

T.C.

TRAKYA ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİBÖLÜMÜ

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,

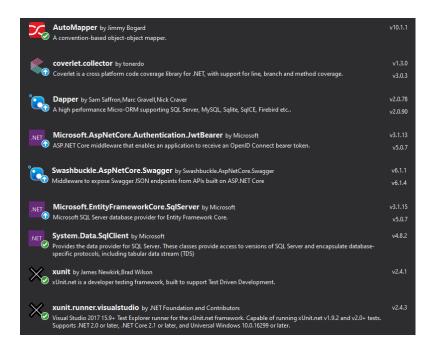
Test kodları için **xUnit**,

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

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

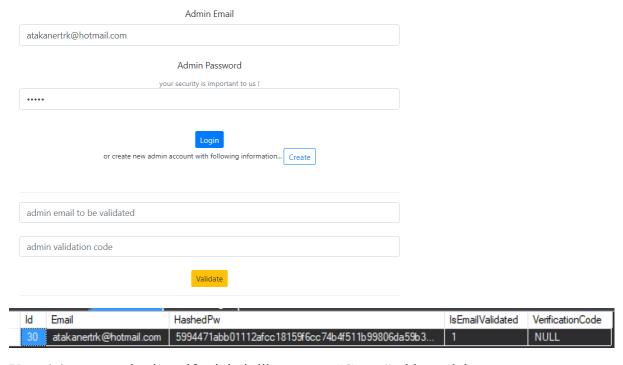
Seçmen ve yönetici şifreleri için SHA256, (System.Security.Cryptography)

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



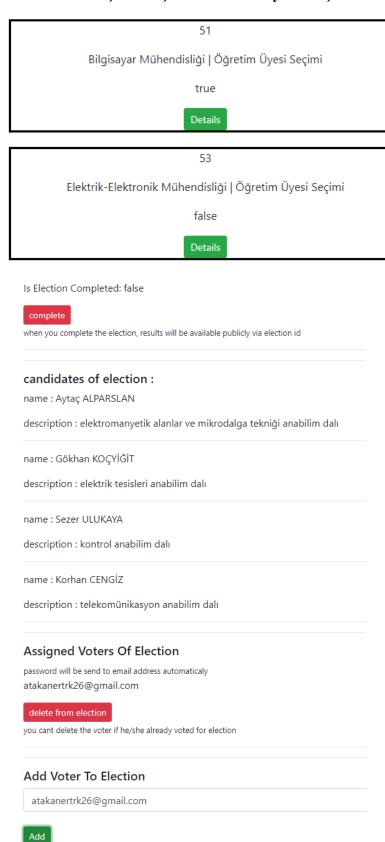
3 Uygulamanın Çalışması, Aşamaları ile Sırayla Anlatım

3.1 Yönetici Hesap Oluşturma ve Sisteme Giriş Yapması



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

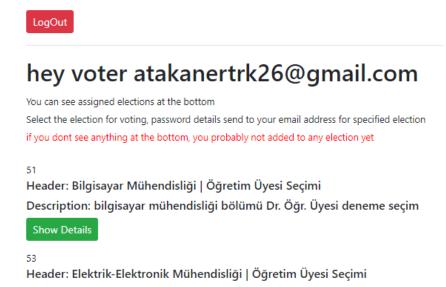
3.2 Yönetici Seçim Oluşturması ve Adayları Seçime Eklemesi



	ld	Email	HashedPw	ElectionId	Voted
1			a341c5f924e6e78ce37c40665bee10333d68cf850006fc33	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



Description: elektrik-elektronik mühendisliği öğretim üyesi deneme seçimi

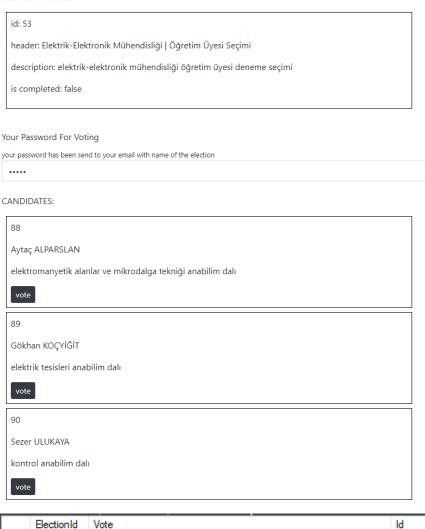
Seçmen e-mail adresi ile giriş yaptıktan sonra ilgili seçim için mail adresine gelen şifre ile oy kullanabilir.

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



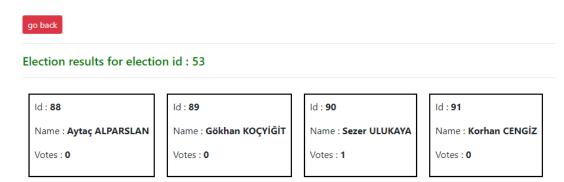
Show Details

ELECTION DETAILS:



Г		ElectionId	Vote	ld
1		51	PxI9WuJSbSXqXsTmNw3fU+F3wJ44nsm&tNpoAZ1F1AXkZunC	1007
2	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



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 Kodlari: 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/guestions/32785417/how-to-properly-create-a-sha256-hash

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