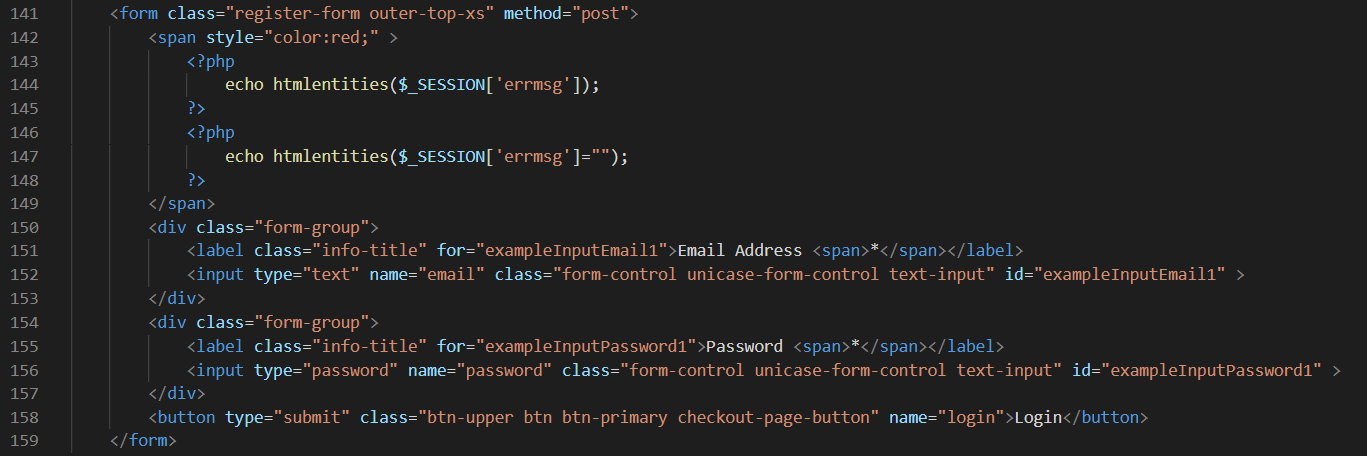
Parallel comparison of two sites, one unprotected and the other protected against **SQL INJECTION, XSS,** and **CSRF** hacking methods

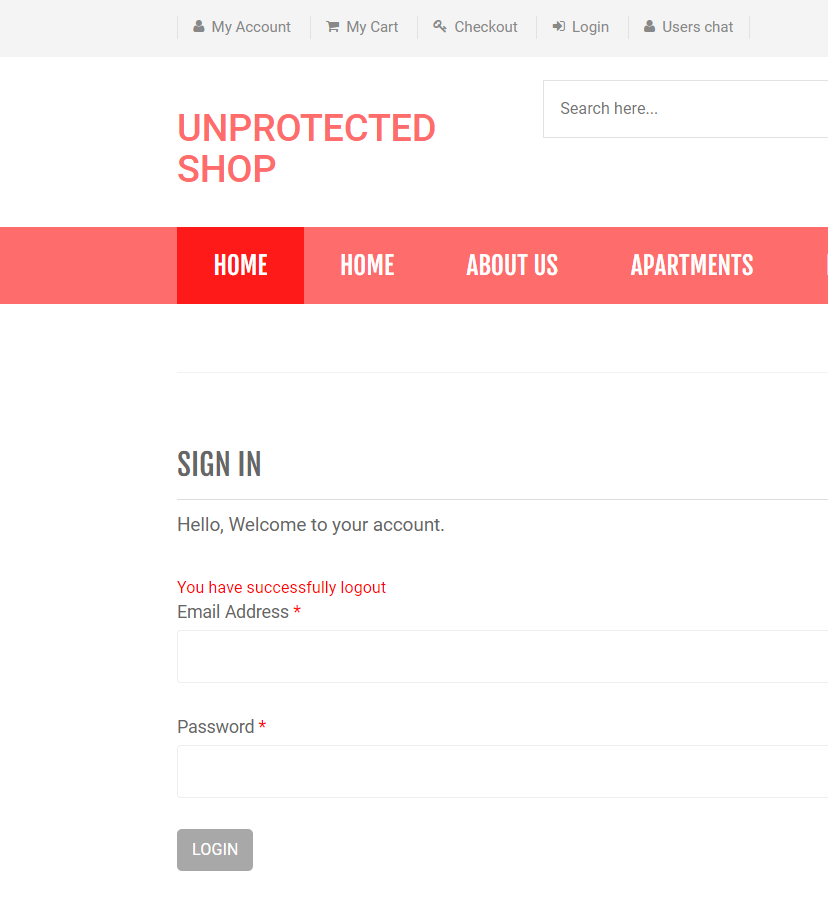
unprotectedshop – unprotected site

protectedshop – protected site

**SQL INJECTION**

Unprotectedshop – login.php 

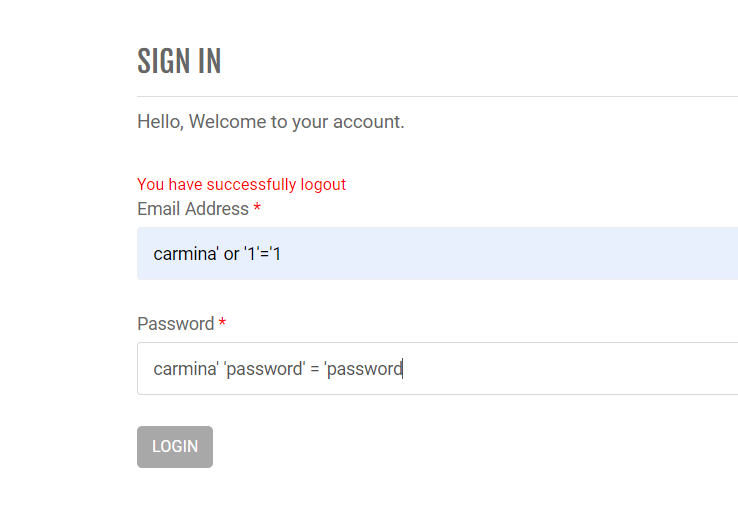
**Code of form to login in unprotected shop site**



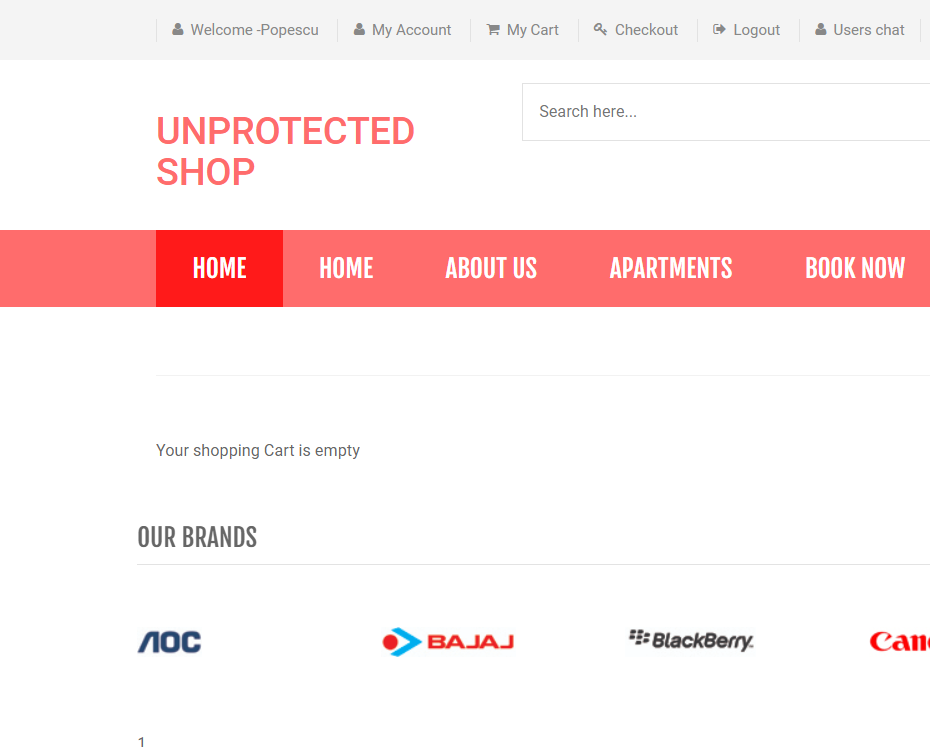
**Form to login in unprotected shop site**



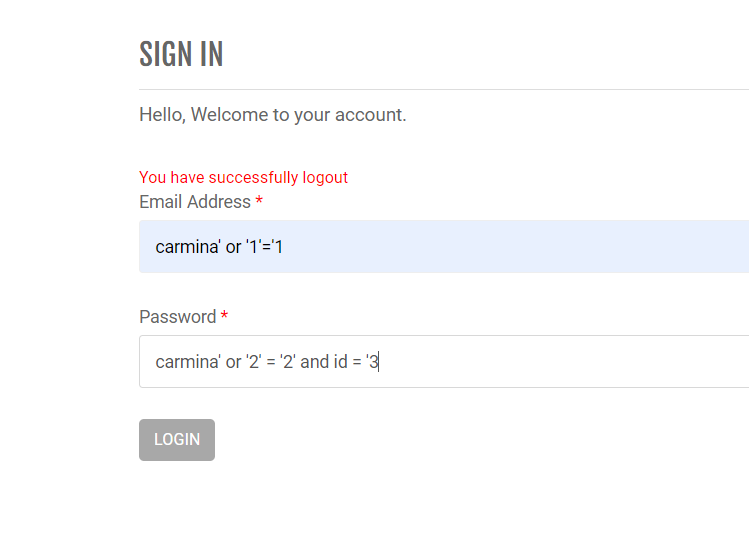
**Code for login**



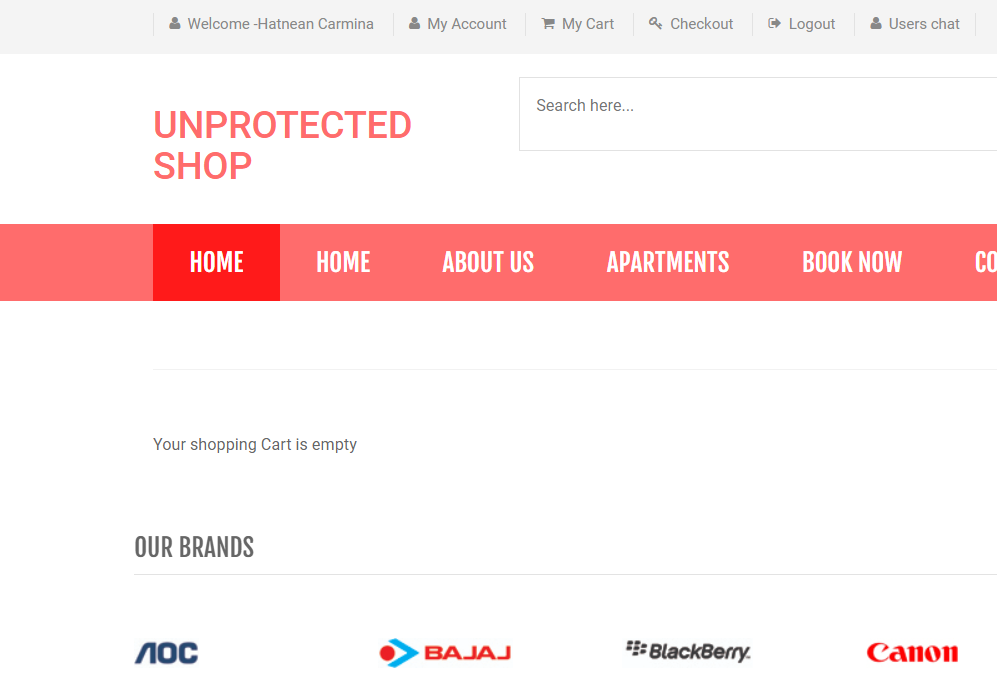
**The entry code in the account of the first user in the database**



**First user logged**

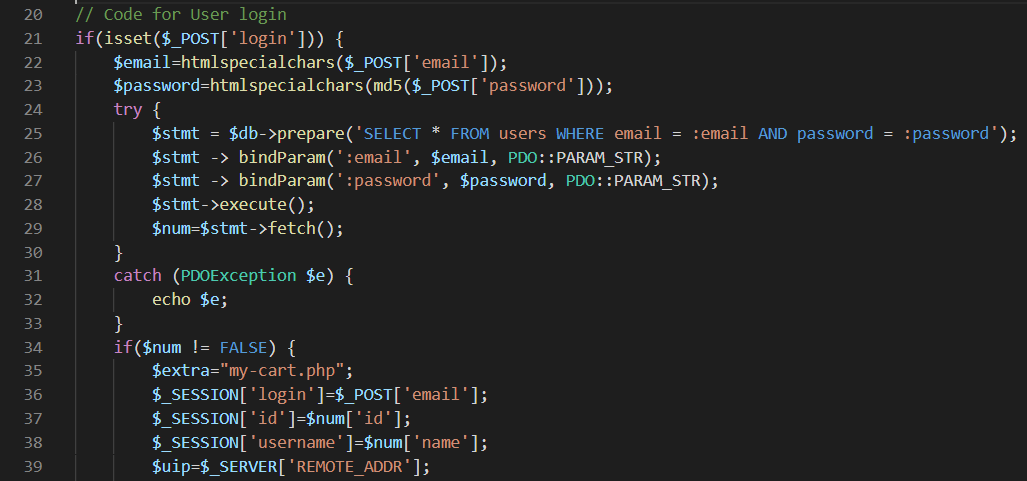
****

**The entry code in the account of the n-th user in the database**

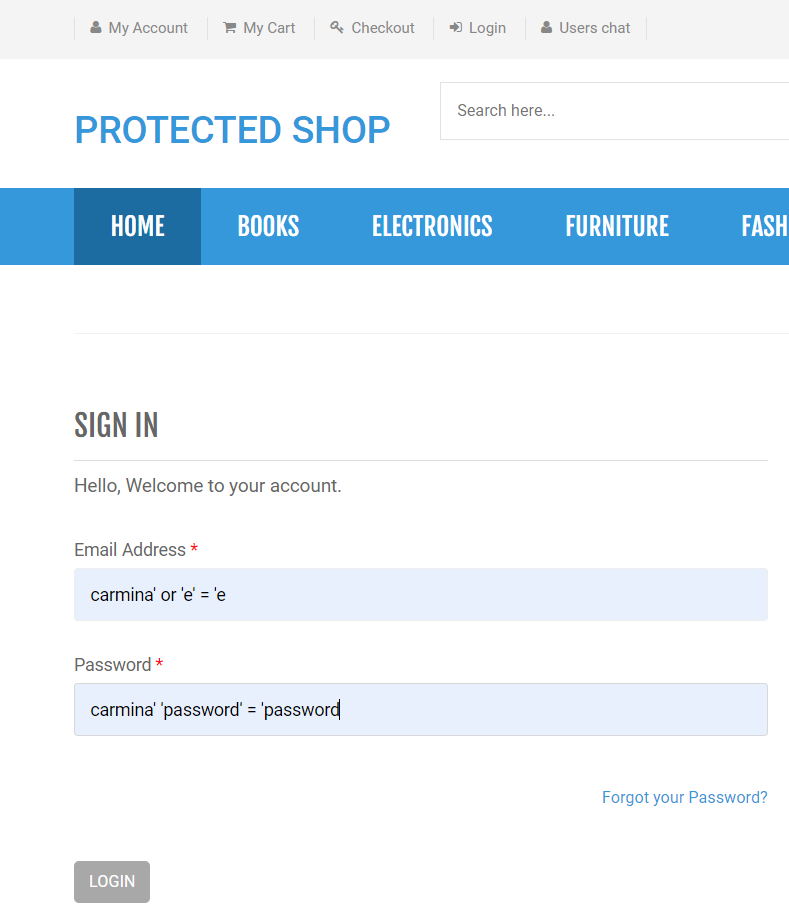
****

**N-th user logged**

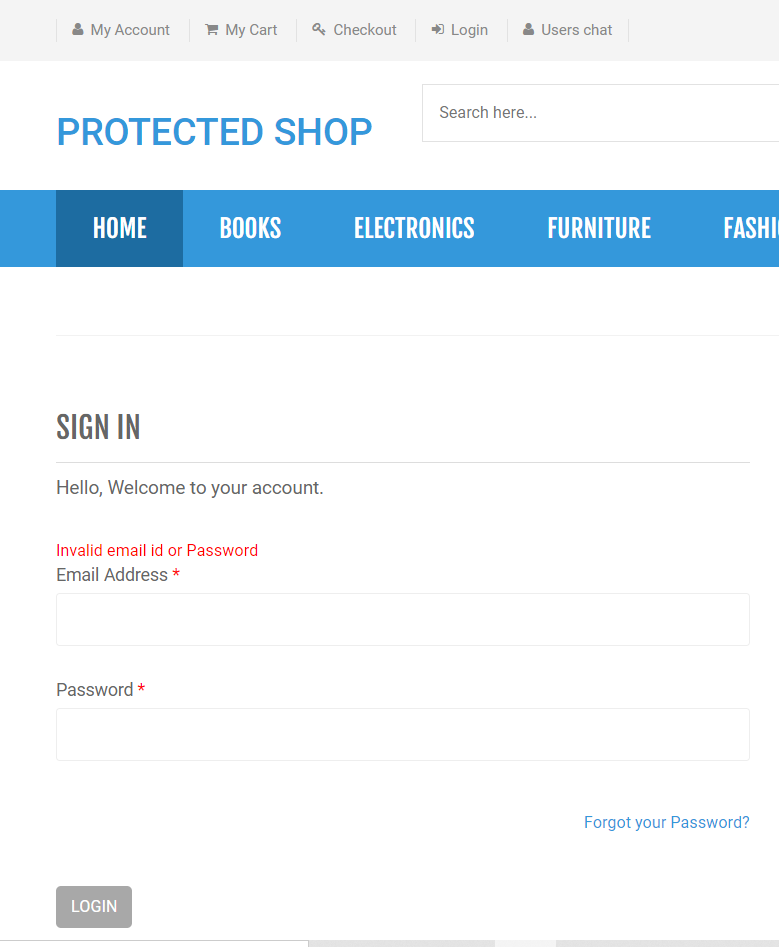
Protectedshop – login.php

****

**Password encryption code and method of using bind parameters**



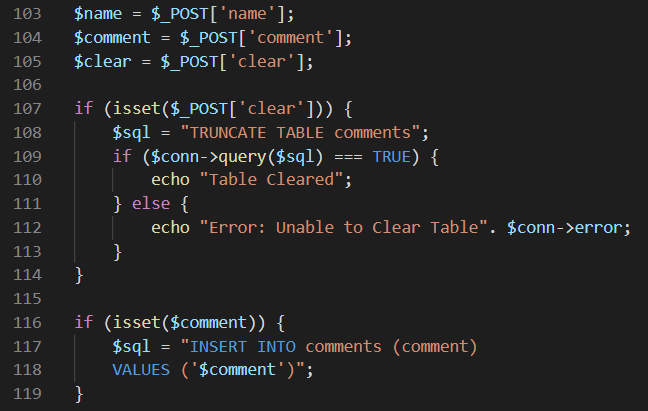
**Malitious code for entering into on account from database**



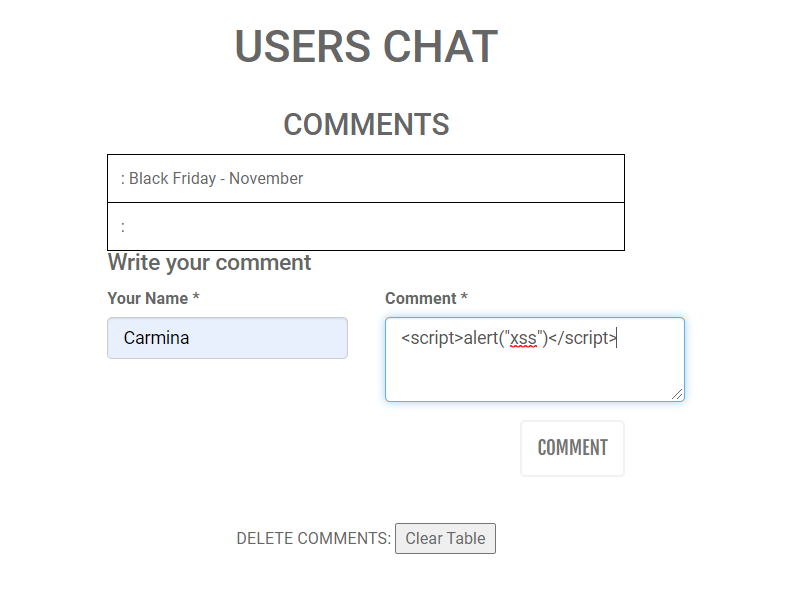
**Query unchanged**

# XSS - Cross Site Scripting

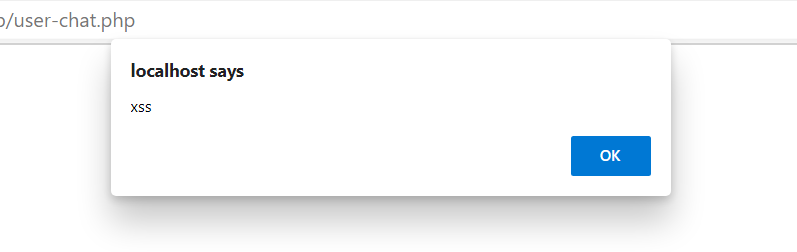
Unprotectedshop – user-chat.php



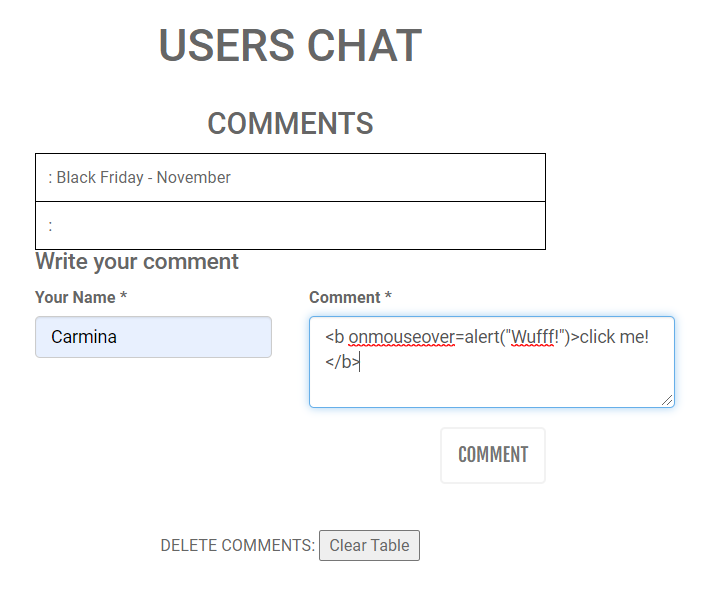
**Code for entering comments into database**

****

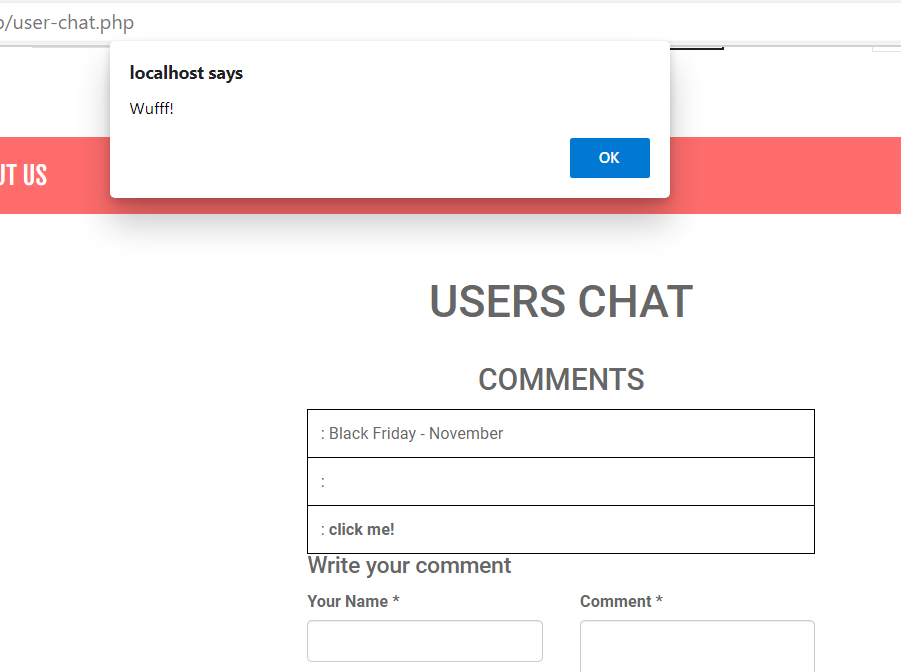
**<script>alert(“xss”)</script>**

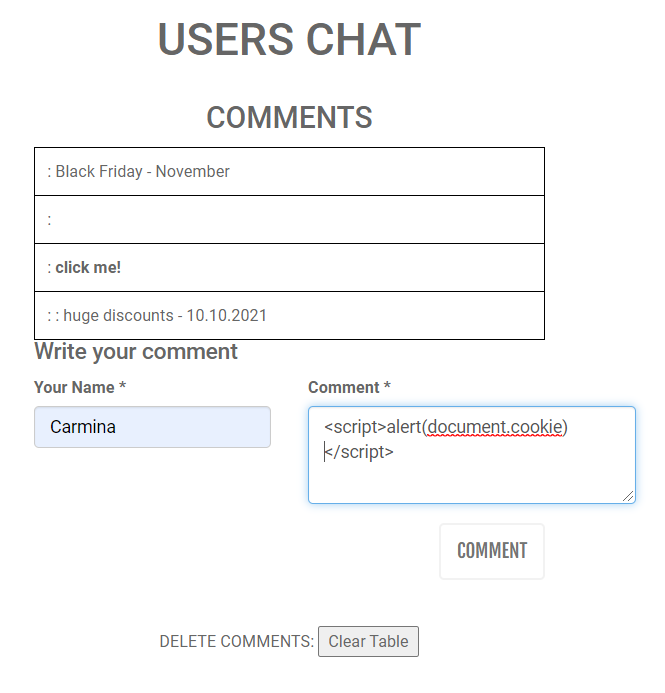
****

**The result of accessing the page in the future**

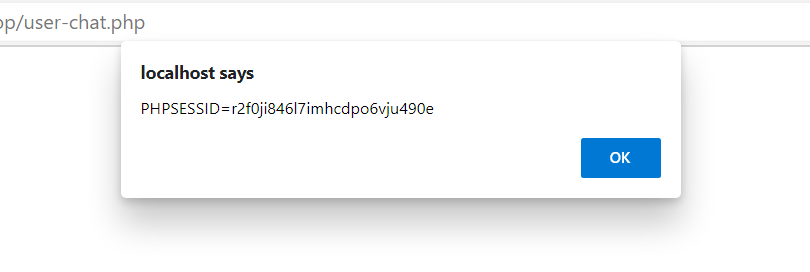
****

**<b onmouseover=alert(“Wufff!”)>click me!</b>**

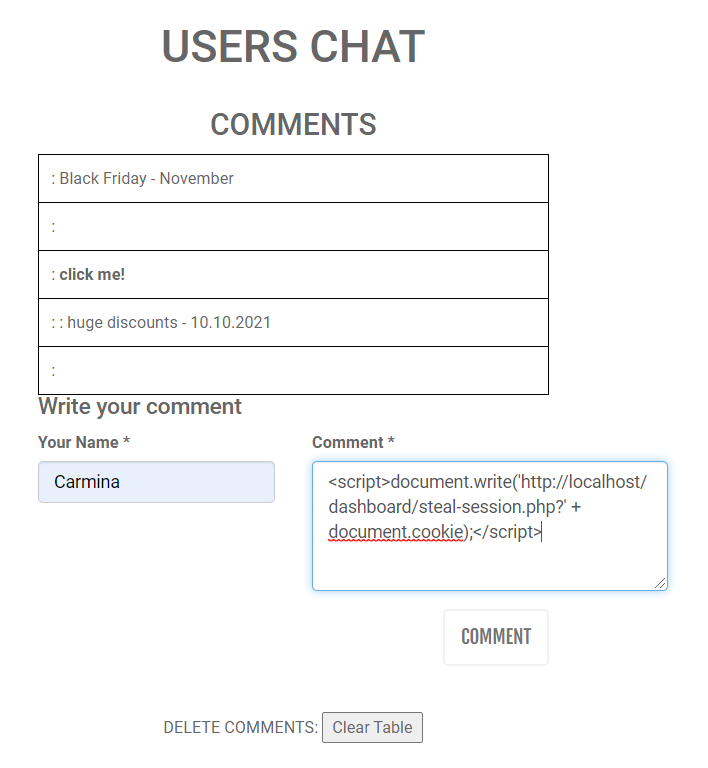
****

****

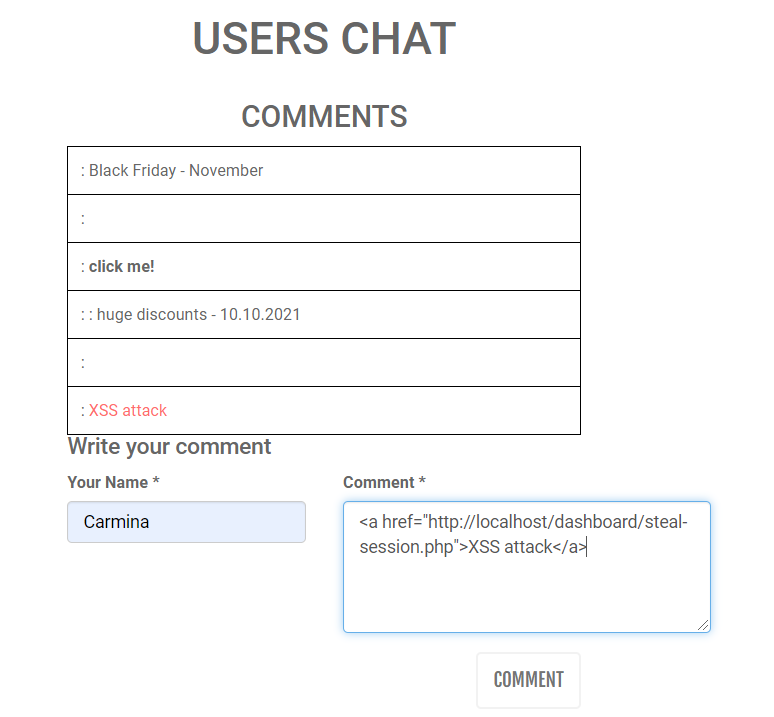
**Session of current user**

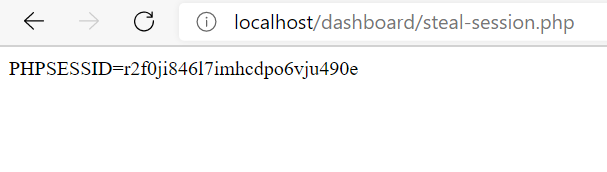
****

**Message to discourage users about site protection**

****

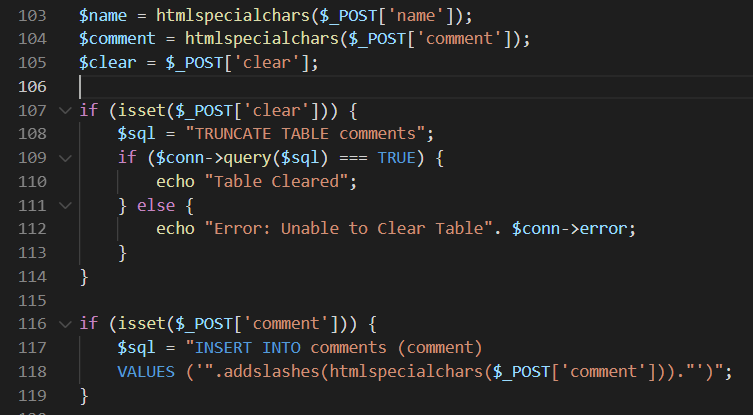
**Code for stealing session of current user**

****

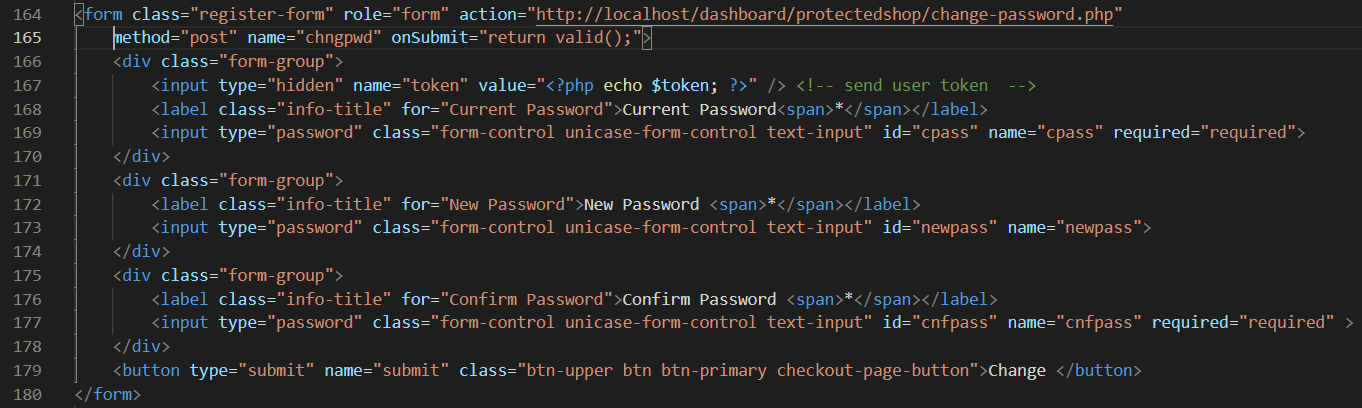
****

**Session of current user sent on hacker’s site**

Protectedshop – user-chat.php



**Code for transforming special characters**



**Data validation. Compleating all fields. Required**

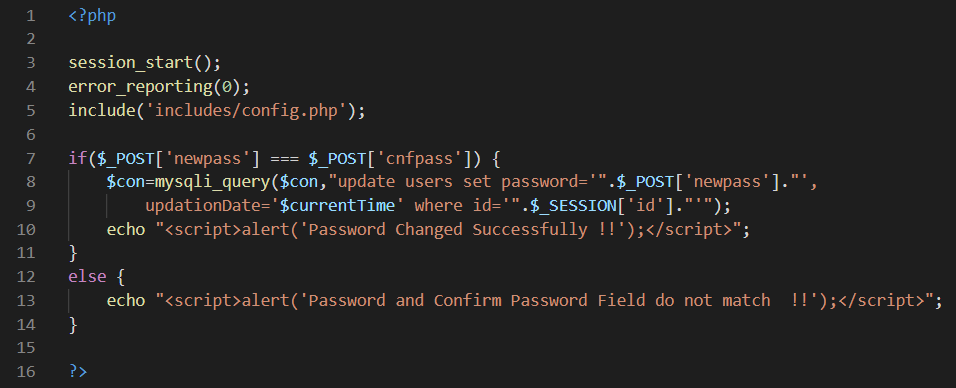
# CSRF - Cross-site request forgery

Unprotectedshop – my-account.php

# 

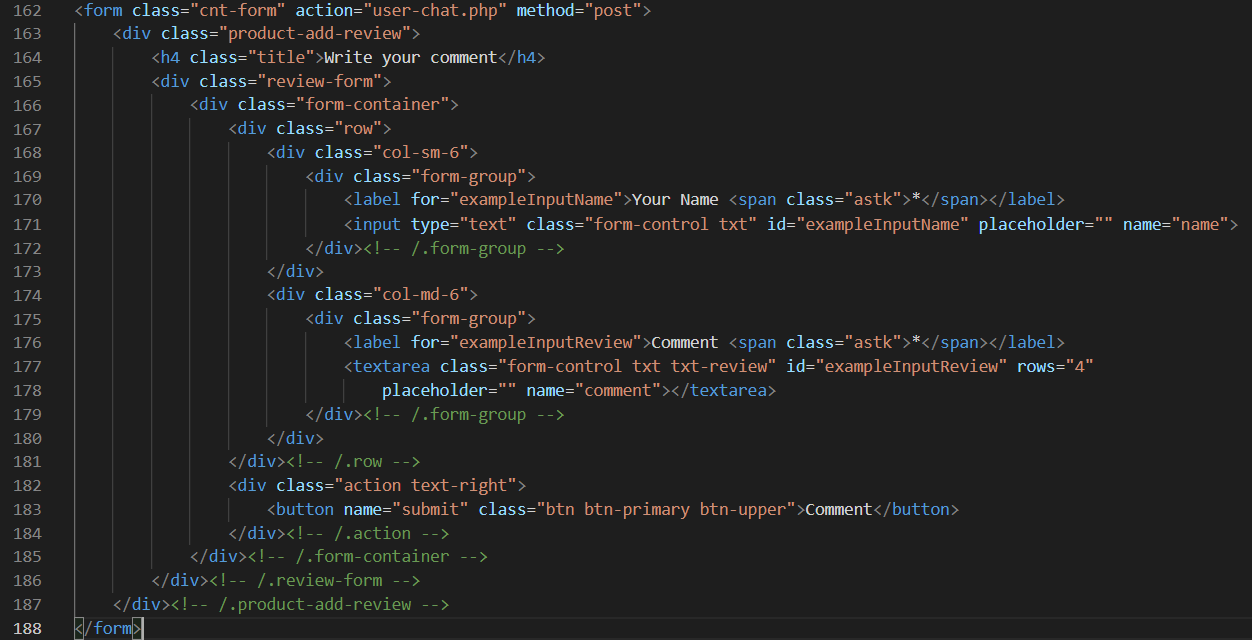
**Password change form**

Unprotectedshop – change-password.php



**Password change code**

Unprotectedshop – user-chat.php



**Form to adding comments**

Shopping database – users table

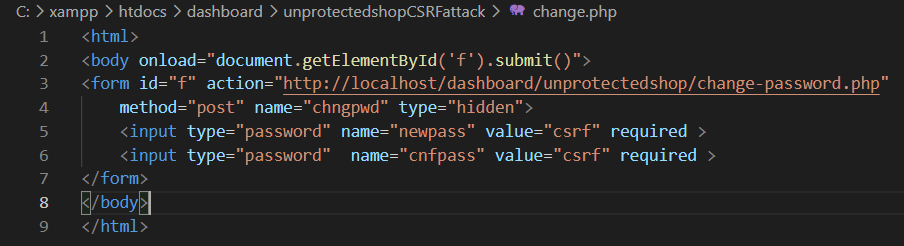
****

**The third user – Hatnean Carmina and current password – carmina.**

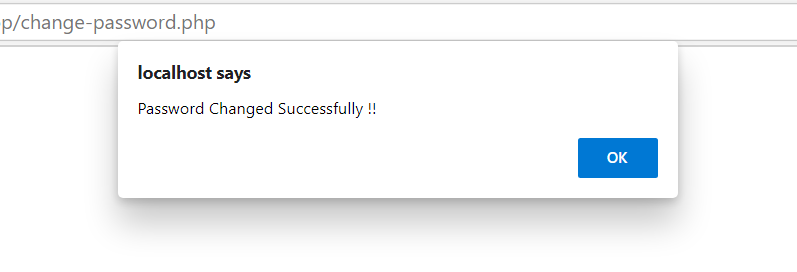
****

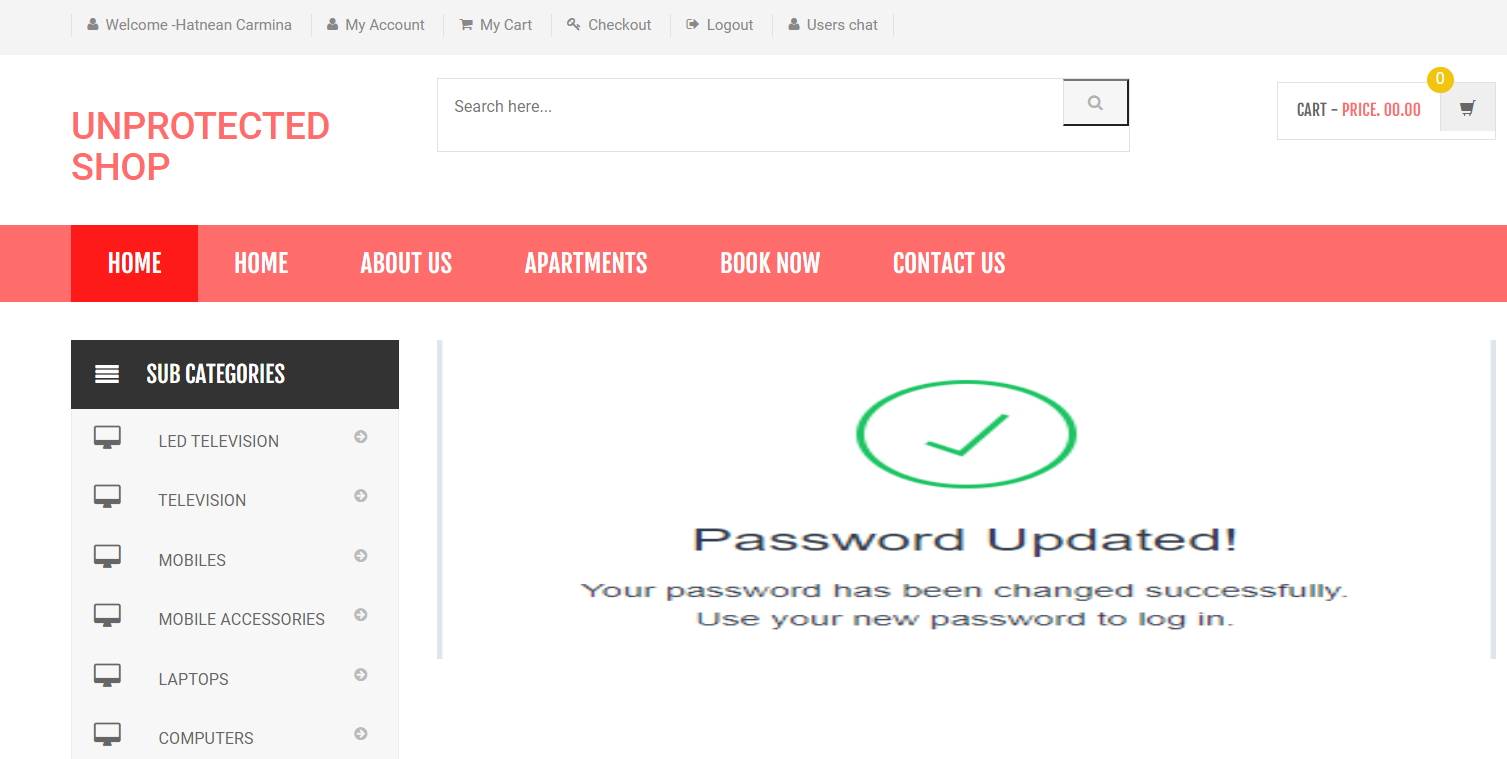
**CSRF attack - <a href=”http://localhost/dashboard/unprotectedshopCSRFattack/change.php”> CSRF attack </a> Redirect current user on page change.php from hacker’s site unprotectedshopCSRFattack after accessing hacker’s link**

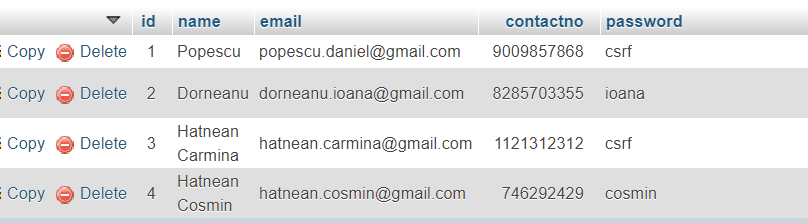
UnprotectedshopCSRFattack – change.php



**Current user automatically sends the data for changing the password on the official site** –unprotectedshop – change-password.php – **with the value csrf without the user knowing and wanting**







**The third user – Hatnean Carmina and current password after accessing hacker’s malitious link – csrf**

Protectedshop

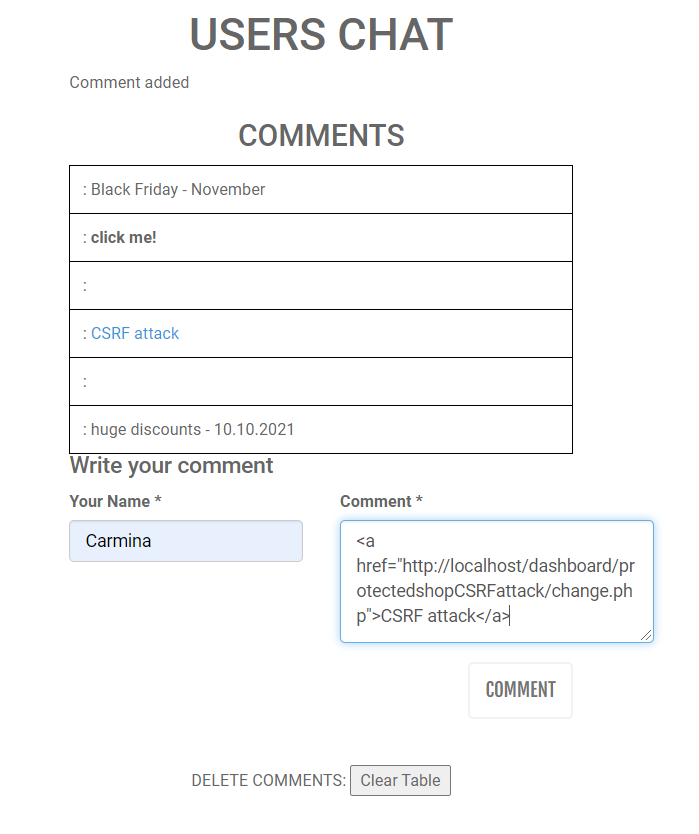
!!! In order to show how to protect against CSRF I removed for a while function htmlspecialchars !!!

Shopping-protected database – users table

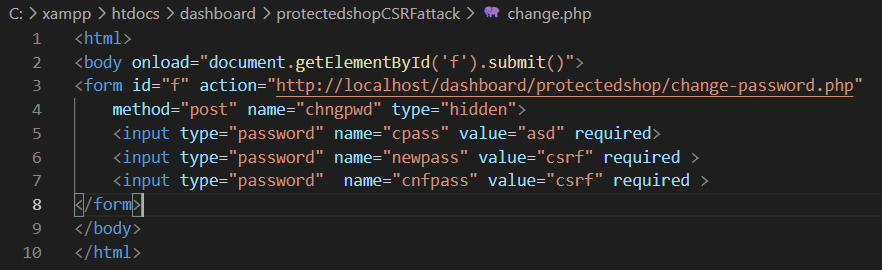


**The third user – Hatnean Carmina and current password – 2fde1f72d0cd367122870bf520210b1b (carmina)**

Protectedshop – user-chat.php

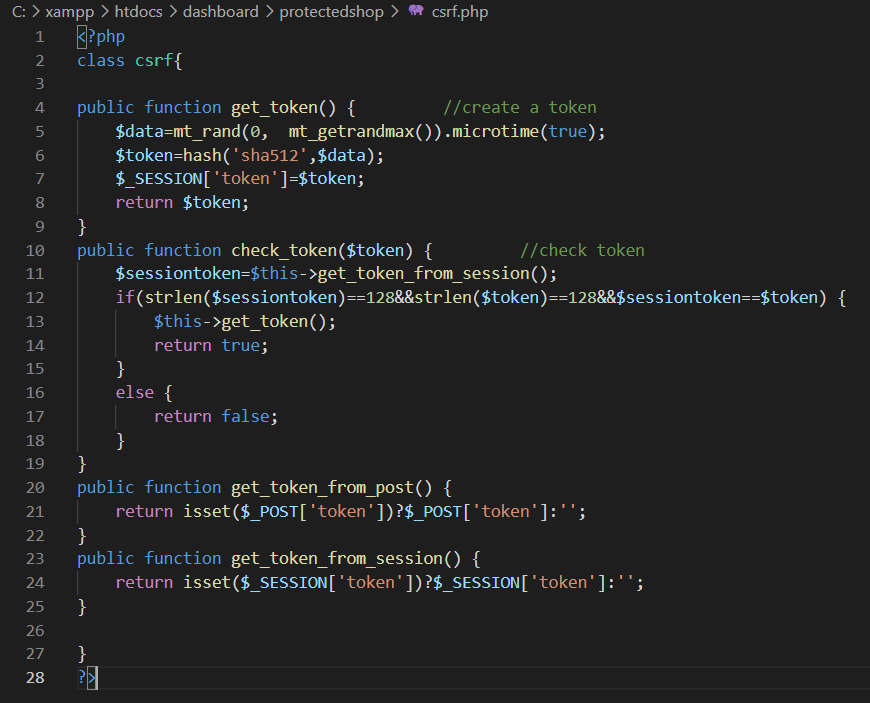


ProtectedshopCSRFattack – change.php



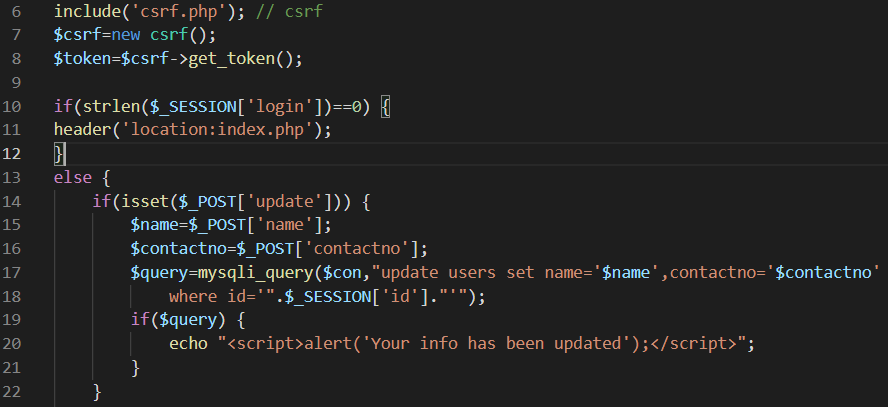
**Current user automatically sends the data for changing the password on the official site** –protectedshop – change-password.php – **with the value csrf without the user knowing and wanting, but without current** user token or right token

Protectedshop – csrf.php

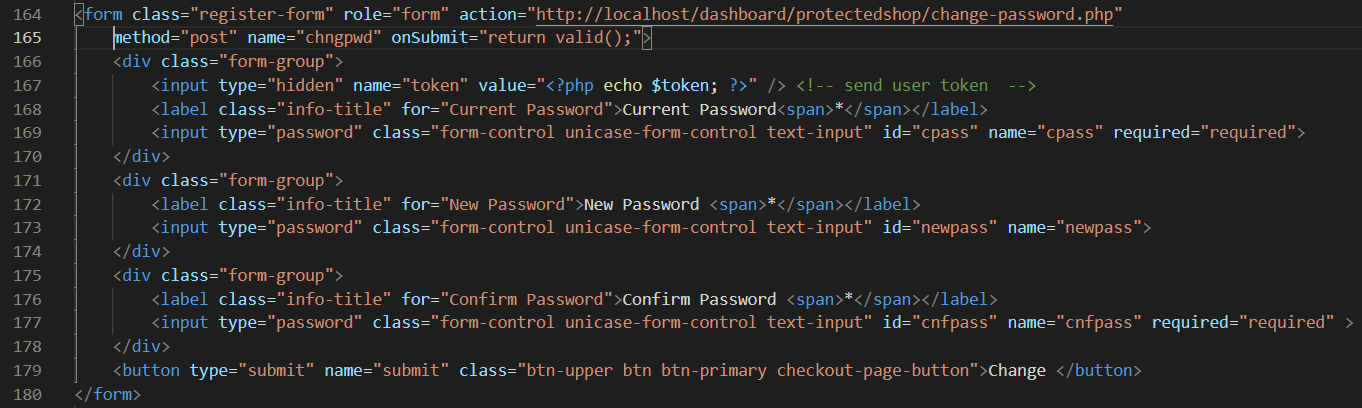


**Creating and verifying the user token**

Protectedshop – my-account.php

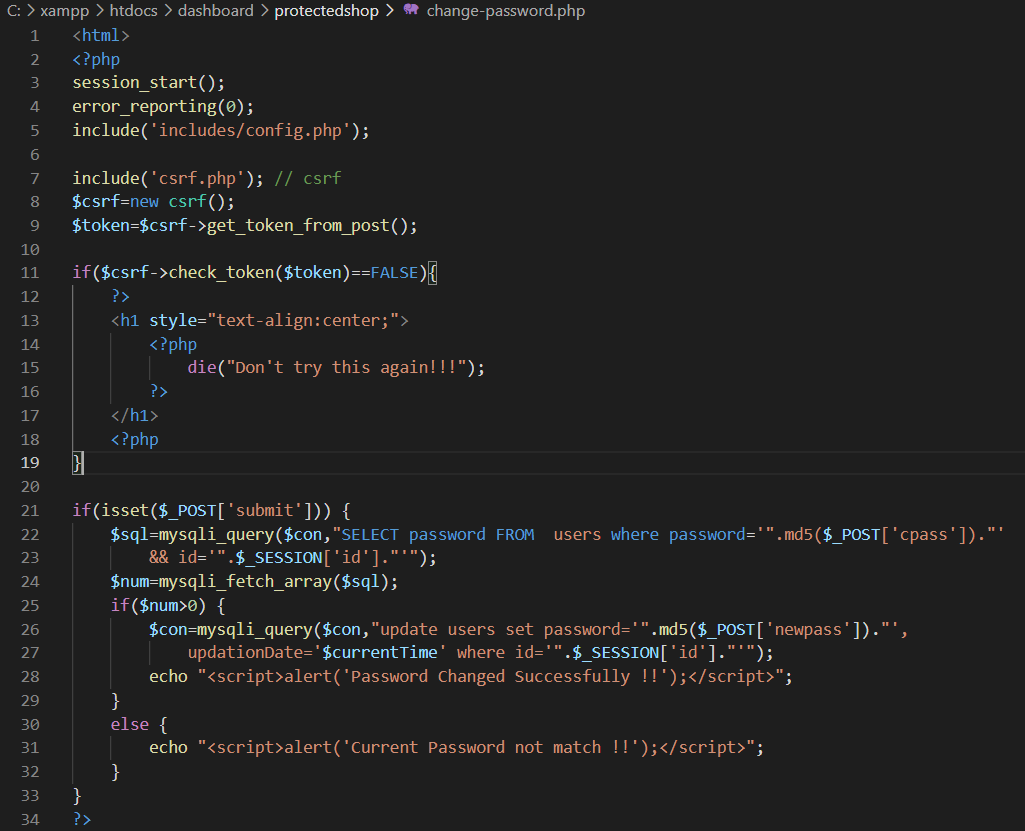


**Creating a token for current user**

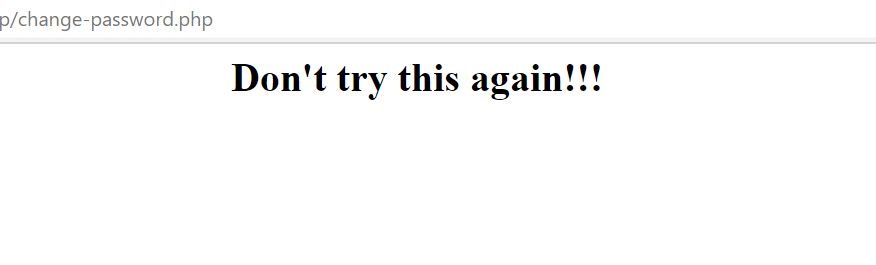


**Form to change password with third hidden input -** the current user's token

Protectedshop – change-password.php



**The server-side application verify that the request includes a token which matches the value that was stored in the user's session**

****

**Message sent after the expected token is missing or invalid**

****

**The third user – Hatnean Carmina and current password – 2fde1f72d0cd367122870bf520210b1b (carmina)**

The password remained unchanged after the csrf attack