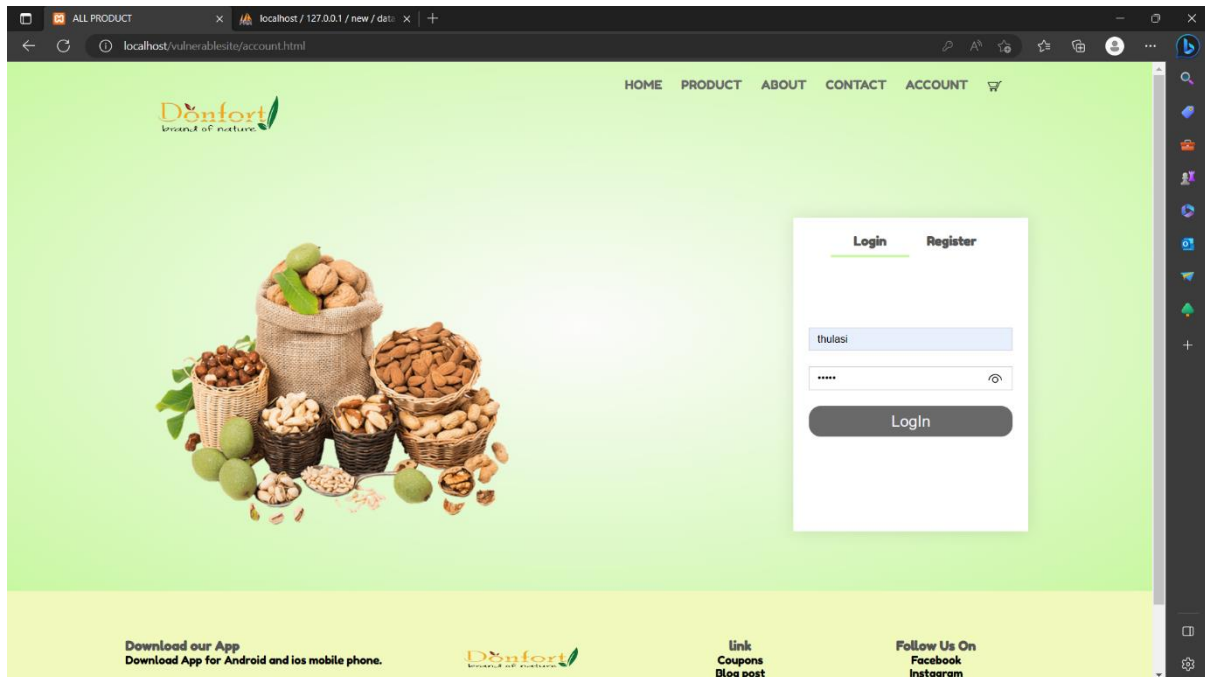
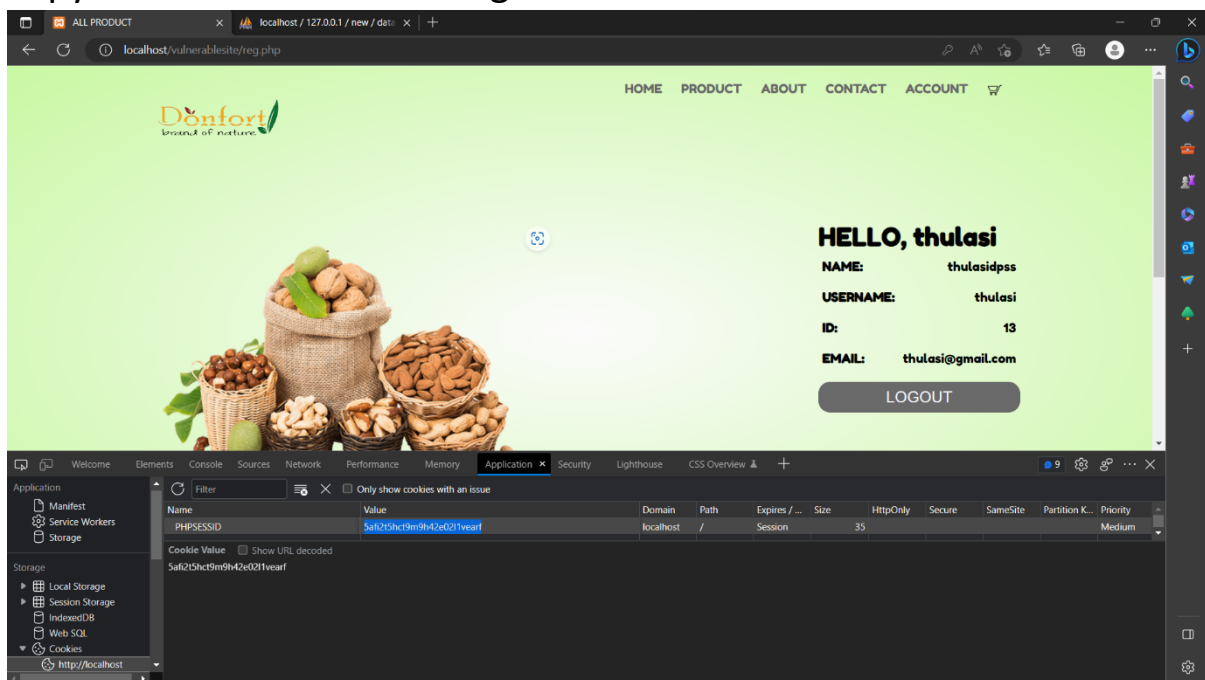


SESSION-HIJACKING:

STEP 1: just login with user details in account.html



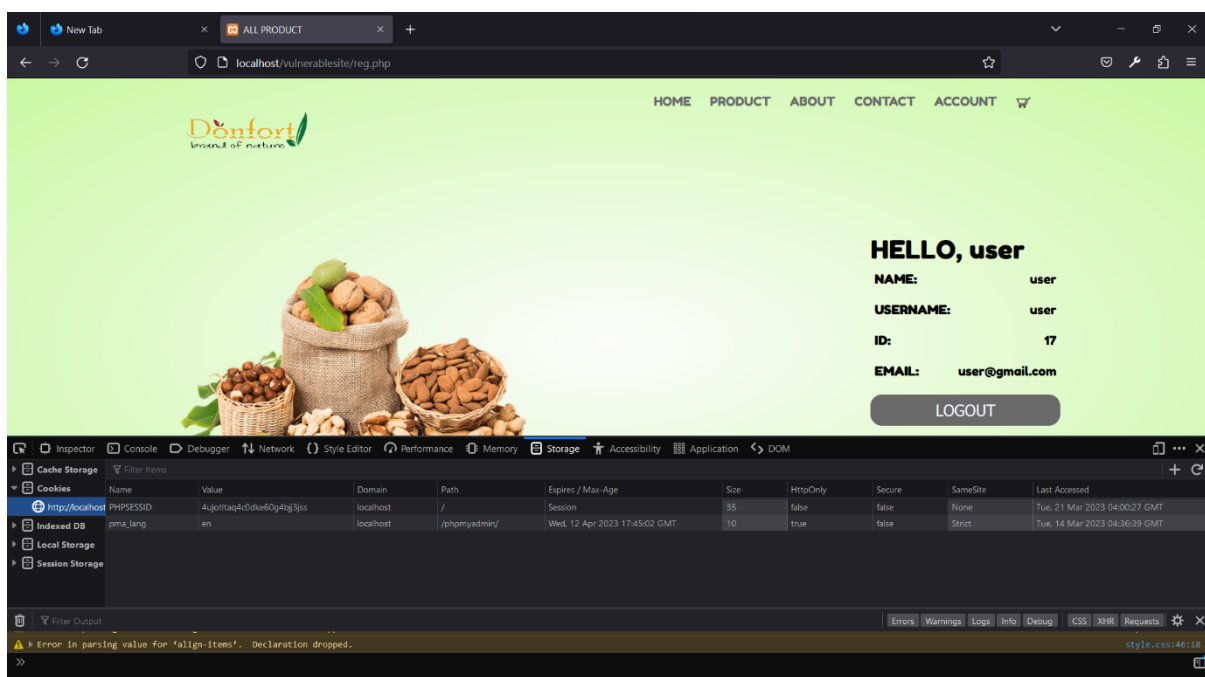
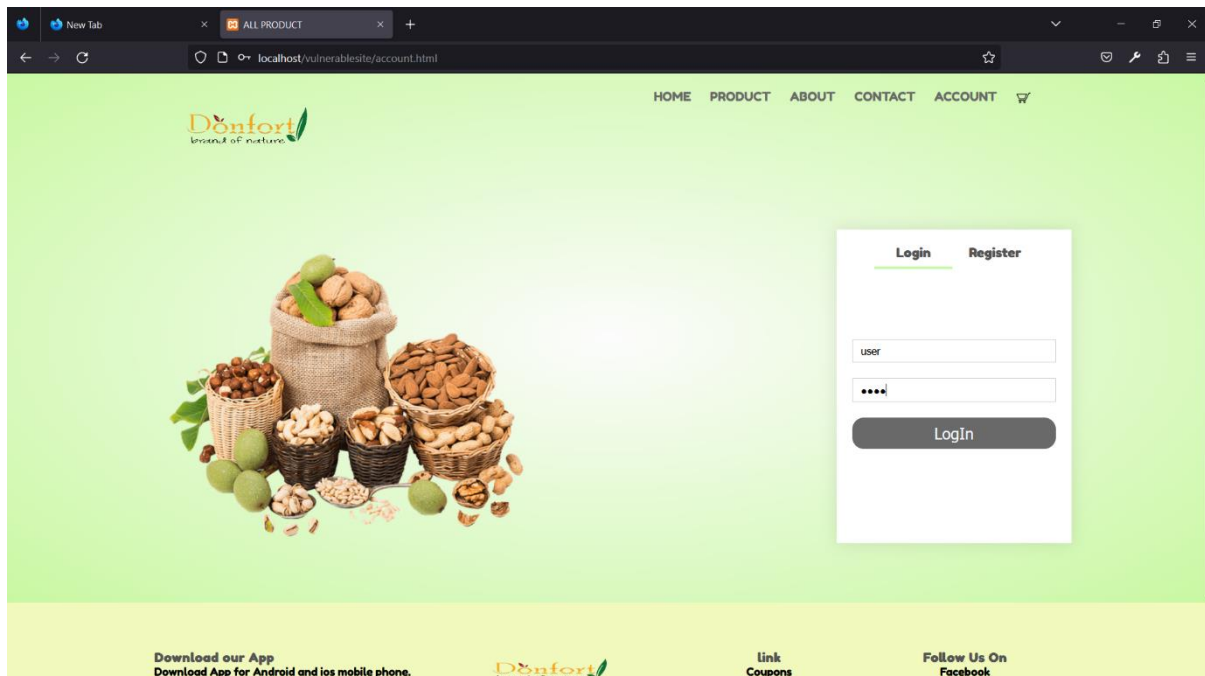
STEP 2: inspect into the site goto > application>cookies and make copy of session value and logout



STEP 3: open another web site and do login with different user details

And inspect into site and now past the copy value in this new value

And press F5




New Tab

ALL PRODUCT

localhost/vulnerablesite/reg.php

Donfort
brand of nature

HOMEPRODUCTABOUTCONTACTACCOUNT



HELLO, user

NAME:

user

USERNAME:

user

ID:

17

EMAIL:

user@gmail.com

LOGOUT

InspectorConsoleDebuggerNetworkStyle EditorPerformanceMemoryStorageAccessibilityApplicationDOM

Cache Storage

Indexed DB

Local Storage

Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	5af215hct9m9h42e021v...	localhost	/	Session	35	false	false	None	Tue, 21 Mar 2023 04:01:54 ...
pma_lang	en	localhost	/phpmyad...	Wed, 12 Apr 2023 17:45:02 ...	10	true	false	Strict	Tue, 14 Mar 2023 04:36:39 ...

Filter values

Data

PHPSESSID: "5af215hct9m9h42e021vearf"
Created: "Tue, 21 Mar 2023 03:30:41 GMT"
Domain: "localhost"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Tue, 21 Mar 2023 04:01:54 GMT"
Path: "/"

Filter Output

Error in parsing value for 'animation'. Declaration dropped.

blank.html:575:19


New Tab

ALL PRODUCT

localhost/vulnerablesite/reg.php

Donfort
brand of nature

HOMEPRODUCTABOUTCONTACTACCOUNT



HELLO, thulasi

NAME:

thulasidpss

USERNAME:

thulasi

ID:

13

EMAIL:

thulasi@gmail.com

LOGOUT

InspectorConsoleDebuggerNetworkStyle EditorPerformanceMemoryStorageAccessibilityApplicationDOM

Cache Storage

Indexed DB

Local Storage

Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	5af215hct9m9h42e021vearf	localhost	/	Session	35	false	false	None	Tue, 21 Mar 2023 04:01:54 GMT
pma_lang	en	localhost	/phpmyadmin/	Wed, 12 Apr 2023 17:45:02 GMT	10	true	false	Strict	Tue, 14 Mar 2023 04:36:39 GMT

Filter values

Data

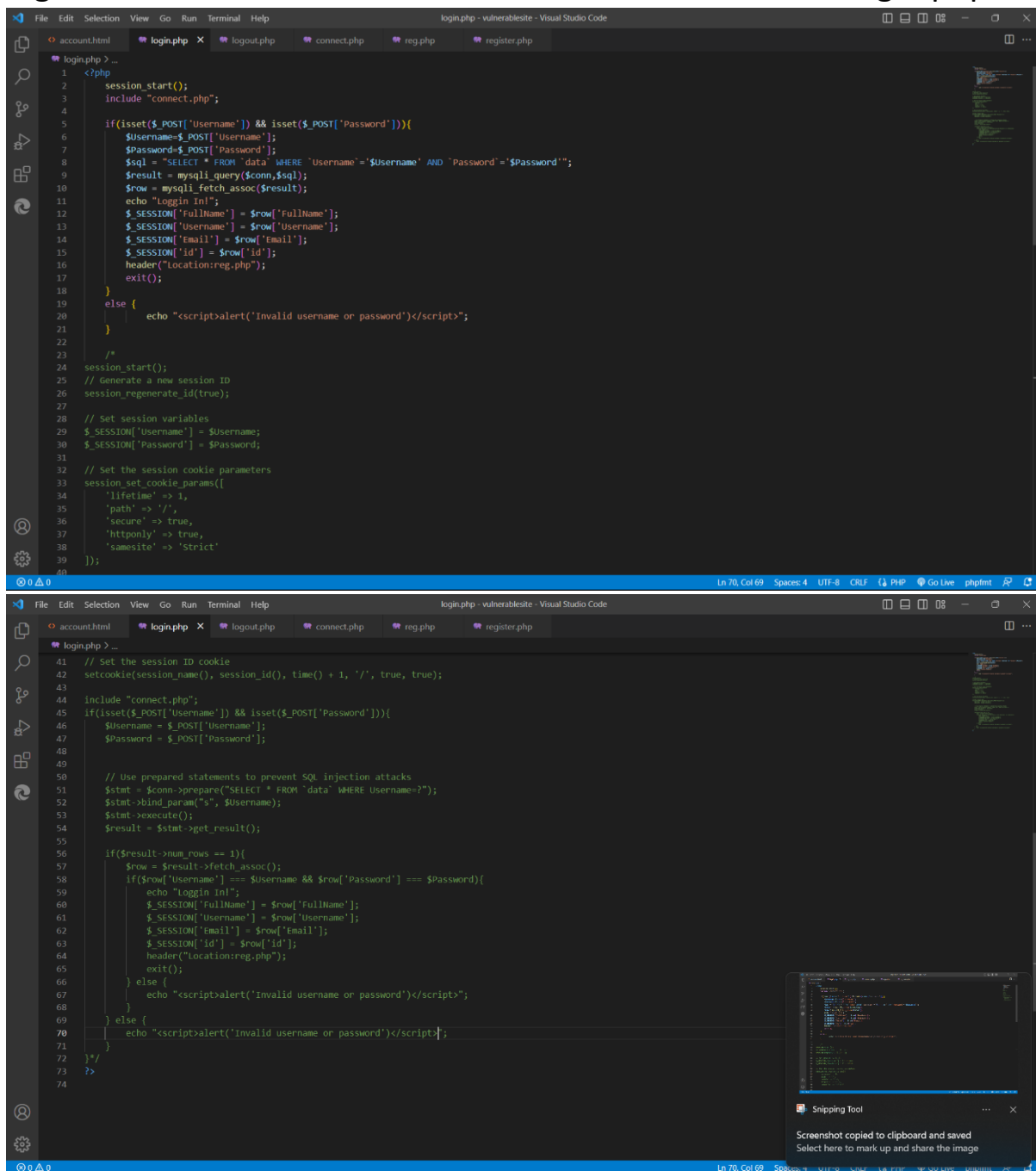
PHPSESSID: "5af215hct9m9h42e021vearf"
Created: "Tue, 21 Mar 2023 03:30:41 GMT"
Domain: "localhost"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Tue, 21 Mar 2023 04:01:54 GMT"
Path: "/"

Filter Output

Error in parsing value for 'align-items'. Declaration dropped.

style.css:46:18

STEP 4: to prevent session hijack just use `session_regenerater_id(true)`. This will regenerate every time when login uncommand line 24 to 72 and command 2 to 21 in login.php



```
login.php > ...
1  <?php
2  session_start();
3  include "connect.php";
4
5  if(isset($_POST['Username']) && isset($_POST['Password'])){
6      $Username = $_POST['Username'];
7      $Password = $_POST['Password'];
8      $sql = "SELECT * FROM 'data' WHERE 'Username'='$Username' AND 'Password'='$Password'";
9      $result = mysqli_query($conn,$sql);
10     $row = mysqli_fetch_assoc($result);
11     echo "Login In!";
12     $_SESSION['FullName'] = $row['FullName'];
13     $_SESSION['Username'] = $row['Username'];
14     $_SESSION['Email'] = $row['Email'];
15     $_SESSION['id'] = $row['id'];
16     header("Location:reg.php");
17     exit();
18 }
19 else {
20     echo "<script>alert('Invalid username or password')</script>";
21 }
22
23 /*
24 session_start();
25 // Generate a new session ID
26 session_regenerater_id(true);
27
28 // Set session variables
29 $_SESSION['Username'] = $Username;
30 $_SESSION['Password'] = $Password;
31
32 // Set the session cookie parameters
33 session_set_cookie_params([
34     'lifetime' => 1,
35     'path' => '/',
36     'secure' => true,
37     'httponly' => true,
38     'samesite' => 'strict'
39 ]);
40
41 // Set the session ID cookie
42 setcookie(session_name(), session_id(), time() + 1, '/', true, true);
43
44 include "connect.php";
45 if(isset($_POST['Username']) && isset($_POST['Password'])){
46     $Username = $_POST['Username'];
47     $Password = $_POST['Password'];
48
49
50     // Use prepared statements to prevent SQL injection attacks
51     $stmt = $conn->prepare("SELECT * FROM 'data' WHERE Username=?");
52     $stmt->bind_param("s", $Username);
53     $stmt->execute();
54     $result = $stmt->get_result();
55
56     if($result->num_rows == 1){
57         $row = $result->fetch_assoc();
58         if($row['Username'] == $Username && $row['Password'] == $Password){
59             echo "Login In!";
60             $_SESSION['FullName'] = $row['FullName'];
61             $_SESSION['Username'] = $row['Username'];
62             $_SESSION['Email'] = $row['Email'];
63             $_SESSION['id'] = $row['id'];
64             header("Location:reg.php");
65             exit();
66         } else {
67             echo "<script>alert('Invalid username or password')</script>";
68         }
69     } else {
70         echo "<script>alert('invalid username or password')</script>";
71     }
72 }
73 }
74
```

STEP 5:now do again step1 to step3

This time you can notice the change in value

The image displays two screenshots of a web browser showing the Donfort website's login and registration process.

Top Screenshot (Login Page):

- URL: `localhost/vulnerable/site/account.html`
- Page Title: ALL PRODUCT
- Navigation: HOME, PRODUCT, ABOUT, CONTACT, ACCOUNT
- Form: Login / Register. Username: `thulasi`. Password: `*****`. Button: Login.
- Application Panel: Cookies. Table with columns: Name, Value, Domain, Path, Expires / ... , Size, HttpOnly, Secure, SameSite, Partition K..., Priority.

Bottom Screenshot (Registration Page):

- URL: `localhost/vulnerable/site/reg.php`
- Page Title: ALL PRODUCT
- Navigation: HOME, PRODUCT, ABOUT, CONTACT, ACCOUNT
- Message: **HELLO, thulasi**
- User Details: NAME: `thulasiidpss`, USERNAME: `thulasi`, ID: `13`, EMAIL: `thulasi@gmail.com`. Button: LOGOUT.
- Application Panel: Cookies. Table with columns: Name, Value, Domain, Path, Expires / ... , Size, HttpOnly, Secure, SameSite, Partition K..., Priority.

ALL PRODUCT localhost / 127.0.0.1 / new / dat... x | +

localhost/vulnerablesite/account.html

Donfort brand of nature

HOME PRODUCT ABOUT CONTACT ACCOUNT

Login Register

thulasi

.....

Login

Application

Filter

Only show cookies with an issue

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition K...	Priority
PHPSESSID	ks2f8dtpitbm2hmcl087jtk26	localhost	/	Session	35					Medium

Select a cookie to preview its value

ALL PRODUCT localhost / 127.0.0.1 / new / dat... x | +

localhost/vulnerablesite/reg.php

Donfort brand of nature

HOME PRODUCT ABOUT CONTACT ACCOUNT

HELLO, thulasi

NAME: thulasi dpss

USERNAME: thulasi

ID: 13

EMAIL: thulasi@gmail.com

LOGOUT

Application

Filter

Only show cookies with an issue

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition K...	Priority
PHPSESSID	21rc8fa43r6k6bhhspcnajbhnc	localhost	/	Session	35					Medium

Select a cookie to preview its value