1-

Profile Anotasyonu:

@Profile

Bu anotasyonu uygulamamızdaki amacımız farklı çalışma isteklerine göre programımızın hangi istere göre çalışacağını seçmemizi sağlamaya yarar.

İşbaşı uygulamamızdaki kayıt işlemlerinin bireysel ve kurumsal şekilde yapıldığını düşünürsek, service katmanındaki kayıt işlemleri için loginService isminde bir interface oluşturup bu interface'den implement eden iki class oluşturacağız, bunlar loginServiceIndividual ve loginServiceCorporate olacak. Service kısmındaki bu iki class'ımıza ait @Profile("indivudual") ve @Profile("corporate") anotasyonunu ekleyeceğiz. Bu spring componentlerinin hangisinin çalışmasını istiyorsak eğer application.proporties dosyasında bunu belirliyoruz ve şu şekilde yapıyoruz:

spring.profiles.active=induvidual ya da

spring.profiles.active=corporate

şeklinde gerçekleştiriyoruz.

2-

SQL İnjection:

Veri tabanına dayalı uygulamalara saldırmak için kullanılan bir atak şeklidir, burada saldırgan SQL dilinden faydalanarak uygulama ekranındaki ilgili yere yeni SQL ifadelerini yazarak elde eder.

Web sitesinde herhangi bir form doldururken ya da yorum yaparken, arka planda veri tabanına bir SQL sorgusu göndeririz ve veri tabanı ile bir iletişim kurulur.

Örnek:

Kullanıcı adı ve şifresi:

ID: mujdat

Password: 9876543210

Şeklinde olsun. Biz bu sisteme bu kullanıcı adı ve şifresi ile giriş yapabiliyoruz ancak şifreyi şu şekilde yaparsak eğer;

555' OR 1=1 #

Sisteme aynı şekilde yine giriş yapacaktır ve bunun anlamı ise şudur: Eğer şifre 555 ise sisteme giriş yap eğer değilse 1=1 ise giriş yap, zaten bu sürekli true olduğu için sisteme giriş yapacaktır.

Biz şifre girmeden bile sisteme şu şekilde giriş yapabiliriz:

mujdat'#

şeklinde denediğimizde şifre kullanmadan sisteme giriş yapabileceğimizi göreceğiz.

Nasıl Engellenir?

- Yazılımların güncel olmasına dikkat edeceğiz.
- Web uygulamanızdaki tüm formlarda ben robot değilim doğrulamasını kullanacağız.
- Kullanıcılara çift faktörlü giriş yapmalarını zorlayacağız.
- Web uygulaması üzerinde gerçekleşen şüpheli sorguları ve istekleri analiz edebilen web tabanlı bir firewall (WAF) yazılımını devreye alacağız.
- Uygulamanızın arka planda sorduğu soruları gözden geçirip özellikle NULL karakterlerin yer aldığı sorguları tekrar düzenleyeceğiz.
- Yönetici ve tam yetkili rolündeki kullanıcı adlarında ‘administrator’, ‘admin’, ‘yönetici’ gibi akla gelebilecek kullanıcıları devre dışı bırakıp yetkili rolündeki kullanıcı adlarının gerçek isim veya uygulama ismi olmasına dikkat edeceğiz.
- Tüm hareketleri merkezi log toplama veri tabanında toplayıp şüpheli işlemler için anlık alarm ve yetkili kullanıcıya e-posta gönderimini sağlayacağız.
- Kişisel Verileri Koruma Kanunu kapsamında verilerimizi koruyabileceğimiz Berqnet firewall cihazını kullanacağız.