# T.C. ADANA ALPARSLAN TÜRKEŞ SCIENCE AND TECHNOLOGY UNIVERSITY FACULTY OF COMPUTER AND INFORMATICS

## COMPUTER ENGINEERING DEPARTMENT

## Secure E-Learning Website


PREPARED BY

Kerem Keskin – 190101055

Ece Nur Balkan – 180101021

## 1) ABSTRACT

This project describes how we can secure E-Learning website and shows what techniques used in E-Learning demo. In primary security, access control authentication implemented in login and register screen. Users should first register in register screen and then users can login in login screen. Captcha also implemented in login area and in login screen they have to pass second security system for bot security. In backend side, without access control authentication there is a hashing mechanism in database. These implementations purpose the secureity our E-Learning demo.

## 2) OVERVIEW

This security system for E-learning site increase user security and makes security efficient in some level. Captcha system, access control authentication and data security are the steps of how we secure E-learning website. Also this security system in website provides user-friendly expreience and it does not require any formal knowledge in order for a user to use the website.

## 3) PROBLEMS For Securing E-Learning Website

In Web Applications there are many security issues. Some are as follows:

1) Cyber Attacks like spyware, phishing, sql injection , viruses etc.
2) Store user and general informations.
3) Logging and register activity
4) Maintaining integrity
5) Data integrity and interacting between database and web applications
6) User access control
7) Code errors and exception issues
8) Library implementation problems

## 4) AIM AND OBJECTIVES

The Securing E-Learning Sites project aims to create a system that should be as secure as possible for instructors and students. Additionally, this project seeks to secure both the frontend side and the backend side. By bringing together all implementations, the app shall deliver a good functionality providing efficiency, accuracy and user friendly experience for secure E-Learning web applications.

In Summary:

1) To provide user friendly security,
2) To develop strong database for user records,
3) Easily access to secure passwords.
4) To have multiple elements and security techinques for securing E-Learning.

## 5) SIGNIFICANCE OF THE PROJECT

There are many researchers and developers to find How we secure web applications and yet some answers are not certain and unknown. We try to find how we secure E-learning we application for our side and this project offers a variety of crucial perspectives on web security. Discovering how to secure user screens and database sides is one of them. In addition, we asked ourselves how we can distinguish between humans and bots on the web. This project also shows us about security exceptions and vulnerabilities that are beneficial for secure E-learning websites.

## 6) TOOLS AND ENVIRONMENT

For this project we use more than one tools and environments.

### 6.1)

In backend part; we use ASP.NET web framework, C# Programming Language and Visual Studio integrated development environment (IDE).

### 6.2)

In frontend part; we use HTML, CSS , web forms, asp forms.

### 6.3)

Microsoft SQL Server Management and DataSetTable Adapters for SQL database part.

### 6.4)

Web Configurations and implementation libraries. ( Except C#, also we use DevExpress Libraries)

**Some library examples:**

using System;

using System.Collections.Generic;

using System.Security.Claims;

using System.Security.Principal;

using System.Web;

using System.Web.Security;

using System.Web.UI;

using System.Web.UI.WebControls;

using Microsoft.AspNet.Identity;

Etc..

### 6.5) Documentation

## 7) How we Secure E-Learning Site ?

There are various ways to answer this. Therefore, in this E-learning project, we attempt to provide a solution. For solutions, we should examine the issue from both the user's and the data information's perspectives.  The solutions we discovered are shown in the steps below.

## 7.1)

## Authentication : What Is  And Why Is Important for Security?

Any process used by a system to confirm the identity of a person attempting to access the system is known as authentication. Authentication is necessary for effective security since access control is often based on the identity of the user making a request for access to a resource. Personal informations are used to implement user authentication, and these must at the very least include a user ID and password.

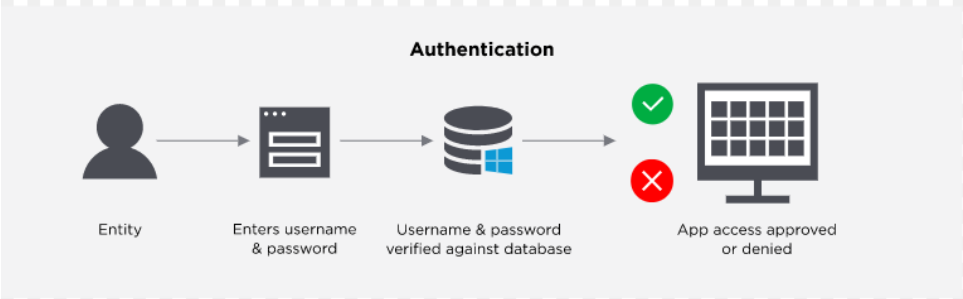



Figure1: Authentication Example between Client and Server

## How Work ?

Entering the login information on the login page is the initial step in the user's authentication process. Authenticating this login information is the next step. When the server you are attempting to reach decrypts the personalized data it has received, this process begins.

Following a comparison with this data, the credentials are entered into the database.

You may have entered erroneous information or forgotten your passcode combination if the computer rejects your request.

Depending on the settings, you might be given the option to make another request or you can be completely barred from using the web application.

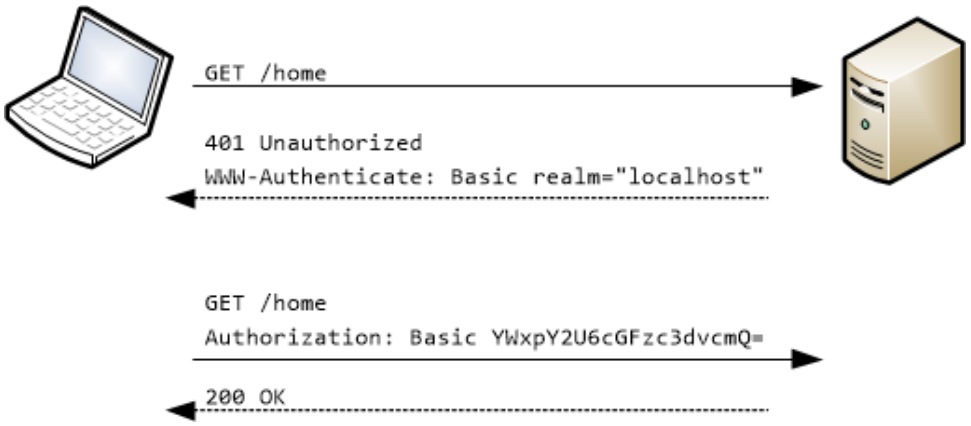



Figure2: Authentication in Web

7.2)

## Cookies: What Is And Why Is Important for Security ?

Websites set cookies to store your preferences when you use a browser like Google Chrome or Mozilla Firefox . These include your login information, so you don't have to enter your username and password each time you come, your preferred language preference whether it's English or another language and the products in your shopping card.

Permanent cookies are used to keep track of you in several sessions and a longer timeline. These cookies won't be automatically removed because they are saved on your hard disk. Authentication and tracking are the two fundamental purposes of permanent cookies. For instance, whether you select "remember me" or "keep me logged in" on a website, a permanent cookie is being used for authentication. In the tracking part, the most of the time, they are activated automatically, and unless the website warns you or gives you the choice to disable unwanted cookies, this could be done without your knowledge.

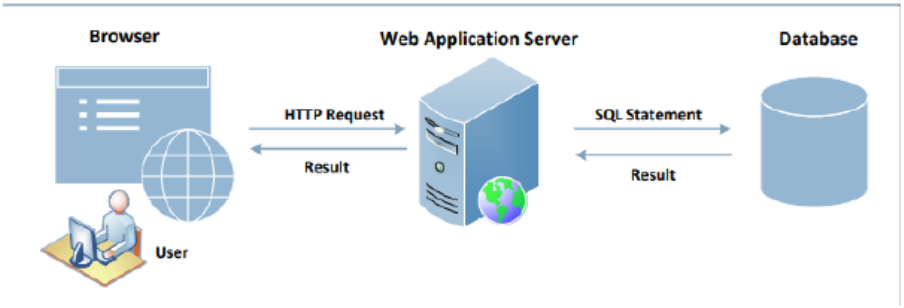
Is enabling cookies secure? In a summary, yes.  Although there are a number of security and privacy dangers associated with cookies, they are also incredibly helpful and perform essential functions for the majority of modern websites. Therefore, it is not reasonable to entirely disable cookies.

7.3)

## Hashing: What Is and Why Is Important for Secure a System?

Any key or string of characters can be transformed into another value by hashing. The original string is typically represented with a shorter, fixed-length value or key that makes it simpler to locate or use. Implementing hash tables is the most well-liked application of hashing. Using algorithms or functions, hashing converts object data into a useful integer value. For example if we have a user information stored in a database we can use some hash functions to secure these informations and then if some attackers try to access this special information then we can understand the changes by looking hash data.

For many input datas we should connect database and web interface. Some components have to connect each other which you can see how in below interaction.

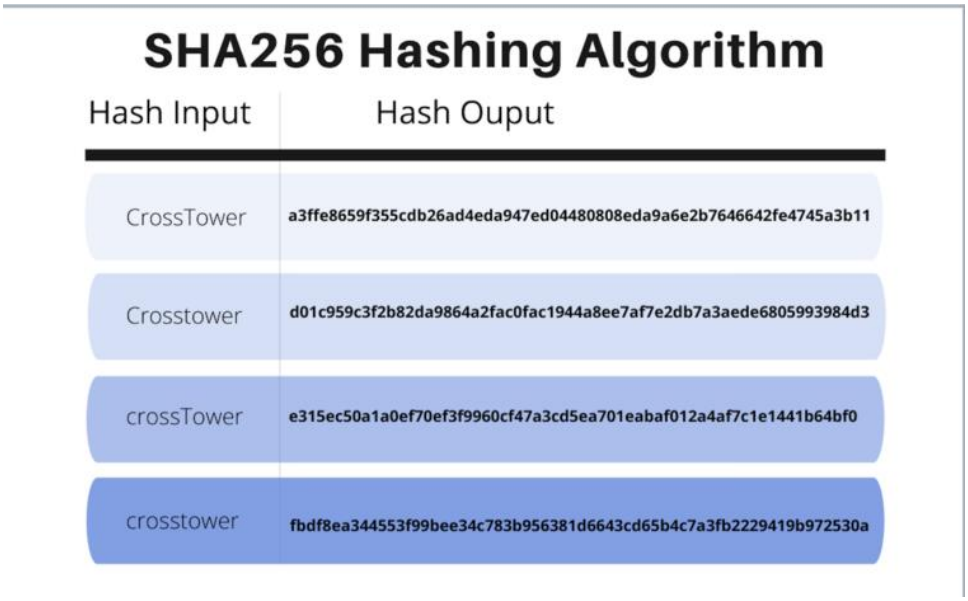



Database and Web Interaction Components

In general, hash algorithms are employed to provide a digital fingerprint of a file's contents, frequently used to ensure that the file has not been changed by a virus or unwanted party. Some operating systems also use hash functions to encrypt passwords. The integrity of a file can be checked with the use of hash functions. Key and value combinations are kept in a list that can be accessed by a hash table's index. The hash function will relate the keys to the size of the table because key and value combinations are infinite. The value for a given components is then changed to a hash value.

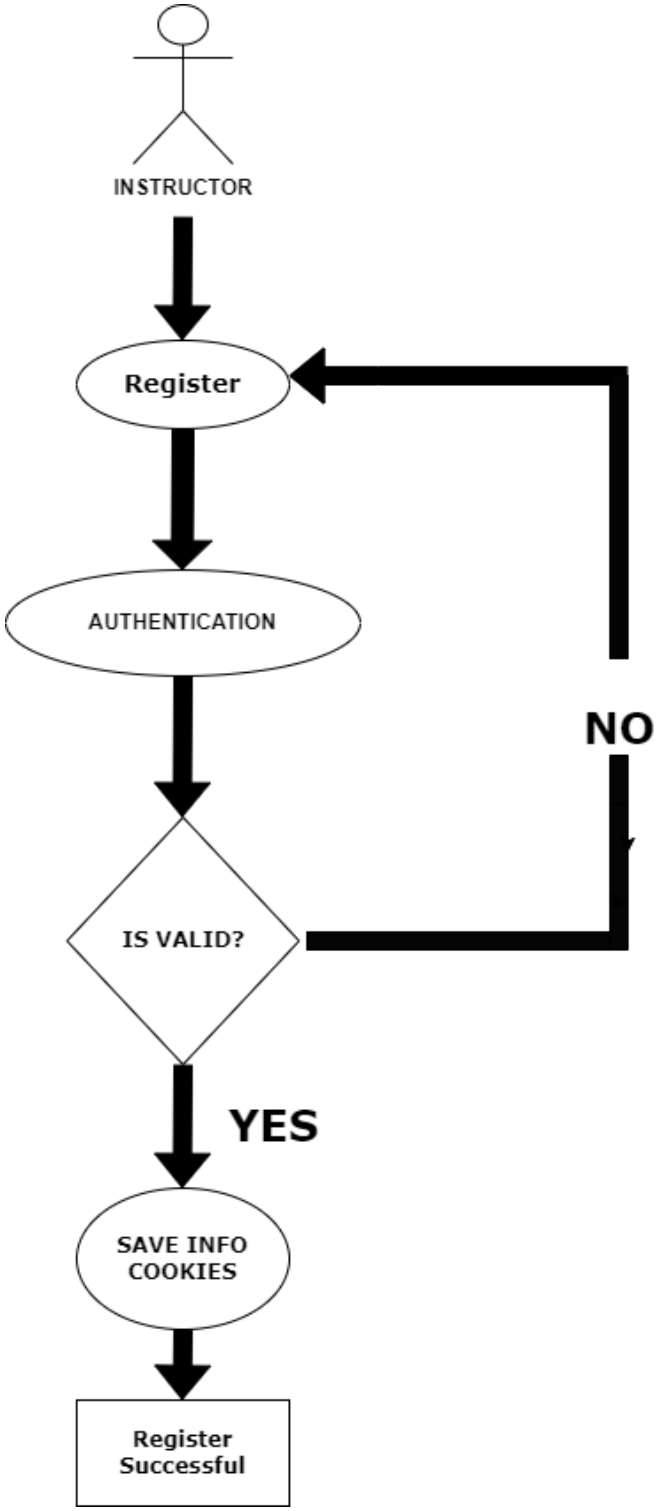

How Hashing Works

**We can clearly see that hash algorithm has a case sensivitiy and important for secure a wep application.**

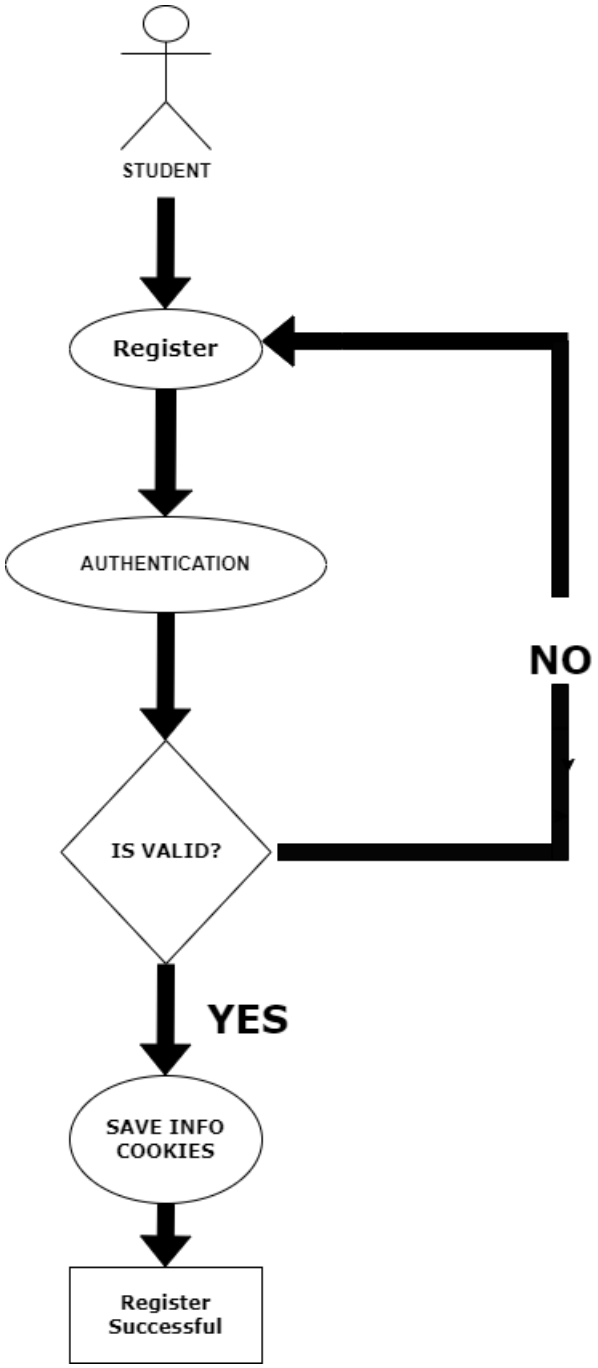



Hashing Example

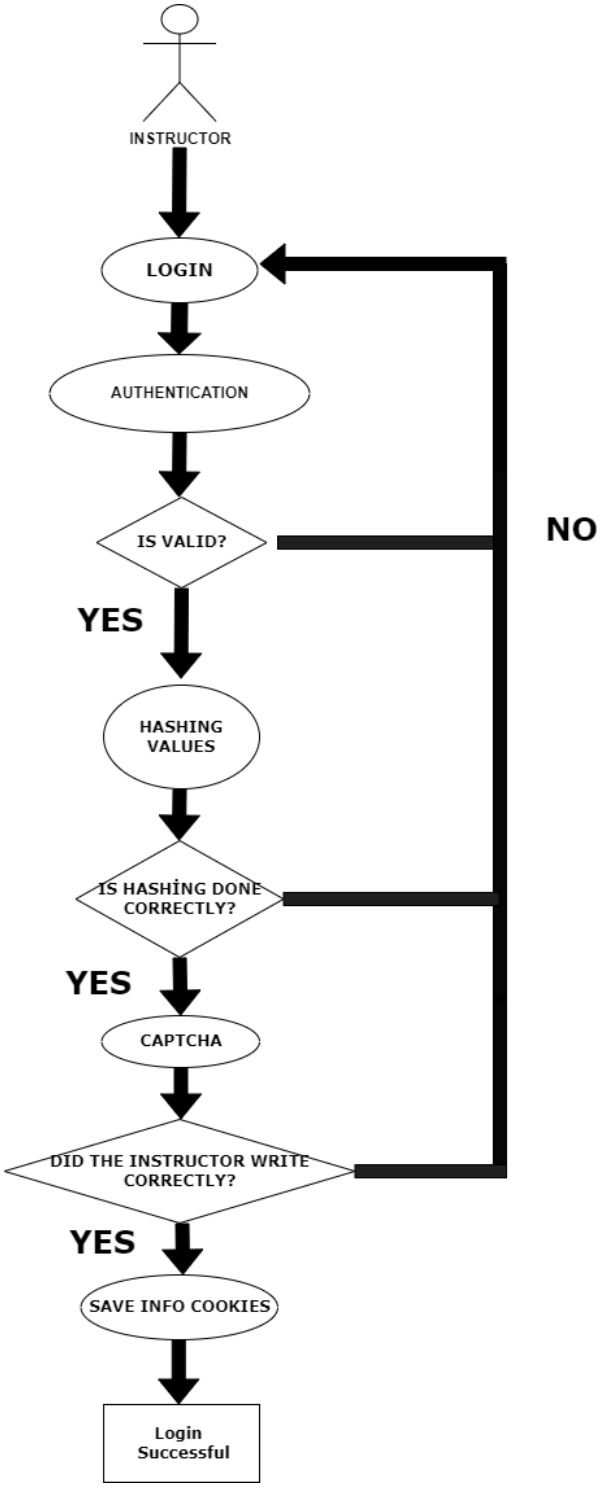
8) INSTRUCTOR REGISTER DIAGRAM



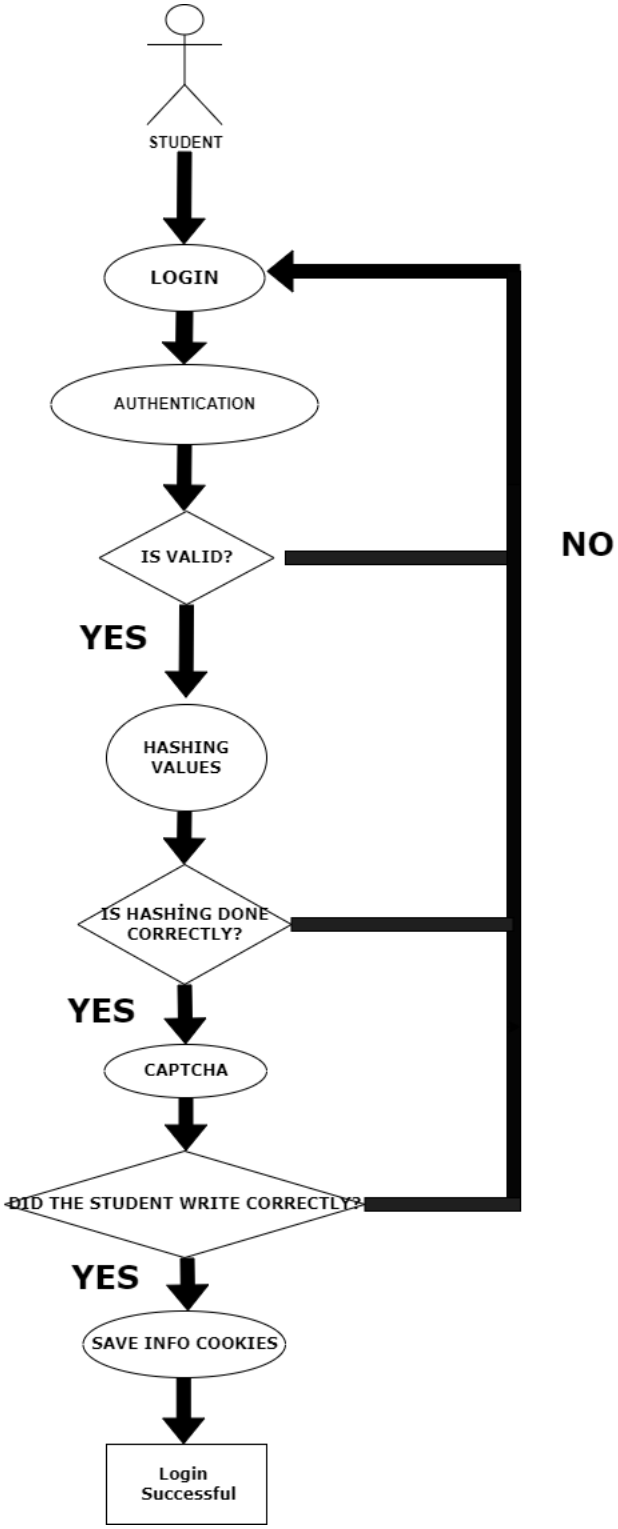
9) STUDENT REGISTER  DIAGRAM



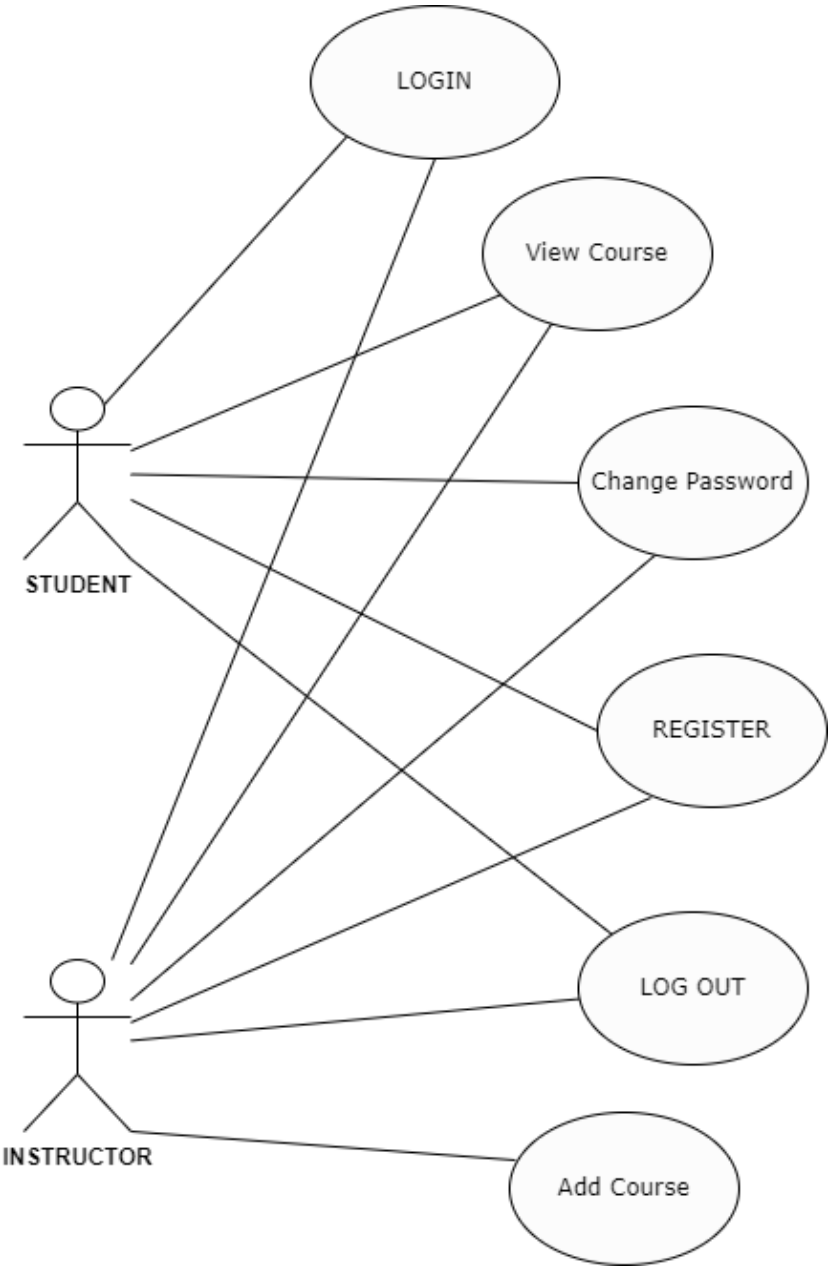
10) INSTRUCTOR LOGIN DIAGRAM



11) STUDENT LOGIN DIAGRAM



12) USE – CASE DIAGRAM



## 13) GOALS (What We Learn When We do This Project ?)

When we doing this project we learn too much lessons and subjects. So We learn;

1) How we can completely develop a Secure Elearning project.

2) Team Working

3) Handle too many exceptions and code errors

4) Learning Asp.net from zero.

5) How we can use DevExpress library  (especially configuration part)

6) How we can implement Authentication in Elearning website

7) How  we can implement CAPTCHA

8) How we can implement Hashing in passwords

9) How we can implement cookies.

10) Time Management (😊)

11) How we add and connect different pages with C# and web languages.

12) Generally criticizing how we can secure a website.

13) Why secure a website is important.

## 14) OUR CHALLENGES AND PROBLEMS

1) First weeks we have couple of problems with configurations for devexpress libraries.

2) Handle code errors in authentication part

3) For add course function we had couple of code problems

4) Our program crash one time and we have to start again from zero

5) Time management problem because we have to do many projects at the same semester

6) Some security methods did not work so we just add working methods

## 15) REFERENCES


1)DevExpress Documentations, for asp.net , https://docs.devexpress.com/eXpressAppFramework/113366/data-security-and-safety/security-system

2)DevExpress, passwords in the security systems, https://docs.devexpress.com/eXpressAppFramework/112649/data-security-and-safety/security-system/authentication/passwords-in-the-security-system

3)Asp.net, https://www.prowaretech.com/articles/current/asp-net-core/add-local-authentication#!

4) Article, Securing Shared Data in E-Learning Using Three Tier Algorithm of Compression Combined Hybridized Encryption, A. Revathi, Paul Rodrigue, J. Raja

5)Article, Secure E-Learning using Data Mining Techniques, Anshu Agarwala ,Alex V. Patelb, Dr Akash Saxenac

6)Article, Review on Secure E-Learning using Data Mining Techniques and Concepts, Priyanka R. Pradhan, Mr. R. B. Kulkarni

7) hashing, https://learn.microsoft.com/en-us/aspnet/core/security/data-protection/consumer-apis/password-hashing?view=aspnetcore-7.0

8) hashing passwords, https://nishanc.medium.com/net-core-3-0-preview-4-web-api-authentication-from-scratch-part-2-password-hashing-7e43b64cbe25

9) cookies learn, https://learn.microsoft.com/en-us/dotnet/fundamentals/code-analysis/quality-rules/ca5383

10) Course Slide, Lecture11 – Web Application Security

11) Course Slide, Lecture12 – Digital Forensics

12) Course Slide, Lecture06 – Software Security

13) Lecture 03 - Access-Control-Authentication

14) Lecture 04 - Access-Control-Authorization