

**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 - 3

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:

Implementation of Cross site request forgery (CSRF) attack.

2. Task to be done/ Which logistics used:

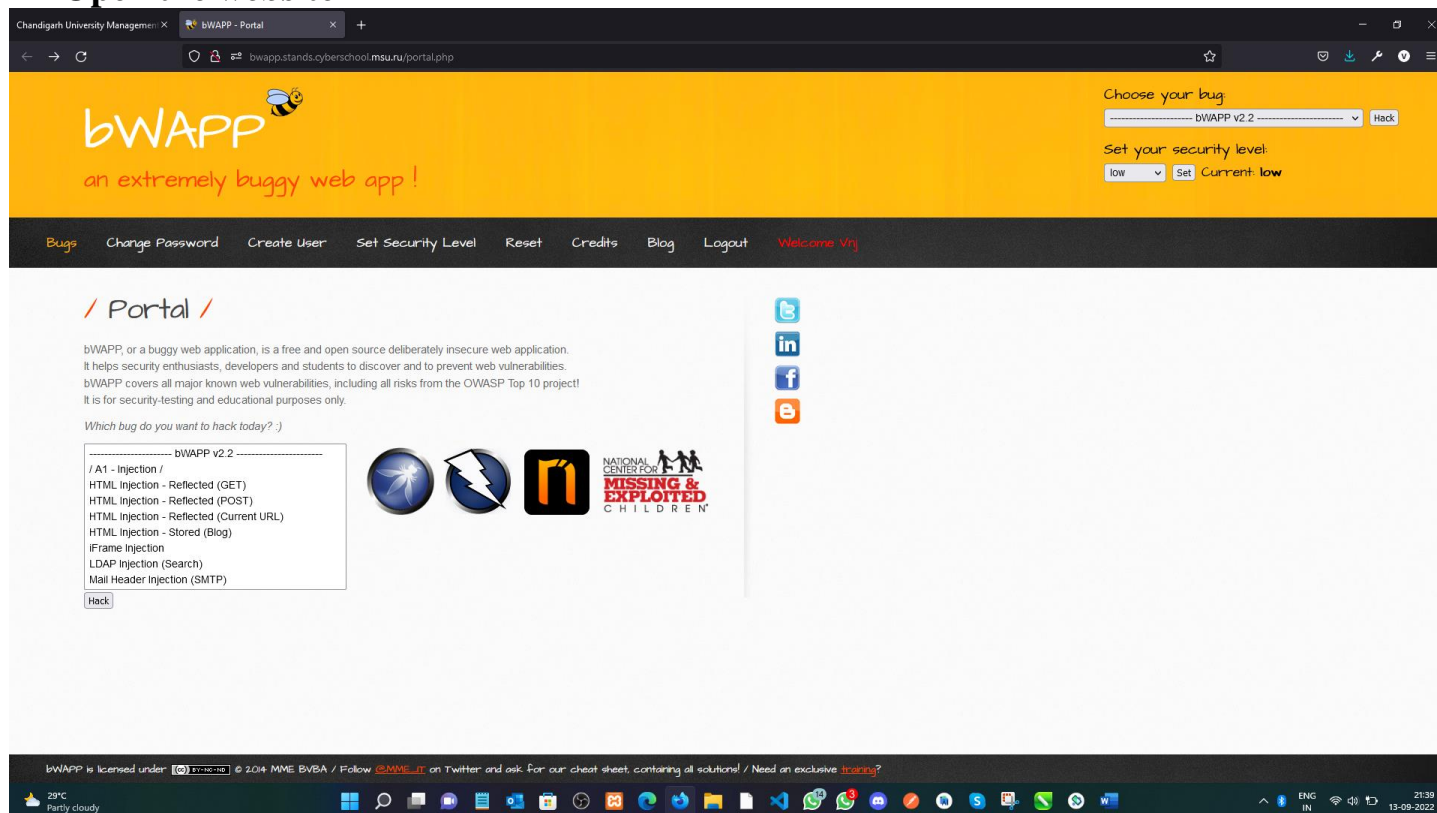
Analyse the Cross Site Request Forgery.

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 Vrij

/ 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)

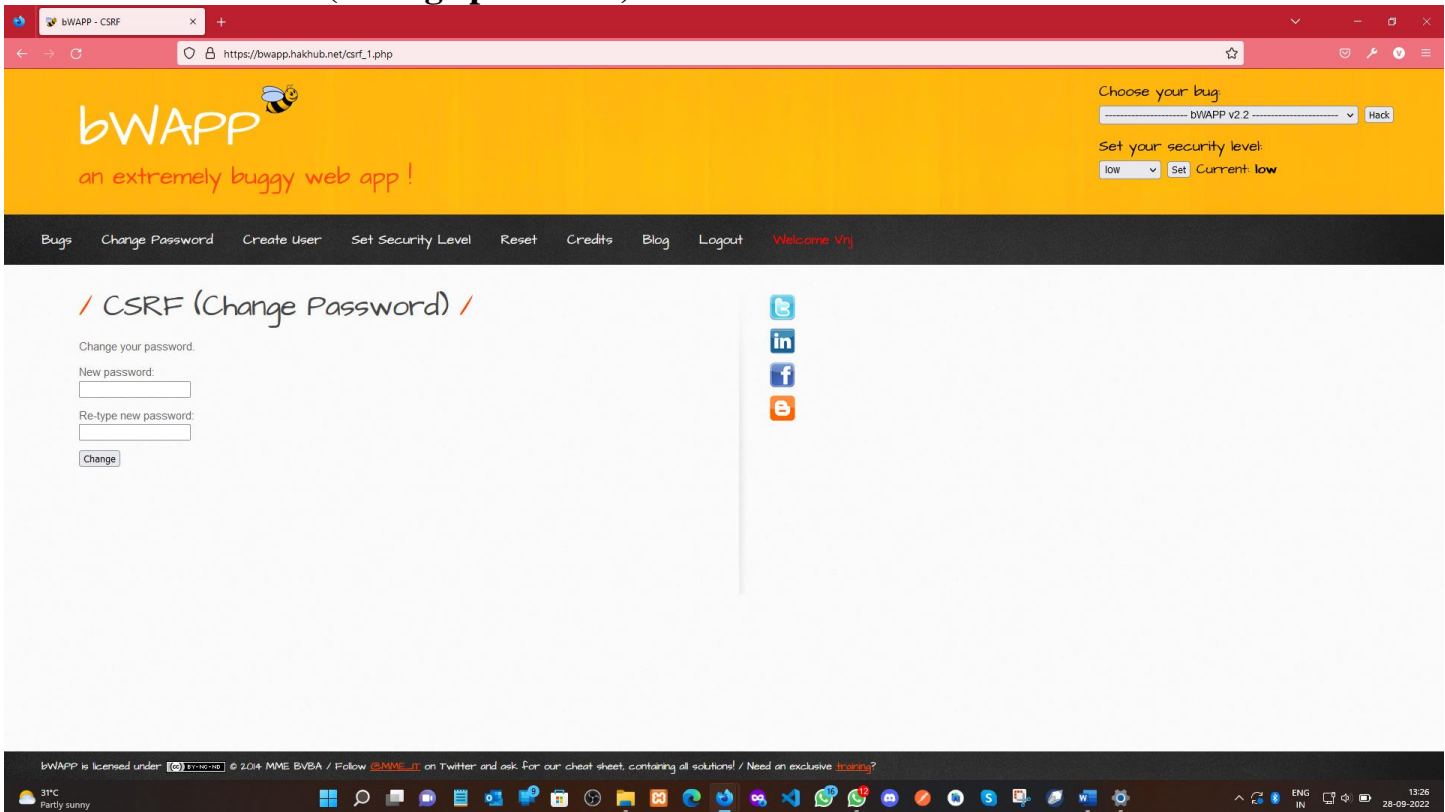
Hack

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

29°C Partly cloudy

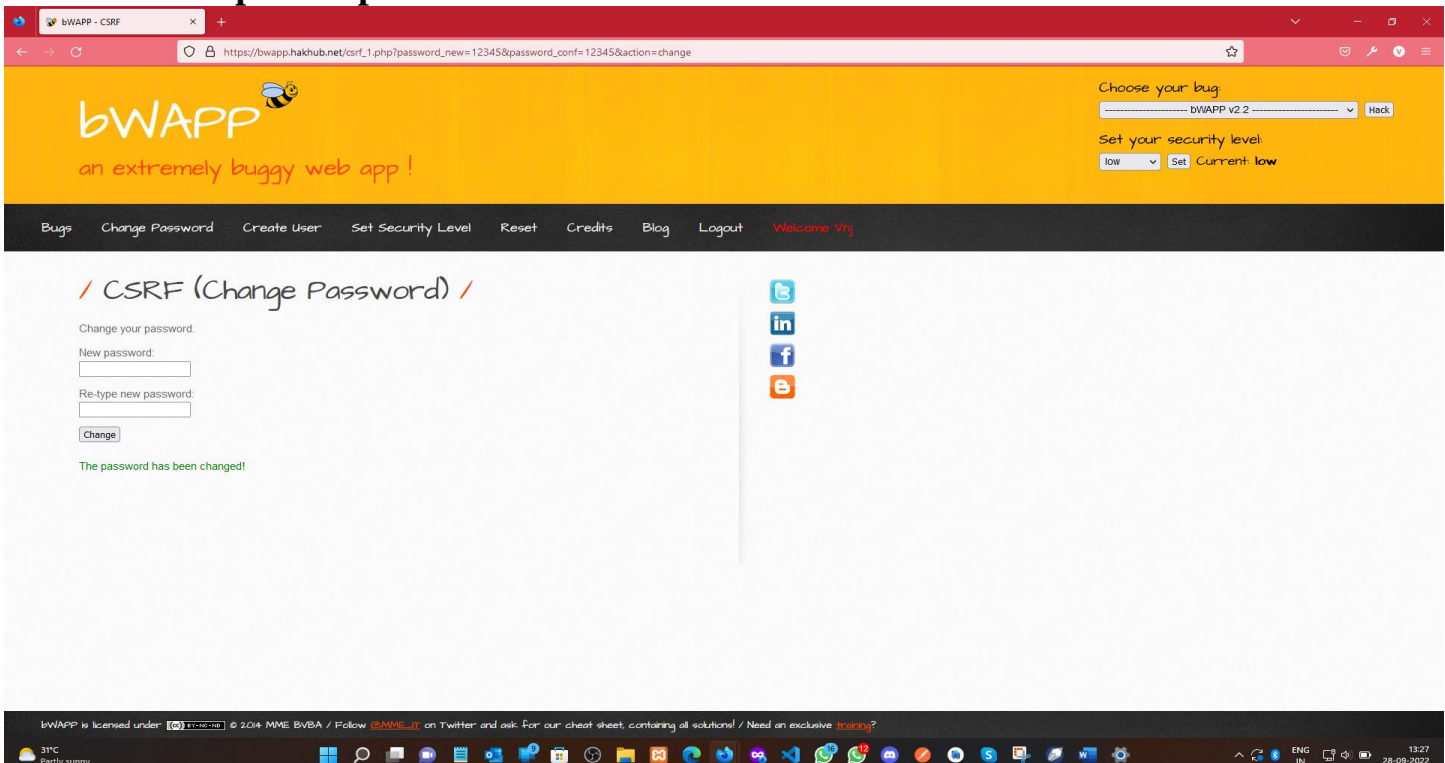
ENG IN 21:39 13-09-2022

2. Select the CSRF (Change password) *method*:



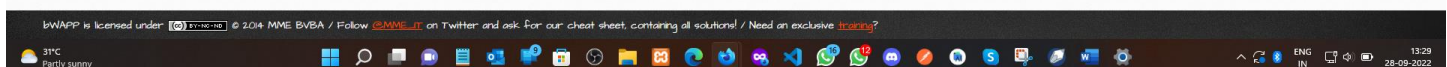
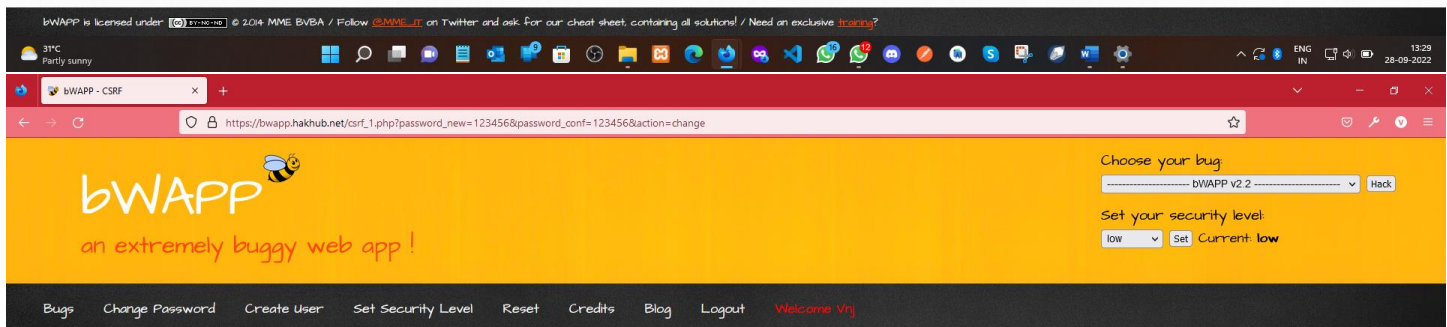
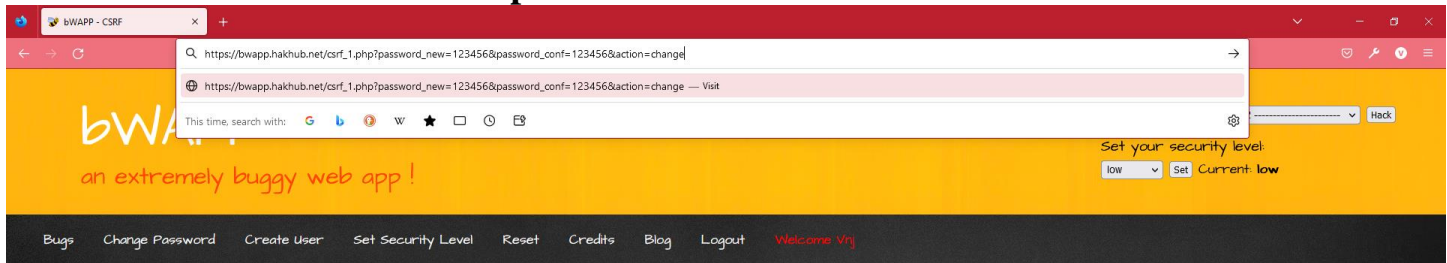
The screenshot shows the bWAPP - CSRF page in a web browser. The browser's address bar displays the URL https://bwapp.hakhub.net/csrf_1.php. The page has a yellow header with the bWAPP logo and the tagline "an extremely buggy web app!". On the right side of the header, there are two dropdown menus: "Choose your bug" (set to "bWAPP v2.2") and "Set your security level" (set to "low"). Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Vrij. The main content area is titled "/ CSRF (Change Password) /" and contains a form with the following fields: "Change your password.", "New password:", "Re-type new password:", and a "Change" button. To the right of the form are social media icons for Twitter, LinkedIn, Facebook, and Email. The footer of the page contains a license notice: "bWAPP is licensed under [CC BY-NC-SA] © 2014 MME BVBA / Follow @MME_BVBA on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive training?". The system tray at the bottom shows the date and time as 13:28 on 28-09-2022.

3. Give the Input the passwords and submit:



The screenshot shows the bWAPP - CSRF page after the password change. The browser's address bar displays the URL https://bwapp.hakhub.net/csrf_1.php?password_new=12345&password_conf=12345&action=change. The page layout is identical to the previous screenshot, but the "Change" button is now disabled. Below the form, a green message states: "The password has been changed!". The system tray at the bottom shows the date and time as 13:27 on 28-09-2022.

4. Edit the URL submitted password and Enter



5. Observations/Discussions/ Complexity Analysis:

In this Experiment we have learn about the Cross Site Request Forgery and how it works on our network and websites through URL.

Learning outcomes (What I have learnt):

We learn what is Cross Site Request Forgery. An overview of how these attacks is constructed and applied to real systems. If the app or website submit any request the Hacker doing their own changes in the Submitted URL and Modifying the User Password and Personal data.

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:	