**Ecommerce Security Project**

**E-store for sports Apparel (Sporty)**

**By**

**Rajat Vij**

**Sneha Sachdev**

**Wesam**

Sporty is a commercial online shopping website which can be used for purchasing sports apparel online.

**Basic Functionality of the website**

**­­­­**The online shopping web application have the following basic functions:

1. Provides a secure login functionality for both customers and admin. We are using SHA512 algorithm and salt while saving password for security.
2. The user used in database connection file only has permission to SELECT, UPDATE and INSERT. So even in case of a breach, nobody would be able to drop any tables or change structure of tables.
3. We are using sql prepared statements wherever possible to avoid sql injection attacks.
4. We are providing different screens to register admin and users. Once registered, users are flagged as customer and admin and based on that they are sent to item\_list or admin\_list page after logging in to the website.
5. Display all the Products available for shopping on the system’s main page from which we can navigate to item details page.
6. Allow the administrator to add new items to the existing list of available items.
7. Allow users to add/remove items from the shopping cart.
8. Allow the administrator to add/remove items from the inventory.
9. Allow the administrator to update item details
10. Customers can add items and update their quantity to their shopping cart.
11. Customers can copy their billing information of their shipping information is same as their billing information
12. Customers can confirm their orders and input their financial details to get a PDF for the Whole order.
13. We are providing luhn mod 10 check for credit cards.
14. We are letting admin add credit cards to hot list.
15. We are providing event monitoring system and blocking a user if there are more than 5 failed login attempts.
16. We are alerting admin for high purchase orders.
17. We are providing admin a way to analyze consumer purchases.

The users of the system, based on their roles, are Customers and Administrator.

1. **Customers**: Customers are able to view the home page of the application, browse the different products, browse and add any number of items from any categories in the shopping cart, look for information about each product, delete the items in the shopping cart, check out or continue shopping after adding the item to the cart, and check out the items by completing the required information in the order form.
2. **Administrator**: The administrator is able to update the inventory in the database from website.

The project basically works as following:

* 1. At first, the customer is required to sign in using the email and the password which is verified with the values stored in the database. If the customer is not registered with the site, he will be asked to sign up and then redirected to the login page.
  2. After logging in, the customer can browse the different items available in the inventory and add items into the shopping cart of their choice. After adding items into the shopping cart, the customer can either continue shopping or checkout.
  3. At checkout, the customers are asked for their valid credit card information, shipping and billing address and can purchase products once they provide valid information.
  4. Once the customer is done with the checkout he is provided with the confirmation of the order.

**Limitations**

1. We were having trouble with div and select tags on our php pages, due to which we were not able to implement following functionalities.
   1. Sorting by Price
   2. Auto filling of customer’s saved information on cart and confirm order screen.
2. We are not able to update quantity in our cart at the moment.
3. We are not providing guest checkout functionality.