



**T.C.**  
**TRAKYA**  
**ÜNİVERSİTESİ**  
**MÜHENDİSLİK**  
**FAKÜLTESİ**  
**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**  
**PROJE 2 RAPORU**

**PROJE ADI**

Güvenli Öğretim Üyesi Seçim Uygulaması

**HAZIRLAYANLAR**

1181602801 - Atakan KARAÇALI

1171602043 - Türkay TUNÇ

1171602040 - Atakan ERTÜRK

**DANIŞMAN**

Dr. Öğr. Üyesi Derya ARDA

**Edirne, Haziran 2021**

## 1 Proje Amacı

Günümüzde güvenlik kritik birçok görevi internet üzerinden veya dijital ortamlarda yapabilmekteyiz, bu projede güvenli bir elektronik seçimin web üzerinden ne şekilde yapılabileceğini, ne gibi güvenlik önlemlerinin alınması gerektiğini, ne kadarını bu projede başarabildik ve başka neler yapılmalıdır gibi sorular üzerinden örnek proje üzerinde bir çalışma gerçekleştirdik.

Gerçekleştirdiğimiz projede herhangi bir kullanıcı yönetici hesabı açıp istediği başlık altında seçim oluşturabildiği genel ve herkesin kullanımına açık bir seçim uygulaması oluşturduk. Fakat rapor ve sunumda “Doktora Öğretim Görevlisi Temsilci Seçimi” başlığında anlatım yapılacaktır.

(Uygulama arayüzü ve kodları İngilizce hazırlanmıştır)

## 2 Kullanılan teknolojiler, Araçlar, Kütüphaneler

Gerçekleştirilen proje bir web uygulamasıdır ve Backend tarafında **C# ASP.NET Core Web API**,

Frontend tarafında ise **ReactJS** kullanılmıştır, veri tabanı olarak ise **MS SQL Server** kullanılmıştır.

Veri erişimi için **Micro ORM Dapper**,










Test kodları için **xUnit**,

Yönetici Authentication (kimlik doğrulama) için **JWT, (HmacSha256)**

Oyların şifrelenmesi için **RSA, (System.Security.Cryptography)**

Seçmen ve yönetici şifreleri için **SHA256, (System.Security.Cryptography)**

Seçmene şifre bilgisi e-posta olarak iletilmiştir, **Gmail & SmtplibClient (System.Net.Mail)**

	<b>AutoMapper</b> by Jimmy Bogard A convention-based object-object mapper.	v10.1.1
	<b>coverlet.collector</b> by tonerdo Coverlet is a cross platform code coverage library for .NET, with support for line, branch and method coverage.	v1.3.0 v3.0.3
	<b>Dapper</b> by Sam Saffron, Marc Gravell, Nick Craver A high performance Micro-ORM supporting SQL Server, MySQL, SQLite, SqICE, Firebird etc..	v2.0.78 v2.0.90
	<b>Microsoft.AspNetCore.Authentication.JwtBearer</b> by Microsoft ASP.NET Core middleware that enables an application to receive an OpenID Connect bearer token.	v3.1.13 v5.0.7
	<b>Swashbuckle.AspNetCore.Swagger</b> by Swashbuckle.AspNetCore.Swagger Middleware to expose Swagger JSON endpoints from APIs built on ASP.NET Core	v6.1.1 v6.1.4
	<b>Microsoft.EntityFrameworkCore.SqlServer</b> by Microsoft Microsoft SQL Server database provider for Entity Framework Core.	v3.1.15 v5.0.7
	<b>System.Data.SqlClient</b> by Microsoft Provides the data provider for SQL Server. These classes provide access to versions of SQL Server and encapsulate database-specific protocols, including tabular data stream (TDS)	v4.8.2
	<b>xunit</b> by James Newkirk, Brad Wilson xUnit.net is a developer testing framework, built to support Test Driven Development.	v2.4.1
	<b>xunit.runner.visualstudio</b> by .NET Foundation and Contributors Visual Studio 2017 15.9+ Test Explorer runner for the xUnit.net framework. Capable of running xUnit.net v1.9.2 and v2.0+ tests. Supports .NET 2.0 or later, .NET Core 2.1 or later, and Universal Windows 10.0.16299 or later.	v2.4.3

### 3 Uygulamanın Çalışması, Aşamaları ile Sırayla Anlatım

#### 3.1 Yönetici Hesap Oluşturma ve Sisteme Giriş Yapması

Admin Email

Admin Password

your security is important to us !

Login

or create new admin account with following information... Create

Validate

Id	Email	HashedPw	IsEmailValidated	VerificationCode
30	atakanertrk@hotmail.com	5994471abb01112afcc18159f6cc74b4f511b99806da59b3...	1	NULL

Yönetici e-posta adresi ve şifresini girdikten sonra “Create” tıklayarak hesap oluşturur, mail adresine gelen şifreyi aşağıdaki forma girerek mail adresini onayladıktan sonra Login yapılabilir.

### 3.2 Yönetici Seçim Oluşturması ve Adayları Seçime Ekleme

51

Bilgisayar Mühendisliği | Öğretim Üyesi Seçimi

true

Details

53

Elektrik-Elektronik Mühendisliği | Öğretim Üyesi Seçimi

false

Details

Is Election Completed: false

complete

when you complete the election, results will be available publicly via election id

#### candidates of election :

name : Aytaç ALPARSLAN

description : elektromanyetik alanlar ve mikrodalga tekniği anabilim dalı

name : Gökhan KOÇYİĞİT

description : elektrik tesisleri anabilim dalı

name : Sezer ULUKAYA

description : kontrol anabilim dalı

name : Korhan CENGİZ

description : telekomünikasyon anabilim dalı

#### Assigned Voters Of Election

password will be send to email address automaticaly  
atakanertrk26@gmail.com

delete from election

you cant delete the voter if he/she already voted for election

#### Add Voter To Election

atakanertrk26@gmail.com

Add

	Id	Email	HashedPw	ElectionId	Voted
1	1106	atakanertrk26@gmail.com	a341c5f924e6e78ce37c40665bee10333d68cf850008fc33...	51	1
2	1107	atakanertrk26@gmail.com	15502178fc14a37aa96960f4ced0bcb2dfcd3c6bf9f03b695...	53	0

Yönetici seçimi oluşturup adayları ve seçmenleri tanımladıktan sonra, seçime eklenen seçmenin e-mail adresine ilgili seçime özel bir şifre gönderilir, bu şifre veritabanında SHA256 ile şifrelenmiş olarak tutulur ve şifrenin açık halini sadece seçmen görebilir.

### 3.3 Seçmenin Oy Kullanması

LogOut

## hey voter atakanertrk26@gmail.com

You can see assigned elections at the bottom

Select the election for voting, password details send to your email address for specified election

if you dont see anything at the bottom, you probably not added to any election yet

51

Header: Bilgisayar Mühendisliği | Öğretim Üyesi Seçimi

Description: bilgisayar mühendisliği bölümü Dr. Öğr. Üyesi deneme seçim

Show Details

53

Header: Elektrik-Elektronik Mühendisliği | Öğretim Üyesi Seçimi

Description: elektrik-elektronik mühendisliği öğretim üyesi deneme seçimi

Show Details

Seçmen e-mail adresi ile giriş yaptıktan sonra ilgili seçim için mail adresine gelen şifre ile oy kullanabilir.

Your Password For Election Elektrik-Elektronik Mühendisliği | Öğretim Üyesi Seçimi



guvenliesecim@gmail.com

Alıcı: ben ▾

i7y\_Q

ELECTION DETAILS:

id: 53  
header: Elektrik-Elektronik Mühendisliği | Öğretim Üyesi Seçimi  
description: elektrik-elektronik mühendisliği öğretim üyesi deneme seçimi  
is completed: false

Your Password For Voting

your password has been send to your email with name of the election

.....

CANDIDATES:

88  
Aytaç ALPARSLAN  
elektromanyetik alanlar ve mikrodalga tekniği anabilim dalı  
[vote](#)

89  
Gökhan KOÇYİĞİT  
elektrik tesisleri anabilim dalı  
[vote](#)

90  
Sezer ULUKAYA  
kontrol anabilim dalı  
[vote](#)

	ElectionId	Vote	Id
1	51	PxI9WuJSbSXqXsTmNw3fU+F3wJ44nsm&tNpoAZ1F1AXkZunC...	1007
2	53	Rp7geRLA1jmaHy7SckzcwOfpilutKHQTKSGx+mQXvqlp+46sJ6h...	1008

Oylar veri tabanında RSA şifreli tutulur, seçim yönetici tarafından bitirildiği zaman sonuçlar RSA Private Key ile deşifrelenip sonuçlar herkese açık bir şekilde seçim id'si ile erişilebilir

[go back](#)

Election results for election id : 53

Id : 88 Name : <b>Aytaç ALPARSLAN</b> Votes : 0	Id : 89 Name : <b>Gökhan KOÇYİĞİT</b> Votes : 0	Id : 90 Name : <b>Sezer ULUKAYA</b> Votes : 1	Id : 91 Name : <b>Korhan CENGİZ</b> Votes : 0
---	---	---	---

#### 4 Proje Değerlendirmesi (Güvenlik ne derecede sağlandı, başka neler yapılabilir)

4.1 Kullanıcı şifreleri için SHA256 kullanılmıştır, SHA256 hızlı hashing olarak bilinir (günümüzde bilgisayarların işlem kapasitelerinin artmasından dolayı SHA256 çok hızlı bir şekilde gerçekleştirilir) şifreleme işlemlerinde hız iyi bir şey değildir, ne kadar yavaş yapılıyor ve algoritması ne kadar karışık ise o kadar güvenlidir. Bu sebeple SHA256 yerine BCrypt gibi salting kullanan kütüphaneler kullanılması daha doğrudur.

4.2 Sisteme isteyen herhangi biri herhangi bir mail adresi ise yönetici hesabı açabilir ve istediği kadar seçim oluşturarak istediği kişiye istediği kadar mail yollayabilir. Mail servisine erişim ve yönetici hesabı oluşturulması/kullanılması aşamasında belirli denetleme veya kısıtlamalar getirilmelidir (Örneğin sadece Trakya.edu.tr mail hesaplarına izin verilebilir)

4.3 Uygulama kodlarına çok basit birkaç fonksiyonun testi yazılmıştır fakat daha fazla test yazılmalı ve uygulama bütünlüğü daha detaylıca gözden geçirilmelidir.

4.4 Şifreleme ve hashing mantığı uygulama içerisinde doğru bir şekilde kullanıldığı konusunda, dönem sürecindeki araştırmalar ve karşılıklı haftalık değerlendirmeler sonucunda hemfikir olunmuştur.

4.5 Ülke geneli seçimlerde veya katılımcı sayısının fazla olduğu seçimler için, Estonya’da bir dönem uygulanmış olan kartlı kimlik doğrulamalı bir seçim mimarisi uygulanabilir, bu seçim türünde seçmen kimlik kartı ile herhangi bir bilgisayarda kart okuyucu ile kimliğini doğruladıktan sonra oy kullanma işlemini gerçekleştirebilmektedir.

#### 6 KAYNAK KODLARI

Backend Kodları : <https://github.com/atakanertrk/Secure-Election-Project-API>

Frontend Kodları : <https://github.com/atakanertrk/Secure-Election-Project-ReactJS>

#### 7 Kaynaklar

<https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.sha256?view=net-5.0>

<https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rsa?view=net-5.0>

<https://core.ac.uk/download/pdf/11779635.pdf>

<https://auth0.com/docs/tokens/json-web-tokens>

<https://stackoverflow.com/questions/32785417/how-to-properly-create-a-sha256-hash>

<https://stackoverflow.com/questions/45418988/storing-passwords-safely-in-a-database>