

**GÜVENLİ YAZILIM GELİŞTİRME DERSİ**  
**SG508**  
**DÖNEM 2**  
**ÖDEV 1**

**Hazırlayan**

**1650Y12054**

**Meliha Eren**

[meleren@yahoo.com](mailto:meleren@yahoo.com)

**1650Y12170**

**Serpil Ercan**

[serpillercann@gmail.com](mailto:serpillercann@gmail.com)

## Tehdit Risklerini Modelleme

1. Saldırgan diğer kullanıcıların mesajlarını okuyabilir  
\* Paylaşılan bir bilgisayarda kullanıcı sistemden çıkmamış olabilir.
2. Veri doğrulanması SQL girişine izin verebilir.
3. Yetkisiz ulaşımın izin vermemesi. Yetki kontrolünü gerçekleştirme

1. Paylaşılan bir bilgisayarda kullanıcı t zaman sonra sistemden çıkarılması.

```
private void GirisKontrol()
{
    if (Session["User_Kod"] != null)
    {
        if
        (Convert.ToDateTime(Session["User_GirisZamani"].ToString()).AddMinutes(1) <
        System.DateTime.Now)
            Session["User_Kod"] = null;
    }
}
```

2. Veri doğrulanması SQL girişine izin verebilir.

```
//güvensiz giriş için yazılan kod
string query = " select KulAdi,KulAdi Tanim,Yetki,BayiId from Kullanici
where KulAdi= '" + TxtKullanici.Text + "' and Sifre= '" + TxtSifre.Text +
"'" ;
// güvensiz Kullanıcı: ' or 1=1--

SqlCommand cmd = new SqlCommand (query, conn);

//güvenli giriş için yazılan kod ile değiştirildi

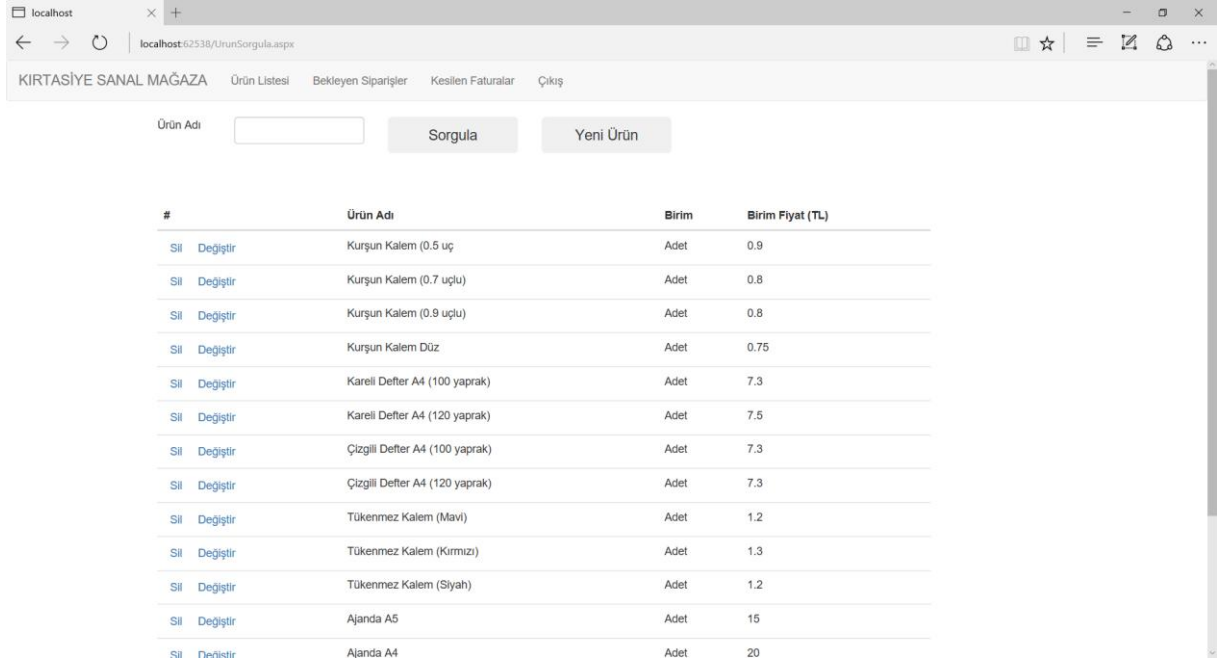
string query = " select KulAdi,KulAdi Tanim,Yetki,BayiId from Kullanici
where KulAdi= @KulAdi and Sifre= @Sifre";

SqlCommand cmd = new SqlCommand(query, conn);
cmd.Parameters.Add("@KulAdi", SqlDbType.VarChar, 20).Value =
TxtKullanici.Text;
cmd.Parameters.Add("@Sifre", SqlDbType.VarChar, 30).Value = TxtSifre.Text;
```

### 3. Yetki kontrolünü gerekleřtirme . Yetkisiz ulařıma izin vermeme.

Toptancı kullanıcısıyla girildiğinde Urunsorgula.aspx sayfasında insert, delete, update iřlemleri yapılabilmekte (bakınız 1.urunsorgula.aspx)

#### 1.Urunsorgula.aspx



#	Ürün Adı	Birim	Birim Fiyat (TL)
Sil Değiřtir	Kurřun Kalem (0.5 uç	Adet	0.9
Sil Değiřtir	Kurřun Kalem (0.7 uçlu)	Adet	0.8
Sil Değiřtir	Kurřun Kalem (0.9 uçlu)	Adet	0.8
Sil Değiřtir	Kurřun Kalem Düz	Adet	0.75
Sil Değiřtir	Kareli Defter A4 (100 yaprak)	Adet	7.3
Sil Değiřtir	Kareli Defter A4 (120 yaprak)	Adet	7.5
Sil Değiřtir	Çizgili Defter A4 (100 yaprak)	Adet	7.3
Sil Değiřtir	Çizgili Defter A4 (120 yaprak)	Adet	7.3
Sil Değiřtir	Tükenmez Kalem (Mavi)	Adet	1.2
Sil Değiřtir	Tükenmez Kalem (Kırmızı)	Adet	1.3
Sil Değiřtir	Tükenmez Kalem (Siyah)	Adet	1.2
Sil Değiřtir	Ajanda A5	Adet	15
Sil Değiřtir	Ajanda A4	Adet	20

Senaryoya göre bayi kullanıcısının ürünler tablosunda sadece select yapma yetkisi olmalı. Buna göre Bayi kullanıcısı ile sisteme girilip urunsorgula.aspx çağrıldığında ařağıdaki sayfa ile karşılaşılmakta(bakınız 2.urunsorgula.aspx )

## 2. urunsorgula.aspx

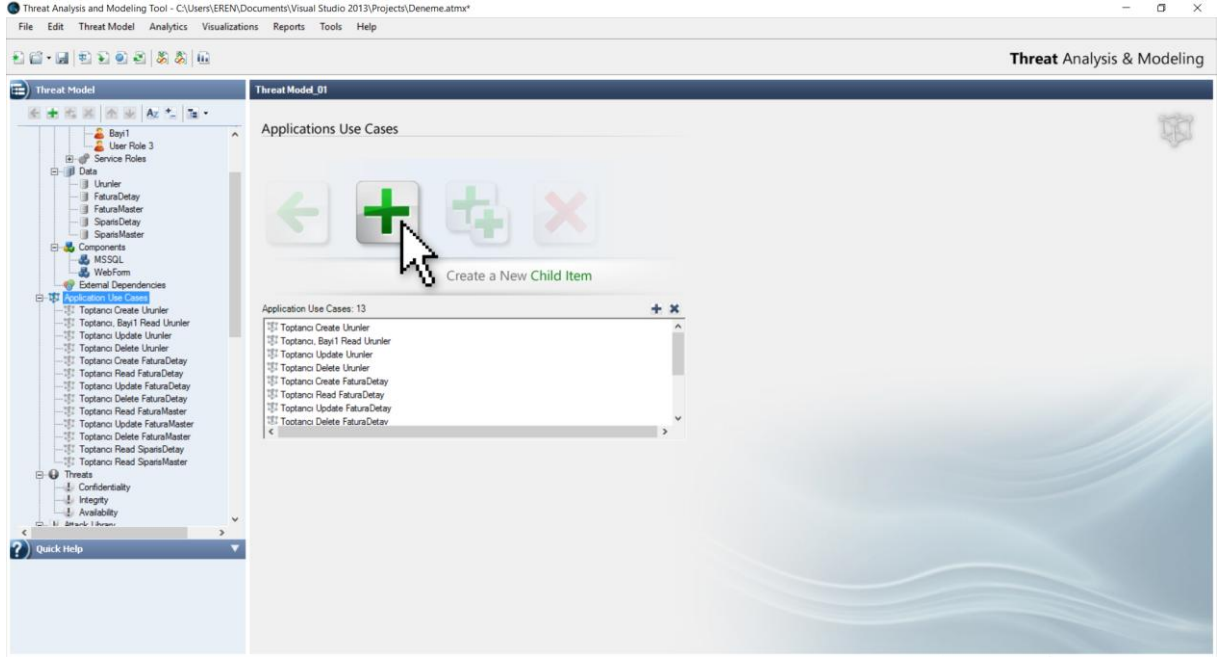


Yetkiniz Yok(Yetki seviyesi:1)

[Giriş Sayfası için tıklayın...](#)

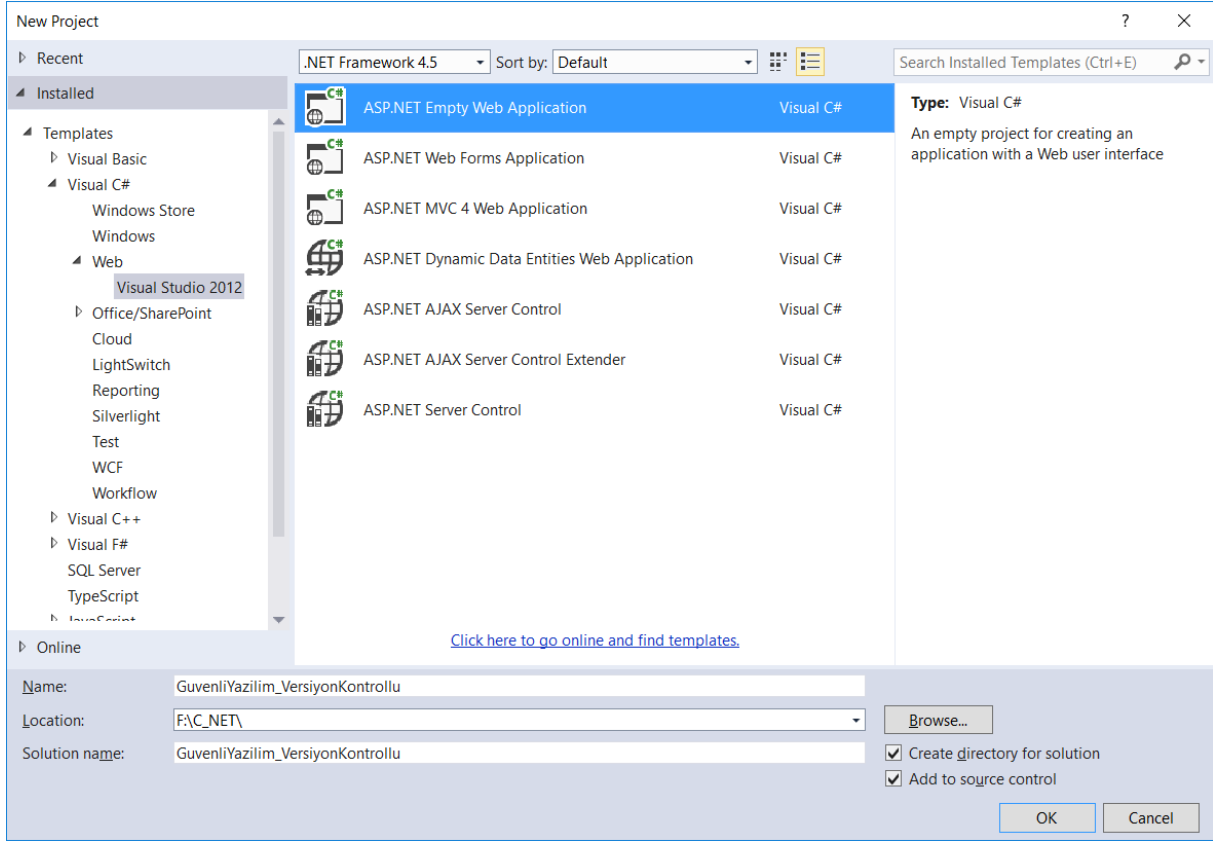
## Tehdit Risklerini Modelleme

Microsoft'un tehdit modelleme yöntemi kullanıldı. Threat Analysis and Modeling Tools [1] programı kuruldu ve program modeli oluşturuldu.

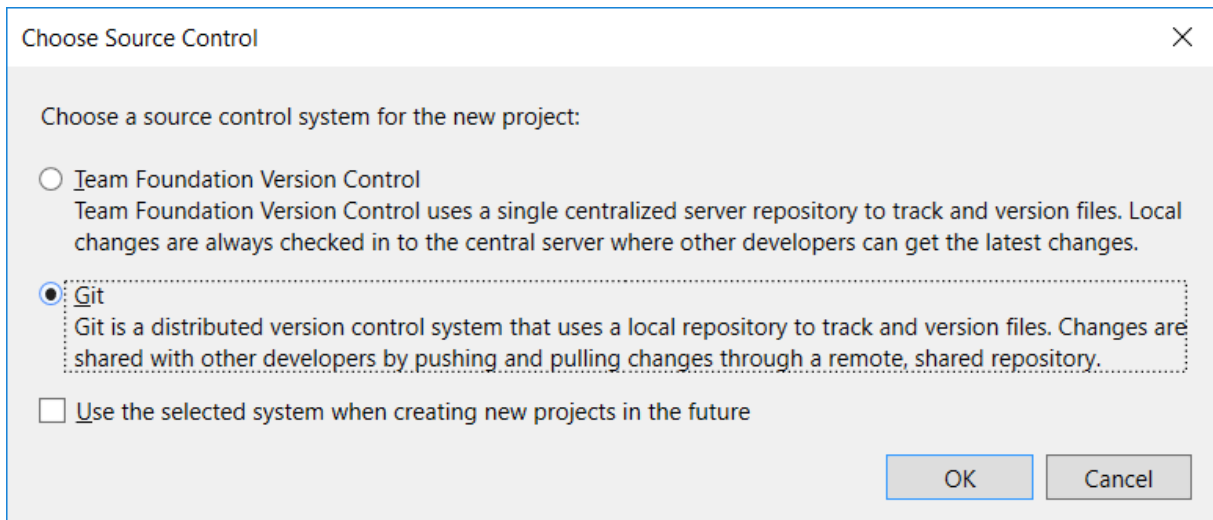


## Sürüm Denetimi

Yeni proje oluşturulurken sağ alt kısımda Add to source control seçeneği seçilir.



Git sürüm denetimi standardı kullanıldı.



Sızma testi için OWASP ZAP kullanıldı.

[illegible]

## KAYNAKLAR

1. <http://realsearchgroup.org/SEMaterials/tutorials/msthreatmodeling/>
- 2.