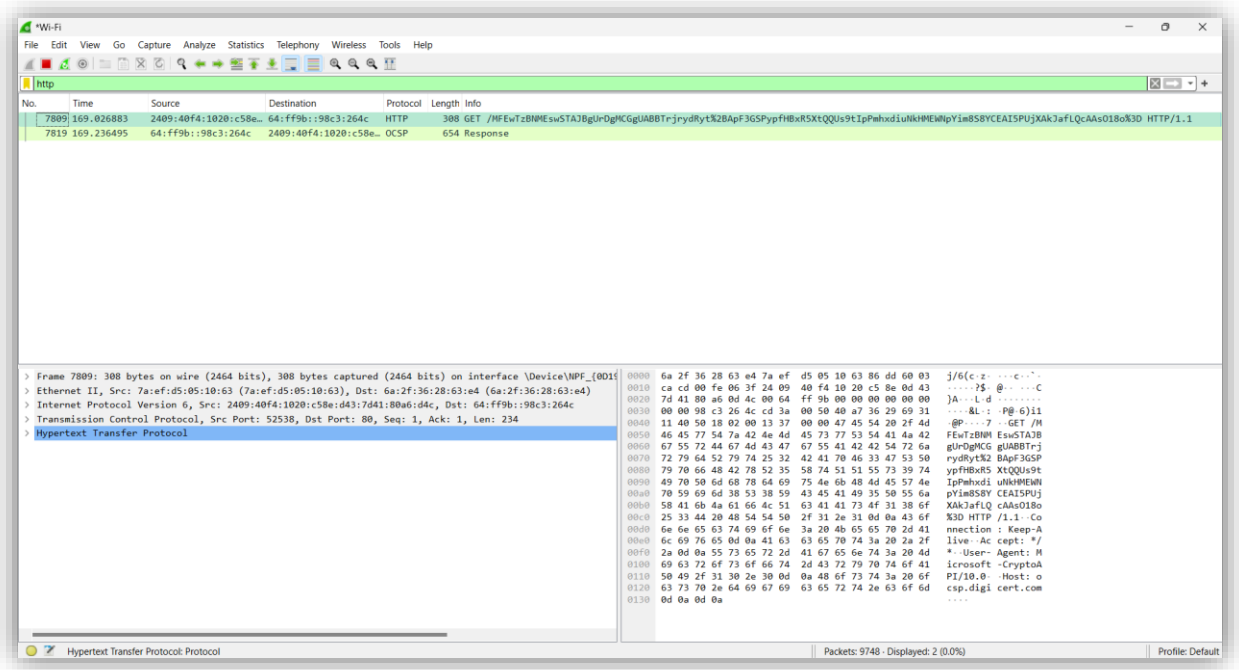
- Wireshark should now be installed on your system. You can launch it from the desktop shortcut or the start menu.

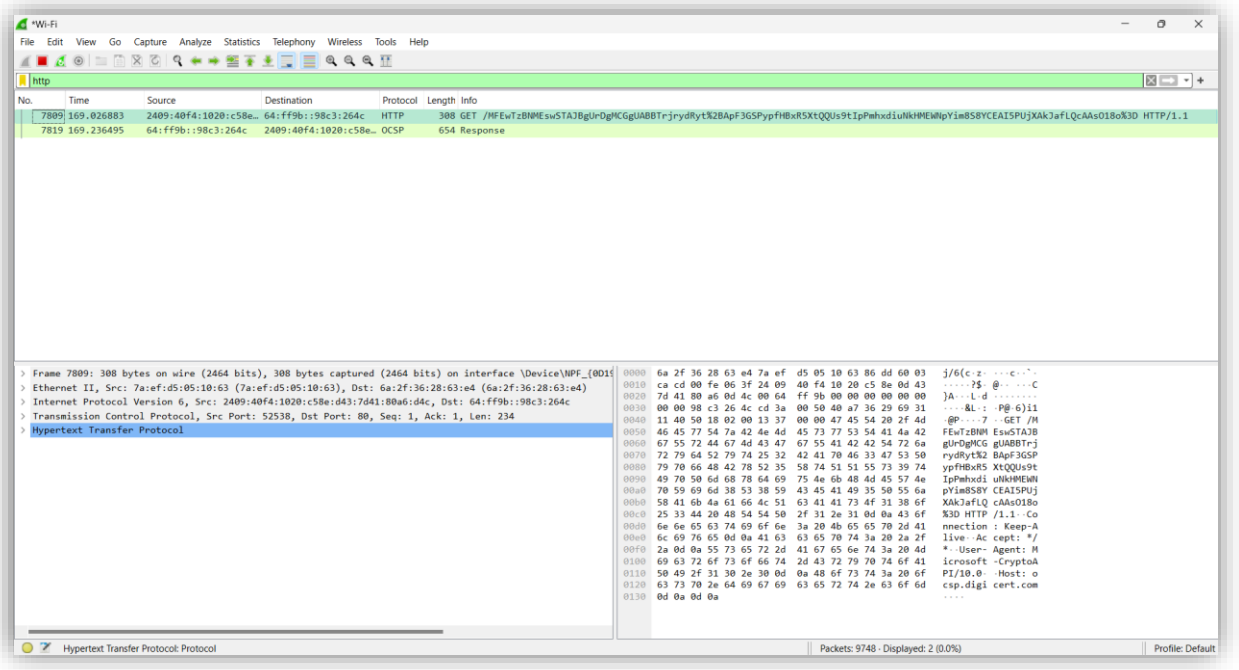
- When you run Wireshark for the first time, you may be prompted to install the WinPcap/Npcap driver if it was not installed earlier. Follow the prompts to complete the driver installation.

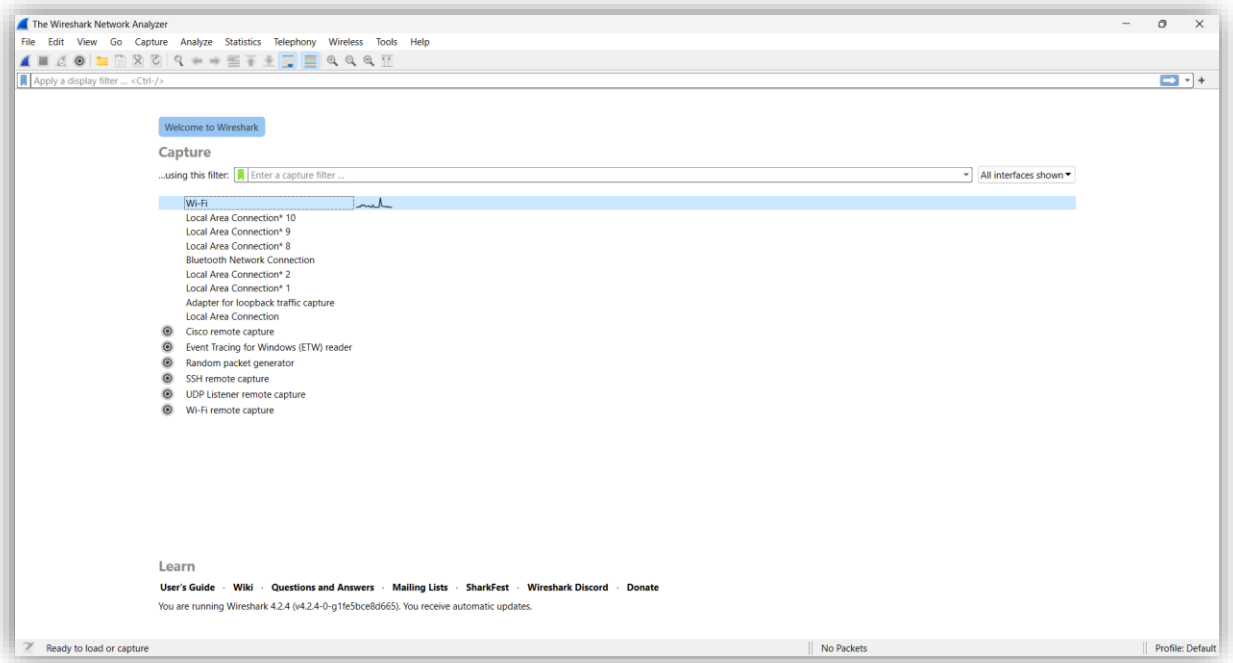
9. Capture Network Traffic:

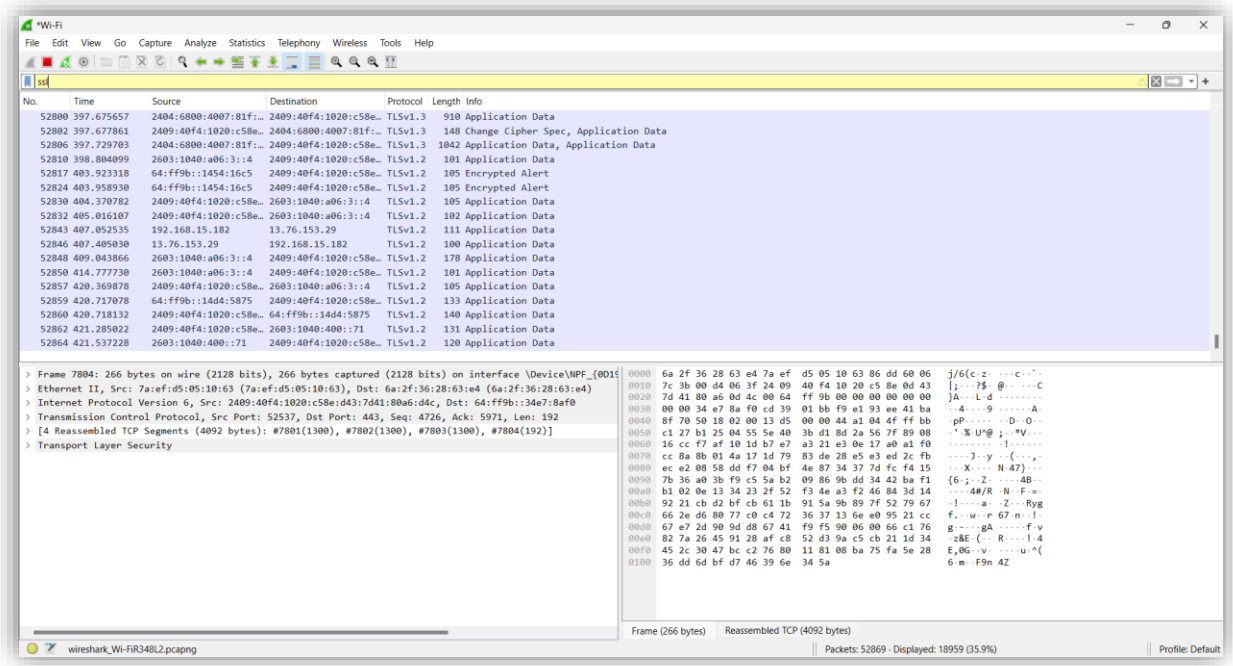
- After installation, you can start capturing network traffic by selecting a network interface and clicking the "Start" button in Wireshark.

Output:









Result:

Thus, the experiment to analyse the difference between HTTP vs HTTPS is executed and verified successfully.

Exp no : 1B	Analyze the Various Security Mechanisms Embedded With Different Protocols
Date :	

Aim :

To Analyze the various security mechanism embedded with different protocols.

Algorithm:

Step 1: Start
Step 2: Start wireshark
Step 3: Analyze the various security mechanism embedded with different protocols
Step 4: View Server Output
Step 5: Stop

Procedure:

To analyze the various security mechanisms embedded in different protocols using Wireshark, follow these steps:

1. Capture Network Traffic:
- Start Wireshark and begin capturing network traffic on the interface of interest.

2. Filter Captured Traffic:
- Use Wireshark's display filters to focus on the protocols and traffic you are interested in analyzing.
- For example, to filter for HTTP traffic, use the filter `http`.

3. Analyze Security Mechanisms:
- Look for packets related to the protocols you are interested in, such as HTTPS (secure HTTP), SSH (Secure Shell), TLS (Transport Layer Security), etc.
- For example, to analyze HTTPS traffic, look for packets with the `TLS` protocol and examine the handshake process and encryption parameters.

4. Examine Packet Details:
- Select a packet of interest and examine its details in the packet view pane.
- Look for security-related information, such as cryptographic algorithms, key exchange methods, certificate details, etc.

5. Follow the Protocol Flow:

- Follow the flow of the protocol to understand how security mechanisms are implemented.
- For example, in HTTPS, follow the handshake process to see how the client and server establish a secure connection.

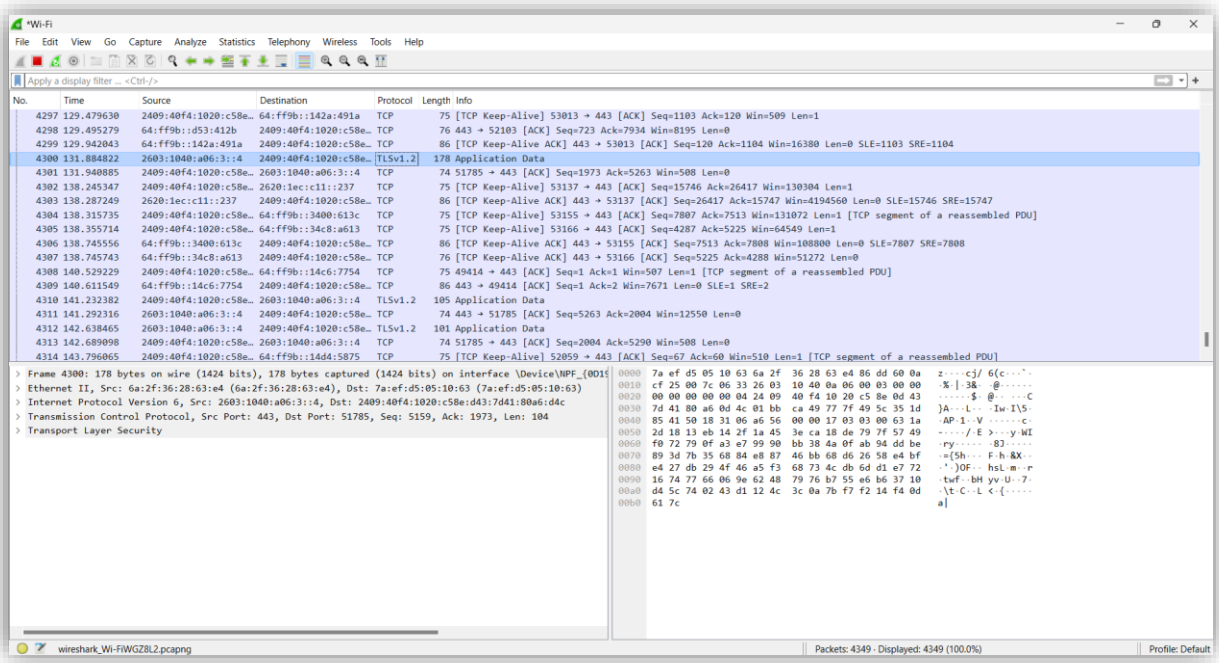
6. Analyze Certificate Details:

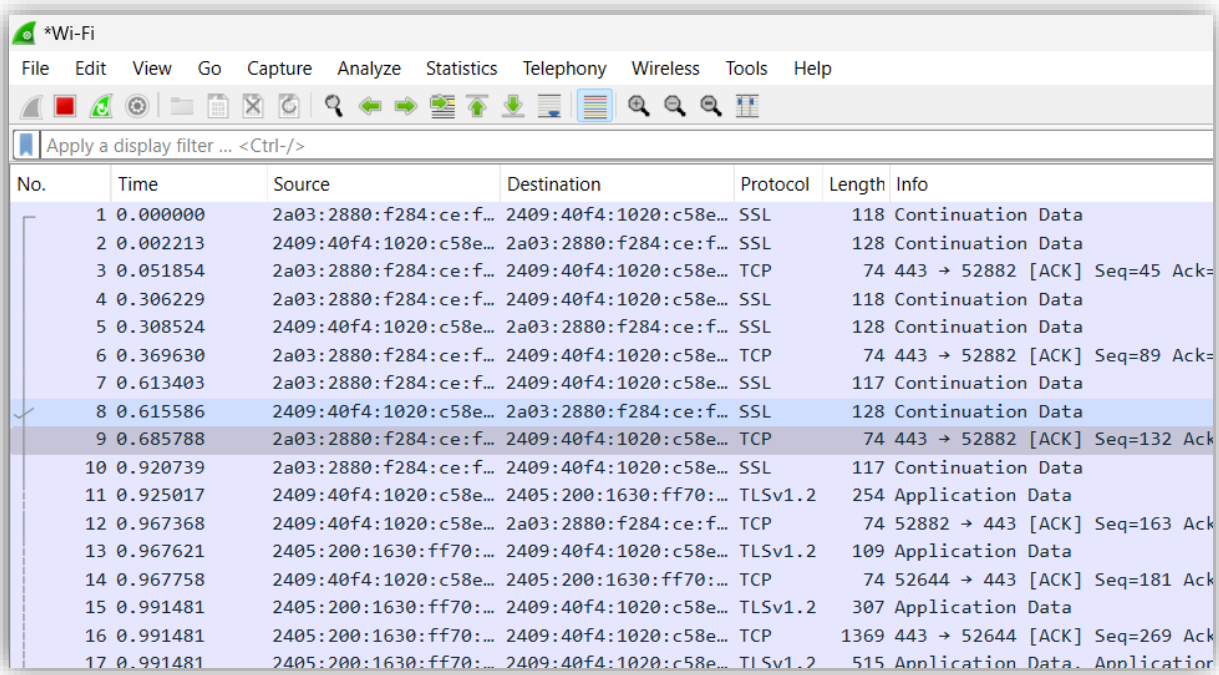
- If analyzing HTTPS or other protocols using certificates, examine the certificate details to understand its validity, issuer, subject, etc.
- Right-click on a packet containing a certificate, select "Decode As," and choose "SSL" to see the certificate details.

7. Look for Security Events:

- Keep an eye out for security-related events, such as failed authentication attempts, renegotiation of security parameters, or unexpected protocol behaviors.

Output:





Result:

Thus, the experiment to analyze the various security mechanism embedded with different protocols is executed and verified successfully.

Exp no : 2	Identification the Vulnerabilities Using Owasp Zap Tool
Date :	

Aim :

To Identify the Vulnerabilities Using Owasp Zap Tool.

Procedure :

1. Install OWASP ZAP:
   - Download and install OWASP ZAP from the official website.
2. Configure Browser Proxy
   - Set up your browser to use ZAP as a proxy server (Default: localhost, Port: 8080).

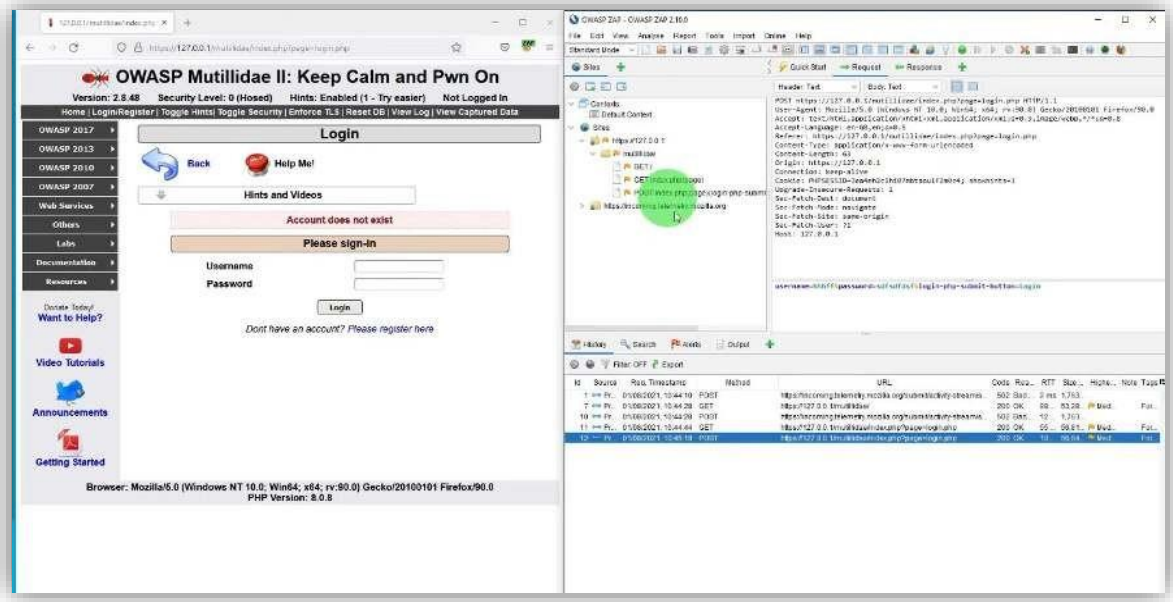
Experiment Steps:

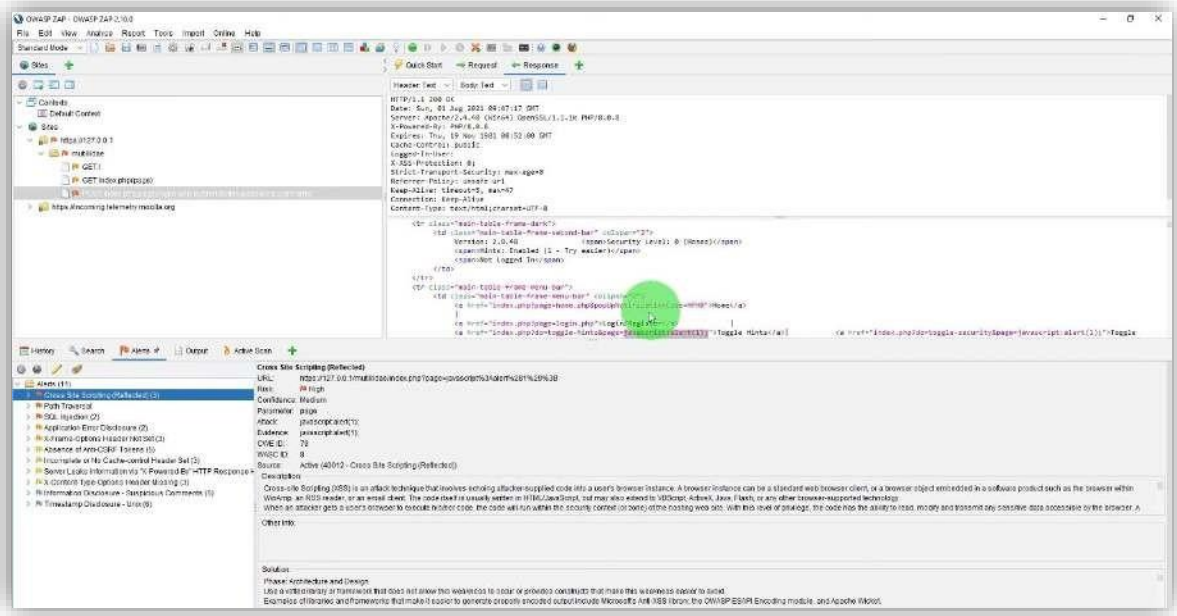
1. Launch OWASP ZAP:
   - Open the OWASP ZAP tool
2. Start ZAP Proxy:
   - In ZAP, click on the 'Quick Start' tab.
   - Start the ZAP Proxy.
3. Set Target Application:
   - Go to the "Sites" tab.
   - Enter the URL of the target application.
   - Right-click on the URL and choose "Include in Context" > "Default Con- text" to add it for scanning.
4. Spider the Application:
   - Go to the "Spider" tab.
   - Right-click on the target URL and select "Spider" to crawl the application.
   - Let ZAP crawl and map the application structure.
5. Active Scan:
   - Go to the "Attack" tab.
   - Choose "Active Scan."
   - Configure the scan settings (scope, intensity, etc.).
   - Start the active scan on the target application.
6. Review Scan Results:
   - After the scan completes, go to the "Alerts" tab.
   - View the list of vulnerabilities discovered by ZAP.

7. Investigate Vulnerabilities:
    - Click on each vulnerability to get detailed information.
    - Verify and understand the nature and potential impact of each issue.

8. Prioritize and Document:
    - Prioritize vulnerabilities based on severity and potential impact.
    - Document the identified vulnerabilities with descriptions, severity levels, affected URLs, and possible remediation steps.

9. Report Generation:
    - Go to the "Report" tab.
    - Generate a comprehensive report summarizing the identified vulnerabili- ties and their details.
    - Choose the appropriate report format (HTML, PDF, etc.).





Result :

Thus, the experiment to identify vulnerabilities using OWASP Zap tool is executed and verified successfully

Exp no : 03	Create simple REST API using python & Perform HTTP Requests
Date :	

Aim :

To create a simple REST API using python to do the GET, POST, PUT and DELETE operations.

Algorithm :

Step 1: Start

Step 2: Install Flask

Step 3: Start the Flask App

Step 4: Use Postman to Test Endpoints

Step 5: View Server Output

Step 6: Stop

Program :

```
from flask import Flask, jsonify, request
app = Flask(__name__)
# Sample data
data = [
    {'id': 1, 'name': 'Alex},
    {'id': 2, 'name': 'Vijay},
    {'id': 3, 'name': 'Sharukh'}
]
# GET request to retrieve all items
@app.route('/items', methods=['GET'])
def get_items():
    return jsonify({'items': data})

# GET request to retrieve a specific item by ID
@app.route('/items/<int:item_id>', methods=['GET'])
def get_item(item_id):
```

```
    item = next((item for item in data if item['id'] == item_id), None)
    if item:
        return jsonify({'item': item})
 else:
        return jsonify({'message': 'Item not found'}), 404

# POST request to add a new item
@app.route('/items', methods=['POST'])
def add_item():
    new_item = {'id': len(data) + 1, 'name': request.json['name']}
    data.append(new_item)
    return jsonify({'item': new_item}), 201

# PUT request to update a specific item by ID
@app.route('/items/<int:item_id>', methods=['PUT'])
def update_item(item_id):
    item = next((item for item in data if item['id'] == item_id), None)
    if item:
        item['name'] = request.json['name']
        return jsonify({'item': item})
    else:
        return jsonify({'message': 'Item not found'}), 404

# DELETE request to remove a specific item by ID
@app.route('/items/<int:item_id>', methods=['DELETE'])
def delete_item(item_id):
    global data
    data = [item for item in data if item['id'] != item_id]
    return jsonify({'message': 'Item deleted'}), 200

if __name__ == '__main__':
    app.run(debug=True)
```

Procedure and Output:

Step 1: Install Flask >>> `pip install flask`

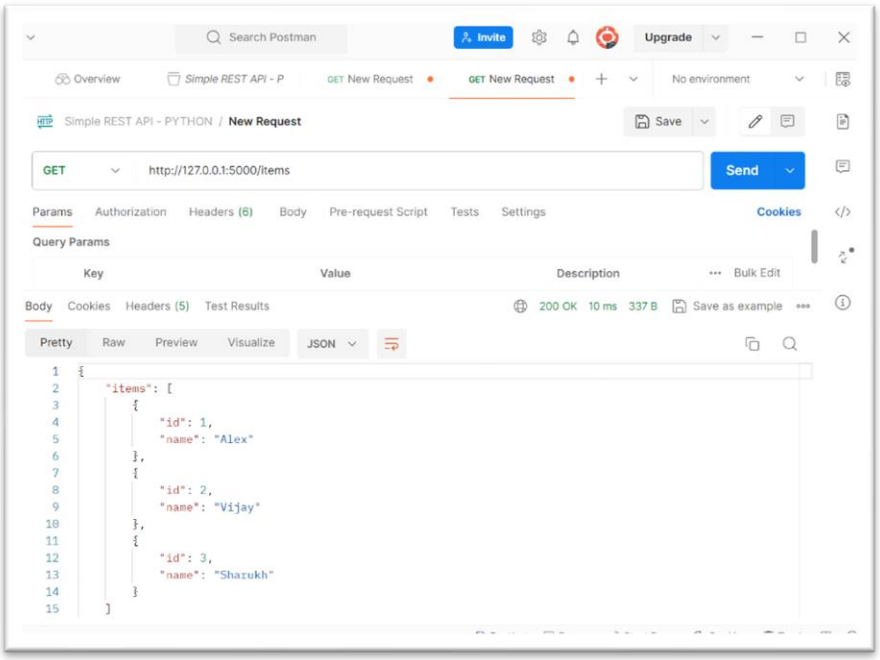
Step 2: Start the Flask App Save the code as app.py and

execute >>> `python app.py`

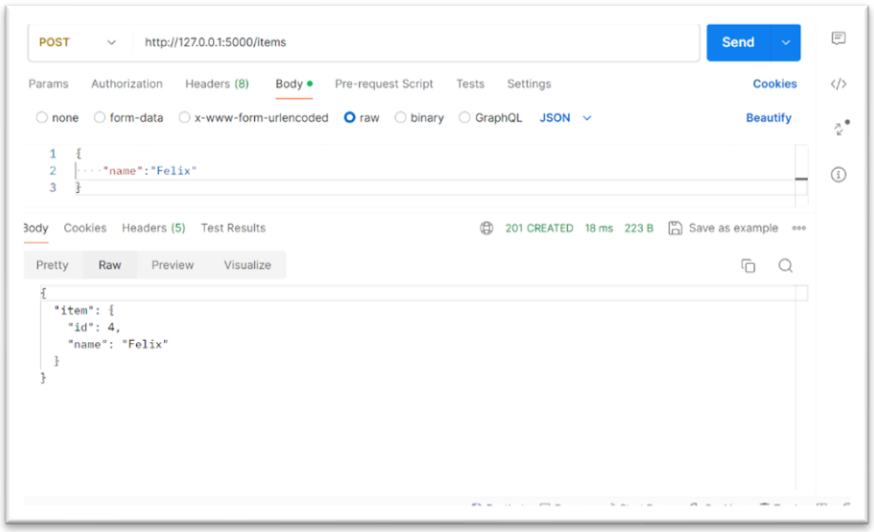
Copy the url produced http://127.0.0.1:5000

Step 3: Use Postman to Test Endpoints

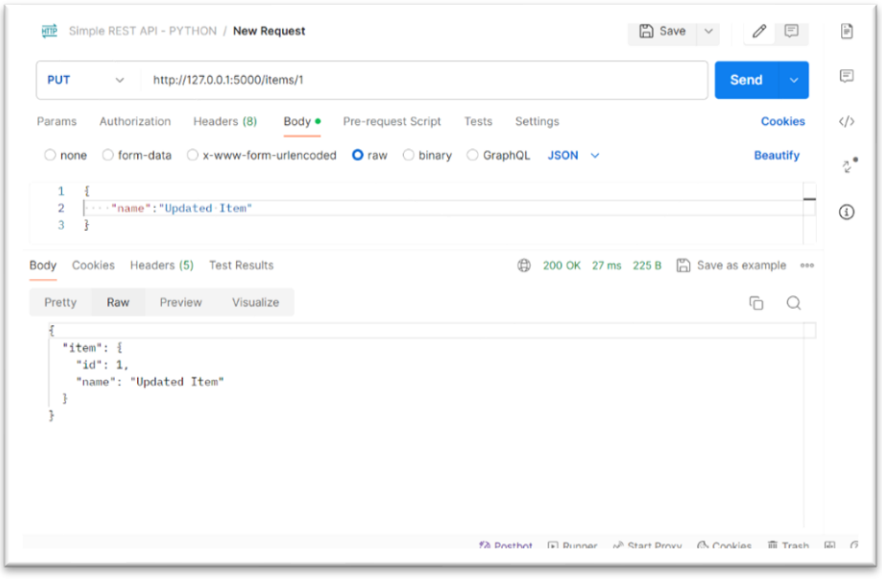
1. GET Request
   - Set the request type to GET.
   - Enter the URL: http://127.0.0.1:5000/items
   - Click "Send."



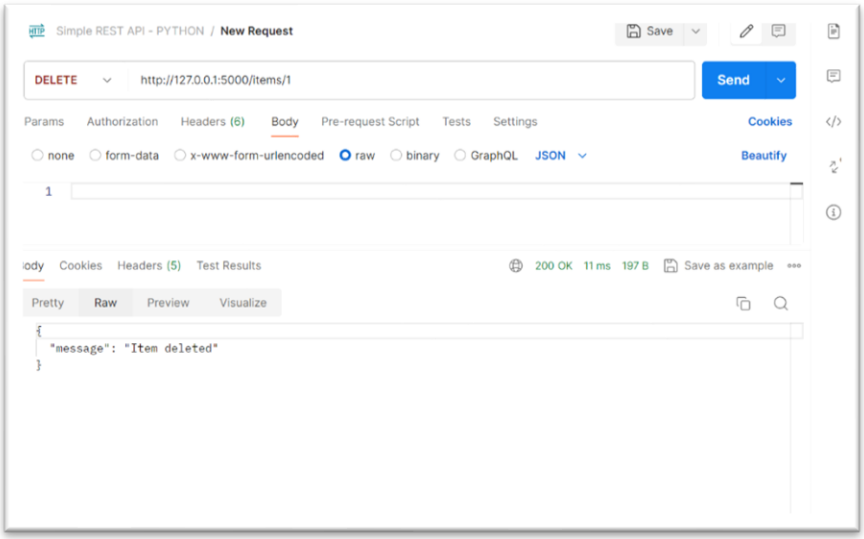
2. POST Request to Add a New Item
   - Set the request type to POST.
   - Enter the URL: http://127.0.0.1:5000/items
   - Go to the "Body" tab, select "raw" and choose "JSON (application/json)".Enter the request body
   - Click "Send."



3. PUT Request to Update an Existing Item:
    - Set the request type to PUT.
    - Enter the URL for a specific item ID, for example: http://127.0.0.1:5000/items/1
    - Go to the "Body" tab, select "raw" and choose "JSON (applica tion/json)".
    - Enter the updated information . Click "Send."



4. DELETE Request to Remove a Specific Item by ID:
    - Set the request type to DELETE.
    - Enter the URL for a specific item ID, for example: http://127.0.0.1:5000/items/1
    - Click "Send."



Result :

Thus the simple REST API using python to do the GET, POST, PUT and DELETE operations has been successfully created and the output has been verified.

Exp no : 04	Installation of Burp Suite to Perform Vulnerabilities Testing
Date :	

Aim :

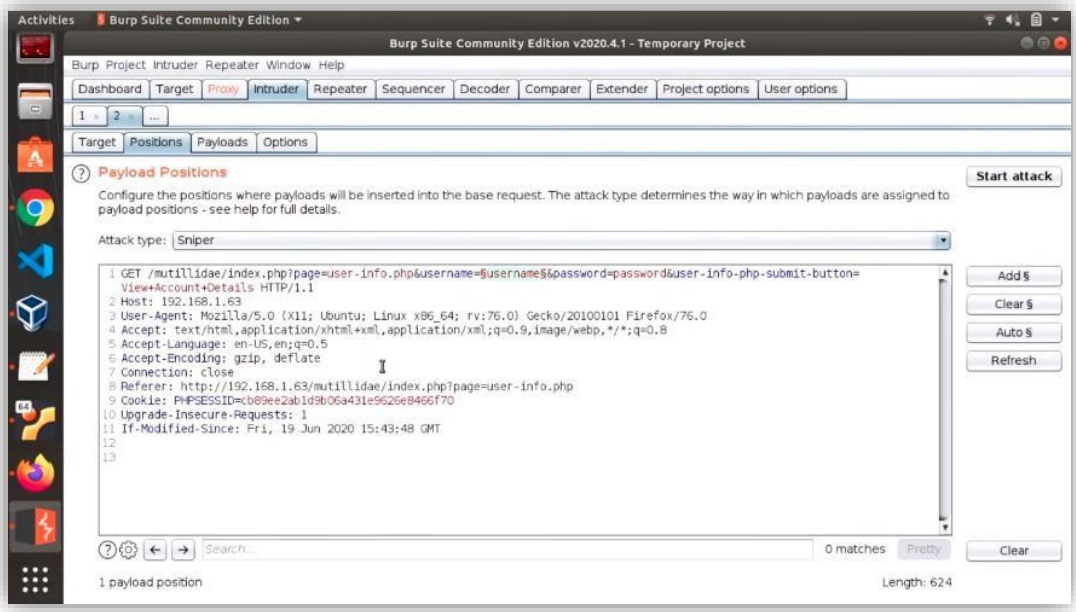
To Install Burp Suite to do perform following vulnerability testing:

- SQL Injection
- Cross-site Scripting (XSS)

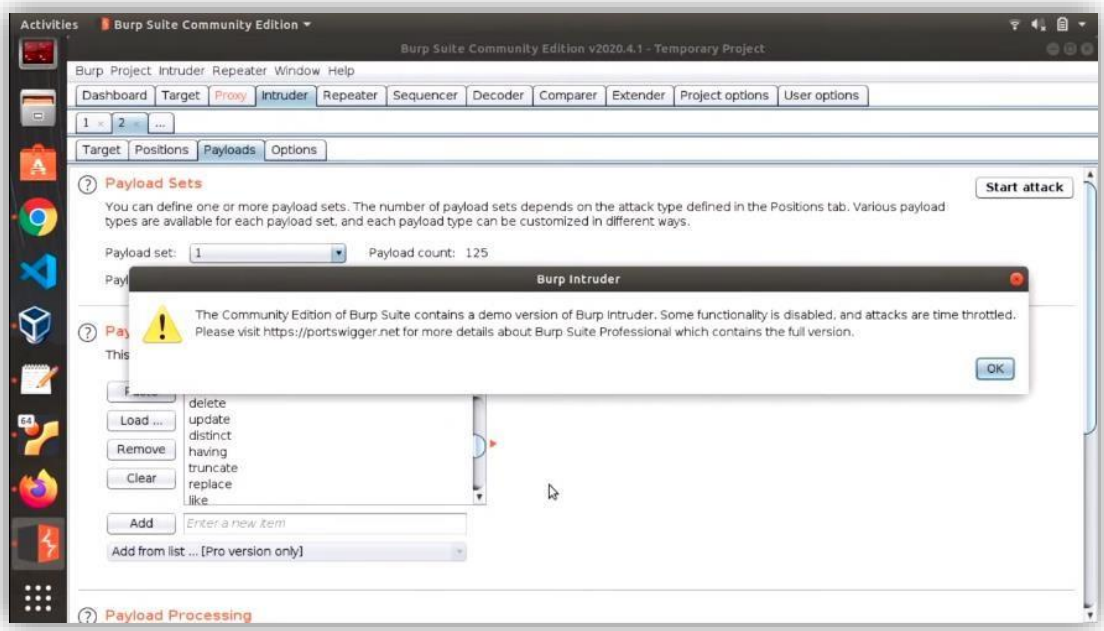
Procedure (SQL Injection) :

1. Install Burpsuite and connect the burpsuite proxy in browser proxy settings
2. Turn on the intercept and search for the website which needs to be captured.

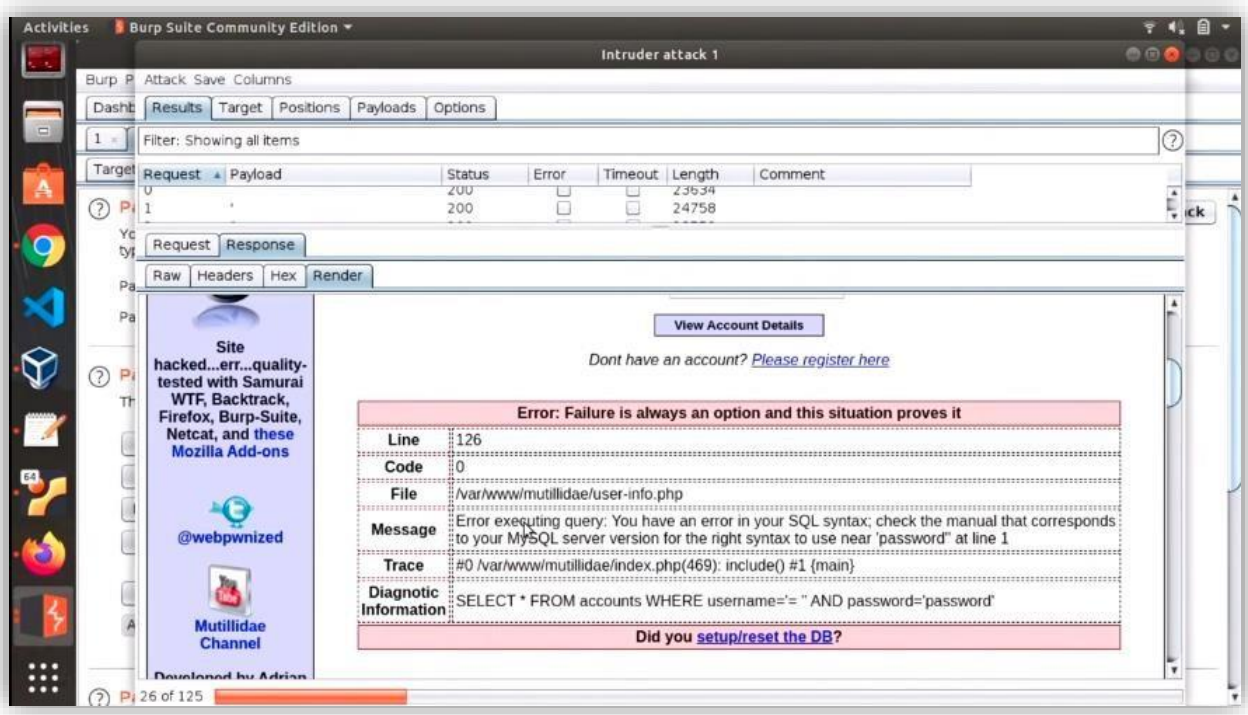
3. Send the intercepted request to the intruder and load the SQL Injection File from the device which is already installed.



4. Start the attack in the intruder and search for the requests & responses in the render screen for SQL Injection.

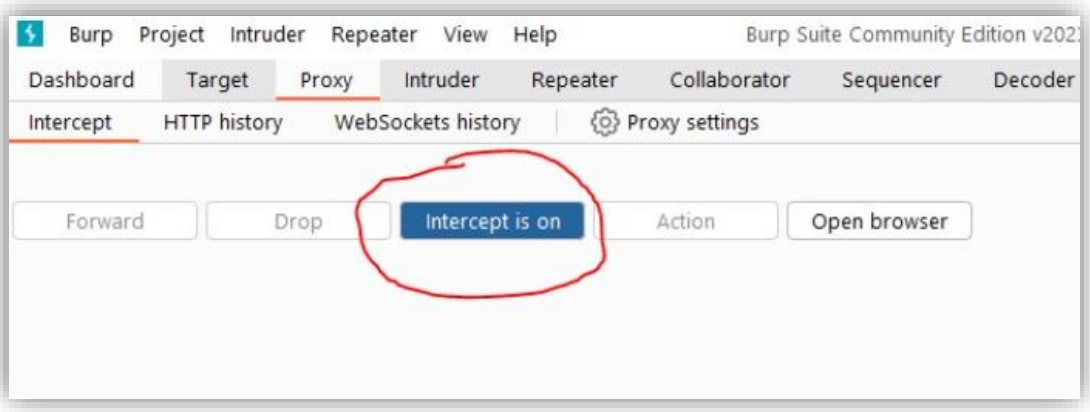


5. After the attack, some response render shows the username and password for the webpage.

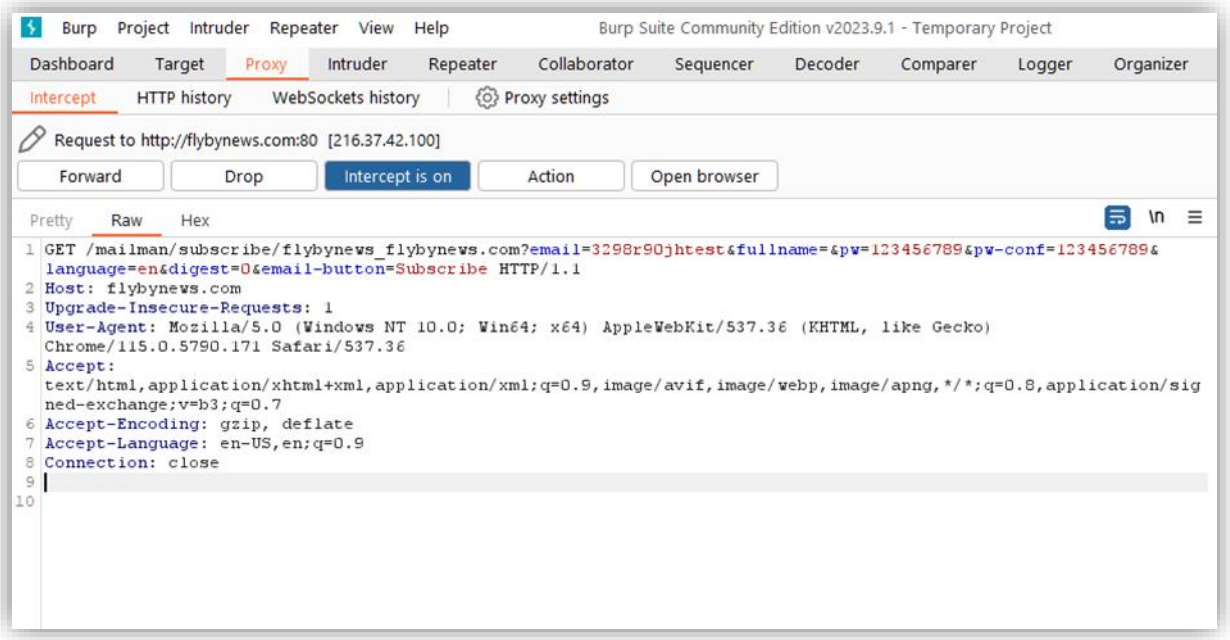


Procedure (Cross-site Scripting (XSS)):

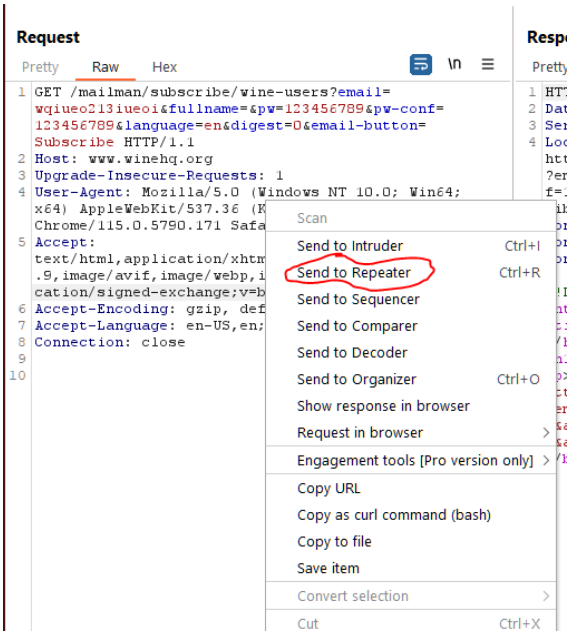
1. Ensure that Burp is correctly configured with your browser.
2. With intercept turned on in the Proxy "Intercept" tab, visit the web application you are testing.



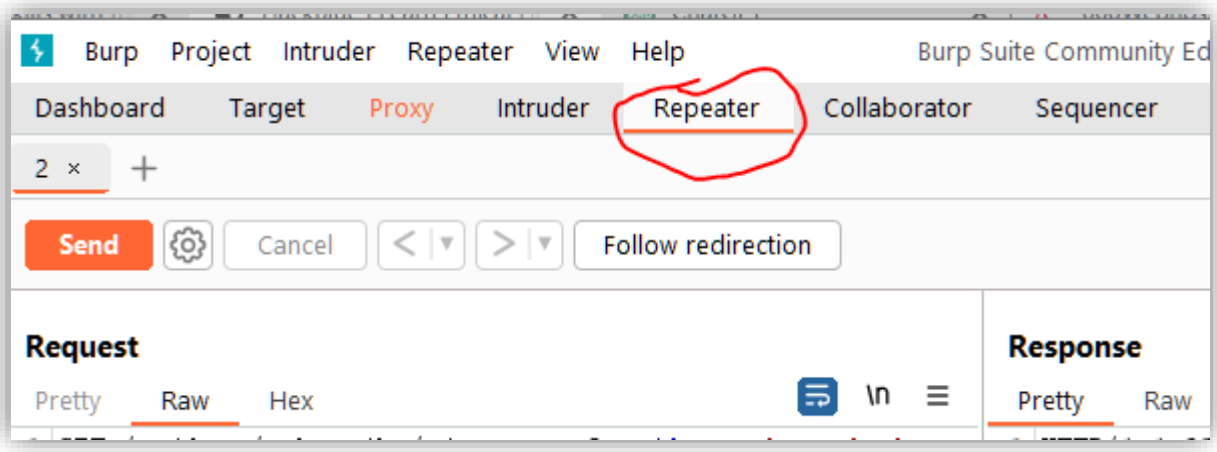
3. Enter an arbitrary string that doesn't appear within the application and contains only alphabetic characters



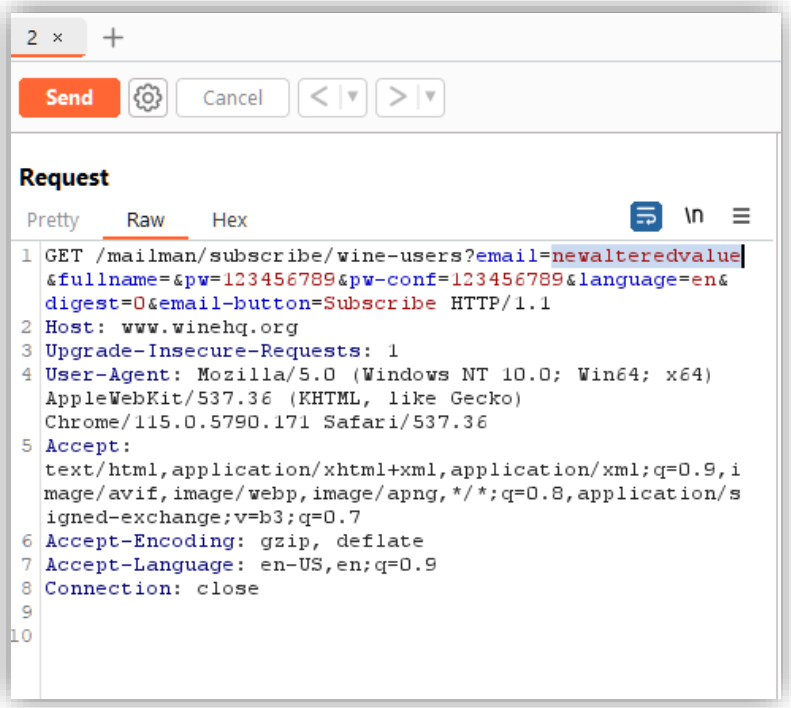
4. The request will be captured by Burp. Right-click on the request and select "Send to Repeater".



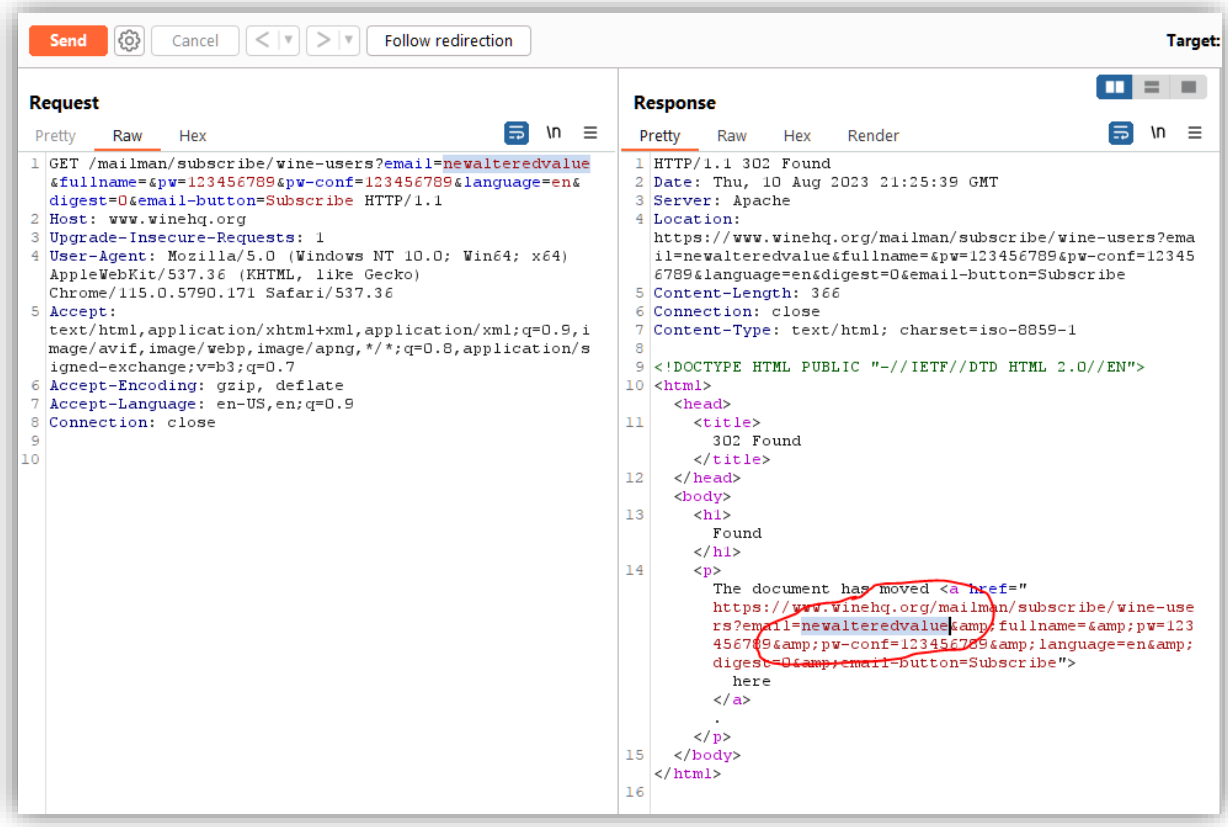
5. In the Repeater tab, input various XSS payloads into the input field of the web application.



6. Submit this string as every parameter to every page, targeting only one parameter at a time.



7. Review the HTML source to identify the location(s) where your unique string is being reflected.



8. Introduce JavaScript without causing an error and work around any defensive filters.
9. Test your exploit by submitting it to the application. If your crafted string is returned unmodified, the application is vulnerable.

Result :

Thus the above vulnerability is successfully executed and verified.

Exp no : 05	Attacking a Website Using Social Engineering Method
Date :	

Aim :

To attach the website using social engineering method.

Procedure:

Installation of Social engineering toolkit :

Step 1: Open your Kali Linux Terminal and move to Desktop

>>>cd Desktop

Step 2: As of now you are on a desktop so here you have to create new directory named SEToolkit using the following command.

>>>mkdir SEToolkit

Step 3: Now as you are in the Desktop directory however you have created a SEToolkit directory so move to SEToolkit directory using the following command

>>>cd SEToolkit

Step 4: Now you are in SEToolkit directory here you have to clone SEToolkit from GitHub so you can use it.

>>>git clone https://github.com/trustedsec/social-engineer-toolkit setoolkit/

Step 5: Social Engineering Toolkit has been downloaded in your directory now you have to move to the internal directory of the social engineering toolkit using the following command.

>>>cd setoolkit

Step 6: Congratulations you have finally downloaded the social engineering toolkit in your directory SEToolkit. Now it's time to install requirements using the following command.

>>> pip3 install -r requirements.txt

```
root@kali:~/Desktop/SEToolkit/setoolkit# pip3 install -r requirements.txt
Requirement already satisfied: pexpect in /usr/lib/python3/dist-packages (from -r requir
ements.txt (line 1)) (4.6.0)
Requirement already satisfied: pycrypto in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 2)) (2.6.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 3)) (2.22.0)
Requirement already satisfied: pyopenssl in /usr/lib/python3/dist-packages (from -r requ
irements.txt (line 4)) (19.0.0)
Requirement already satisfied: pefile in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 5)) (2019.4.18)
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 6)) (0.9.20)
Requirement already satisfied: qrcode in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 8)) (6.1)
Requirement already satisfied: pillow in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 9)) (6.2.1)
Requirement already satisfied: pymssql<3.0 in /usr/lib/python3/dist-packages (from -r re
quirements.txt (line 11)) (2.1.4)
Requirement already satisfied: ldapdomaindump≥0.9.0 in /usr/lib/python3/dist-packages (
from impacket->-r requirements.txt (line 6)) (0.9.1)
```

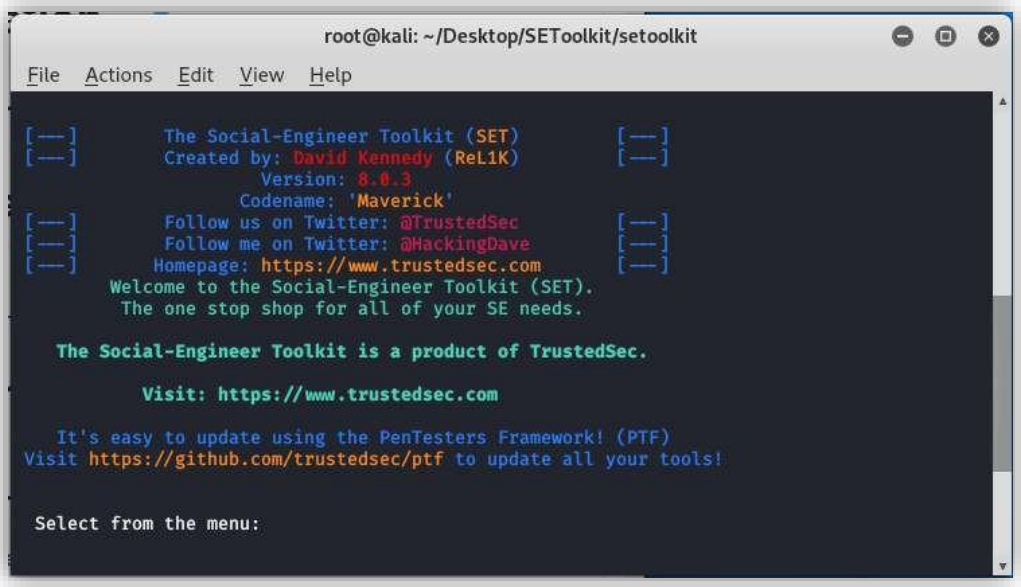
Step 7: All the requirements have been downloaded in your setoolkit. Now it's time to install the requirements that you have downloaded

>>>python setup.py

Step 8: Finally all the processes of installation have been completed now it's time to run the social engineering toolkit .to run the SEToolkit type following command.

>>>Setoolkit

Step 9: At this step, setoolkit will ask you (y) or (n). Type y and your social engineering toolkit will start running.



Step 10: Now your setoolkit has been downloaded into your system now it's time to use it .now you have to choose an option from the following options .here we are choosing option 2
Website Attack Vector

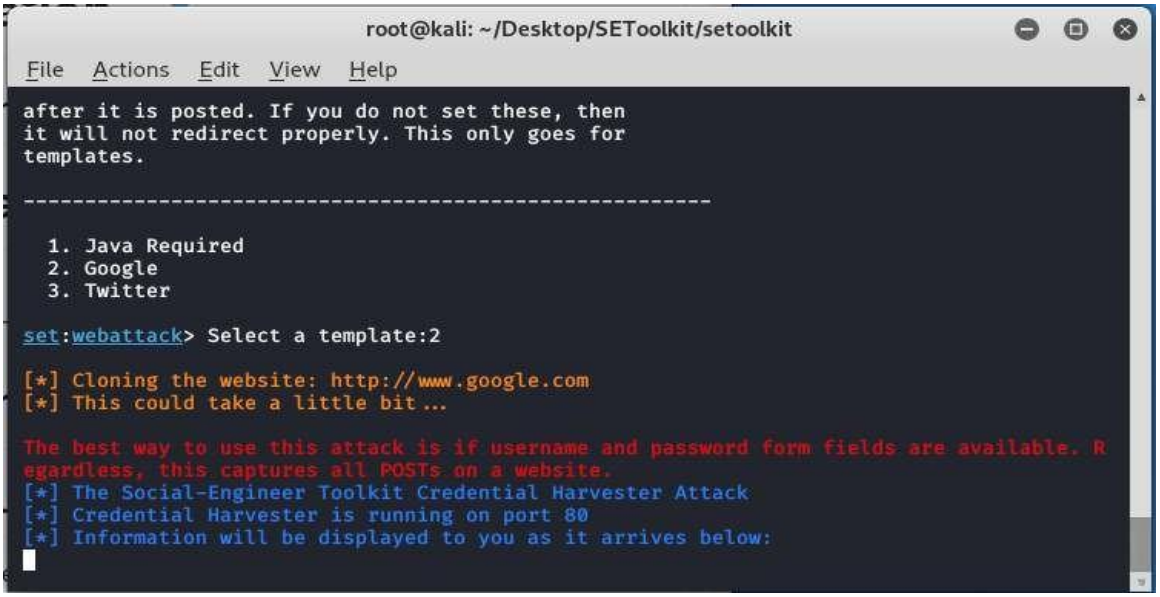
Option: 2

Step 11: Now we are about to set up a phishing page so here we will choose option 3 that is the credential harvester attack method.

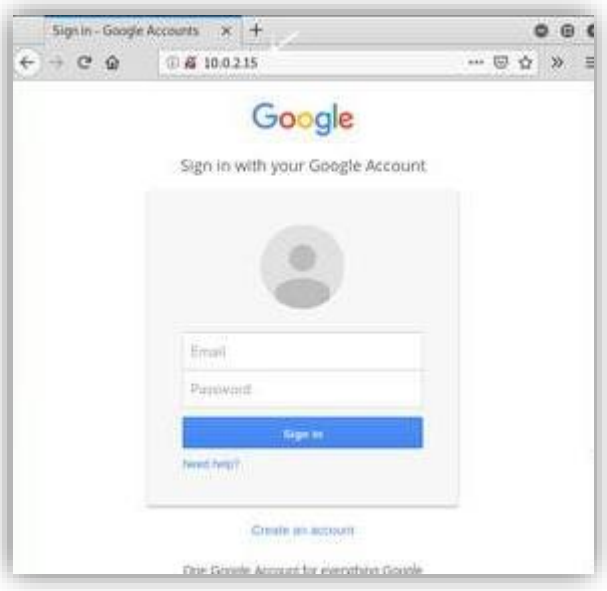
Option: 3

Step 12: Now since we are creating a Phishing page so here we will choose option 1 that is web templates. Option: 1

Step 13: Create a google phishing page so choose option 2 for that then a phishing page will be generated on your localhost.



Step 14: Social engineering toolkit is creating a phishing page of google.



RESULT:

Thus, the experiment to attach the website using social engineering method is executed and verified successfully.