

SORU 1 :

-SOAP (Simple Object Access Protocol), uzun zamandır var olan protokola ulaşan, standart esaslı web servisidir.Microsoft tarafından geliştirilir.

-REST (Representational State Transfer) SOAP eksikliklerine yanıt olarak yapılmış başka bir standarttır.SOAP'taki sorunları düzeltmek ve web servisine ulaşan saha kolay methodlar bulmak için kullanılır.

SORU 2:

Functional test geliştirici çalıştığını düşündüğü sürece ürünün çalıştığını söyler.Acceptance test ürünün aynı zamanda çözmek için yapıldığı sorunları da çözdüğünü söyler.Bu en iyi kullanıcı tarafından yapılabilir, örneğin yazılımın asist ettiği görevleri yerine getirmek.

SORU 3 :

Mocking test edilen birim dış bağımlılıklara sahip olduğunda kullanılan bir tür süreçtir.Mocking yapmadaki amaç test edilen koda odaklanmak, izole etmektir.

SORU 5:

Post: db ye veri create etmek için kullanılır.

Put: var olan veriyi değiştirmek veya güncellemek için kullanılır.

SORU 6 :

-GET/HEAD/OPTIONS/TRACE = Safe methods

-PUT/DELETE = Unsafe methods

SORU 7 :

HTTP kontrole ulaşma ve doğrulama için genel bir çerçeve temin eder.En bilinen HTTP doğrulaması 'Basic' şemaya yöneliktir. Bu sayfa, doğrulama için HTTP çerçevesine girişi ve HTTP 'Basic' şemayı kullanarak nasıl sunucumuza girişi engelleyebileceğimizi gösterir.

SORU 8 :

RestTemplate kullanıcı tarafı HTTP ulaşımı için ana Spring sınıfıdır.Konsept olarak JdbcTemplate, JmsTemplate'e benzerdir.

SORU 9 :

Controller, Spring içerisinde uzun zamandır bulunan bir annotation. Diğer yandan ise @RestController, Spring 4.0 ile framework bünyesinde katıldı. Temel amacı adından da anladığımız gibi REST endpoint'leri üretmeyi sağlamak. Aslında bunun bize sağladığı şey @Controller ve @ResponseBody notasyonlarını tek seferde vermesi. Bu sayede REST controller olmasını isteyeceğimiz her metoda @ResponseBody yazmaktan da kurtulmuş oluyoruz.

SORU 10 :

DNS spoofing, genel olarak siber korsanların web trafiğini sahte web sunucularına ve kimlik avı için hazırlanmış web sitelerine yönlendirdiği siber saldırıları kapsar. DNS servis sağlayıcısı veya web sitesi sahipleri, tehditleri yönetmek için çeşitli araçlar ve protokoller kullanarak kullanıcıları korumak adına adımlar atmalıdır.

SORU 11:

Content Negotiation işleyişi HTTP protokolüne özgü bir kavramdır. Kullanıcı ve sunucu arasında yapılan bir içerik anlaşması veya müzakeresidir.

SORU 13:

CSRF (Cross Site Request Forgery) genel yapı olarak sitenin açığından faydalanarak siteye sanki o kullanıcıymış gibi erişerek işlem yapmasını sağlar..Genellikle GET requestleri ve SESSION işlemlerinin doğru kontrol edilememesi durumlarındaki açıklardan saldırganların faydalanmasını sağlamaktadır.