Ministry of Education of the Republic of Moldova
Technical University of Moldova
Department of Applied Informatics

Report

Laboratory Work Nr.4
on Web Technologies

Restrict the access

Performed by Metei Vasile
Supervised by Plugaru Tudor

May 11, 2018

Goals:

- Understand how authentification and authorization works;
- Get more familiar with MVC pattern;

Main requirements:

- Basic authentification system(basycally, the authentificated user can do anything);

Bonus points:

- 2 or more roles are defined and they have different actions and each role has well defined permissions;(2pt)

Laboratory Work Analysis

Authentication is the process of recognizing a users identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized users information on a local operating system or within an authentication server.[1]

The authentication process always runs at the start of the application, before the permission and throttling checks occur, and before any other code is allowed to proceed. Different systems may require different types of credentials to ascertain a users identity. The credential often takes the form of a password, which is a secret and known only to the individual and the system. Three categories in which someone may be authenticated are: something the user knows, something the user is, and something the user has.[1]

Authentication process can be described in two distinct phases - identification and actual authentication. Identification phase provides a user identity to the security system. This identity is provided in the form of a user ID. The security system will search all the abstract objects that it knows and find the specific one of which the actual user is currently applying. Once this is done, the user has been identified. The fact that the user claims does not necessarily mean that this is true. An actual user can be mapped to other abstract user object in the system, and therefore be granted rights and permissions to the user and user must give evidence to prove his identity to the system. The process of determining claimed user identity by checking user-provided evidence is called authentication and the evidence which is provided by the user during process of authentication is called a credential.[1]

Authorization is a security mechanism to determine access levels or user-client privileges related to system resources including files, services, computer programs, data and application features. This is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.[2]

Most web security systems are based on a two-step process. The first step is authentication, which ensures about the user identity and the second stage is authorization, which allows the user to access the various resources based on the user's identity. Modern operating systems depend on effectively designed authorization processes to facilitate application deployment and management. Key factors contain user type, number and credentials, requiring verification and related actions and roles.[2]

In security systems, authentification is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Laboratory Work Implementation

In this laboratory work I have continued the development of the previous assignments. Here I added authentication and authorization processes. In order to make it easier I used Identity framework. ASP.NET Identity Framework is used for managing user credentials. It also helps us to manage the user accounts. It allows users to self-register on the site. It allows users to select user id and password.

Firstly I want to explain how my authentication system work. A simple web site's guest will have access to the home page and navigate through about page. Also he can log in or register. Nothing more he will be able to do. In order to have access to the main functionality of the site the guest will have to log in or register.

In case that he or she does not have an account it seems logic to choose register option. Choosing it, a register form view as in Figure 1 will be displayed. It ask the guest to introduce some information. In case you accidentally picked the wrong option I mean log in. There will be a button "Register as a new user" that will redirect you on the register page.

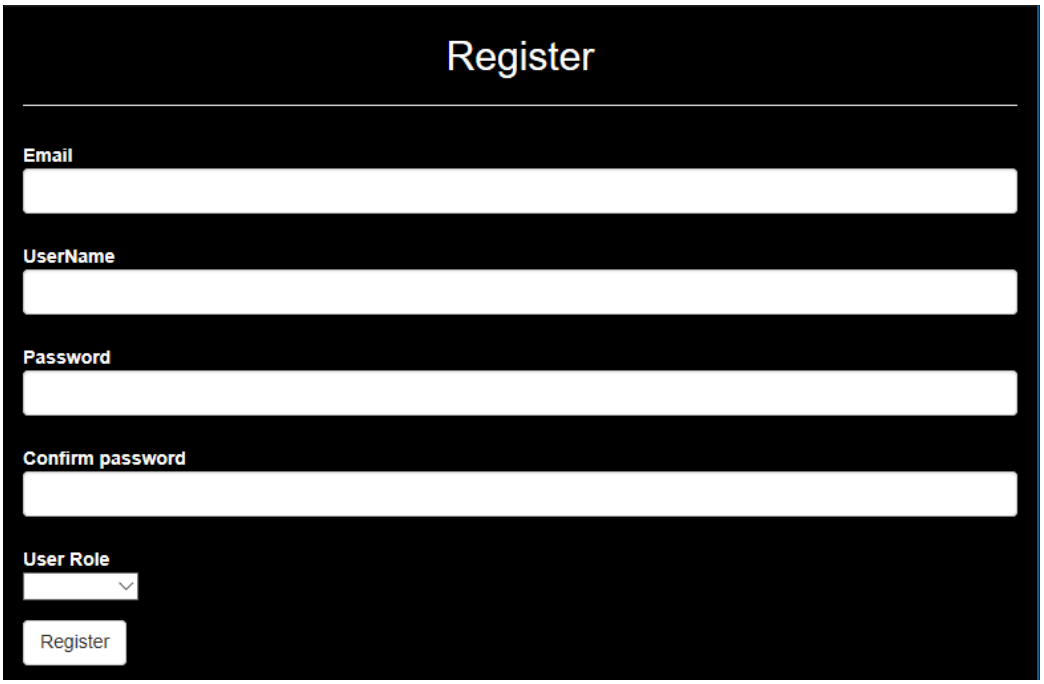

Figure 1: Register Form View

In case you do not have an account pick the log in option. And a log in form view as in Figure 2 will be show up. There you will have to introduce your credentials. After you click the log in button the system will check for such an user. If he or she exists the log in process will be successfully completed if not an error will occur. It will inform about log in failure.

Figure 2: Log In View

After we are done with authentication process, authorization process takes place. To be more exactly it is performed immediately after authentication. After credentials are accepted the system checks which role is assigned to the specific user. Depending on the assigned role, different permissions are given.

Now, that you are logged in, you may navigate to football page where you may find available products in the store. Clicking on the "View" button all the products will be displayed on the screen. And what about the CRUD? Is there any possibilities to create, edit or delete a certain product from the database? Of course yes, all that features are assigned to the Admin role.

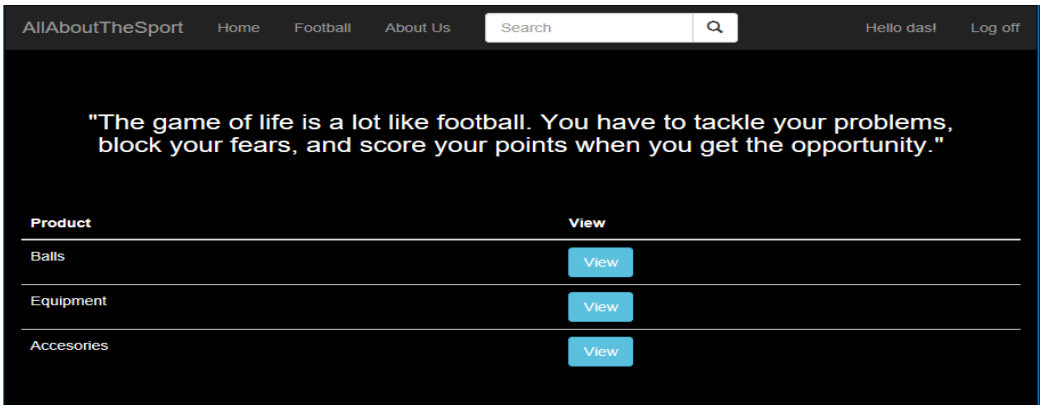

Figure 3: Simple User Role

First thing I want to remark about admins is that they can be created only from the code. They will be added to the database with Admin assigned in the role field. There is no way to create them from the web site.The main feature of the admin is to supervise the site that's why CRUD operation are enabled for him.

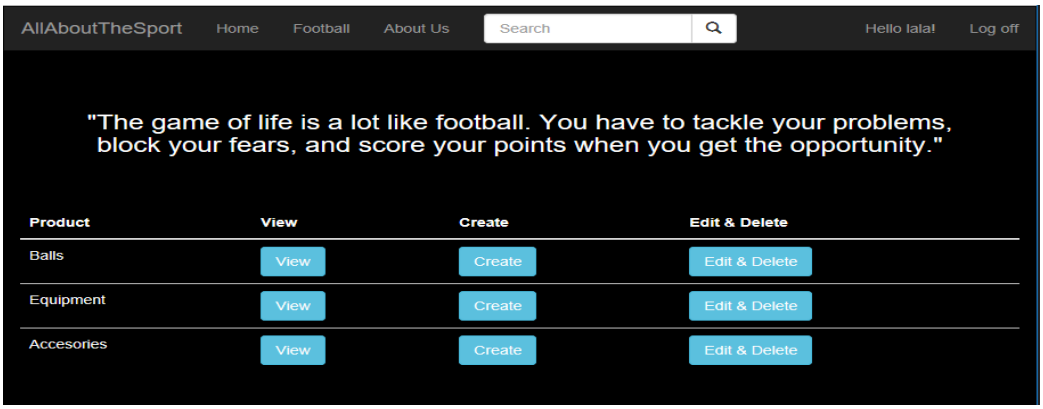

Figure 4: Admin Role

Conclusion:

In this laboratory work I discovered what authentication and authorizations processes are and how they should be organized in order to differentiate a simple guest from an user. Also I learned about roles what they basically mean and why we need them.

Adding different roles to my web application I limited access to some type of users and increased it for another type of users.

This laboratory work gave me the possibility to have a better understanding about how a Web Site is created and how it deals with authentication and authorization processes.

References

[1] URL: `https://economictimes.indiatimes.com/definition/authentication`. (accessed: 11.05.2018).

[2] URL: `https://economictimes.indiatimes.com/definition/authorization`. (accessed: 11.05.2018).