

XSS:

Step 1 : `<script>location.href=https://google.com</script>` just enter this script to fullname field in register and click register

Donfort
brand of nature

HOME PRODUCT ABOUT CONTACT ACCOUNT

Login Register

`<script>location.href=https://google.com</script>`

admin

admin@gmail.com

Register

Download our App
Download App for Android and ios mobile phone.

GET IT ON
Google Play

Download on the
App Store

Our purpose to sustainably make the pleasure
and Benefits of Healthy products

link
Coupons
Blog post
Feedback
Join Affiliate

Follow Us On
Facebook
Instagram
Twitter
Youtube

Check in database you can see the script in fullname field

Showing rows 0 - 2 (3 total, Query took 0.0002 seconds.)

SELECT * FROM `data`

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Extra options

				id	Username	Email	Password	FullName
<input type="checkbox"/>	Edit	Copy	Delete	13	thulasi	thulasi@gmail.com	12345	thulasidpss
<input type="checkbox"/>	Edit	Copy	Delete	14	ajith	ajith@gmail.com	qwerty	ajith
<input type="checkbox"/>	Edit	Copy	Delete	15	admin	admin@gmail.com	admin	<code><script>location.href=https://google.com</script></code>

Check all | With selected: Edit Copy Delete Export

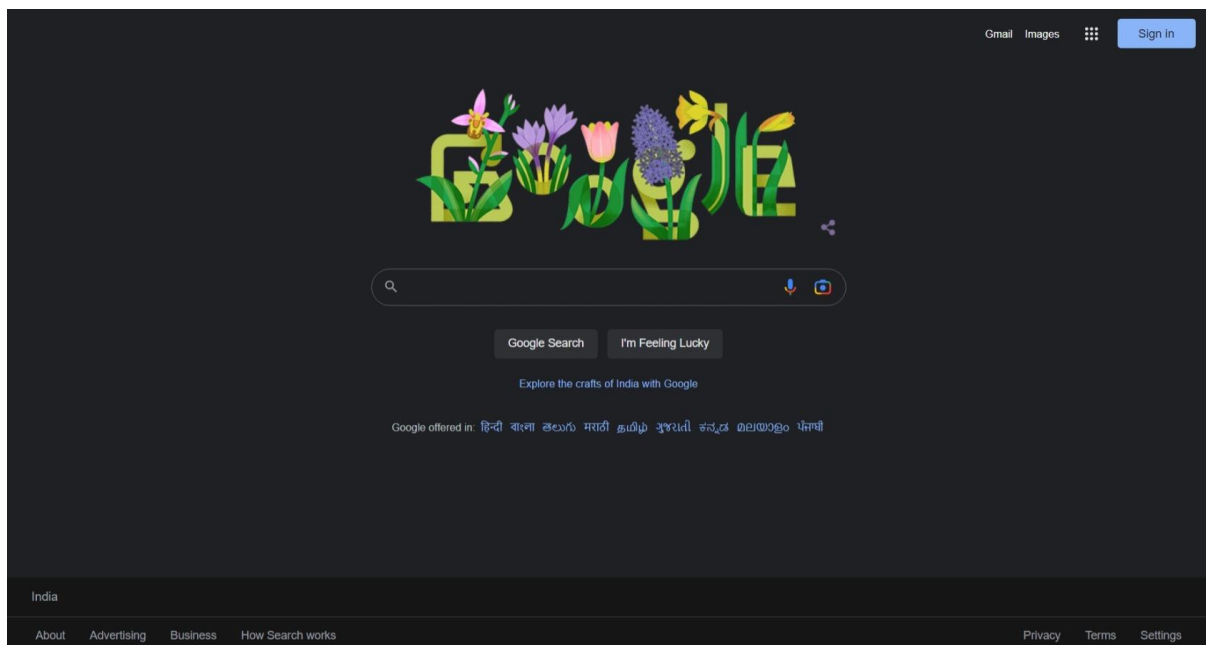
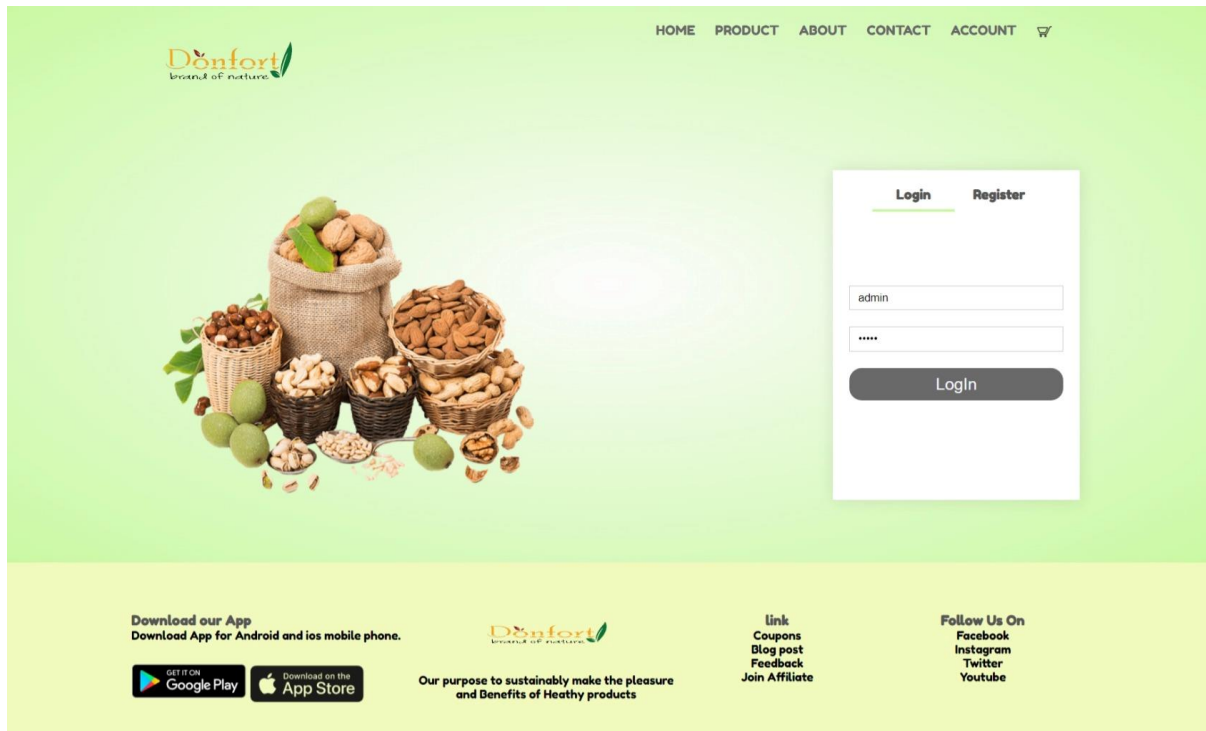
Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Query results operations

Print Copy to clipboard Export Display chart Create view

Step 2 : now login to the username and password which is you create before .

It will redirect to www.google.com

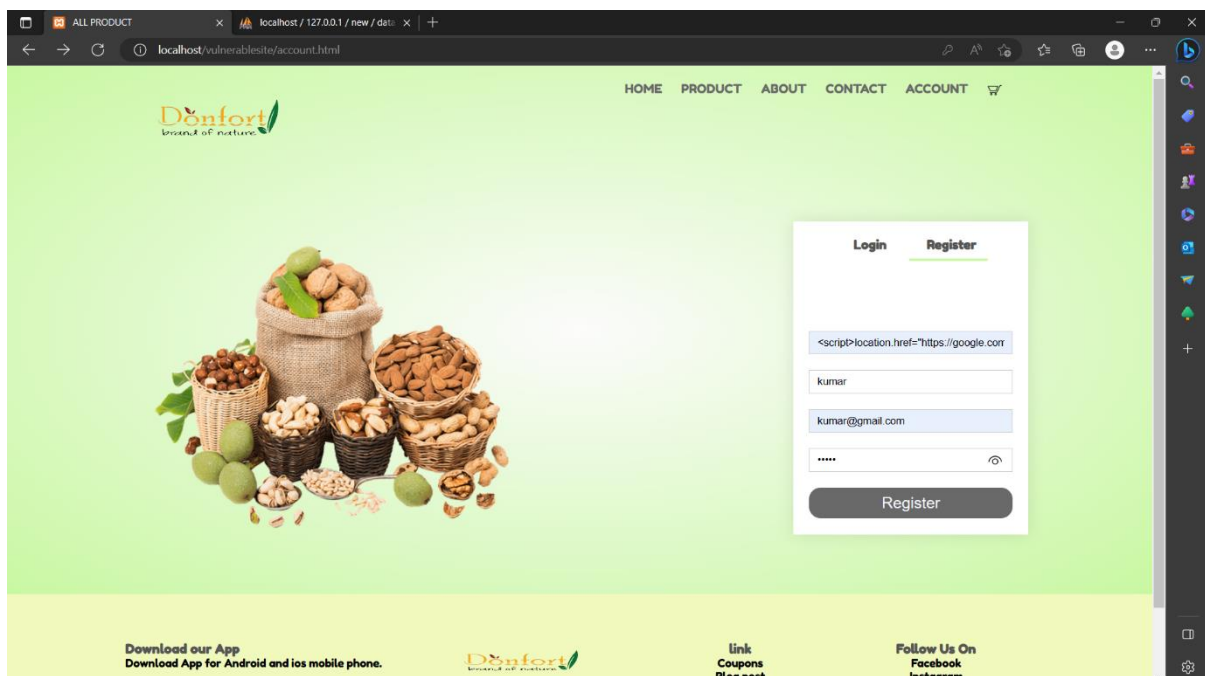


Step 3 : to prevent this use htmlspecialchars()

Just uncommand line 9 in register.php

```
1 <?php
2 if($_SERVER['REQUEST_METHOD']=='POST' && isset($_POST['submit'])){
3     $conn=mysqli_connect('localhost', 'root', '', 'new') or die("Connection Failed:".mysqli_connect_error());
4     if(isset($_POST['Username']) && isset($_POST['Email']) && isset($_POST['Password'])){
5         $FullName=$_POST['FullName'];
6         $Username=$_POST['Username'];
7         $Email=$_POST['Email'];
8         $Password=$_POST['Password'];
9         /*$FullName=htmlspecialchars($FullName);*/
10        $sql="INSERT INTO `data` (`FullName`,`Username`,`Email`,`Password`) VALUES ('$FullName','$Username','$Email','$Password')";
11
12        $query = mysqli_query($conn,$sql);
13        if($query){
14            header('Location: account.html');
15        }
16        else{
17            echo'Error Occurred';
18        }
19    }
20 }
21 ?>
```

Step 4 :repeat step 1 again with new register details



Showing rows 0 - 3 (4 total, Query took 0.0002 seconds)

SELECT * FROM `data`

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Extra options

		id	Username	Email	Password	FullName
<input type="checkbox"/>	Edit Copy Delete	13	thulasi	thulasi@gmail.com	12345	thulasidpss
<input type="checkbox"/>	Edit Copy Delete	14	ajith	ajith@gmail.com	qwerty	ajith
<input type="checkbox"/>	Edit Copy Delete	15	admin	admin@gmail.com	admin	<script>location.href="https://google.com"</script>...
<input type="checkbox"/>	Edit Copy Delete	16	kumar	kumar@gmail.com	kumar	<script>location.href="https://google.c...

Check all | With selected: Edit Copy Delete Export

Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None


Query results operations

Print Copy to clipboard Export Display chart Create view

Console

Step 5 : now log in with user name and password

localhost / vulnerablesite / account.html



Login Register

kumar

Login

Download our App
Download App for Android and ios mobile phone.

GET IT ON Google Play Download on the App Store

Our purpose to sustainably make the pleasure and Benefits of Healthy products

Link Coupons Blog post Feedback Join Affiliate

Follow Us On Facebook Instagram Twitter Youtube

