**WORKSHEET 3:**

# Student Name: Sahul Kumar Parida UID: 20BCS4919

**Branch: CSE Section/Group - B**

**Semester: 5th Date of Performance: 11th Aug 2022 Subject Name: Web and Mobile Security Subject Code: 20CST-333**

**Aim:**

Working of CSRF (cross site request forgery) attack/ Vulnerability.

**Objective:**

To understand how to find CSRF Vulnerability.

**Software/Hardware Requirements:**

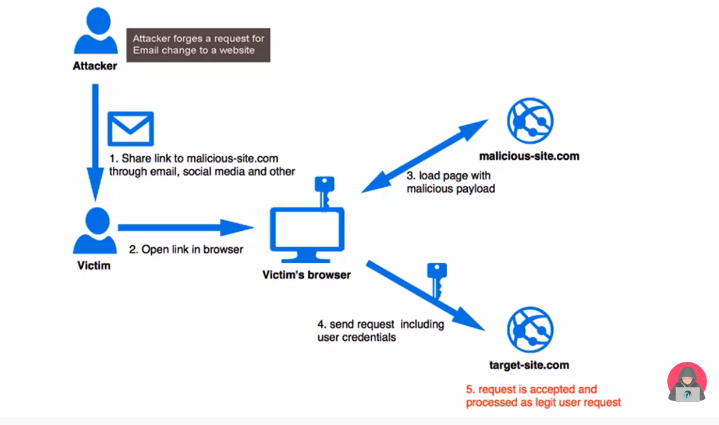
Windows 7 & above version, Kali Linux

**Tools to be used:**

DVWA**/**OWAPP website, Notepad, Burpsuite

**Discussion:**

CSRF: Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they’re currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker’s choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.



**Steps/Methods/Code:**

**CSRF attack on DVWA (Kali Linux)**

1. Firstly download oracle virtual box and install kali Linux**.**

Link to setup virtual box:[**https://www.youtube.com/watch?v=4OPfRVdKmGY**](https://www.youtube.com/watch?v=4OPfRVdKmGY)

Link to download kali Linux:[**http://old.kali.org/kali-images/kali-2017.1/**](http://old.kali.org/kali-images/kali-2017.1/)

1. Install Kali Linux in Oracle Virtual box. Check video for installation:

<https://www.youtube.com/watch?v=9ay_0dH5ZyA>

1. To perform CSRF attack, we can use various vulnerable websites like BWAPP, DVWA etc. After installing Linux, we have to install these vulnerable websites in Kali Linux to test CSRF vulnerabilities.
2. To install BWAPP in Kali Linux refer the link : <https://www.youtube.com/watch?v=b0Jf4vccmeE>

OR

To install DVWA in Kali Linux refer the link: (terminal commands)

<https://www.youtube.com/watch?v=PaB17Cc0dUg>

1. Now open DVWA on kali Linux browser and check csrf attack working. Follow the steps in this link: <https://youtu.be/Uzp64CNKSss>
2. Login DVWA with credentials: ‘admin’ as user name and ‘password’ as password. Choose CSRF attack from left hand side. ‘Change your admin password’ page will open there. If we insert new password in input field then it will run successfully. Login with new password after changing it and notice the behavior.
3. Save the URL after re-login. Goto Linux terminal and open editor.

Command: gedit

Paste URL here and save it with .txt file.

1. Go to DVWA website and right click to view source code. See the form tag code and copy it as it is. Paste it in editor and make some changes in code. Mandatory to add “value” field.

<form action: paste copied URL here

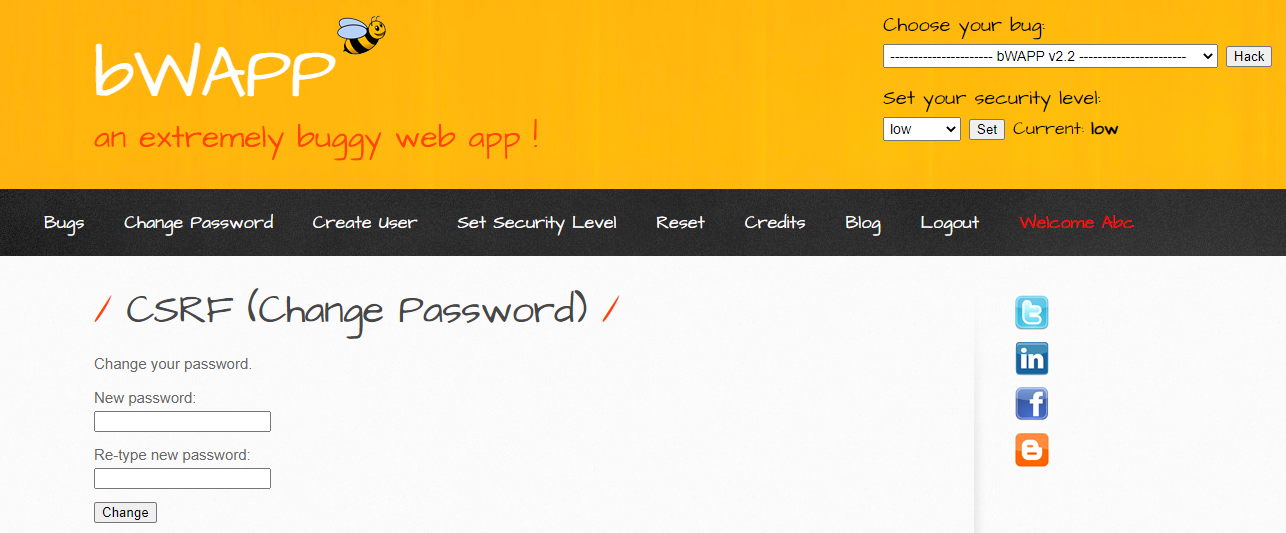
<p> Special Offer</p>

<input type=”hidden” AUTOCOMPLETE=”off” name=”password\_new” value=”hacked”>

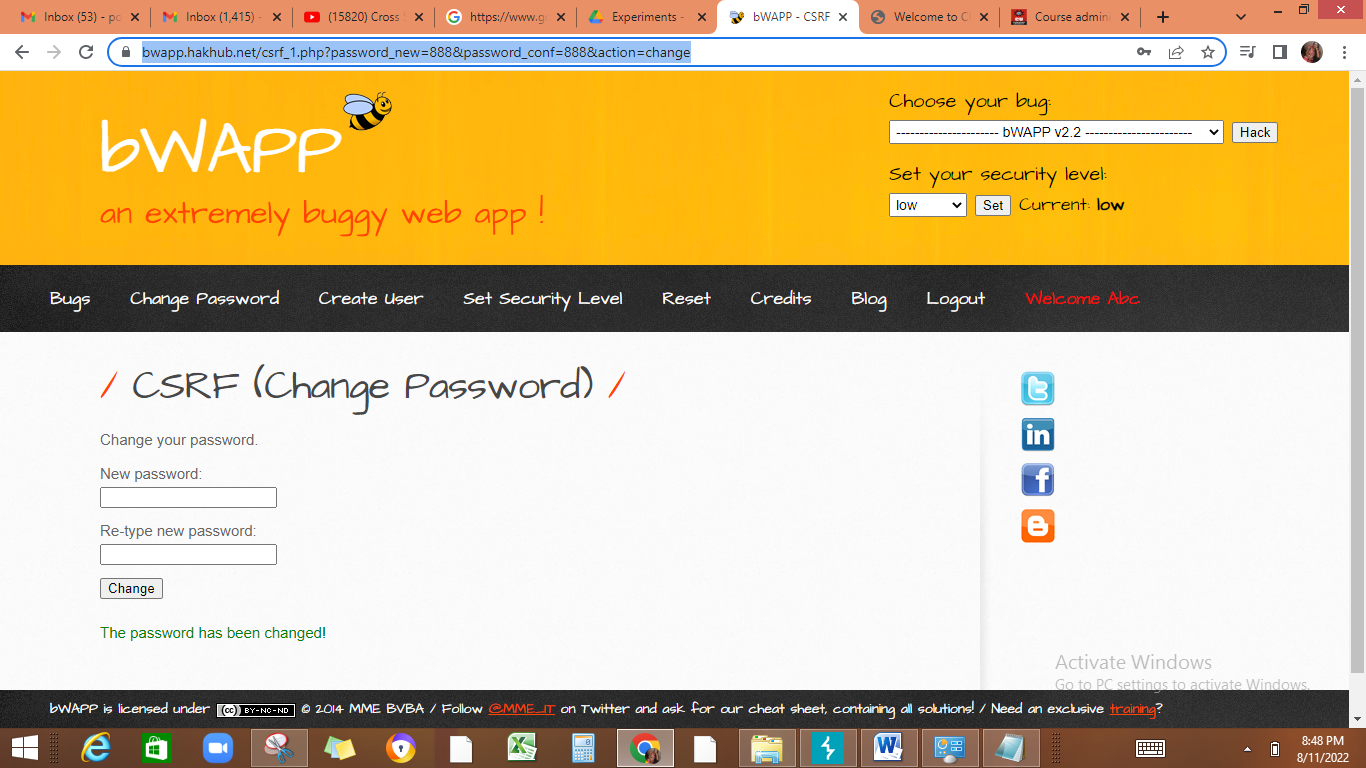
1. Save the file e.g. csrf.html. Types ls in Linux terminal to check whether file exists.
2. Open Firefox from terminal: Firefox csrf.html and you will see a button with name “change” on page. This link is considered malicious sent by some attacker. End user will click on this button/link then password will be changed with one that hacker has added into the code. This is possible when user is login to the website.

**CSRF on BWAPP:**

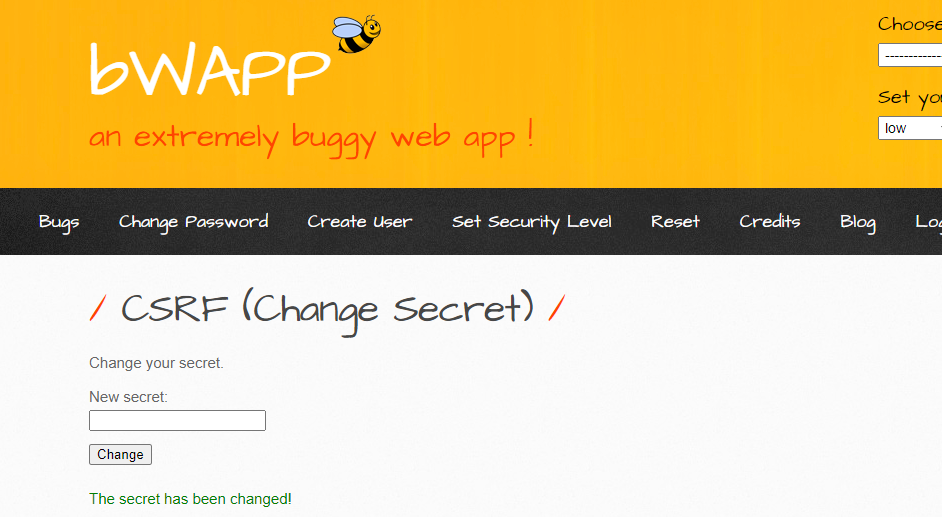
1. Open a website bwapp Login page. Login with credentials given. If not getting login then create new user with a temporary id and then re-login with new id.
2. Now choose “csrf-change password” category and click on hack. (GET Method)



1. Type new password and login again with new password. You will see message that password is changed. You can see the changed password parameters on URL also. Attacker can send the URL to victim and can have access to the password or even can change the password by changing in URL.



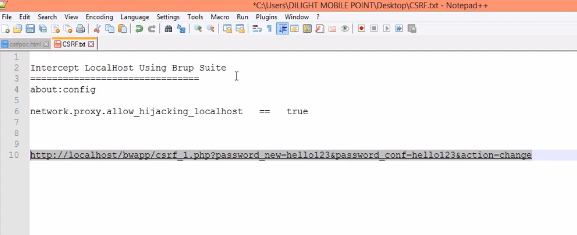
1. Paste URL in notepad, change the password in URL and then copy paste it in new tab. Page will get opened. Then login again with this new password. It will execute successfully.
2. Now choose another option CSRF-Change secret and click on Hack. This is POST based CSRF. Type new password and change it. Input not reflected in URL.



1. To exploit POST based CSRF, we will use burp suite tool. Configure our browser so that burp proxy can intercept local host.

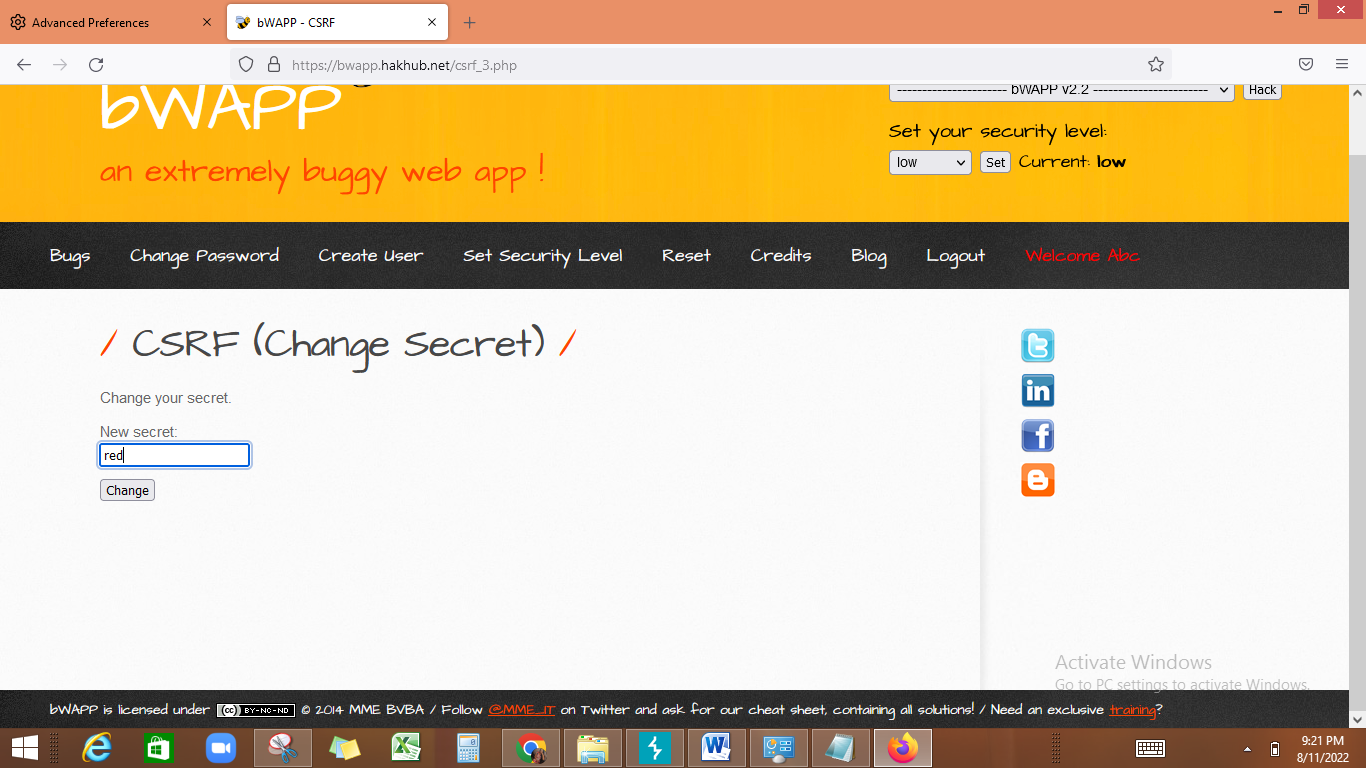
**Intercept LocalHost Using Brup Suite =============================== about:config**

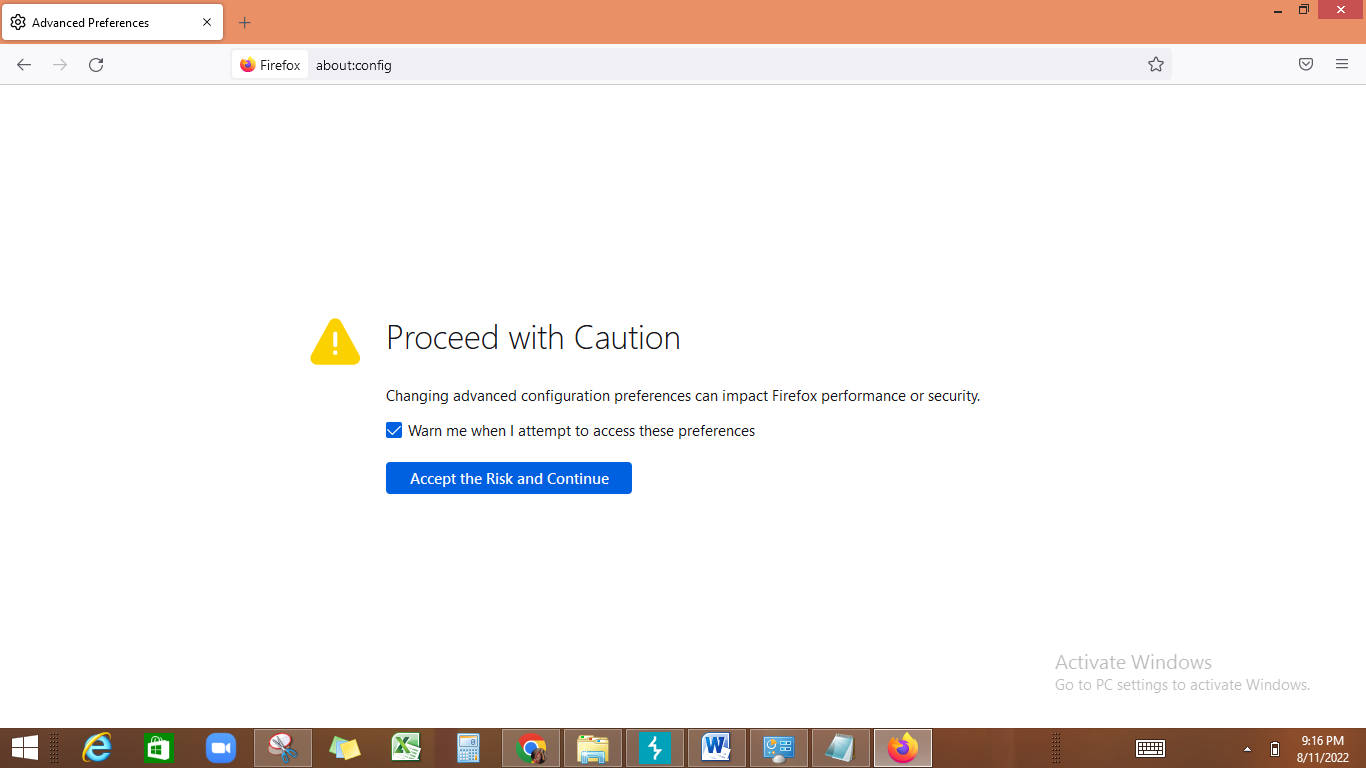
**network.proxy.allow\_hijacking\_localhost == true**

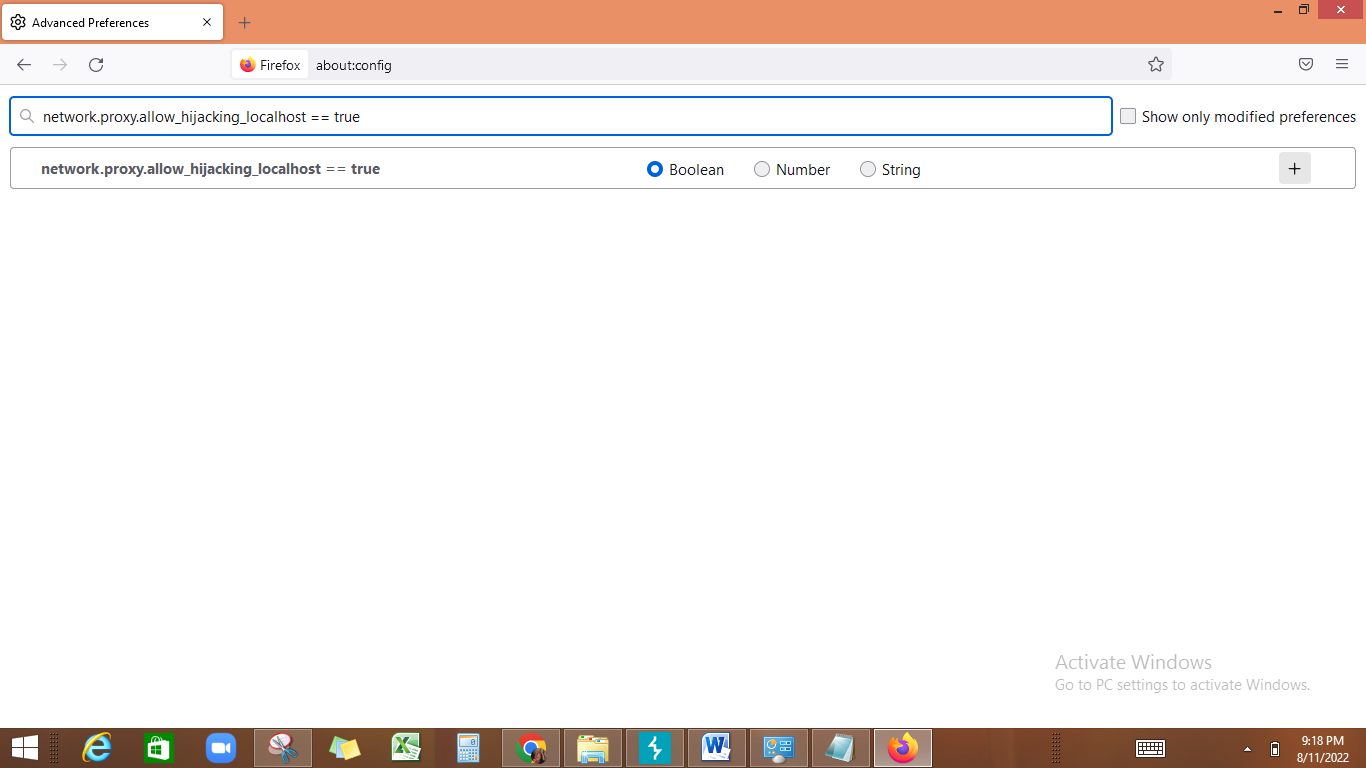


1. Copy and paste: about: config(shown in screenshot) in MOZILLA FIREFOX browser. Click on accept risk as shown in screenshot. Write **network.proxy.allow\_hijacking\_localhost** in search field. And make it true(double click). Then write any secret password in bwapp login and make **burpsuite intercept On** then click on change. Request will go to burpsuite tool.

Config burpsuite on Mozilla : <https://youtu.be/o3gsVWhacjk>







1. Login with changed secret in bwapp app. It will be run. You can use Burpsuite tool also to change the password change request. Check link for more detail.

<https://youtu.be/teVWDzDoWuI>

**Learning Outcome:**

When a website sends a data request to another website on behalf of a user along with the user’s session cookie, an attacker can launch a Cross-Site Request Forgery Attack, which abuses a trustful relationship between the victim’s browser and the webserver.