**VEB PLATFORMADA MÜƏYYƏN ŞİFRLƏMƏ ÜSULLARININ İSTİFADƏSİ**

1. **Məhəmməd TAĞIZADƏ, 2. Aysu QULİYEVA**

İnformasiya Təhlükəsizliyi ixtisası

Dövlət Gömrük Komitəsinin Akademiyası

**Xülasə**

Bu layihə hazırlanmamışdan əvvəl back-end və front-end proqramlaşdırma, şifrələmə alqoritmləri haqqında araşdırmalar edilmiş daha sonra isə tətbiq edilmişdir. HTML, CSS, JavaScript və müxtəlif kitabxanlardan istifadə etməklə yaradılmış bu veb sayt qeydiyyat, dörd növ şifrələmə üsulundan istifadə etməklə şifrələmə, həmin şifrələmə üsulları haqqında qısa məlumat, parolun dəyişdirilməsi və parolun bərpası əməliyyatlarından ibarətdir. Bu şifrələmə üsullarına MD5, tərs mətn, Sezar, base64 aiddir. Veb sayta daxil olmaqla istənilən şəxs bu şifrələmə üsullarından istifadə edərək hər hansı məlumatı şifrələyə və deşifrələyə bilər. Həmçinin, istifadəçinin hesabı yoxdursa qeydiyyatdan keçə, varsa daxil ola bilir.

**1.Giriş**

İstifadəçi veb saytda e-mail və parolunu qeyd edərək hesabına daxil olur. Əsas səhifədə komanda üzvləri, MD5, Sezar, Tərs mətn, Base64 bölmələrini və onlar haqqında qısa məlumatlar ilə tanış olur. Hər hansı bir şifrələmə üsulu seçilir və həmin bölməyə daxil olunur, daha sonra həmin bölmədə düz mətni daxil etmək üçün boş sahə, şifrləmə düyməsi, şifrələnmiş mətni ekranda göstərən sahə bizi qarşılayır. Mətn şifrələndikdən sonra şifrələnmiş mətn, deşifrə olunduqdan sonra isə deşifrələnmiş mətn uyğun olaraq ekranda göstərilir. İstifadəçi mövcud elektron poçt ünvanını və parolunu yazıb hesabına daxil olur, parolu unutduğu təqdirdə “Parolunuzu unutmusunuz?” bölməsinə daxil olub, elektron poçt ünvanını qeyd edib, həmin e-poçt ünvanına göndərilən link vasitəsi ilə parolu bərpa edir və dəyişir. İstifadəçinin hesabı yoxdursa qeydiyyat bölməsində tələb olunan məlumatları daxil edərək qeydiyyatdan keçə bilər.

**2.Əsas məlumatlar**

**Visual Studio:**

Microsoft Visual Studio Microsoft tərəfindən hazırlanmış inteqrasiya edilmiş inkişaf mühitidir (IDE). Microsoft Windows, Windows Mobile, Windows CE, .NET Framework, .NET Compact Framework və Microsoft Silverlight tərəfindən dəstəklənən bütün platformalar üçün yerli kodu və Windows Forms proqramları, vebsaytları, veb proqramları və idarə olunan kodu olan veb xidmətləri ilə konsol və qrafik istifadəçi. proqramların hazırlanmasında istifadə olunur.

Visual Studio-ya IntelliSense, eləcə də "kod refaktorinqini" dəstəkləyən kod redaktoru daxildir. İnteqrasiya edilmiş sazlayıcı həm mənbə səviyyəsində, həm də maşın səviyyəsində işləyir. Digər daxili alətlərə GUI proqramları yaratmaq üçün forma dizayneri, veb dizayneri, sinif dizayneri və verilənlər bazası sxemi dizayneri daxildir. O, demək olar ki, istənilən funksionallıq səviyyəsində daxil olmaqla, mənbə idarəetmə sistemləri (məsələn, Subversion və Visual SourceSafe kimi) üçün dəstək təklif edən plaginləri qəbul edir.

**MVC:**

MVC, yəni Model-View-Controller, hazırlanmış tətbiqləri hissələrə bölmək üçün ən sadə üsuldur. Onun hissələrə bölünməsinin səbəbi SOC Separation Of Concerns prinsipidir. Hər hissənin öz vəzifələri var.

Model – Tətbiqdə istifadə olunacaq məlumatların yerləşdiyi və verilənlər bazası ilə əlaqənin qurulduğu təbəqədir.

Görünüş - Modeldəki məlumatların vizuallaşdırılmasına cavabdeh olan təbəqədir.

Nəzarətçi – Model və Görünüş arasında əlaqəni təmin edən təbəqədir. Görünüşdən əlavə etmək, silmək, yeniləmək və s. sorğulara cavab verir.

Məsələn; istifadəçi məlumatları daxil etmək üçün görünüş qatında vizual forma sahəsi vasitəsilə təqdim edir. Göndərilən məlumatlar Controller səviyyəsində idarə olunur. Yoxlanılan məlumatlar uyğundursa, Model qatına köçürülür və əlavə tamamlanır. Yoxlama uğursuz olarsa, rəy View qatına göndərilir. Nəzarətçi qatında nəzarət əməliyyatları məcburi deyil.

**SQL Server Management Studio:**

SQL Server Management Studio (SSMS) Microsoft SQL Server daxilində bütün komponentləri konfiqurasiya etmək, idarə etmək üçün ilk dəfə Microsoft SQL Server 2005 ilə işə salınmış proqram təminatıdır. O, SQL 2000 və ya əvvəlki versiyalarda Enterprise Manager-in varisidir. Alətə həm skript redaktorları, həm də serverin obyektləri və xassələri ilə işləyən qrafik alətlər daxildir.

SSMS-in mərkəzi xüsusiyyəti istifadəçiyə serverdəki hər hansı obyekti nəzərdən keçirməyə, seçməyə və fəaliyyət göstərməyə imkan verən Object Explorer-dir. Microsoft həmçinin SQL Serverin köhnə versiyaları üçün geriyə uyğunluğu təmin etdi və beləliklə, SSMS-in daha yeni versiyasına SQL Server nümunələrinin köhnə versiyalarına qoşulmağa imkan verdi.

**3.İnkişaf etdirilən arxitektura**

**3.1 İstifadə olunan resurslar haqqında məlumat**

Web saytın hazırlanmasında ASP.NET Core Web App(Model-view-controller) istifadə olunmuşdur. MVC View-lar və Controller-lərdən ibarət olur. Buna əsasən bir neçə view və controller yaradılmışdır. Proqram Controller əsasında işləyir.

Hər bir Controllerin özünün View və uyğun olaraq metodları olur.

**1.HomeController**

HomeControllerdə olan view və metodlar:

**1.1.İndex:İndex view əsas səhifədir.**

**1.2.MD5:**

MD5 view MD5 şifrələmə səhifəsi üçündür. Burada MD5 metodunnan istifadə edərək düz mətn MD5 şifrələmə ilə şifrələnir.Burda əsas olaraq MD5 kitabxanasından istifadə olunmuşdur.

**1.3.Sezar:**

Sezar view sezar şifrələmə səhifəsi üçündür. Sezar metodunda js-də yazılmış encrpt funksiyasından istifadə olunmuşdur. Reset funksiyasında isə inputların dəyərləri sıfırlanır.

**1.4. Tərs mətn:**

Reverse view tərs mətn şifrələmə səhifəsi üçündür. Tərs mətn metodunda js-də yazılmış tərs mətn funksiyasından istifadə edərək düz mətn tərsinə çevrilir. Reset funksiyasında isə inputların dəyərləri sıfırlanır.

**1.5. Base-64:**

Base view base-64 şifrələmə səhifəsi üçündür. Base-64 şifrələmədə proqramlaşdırma istifadə olunan btoa, deşifrələmədə isə atob funksiyalarından istifadə olunub. Reset funksiyasında isə inputların dəyərləri sıfırlanır.

**2.AccountController**

**2.1. Daxil ol**

Login view sayt açılarkən bizi qarşılayan daxil ol səhifəsidir. Burada istifadəçi qeydiyyatdan keçdiyi istifadəçi adı və parol ilə daxil olur.

**2.2. Qeydiyyat**

Register view istifadəçinin qeydiyyatdan keçməsi üçündür. Qeydiyyatdan keçdikdən sonra email təsdiqləmək üçün daxil olunan mailə təsdiqləmə mail-i gedir və “Təsdiqlə” seçərək tam olaraq qeydiyyatdan keçilir.

**2.3. Parolunuzu unutmusunuz**

ForgotPassword view, istifadəçi parolunu unutmuş olarsa, “Daxil ol” bölməsində olan “Parolu Unutmusunuz?” seçərək parolun bərpası səhifəsinə keçid edir. Burada qeydiyyatdan keçdiyi email-i daxil edir. Daha sonra email-ə parolun bərpası üçün mail gəlir.

**2.4. Parolunuzu dəyişin**

ChangePassword view mail-ə gələn parolun bərpasında parolu dəyişmək üçün istifadə olunur.

HomeController və AccountController olmaqla iki controllerdən istifadə edirik. HomeControllerdə Əsas Səhifə, Md5, Sezar, Tərs mətn və Base-64 Viewlarını idarə etmək üçün metodlar vardır.

AccountControllerdə isə daxil olma, qeydiyyat, email təstiqləmə, parolun bərpası və dəyişdirilməsi üçün metodlar vardır.

**3.2 Qarşıya çıxan problemlər və onların həlli:**

**Problem:** Veb platformada sayt yaradılması üçün lazım olan proqram və məlumatlar.

**Həlli:** Veb saytın yazılması üçün Visual Studio 2019 proqramından istifadə edildi və saytın yazılması üçün lazım olan məlumatlar araşdırma aparılaraq əldə edildi.

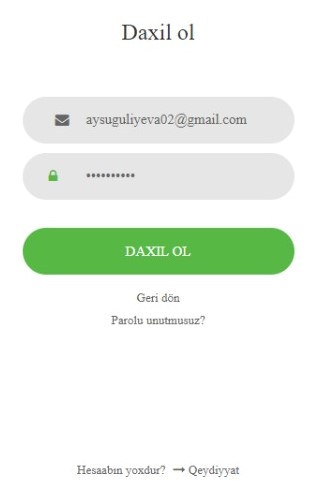
**Problem: “**Daxil ol” və “Qeydiyyat” bölmələrində istifadə olunacaq istifadəçi məlumatlarının saxlanılması üçün verilənlər bazası.

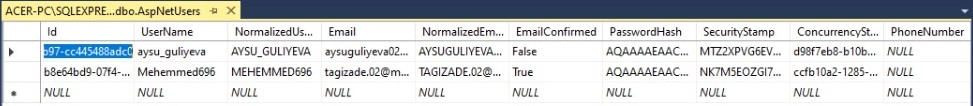
**Həlli:** Verilənlər bazasından istifadəyə olan ehtiyac SQL Server Management Studio (SSMS) istifadə edilməklə ödənildi. İstifadəçi məlumatlarının müvafiq olaraq sayta inteqrasiyası üçün lazım olan məlumatlar araşdırıldı.

**3.3 Proqramın yaradılması üçün istifadə olunan müddətlər:**

**Məhəmməd Tağızadə:** 11 gün, gün ərzində təxmini 2-3 saat

**Aysu Quliyeva:** 7 gün, gün ərzində 1-2 saat

**4. İstifadəçi kataloqu**

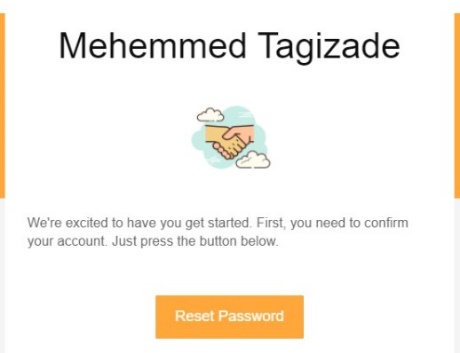
****

1. İstifadəçi sayta daxil olarkən e-mail və parolunu daxil edir, əgər məlumatlar sistemdə varsa girişə icazə verilir. Giriş e-mail ilə təsdiqlənir.

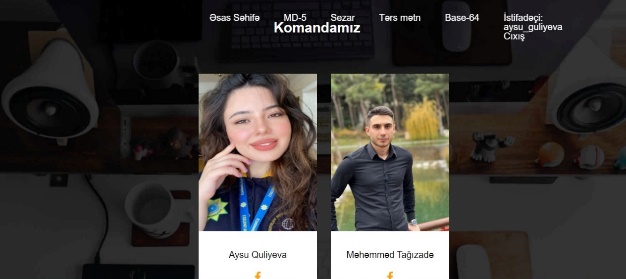


1. İstifadəçinin hesabı yoxdursa tələb olunan məlumatları daxil edərək qeydiyyatdan keçir.

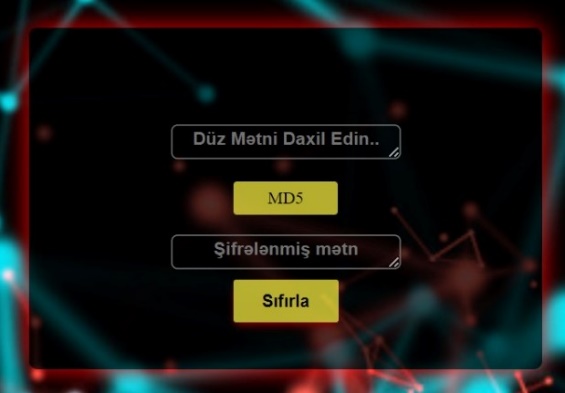




1. İstifadəçi parolunu unudarsa parolunu dəyişə və ya bərpa edə bilər.



1. Sayta daxil olduqda ekrana çıxan əsas səhifə. Müvafiq şifrələmə, deşifrələmə və qeydiyyat üçün bölmələr, komanda üzvləri və şifrələmə üsulları haqqında qısa məlumatlar mövcuddur.



1. İstifadəçi daxil etdiyi düz mətni MD5 şifrələmə üsulundan istifadə edərək şifrələyə bilər.



1. Sezar şifrəsindən istifadə etməklə mətnin şifrələnməsi. Burada istifadəçi düz mətni və sürüşdürmə dəyərini müvafiq olaraq daxil etməklə istədiyi mətni şifrələyə bilir.



1. İstifadəçi tərs mətn şifrələmə üsulu ilə daxil etdiyi mətni şifrələyə və prosesi sıfırlayıb yenidən başqa bir mətn daxil edə bilər.
2. İstifadəçi base64 şifrələmə üslundan istifadə etməklə istədiyi mətni şifrələyə və deşifrələyə bilir

**5. Nəticə**

Nəticədə, veb platformada istifadə olunan texnologiyalar, proqramlaşdırma dilləri, proqramın istifadəsi və kitabxanalar üzrə araşdırmalar nəticəsində yeni məlumatlar öyrənilib. Şifrələmə/Deşifrələmə, proqramlaşdırma məntiqi, veb proqramlaşdırma ilə bağlı bilik və təcrübə qazanılıb. Biz komanda olaraq nəticəyə çata bildik və kodlarımızda heç bir problem yaşamadıq.

**İstinadlar:**

1. <https://tr.wikipedia.org/wiki/Microsoft_Visual_Studio>
2. <https://www.yusufsezer.com./>
3. <https://visualstudio.microsoft.com/tr/>