CHANDIGARH UNIVERSITY

UNIVERSITY INSTITUTE OF NGINEERING

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Submitted By: Vivek Kumar(21BCS8129)	**Submitted To:** Er. Himanshi (13362)
Subject Name	Web and Mobile Security Lab
Subject Code	20CSP-338
Branch	Computer Science and Engineering
Semester	5th

Experiment - 2

Student Name: Vivek Kumar **UID: 21BCS8129**
Branch: BE-CSE(LEET) **Section/Group: WM-20BCS-616/A**
Semester: 5th **Date of Performance: 19/08/2022**
Subject Name: Web and Mobile Security Lab **Subject Code: 20CSP-338**

1. Aim/Overview of the practical:

Design a method to simulate the HTML injection and cross-site scripting to exploit the attacker.

2. Task to be done/ Which logistics used:

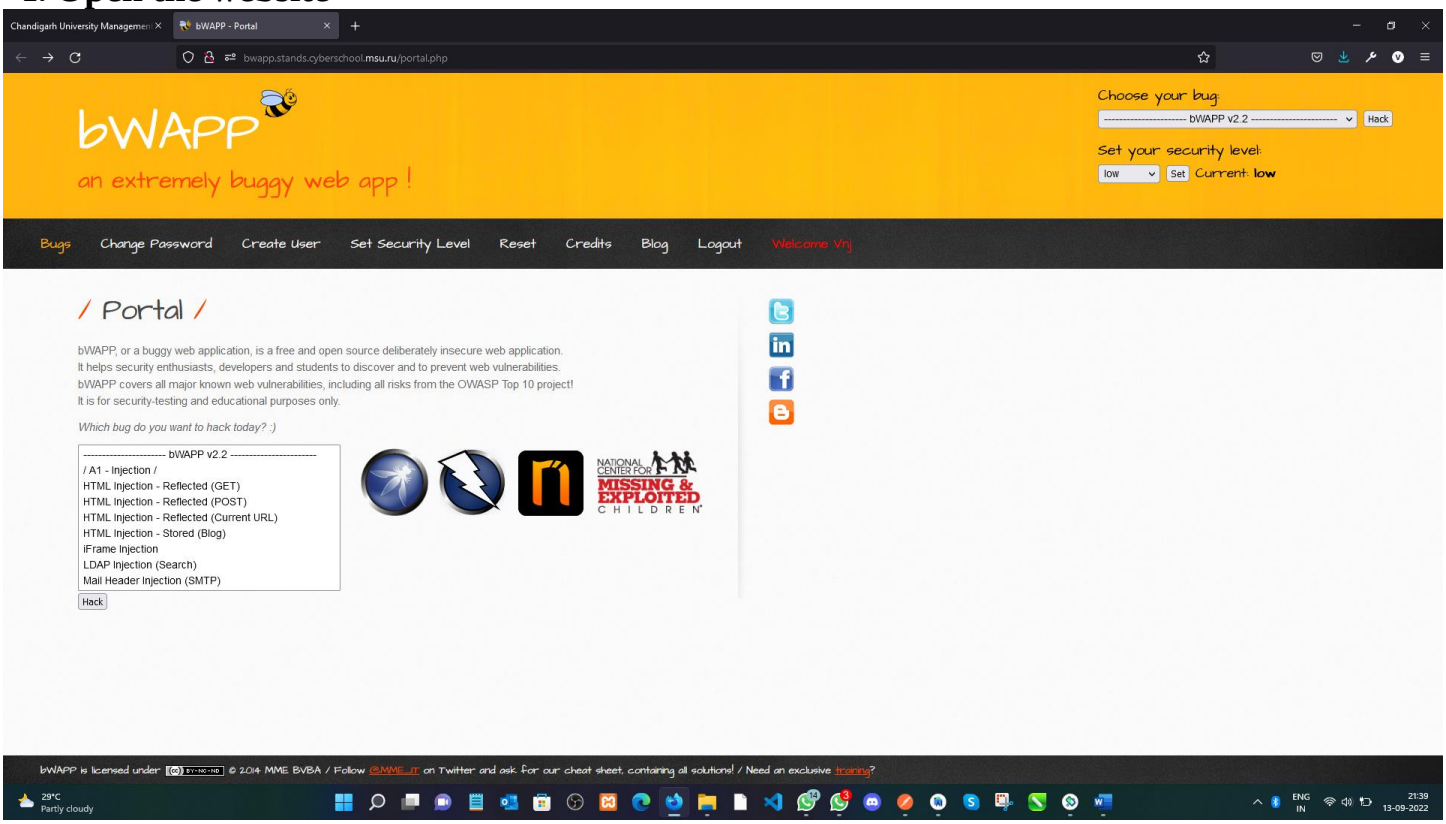
Analyse the HTML injection.

3. Requirements (For programming-based labs):

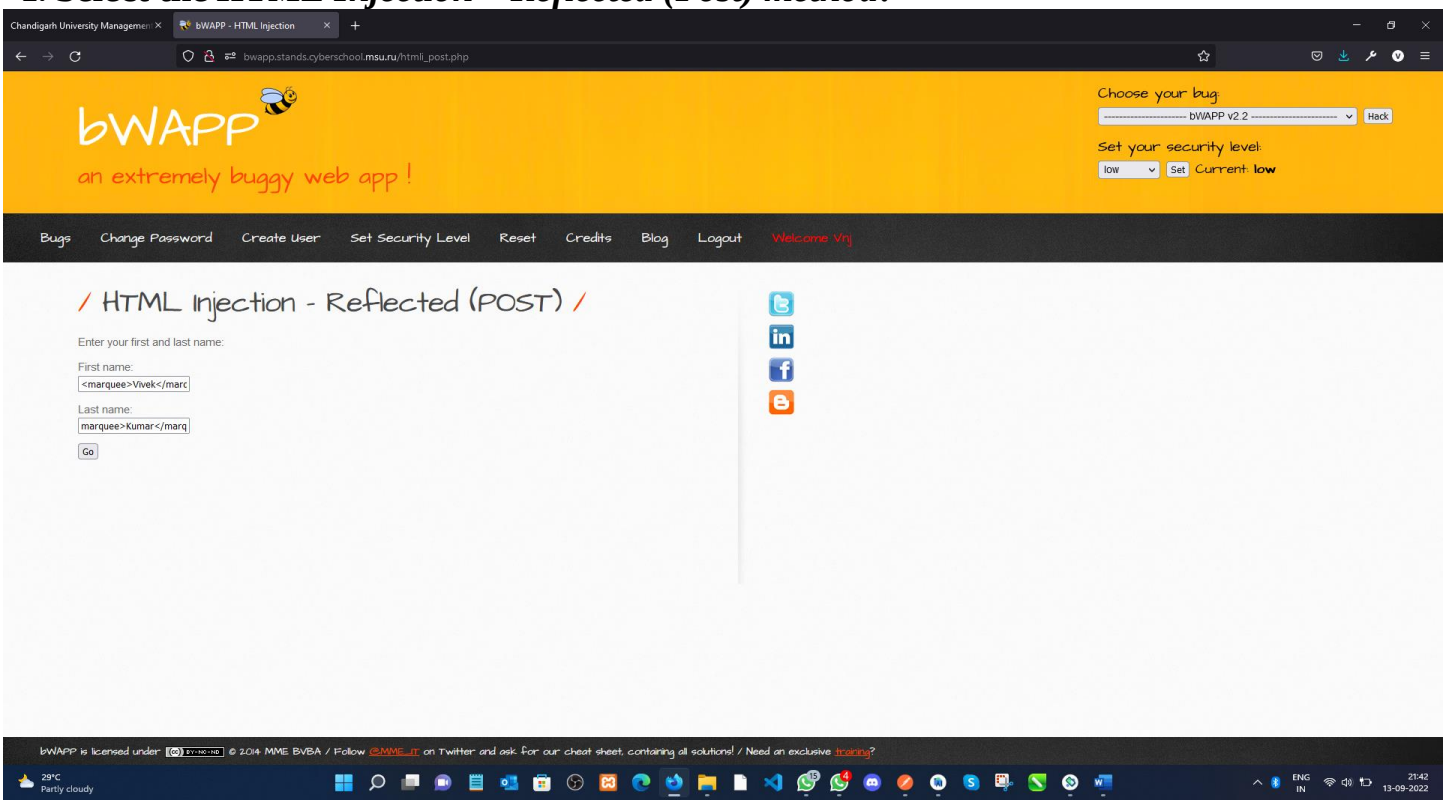
PC with Windows 7 or above.

4. Steps for experiment/practical/Code:

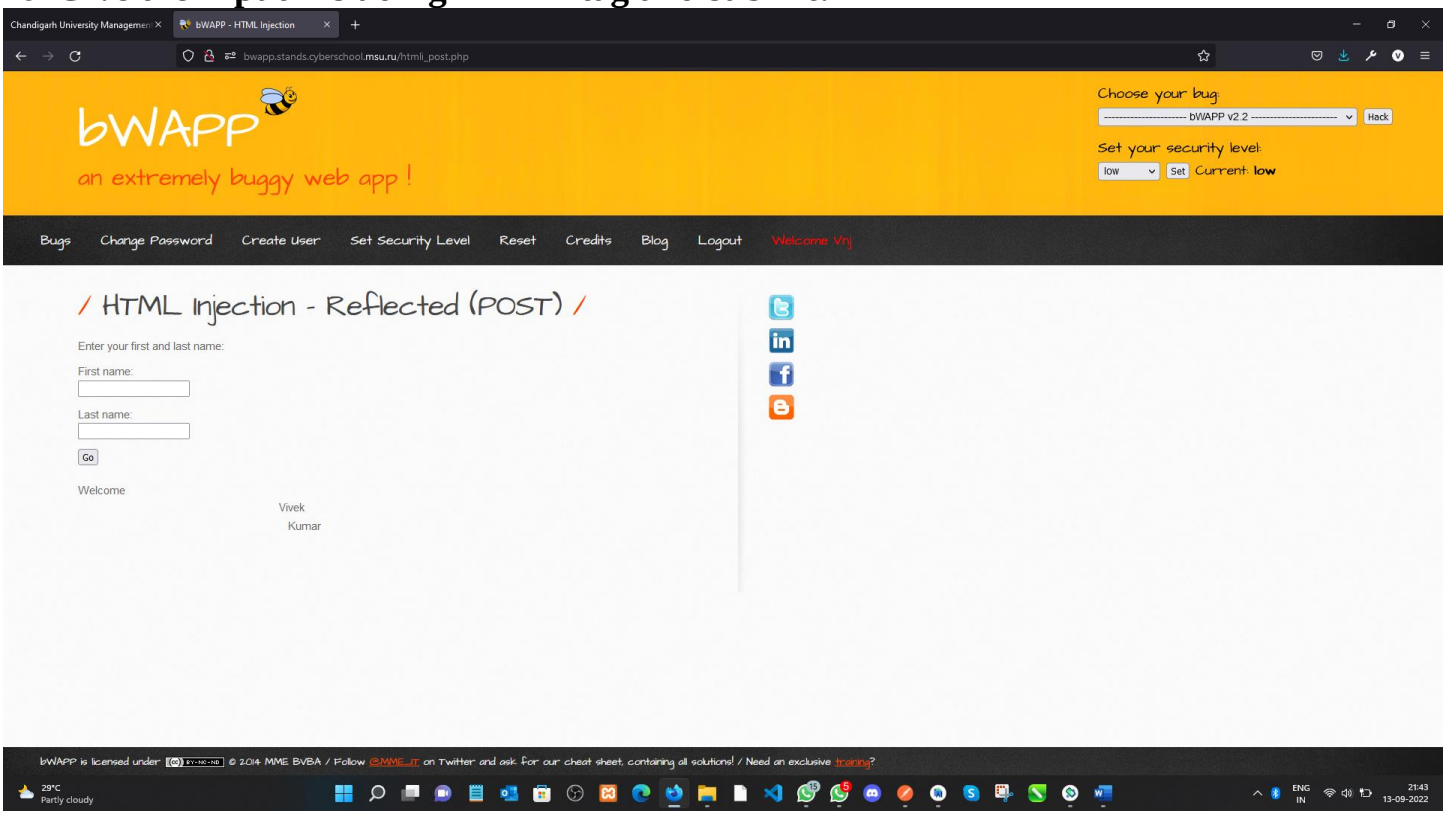
1. **Open the website**



2. Select the *HTML Injection – Reflected (Post) method*:



3. Give the Input including HTML tag and submit:



5. Observations/Discussions/ Complexity Analysis:

In this Experiment we have learn about the HTML injection and XSS injection how it works on our network and websites.

Learning outcomes (What I have learnt):

We learn what is HTML injection and XSS injection. An overview of how these attacks is constructed and applied to real systems. If the app or website lacks proper data sanitization, the malicious link executes the attacker's chosen code on the user's system. As a result, **the attacker can steal the user's active session cookie** which can be harmful to the website.

Evaluation Grid (To be created per the faculty's SOP and Assessment guidelines):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Worksheet completion including writing learning objectives/Outcomes. (To be submitted at the end of the day).		
2.	Post-Lab Quiz Result.		
3.	Student Engagement in Simulation/Demonstration/Performance and Controls/Pre-Lab Questions.		
	Signature of Faculty (with Date):	Total Marks Obtained:	