**1 – SOAP vs Restful ?**

**SOAP:**

İnternet üzerinden küçük miktarda bilgileri yada mesajları aktarma protokoludur. SOAP mesajları XML formatındadırlar ve genellikle HTTP(Hyper Text Transfer Protocol) protokolu(bazende TCP/IP) kullanılarak gönderilirler.

SOAP ,XML tabanlı kullanıma mecbur bırakır. Son zamanlarda xml kullanımı dışına çıkması için çalışmalar yapsa da Restfull servisler sonrası populeritesini yitirmiştir.

**WSDL:**

OAP isteklerini oluşturmak için de bir standart gerekmektedir. İşte burada WSDL devreye girmektedir. WSDL gerçekleştirilebilecek bütün SOAP isteklerinin kayıtarını tutan, XML tabanlı web servisleri tanımlamak ve yerini belirtmek için tanımlanmış dildir.

**RESTFUL**

Rest, HTTP protokolünü kullanarak, URL adresleri üzerinden veri ve dosya alışverişi sağlayan bir yapıdır. Rest API ise Rest işlemini yapabilmek için kurgulanmış modüle verilen isimdir. Bu API (Modül) yardımıyla Rest işlemleri ve veri alışverişi yapılıyor.

Neden Rest?

* Rest ile veri akışları SOAP’taki XML yerine daha hafif bir yapıdaki JSON formatı yardımıyla gerçekleşir.
* SOAP’taki RPC gibi karmaşık bağlantı yapıları yerine HTTP protokolü kullanılır.
* SOAP gibi sert standartlara göre daha esnek yapısı vardır.
* SOAP gibi Proxy kullanımına zorlanmazsınız.
* Kolay entegre edilebilen bir yapıdadır.

Rest ile oluşturulan Server – Client bağlantısı sonucunda veri alışverişi belirli istekler sayesinde gerçekleşir. Rest sırasında kullanılan HTTP istekleri ve işlevleri aşağıdaki gibidir;

* GET, veri listelemek ve görüntülemek için kullanılır.
* POST, veri eklemek için kullanılan bir istektir.
* DELETE, veri silmek için kullanılır.
* PATCH, verinin bir kısmının güncellenmesi için kullanılan bir istektir.

**2 - Difference between acceptance test and functional test ?**

Kabul testlerindeki amaç;

Yazılımın sunulacağı kullanıcı grubunun yazılımı çalışıyor olarak kabul edebilmesi için gerekli olan işlemlerin gerçekleştirilebilip gerçekleştirilemeyeceğinin kontrolüdür.

Fonksiyon test ise;

Yazılım test teknikleri arasında testin kalbi denilebilir. Kapalı kutu testidir. Birçok test türü bu tanımın altında bulunur. Gereksinimlerin sağlanıp sağlanmadığının kontrolü yapılır. Kullanıcı kabul testleri ile büyük ölçüde örtüşür. Çoğu zaman aynı test setleri her ikisine de uygulanabilir. Sistem seviyesindeki fonksiyonel testler, sistemin davranışının gereksinim belirtimlerine uymasını sağlamak için kullanılır. Sistem için tüm fonksiyonel gereksinimler sistem tarafından yerine getirilmelidir. Fonksiyonel testler doğası gereği kapalı kutu testlerdir. Tüm fonksiyonlar test edilmelidir. Aşağıdaki hedeflere odaklanmalıdır:

* İzin verilen tüm girdiler (input) yazılım tarafından kabul edilmelidir. İzin verilmeyen girdiler reddedilmelidir.
* Olası tüm sistem çıktıları (output) incelenmelidir.
* Tüm sistem durumları ve durum geçişleri uygulanmalı ve incelenmelidir.
* Tüm fonksiyonlar için uygulanmalıdır.

**3 - What is Mocking ?**

Mock, test konseptinde sahte (fake) object üretmektir. Faydası Unit Test’in temel kurallarından olan Test In Isolation prensibini karmaşık yapılara uygulayabilmemizdir.  Bir tane web service kullanımı yapan class’ınız varsa bu class’ın aynı method’ları içeren fake versiyonu kodlayıp test içerisinde bu object oluşturularak kullanılır.

**5- HTTP/POST vs HTTP/PUT ?**

POST, veri eklemek için kullanılan bir istektir.

PUT, ekli verileri güncellemek için kullanılan bir istektir.

POST kaynağa veri göndermek için kullanılır. PUT ise aynı kaynağa aynı adres ile erişilir ve eğer içerik var ise gelen veriler ile değiştirilir, eğer içerik yok ise yeni içerik yaratılır. Kısaca PUT veri güncellemek için kullanılır.

**6 - What are the Safe and Unsafe methods of HTTP ?**

Http’de SSL sertifikası yoktur.

Https’de var olan SSL Sertifikası, bilgi aktarım aşamasında şifreleme yöntemi kullanır. Tarayıcıların süzgecinden geçen sertifika, tanınınca site açılır ve güvenle işlem yapılmasını sağlar. Ancak sertifika bulunmuyorsa tarayıcı, siteye güvenip güvenmediğini kullanıcıya sorar. Böylece kullanıcılar, güvenli siteler ile güvenli olmayan siteler arasında ayrım yapabilme özgürlüğüne kavuşur.

– SSL Güvenlik Sertifikası ve bunun URL’deki yansıması olan https, ödeme işlemlerinin yapıldığı e-ticaret sitelerinde, kart bilgilerinin bankaya aktarılırken şifrelenmesini ve bankadan gelen bilgilerin de şifreli olmasını sağlar. Böylece kullanıcı bilgilerinin, 3. şahıslar tarafından ele geçirilmesinin önüne geçer.

– Https, http’ye göre çok daha hızlı yükleme süresine sahiptir. Yani https’li sayfalar, http’li sayfalara göre çok daha hızlı yüklenir. Bu da arama motoru optimizasyonu (SEO) konusuna önem veren e-ticaret sitelerinin https’yi yani SSL Sertifikasını tercih etmeleri için bir başka nedendir.

**7 - How does HTTP Basic Authentication work ?**

Bir kullanıcının o sayfaya girebilmek için kendisini doğrulaması gerekir. HTTP protokolünde yer alan kimlik doğrulama sistemidir. HTTP isteklerinde Authorization başlığının içerisinde bir kelime Basic ve ardından bir boşluk bırakılıp base64 ile şifrelenmiş username:password verisi bulunur.

Örnek olarak kullanıcı adı: admin ve şifre: password123 olsun. Bunun çıktısı aşağıdaki gibi olacaktır.

Authorization: Basic YWRtaW46cGFzc3dvcmQxMjMK

**8 - Define RestTemplate in Spring ?**

RestTemplate, client tarafında senkronize HTTP isteklerini yürütmek için Spring kütüphanesi içindeki default sınıftır.

Avantajları; RestTemplate thread-safe bir yapıdadır RestTemplate servlet yapısı üzerine inşa edilmiştir. Bu yüzden thread-per-request yaklaşımını izler. Sonuç olarak uygulama, thread-pool’u tüketecek veya tüm kullanılabilir belleği kaplayacak birçok thread oluşturacaktır. Bu sebeple performans problemleri ortaya çıkacaktır.

Spring 5 ile birlikte bakım moduna geçmiştir. Muhtemelen ilerleyen sürümlerde desteklenmeyecektir.

**9 – What is the difference between @Controller and @RestController ?**

Controller’lar class düzeyinde @Controller notasyonu ile tanımlanıyor. Bu da aslında class düzeyinde ekstradan @Component notasyonunu yazmaktan bizi kurtarıyor ve bu sınıfın bir Controller olduğunu belirtiyor.

RestController ise @Controller ve@ ResponseBody’nin birleşiminden oluşan bir streotype. Dolaylı olarak da @Controller üzerinden @Component notasyonunu da barındırıyor. @Controller notasyonunun aksine @RestController datanın kendisini JSON veya XML formatı ile direkt olarak sunabiliyor.

**10 – What is DNS Spoofing ? How to prevent ?**

DNS zehirlenmesi, Domain Ad Sistemi sunucusunun ön bellek veritabanına veri eklenmesi ya da oradaki verilerin değiştirilmesiyle oluşur. Bu durum oluşurken; yanlış IP adreslerinin dönmesi veya trafiğin başka bir bilgisayara yönlendirilmesi gerçekleşir. Genellikle, trafiğin; saldırıyı yapanın bilgisayarına yönlendirilmesine neden olur.

DNS zehirlenmesi türünde bir saldırıya uğradığınız zaman, bir internet adresine gitmeye çalıştığınızda; istek, farklı bir adrese doğru yönlendirilir. Yönlendirilen sitelerden kullanıcının bilgisayarına çeşitli virüsler, tarayıcı korsan programları gibi zararlı yazılımlar da yüklenebilir. Ayrıca, kullanıcı; gitmeye çalıştığı siteye çok benzeyen sahte bir siteye yönlendirilebilir ve tuzağa düşürülebilir.

Önlem olarak DNS ön belleği belirli aralıklarla temizlenebilir.

**11 – What is content negotiation ?**

Client ve server arasında yapılan bir içerik anlaşması veya müzakeresidir diyebiliriz.  Amacı, aynı URI ile farklı döküman türlerinde içerik sunabilmektir. Yani daha genel bir ifadeyle kaynak gösterim şeklinin kullanıcılar tarafından belirlenmesi diyebiliriz.

**12 – What is statelessness in RESTful Web Services ?**

 REST standartlarında istemci-sunucu arasında taşınan verilerde ekstra başlık bilgileri saklanmaz, istemciye ait detaylar bulunmaz, bu bilgiler istemci-sunucu arasında taşınmaz.

**13- What is CSRF attack? How to prevent ?**

CSRF saldırısı, daha önce kimliği doğrulanmış başka bir web sitesi aracılığıyla bir web uygulamasına istek gönderen kötü amaçlı bir bağlantı içerir. Elde edilen kimlik bilgileriyle mağdur kimliğine bürünülür ve kötü amaçlı faliyetlerde kimlik doğrulama bilgisi atlanılmış olur.

**Önlemler;**

* Kullanıcıya  her oturum için random ve benzersiz “token” bilgisi verilir.
* Kullanıcıdan alınan önemli veriler POST metodu ile alınmalıdır.
* Bir web formunda captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) bilgisi doğru girilmediği sürece işlem gerçekleştirilemeyeceği için “CSRF” saldırısına karşı alınacak bir önlem niteliğindedir.
* Web uygulama verileri ve cookie bilgileri düzenli aralıklarla temizlenmelidir.
* Kişisel bilgilerin bulunduğu web uygulamalarının oturum bilgileri bilgisayarda kayıtlı tutulmamalıdır.
* Kaynağı belirsiz mail ve bağlantılara dikkat edilmelidir.

**14 - What are the core components of the HTTP request and HTTP response ?**

HTTP Response genel olarak 3 ana bileşene sahiptir:

* Status Line
* Headers
* Body (Optional)

HTTP Response genel olarak 3 ana bileşene sahiptir:

* Request Line
* Request Header
* Request Body