Applied Web Application Security Project

Introduction

This project was created by 4 students from the University of Padua: Trambaiollo Luca, Valentini Giacomo, Squarise Alberto and Lucon Xiccato Gregory.
We implement a deliberately insecure web application with 4 vulnerabilities. It is an e-commerce company that sells cameras, watches and shirts.

Languages and tools used

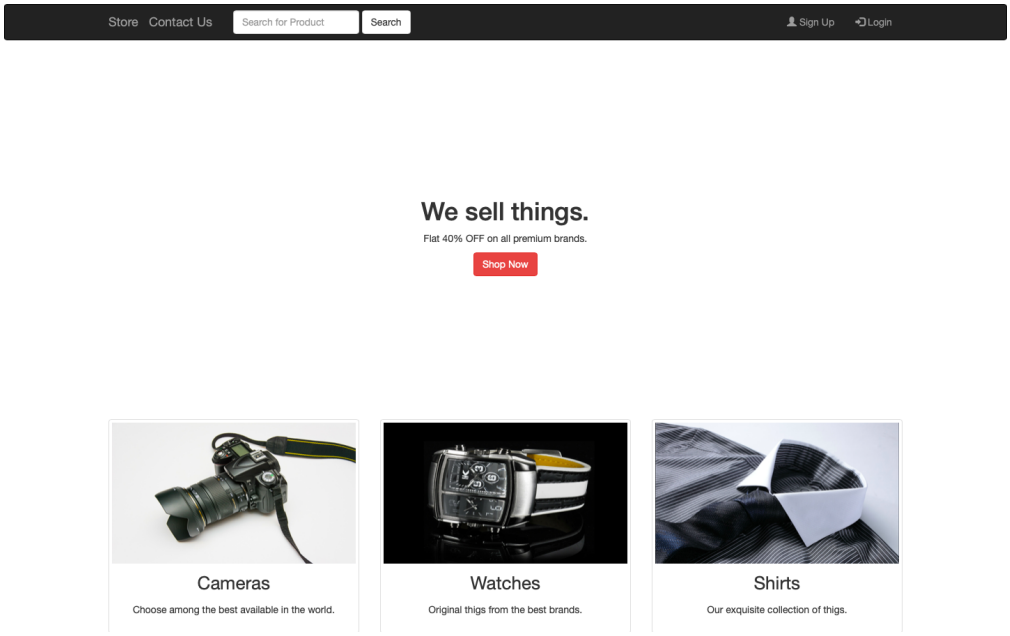
The programming languages and the main tools used for the realization of the project are listed below:

- **SQL :** is a database query language designed to enter, modify and manage data stored in a database management system through the use of programming constructs called queries. It contains both the functionalities of a Data Definition Language (DDL) and those of a Data Manipulation Language (DML). This allows him to both create, modify or delete databases, and to manage the data they contain.
- **MySQL:** is a Relational Database Management System (RDBMS). It is Open Source, supports most SQL syntax, and is also supplied with extensive documentation. Advantages that, combined with very simple management and good speed, make it an excellent choice especially when accompanied by a simplified interface such as the one provided by PhpMyAdmin.
- **PhpMyAdmin:** is a free and Open Source PHP application that allows you to easily manage MySQL databases through any browser. Its graphical interface allows you to create a database from scratch, create tables and perform optimization operations on them. There are also features for data entry, for queries, for exporting and importing data, and much more.
- **HTML:** is the language usually used for hypertext documents available on the World Wide Web. It is not a real programming language as it does not provide any definition of variables, functions, data structures or control structures, but serves to describe the logical content of a page web through the so-called tags.
- **PHP:** is an interpreted scripting language, with an open source license, conceived mainly for the development of server-side web applications and allows the creation of dynamic web pages. The processing of PHP code on the server, in fact, dynamically produces HTML code to be sent to the browser of the user who requests it and it is precisely this dynamism that is the greatest advantage of using PHP.
- **CSS:** is a computer language used to define the formatting of HTML, XHTML and XML pages. More precisely, it allows you to separate the contents of a document from its formatting. In this way, not only is the

code cleaner and more readable, but also its maintenance is considerably simplified.

Description

The web application has a main page where you can see the three types of the product that are sell and above there is a bar where a user can sign up, login, search for product or contact the administrators.



Obviously the application allows the users to register with insertion of Name (max 20 characters), email, password (min 6 characters), contact, city and address. If a user completes all the fields correctly, the screen shows the message: “User successfully registered” and the user is inserted to the database. But if the email is already registered in the database the application shows the message: “Email already exists in our database!”.

In the login page the user has to insert his own email and password to start the session. If the email isn’t registered in the database or if the email doesn’t correspond to the password inserted, the screen shows the message: “Wrong username or password”.

Authentication allows users of the information system to access the system and perform the operations for which they have the rights, in this case to make a purchase.

There is also the possibility for the user to contact the administrators through the specific page where there are the following fields: Name, Surname, email, telephone and the message.

To show all the products in the shop just click the red botton: “Shop now”. So the client can start to select the products that wants.

When the user has selected the articles he can proceed to the checkout through the cart page. Then the user is required to insert the credit card’s data and clicking on “Confirm order” he can place the order.

At the end the client can log out from the system.

The project demonstration is visible at this following link: https://youtu.be/s_rveXkw9p8

Vulnerabilities

In the web application there are 4 vulnerabilities:

1. The first vulnerability is on the registration and authentication page, in fact during the registration the page will not accept a duplice email warning the users that the specified email is already taken. The login page will warn the user if the email or the password is wrong, moreover it will not suspend or disable the page after unsuccessful login attempts, allowing brute force.

2. The second vulnerability is on the “Contact Us” page. There is a form that allows the attacker to do a XSS attack by inserting a script in one of the form fields.

3. The third vulnerability is on the search box that allows the attacker to do a SQL injection. In fact, by inserting specific SQL statements in the search box you can get the data of users registered to the site, such as email and password.

4. The fourth vulnerability regards the checkout process. There is no use of the referrer header and the checkout is done using only the user id as GET request parameter. An attacker can bypass the payment page accessing directly the “success.php” page and passing as URL parameter the user id placing the order for free.