

**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	5 th		

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

Chandigarh University Management x bWAPP - Portal x +

bwapp.stands.cyberschool.msu.ru/portal.php

bWAPP
an extremely buggy web app !

Choose your bug
bWAPP v2.2 Hack

Set your security level:
low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Vrk

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

bWAPP v2.2

/ A1 - Injection /

- HTML Injection - Reflected (GET)
- HTML Injection - Reflected (POST)
- HTML Injection - Reflected (Current URL)
- HTML Injection - Stored (Blog)
- iFrame Injection
- LDAP Injection (Search)
- Mail Header Injection (SMTP)

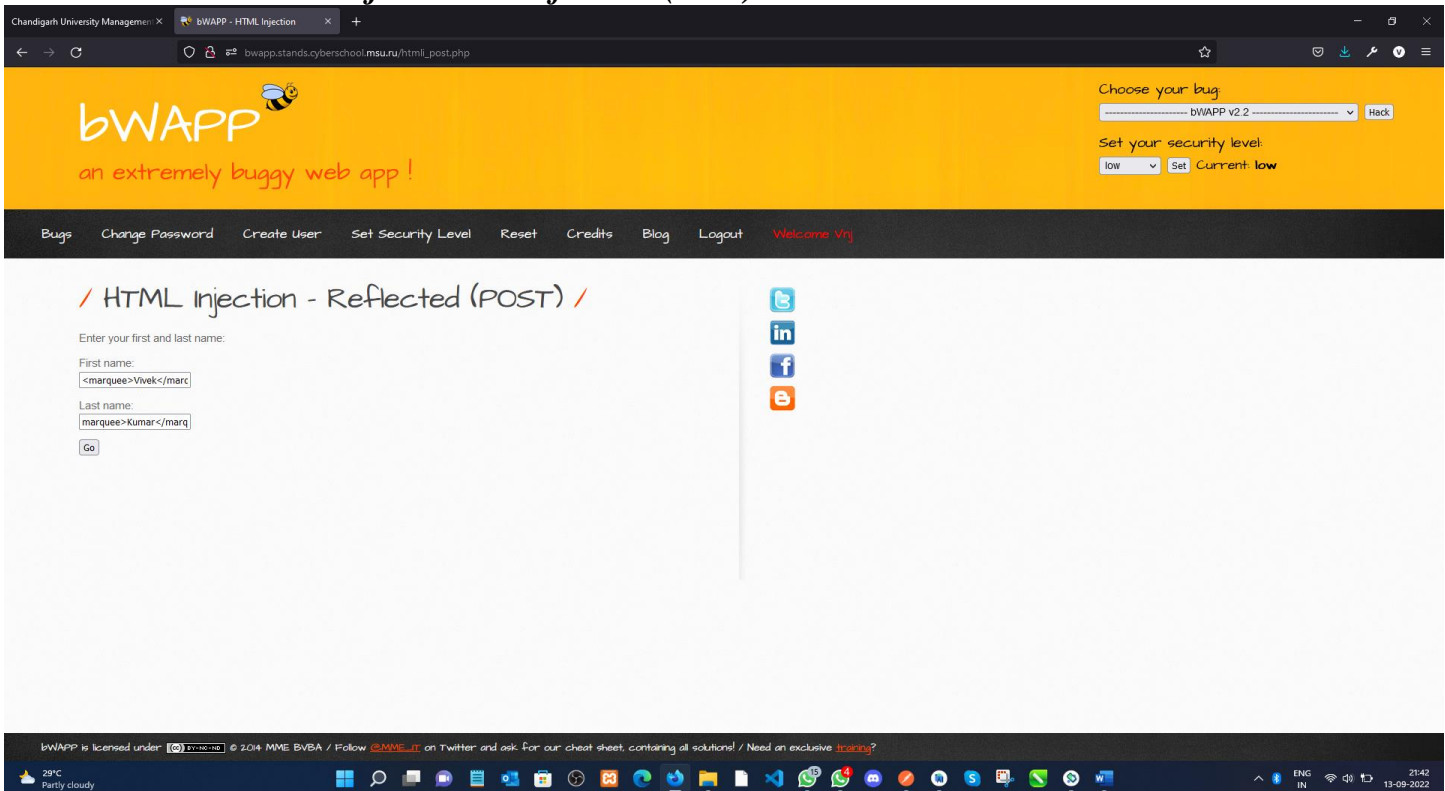
Hack

bWAPP is licensed under: © 2014 MME BVBA / Follow @MME_BVBA on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

29°C Partly cloudy

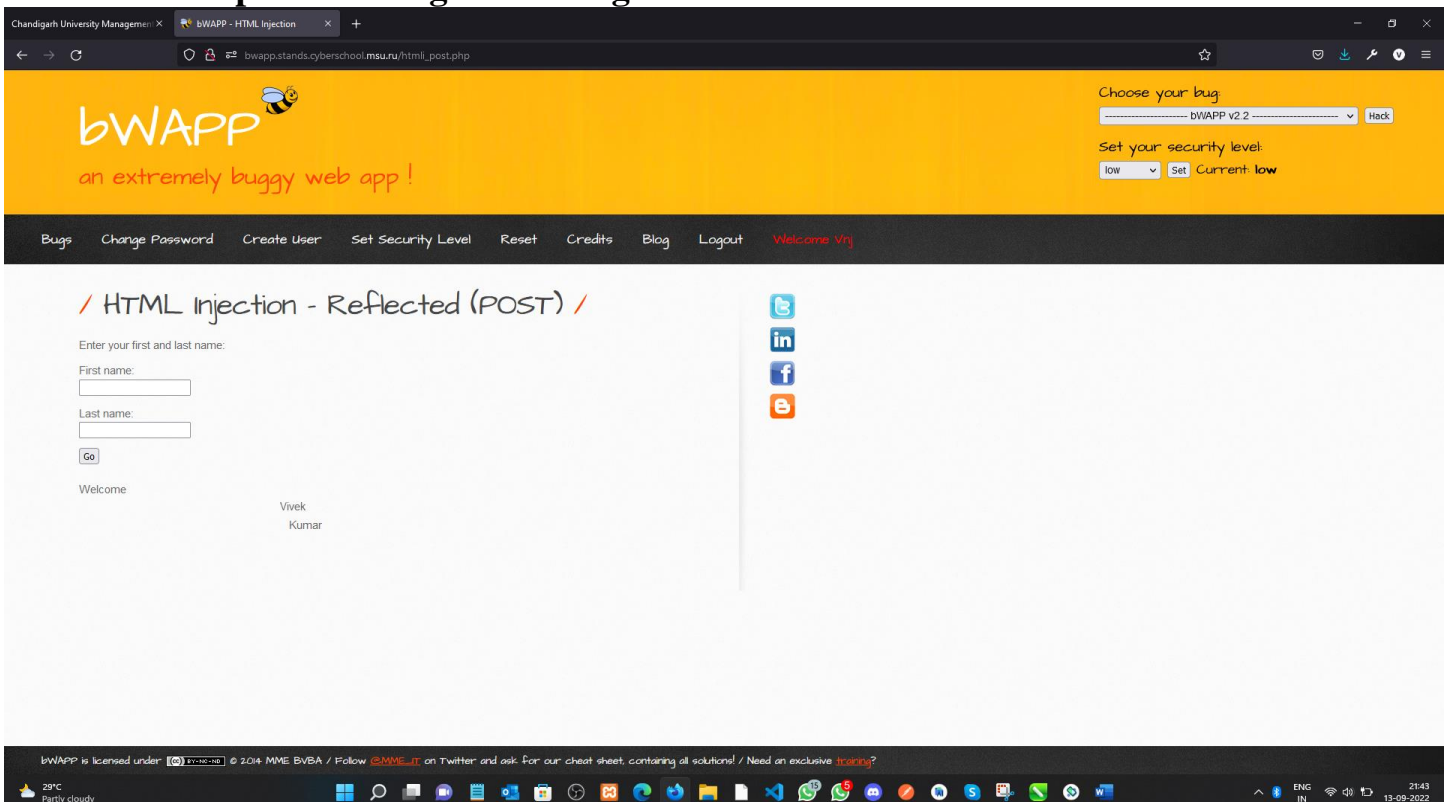
ENG IN 21:39 13-09-2022

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



The screenshot shows the bWAPP web application interface. The header is orange with the bWAPP logo and the text "an extremely buggy web app!". On the right, there are options to "Choose your bug" (set to bWAPP v2.2) and "Set your security level" (set to low). A navigation bar at the top includes links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and a welcome message. The main content area is titled "/ HTML Injection - Reflected (POST) /" and contains a form to "Enter your first and last name:". The form has input fields for "First name:" and "Last name:", both containing the payload "<marquee>Vivek</marque". A "Go" button is at the bottom of the form. To the right of the form are social media icons for Twitter, LinkedIn, Facebook, and Email. The footer of the application contains a license notice and a link to a cheat sheet.

3. Give the Input including HTML tag and submit:



This screenshot shows the same bWAPP interface as the previous one, but with the results of the HTML injection. The "First name:" and "Last name:" input fields are now empty. Below the "Go" button, the text "Welcome Vivek Kumar" is displayed, indicating that the injected payload was successfully reflected in the application's output. The rest of the interface, including the header, navigation bar, and footer, remains the same.

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:	