

GÜVENLİ YAZILIM GELİŞTİRME

ARA SINAV

Çalışma kapsamında, klasik yazılım geliştirme yaşam döngüsünü kullanarak güvenli olmayan bir web uygulaması (konu seçiminde sınırlama yoktur) geliştirmeniz beklenmektedir. **Ara Sınav** için kullanılacak bu çalışmada istenenler aşağıda listelenmektedir.

1. Uygulama nesne yönelimli olarak geliştirilmelidir. Uygulama geliştirme çatısı kullanılmamalıdır.
2. Uygulamada giriş ekranı bulunmalı ve veritabanına bağlanılarak kullanıcı doğrulaması yapılmalıdır. Giriş ekranı dışındaki tüm sayfalara sadece yetkili kullanıcıların (**en az iki yetki düzeyi bulunmalıdır**) girebilmesi sağlanmalıdır.
3. Yetkisiz erişimleri önlemek ve oturum süresini ayarlamak için oturum değişkenleri kullanılmalıdır.
4. Web tabanlı olarak geliştirilmesi gereken uygulama, veritabanı üzerinde arama, ekleme, silme ve güncelleme yapan sayfalar içermelidir.
5. Uygulama içerisindeki giriş noktaları için filtreleme (doğrulama ve temizleme) yapılmamalıdır (Saldırılara açık olmalıdır).
6. İstemci Sunucu arasındaki haberleşme için asenkron iletişim (**AJAX**) kullanılmalıdır.
7. Uygulama geliştirilirken zafiyet oluşturmaya imkan verecek teknolojiler, komutlar, ifadeler v.s., tercih edilmelidir.
8. Kullanılacak programlama dili, VTYS ve teknolojiler konusunda sınırlama bulunmamaktadır.
9. Sürüm Denetim Sistemi kullanılmalıdır.
10. Uygulama içerisinde OWASP Top 10 Listesindeki tüm güvenlik açıklıkları bulunmalıdır.
11. Sızma Testleri Yapılmalıdır.
12. Statik Kod Analizi Yapılmalıdır.
13. Uygulamaya ait ihtiyaç listesi (requirement list), sınıf şeması (class diagram), kullanım senaryosu (use case scenario), en az iki kullanım durumuna (use case) ait; etkinlik şeması (activity diagram) ve zamanlama şeması (sequence diagram) içeren raporu (Kapak sayfasında numara, ad, soyad ve e-posta bilgileri bulunmalıdır) **Rapor.pdf** adı ile uygulamanızın ana klasörü içerisinde yer almalıdır.
14. Uygulamanızın **kaynak kodları**, veritabanını içerisindeki verilerle birlikte oluşturan **sql ifadeleri ve Rapor.pdf** dosyası ara sınav gününden önce **guvenliyazilimgelistirme@gmail.com** e-posta adresine gönderilmelidir.
15. Geliştirilen uygulamalarla ilgili sözlü sınav **Ara Sınav günü ders saatinde yapılacaktır.**
Tüm grup üyelerinin katılımı zorunludur.
16. Uygulama için 2 yada 3 kişilik gruplar oluşturulmalıdır.