Date: 05-12-2020

Course: TY BCA

Enrollment No.: 201803100110002

Subject: 030010517 CC12 Software Testing Techniques

Set: A

Workbook 8

a. Write the steps to perform security testing using SQL Injection

Ans:

Step-1: Navigate to the SQL Injection area of the application.

Step-2: We use String SQL Injection to bypass authentication. Use SQL injection to log in as the boss ('Miloni') without using the correct password. Verify that Miloni's profile can be viewed and that all functions are available (including Search, Create, and Delete).

Step-3: We will Inject a SQL such that we are able to bypass the password by sending the parameter as 'a' = 'a'; or 1 = 1.

Step-4: Post Exploitation, we are able to login as Miloni who is the Admin.

b. Write the steps to perform Cross-site Scripting.

Ans:

Step-1: Login to Webgoat and navigate to cross-site scripting (XSS) Section. Let us execute a Stored Cross-site Scripting (XSS) attack.

Step-2: Let us login as Miloni with password 'miloni'. Click 'view profile' and get into edit mode. Since tom is the attacker, let us inject Java script into those edit boxes.

<script>
Alert ("HACKED")
</script>

Step-3: As soon as the update is over, tom receives an alert box with the message "hacked" which means that the app is vulnerable.
Step-4: We need to login as jerry (HR) and check if jerry is affected by the injected script.
Step-5: After logging in as Mili, select 'Miloni' and click 'view profile'.
Step-6: This message box is just an example, but the actual attacker can perform much more than just displaying a message box.

Test Case	URL	YES/NO	Opinion about the site [Secured/ Not Secured]
c. Try to directly access bookmarked web page without login to the system.	https://www.flipkart.com/	No, one cannot directly access bookmarks without login.	Secured
d. Verify that system should restrict you to download the file without sign in on the system.	https://www.flipkart.com/	Yes, system restricts user.	Secured
e. Verify that previous accessed pages should not accessible after log out i.e. Sign out and then press the Back button to access the page accessed before.	https://www.flipkart.com/	No, does not provide access after logout.	Secured
f. Check the valid and invalid passwords; password rules say cannot be less than 6	https://www.flipkart.com/	No such validations applied.	Not Secured

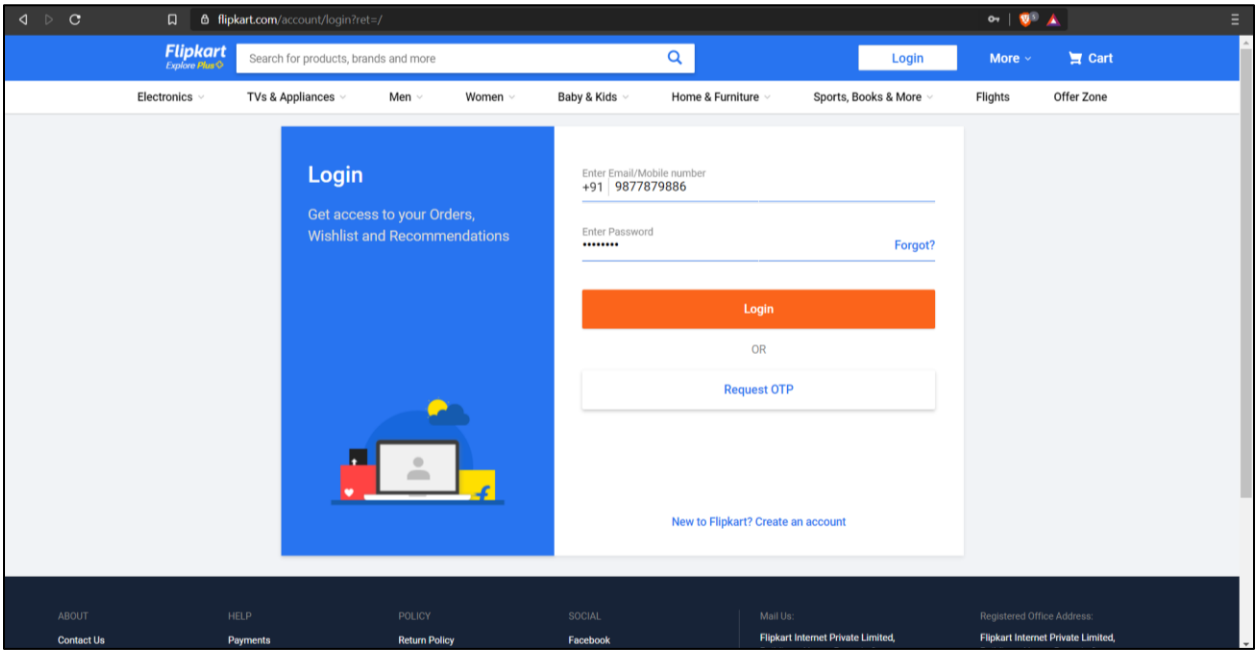
characters, user id and password cannot be the same etc.			
g. Verified that important i.e. sensitive information such as passwords, ID numbers, credit card numbers, etc. should not get displayed in the input box when typing. They should be encrypted and in asterix format.	https://www.flipkart.com/	Yes	Secured
h. Check that bookmarking disabled on secure pages? Bookmarking should be disabled on secure pages.	https://www.flipkart.com/	No, it's not disabled.	Not Secured
i. Check that Right Click, View, Source disabled? Source code should not be visible to user.	https://www.flipkart.com/	Not disabled	Not Secured
j. Is there an alternative way to access secure pages for browsers under lower versions, where SSL is not compatible with those browsers?	https://www.flipkart.com/	No	Secured

k. Check does your server lock out an individual who has tried to access the site multiple times with invalid login/password information?	https://www.flipkart.com/	No	Not Secured
l. Verify the timeout condition, after timeout user should not able to navigate through the site.	https://www.flipkart.com/	Yes	Secured
m. Check that the application prevents the user from doing direct searches by editing content in the URL?	https://www.flipkart.com/	No, it does not prevent.	Not Secured
n. Verify that relevant information should be written to the log files and that information should be traceable.	https://www.flipkart.com/	Yes	Secured
o. In SSL verify that the encryption is done correctly and check the integrity of the information.	https://www.flipkart.com/	Yes	Secured
p. Verify that restricted page	https://www.flipkart.com/	Yes	Secured

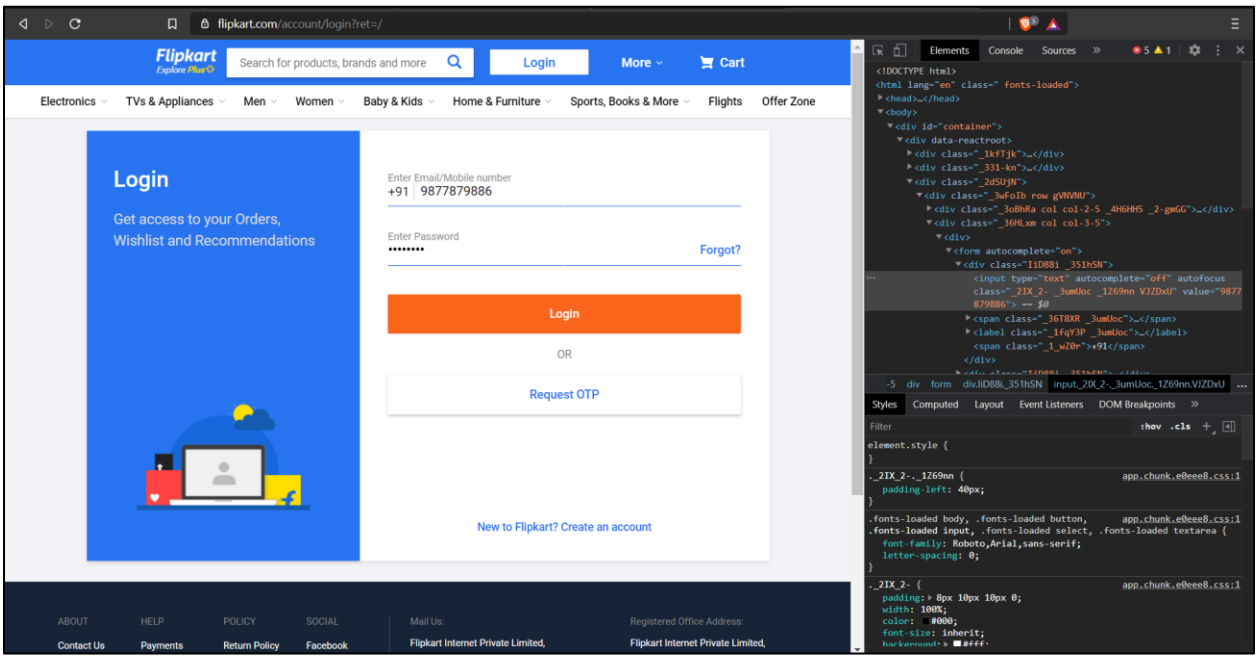
should not be accessible by user after session time out.			
q. ID / password authentication, the same account on different machines cannot log on at the same time. So, at a time only one user can login to the system with a user id.	https://www.flipkart.com/	Yes	Secured
r. ID / password authentication methods entered the wrong password several times and check if the account gets locked.	https://www.flipkart.com/	Yes	Secured
s. Add or modify important information (passwords, ID numbers, credit card number, etc.). Check if it gets reflected immediately or caching the old values.	https://www.flipkart.com/	Yes	Secured

➢ Screenshots:

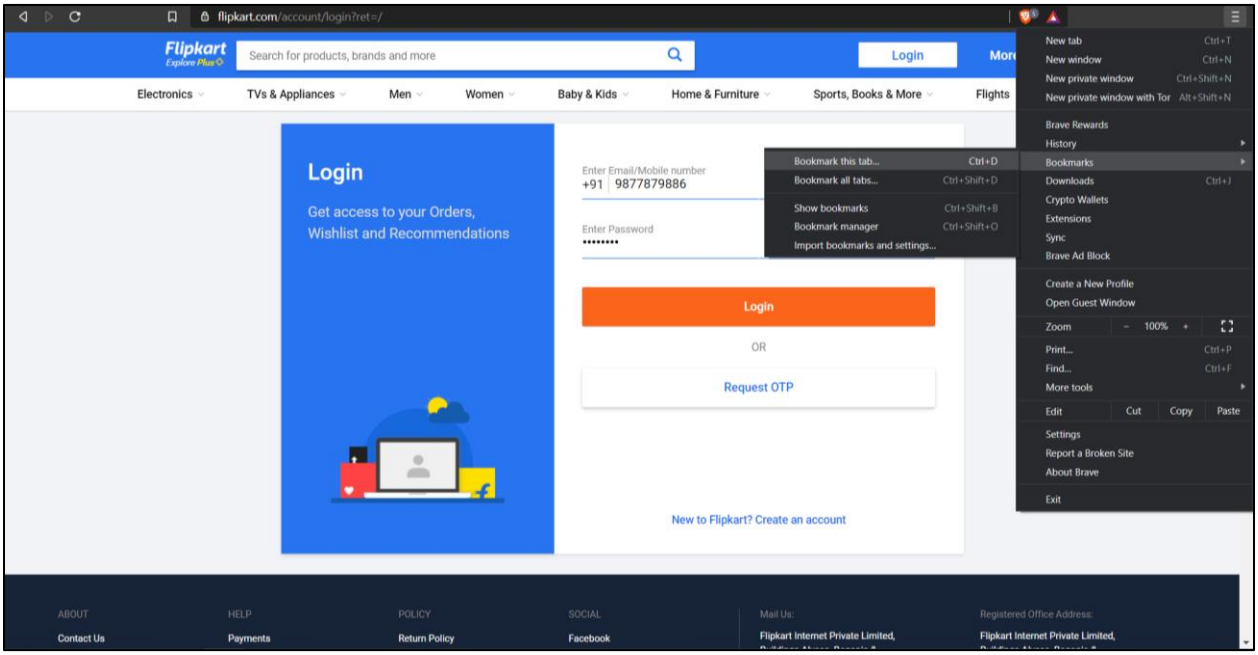
1. Login Page:



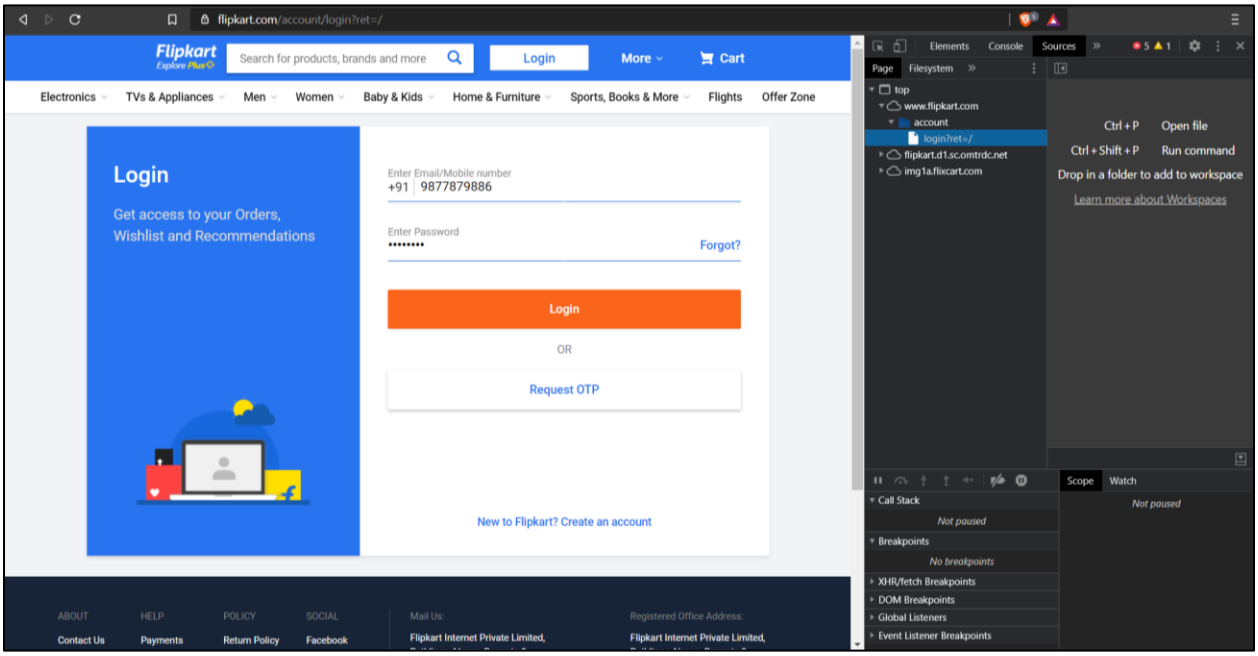
2. Page Code available



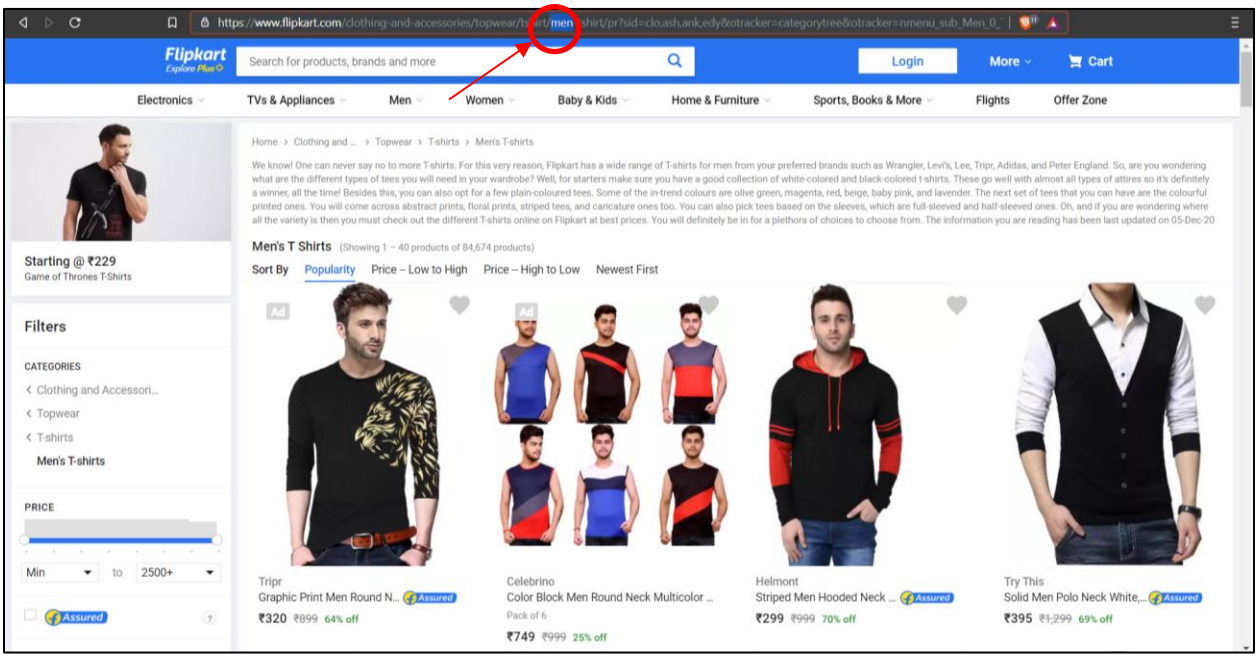
3. Bookmark available



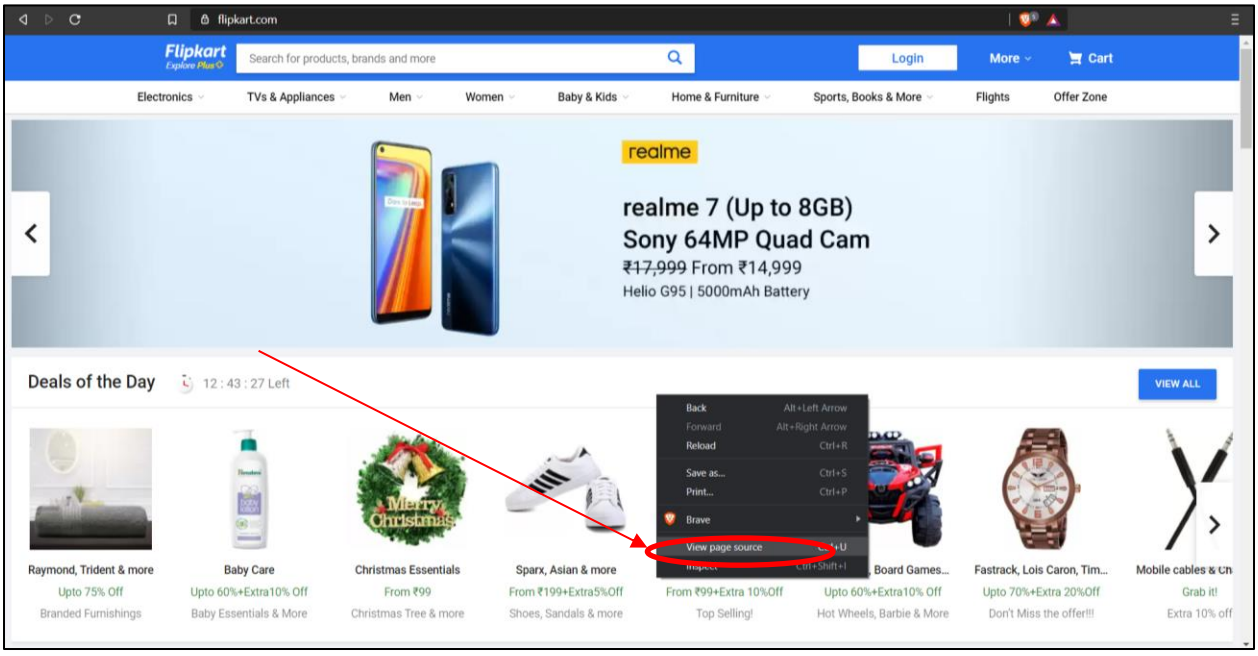
4. Page Source available



5. URL query modification and search possible



6. View Page Source option available on secured site



➢ Enhance your learning:

1. Enlist any two-security testing approaches other than XSS and SQL injection.

Ans:

- Injection flaws
- Broken Authentication

2. What is Cookie Testing?

Ans: Cookie Testing is defined as a Software Testing type that checks Cookie created in your web browser. A cookie is a small piece of information that is stored in a text file on user's (client) hard drive by the web server.

3. Where are the Cookies stored? Can different browsers share same cookies?

Ans:

When any web page application writes a cookie, it gets saved in a text file on

user hard disk drive. The path where the cookies get stored depends upon

the browser. Different browsers store a cookie in different paths.

4. Can one domain access another's domains cookies?

Ans:

The 2 domains mydomain.com and subdomain.mydomain.com can only

share cookies if the domain is explicitly named in the Set-Cookie header.

Otherwise, the scope of the cookie is restricted to the request host.

5. Which cookies can be tested and which are not?

Ans:

- The name of the server the cookie was sent from.
- The lifetime of the cookie.
- A value - usually a randomly generated unique number.

6. **For applications where payments are involved, which payment field(s) is/are never stored in the cookie even not in the encrypted form?**

Ans: CVV Number field is never stored in the cookie even not in the encrypted form.