Web Servis Güvenliğine Dair

written by Mert SARICA | 23 March 2011

Ağırlıklı olarak xml tabanlı olan web servisler genelde iki farklı uygulamanın birbiri ile ortak bir dil üzerinden haberleşmesi amacıyla kullanılmaktadır. Bu sayede farklı programlama dilleri ile yazılmış iki uygulama birbirleri ile haberleşirken bir web servis kullanarak haberleşme esnasında ortaya çıkabilecek yazılımsal/tasarımsal uyumsuzlukları veya engelleri ortadan kaldırmaktadır.

Çoğunlukla son kullanıcı bir web uygulaması ile etkileşimde bulunurken arka planda bu uygulama, kullanıcıya sunacağı içeriği farklı sunuculardan web servis aracılığı ile toplamakta ve harmanladıktan sonra kullanıcıya sunmaktadır.

Web servis denilince çoğu kişinin aklına XML ve SOAP gelmektedir. SOAP, XML kullanarak uygulamalar arası bilgi alışverişinin nasıl sağlayacağını tanımlayan bir standart, bir protokoldür. XML ise veri göstermek amacıyla kullanılan HTML'in aksine, veri taşımak ve saklamak için kullanılan bir dildir.

Web servislerine yönelik tehditlerin başında XML enjeksiyonu, XPath enjeksiyonu, XML bombası, paramatre manipülasyonu, WSDL taraması ve daha bir çok tehdit gelmektedir.

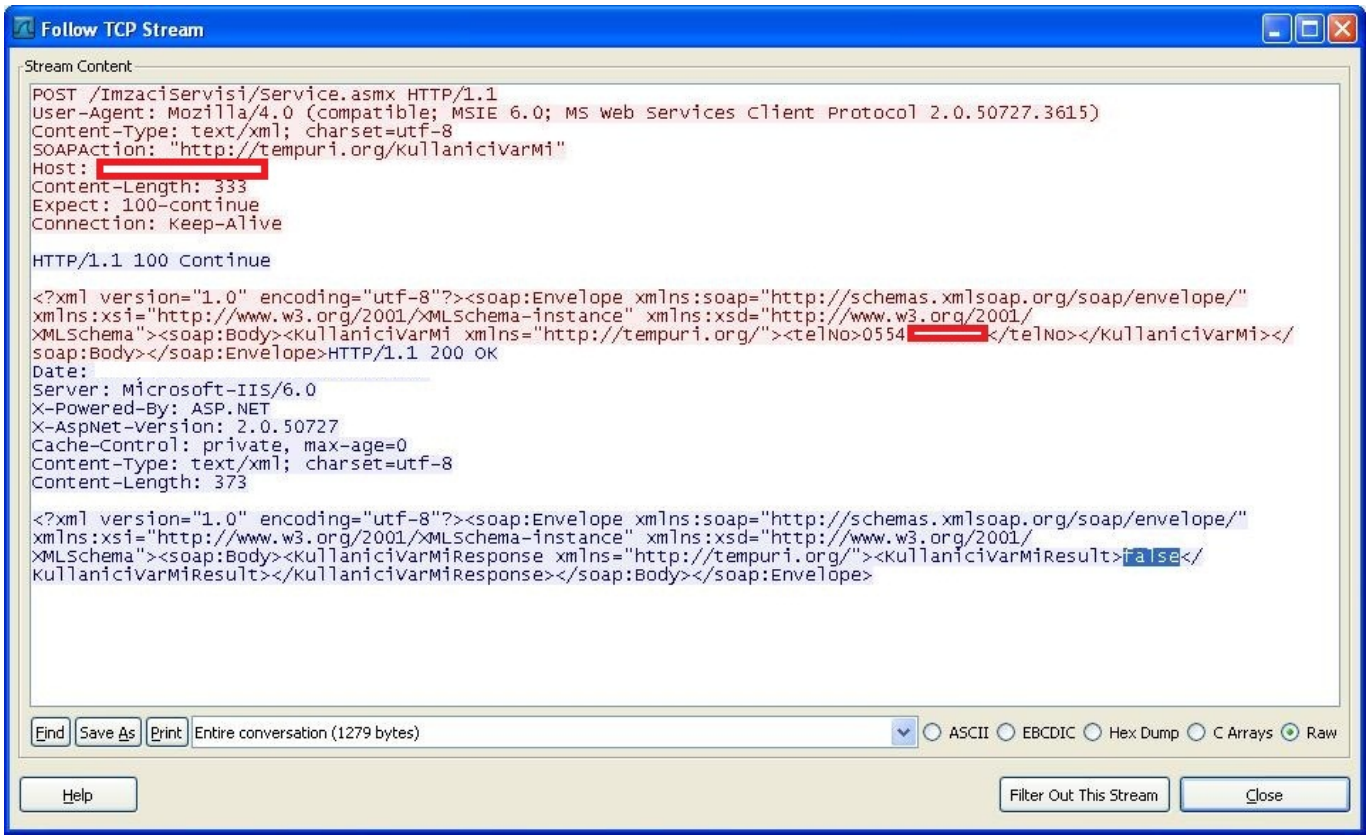
Web Services Description Language (WSDL), bir web servis ile iletişim kurulabilmesi için gerekli parametreleri, metodları içerir. WSDL'i dış dünyaya açık olan bir web servis üzerinde yer alan servis yukarda bahsi geçen tehditlere mağruz kalabildiği gibi servisin ve hizmetin kötüye kullanımını da yol açabilmektedir.

Örnek olarak X firmasının sitesinde yer alan bir gsm firmasına ait olan imzalama yazılımına kısaca göz atalım.

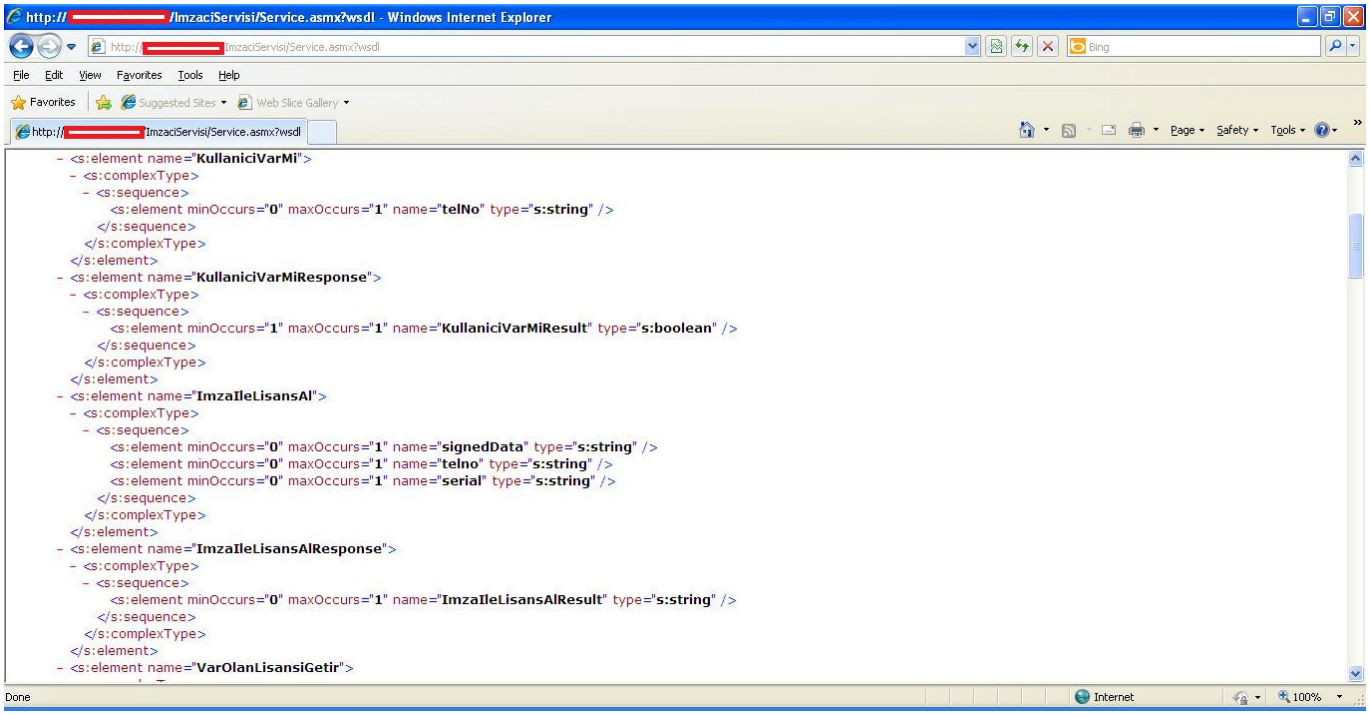
Bu imzalama programı, mobil imza kullanıcılarının kişisel bilgisayarlarındaki dosyaları cep telefonları aracılığıyla elektronik olarak imzalamalarını ve kendilerine gelen elektronik imzalanmış dosyaları doğrulamalarını

sağlayabilen kurulumu ve kullanımı oldukça basit olan bir yazılımdır.

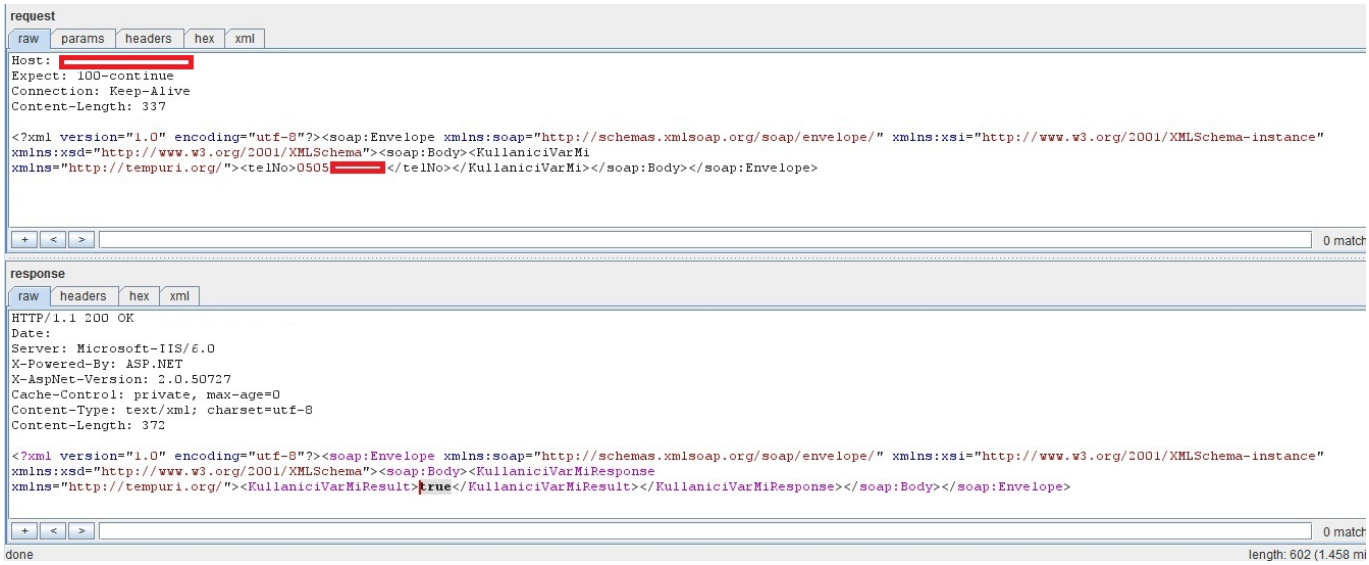
Mobil İmza kullanma gayesiyle göz attığım bu yazılımın doğrudan bir web servis ile haberleşiyor olması ister istemez dikkatimi çekmişti çünkü kurumsal ağlarda ve güvenli tasarlanan yazılımlarda son kullanıcının web servis ile münasebet kurması çok tercih edilmemektedir.



WSDL dosyasına baktığımda KullanıcıVarMi, ImzaIleLisansAl, VarOlanLisansiGetir servisleri ilgimi çekti. Normal şartlarda imzalama uygulaması kullanılarak çağrılabilecek bu servisler, WSDL'den elde edilen bilgiler ile istenildiği taktirde herhangi bir http isteği yapan bir araç üzerinden de çağrılabilir. Kısaca imzalama uygulaması yerine isteyen kendi uygulamasını hazırlayarak bu servisleri çağırabilir ve uygulama üzerinde yer alan kısıtlamalardan etkilenmeyebilir.



Aklıma gelen ilk soru art niyetli bir kişi başkasına ait olan bir lisansı VarOlanLisansiGetir servisini çağırarak getirebilir miydi ? Bu sorunun yanıtını her ne kadar merak etsem de etik açıdan doğru olmayacağını düşündüğüm için aramaktan vazgeçtim. Bunun yerine KullanıcıVarMi servisi ile bir kaç sorgu gerçekleştirdim. Bu servisin bir gsm şirketine ait olan herhangi bir telefon numarası ile çağrılması durumunda sunucudan true (var) ya da false (yok) şeklinde yanıt geldiğini gördüm. Servisin çalışıp çalışmadığını teyit etmek için elimde mobil imza kullanan ve kullanmayan iki farklı cep telefonu numarası ile deneme gerçekleştirdim ve servisin çalıştığını teyit ettim.



Servisin bu şekilde isteyen herkes tarafından kullanılabiliyor olmasının art niyetli kişiler tarafından nasıl istismar edilebileceğini düşünmeye koyulduğumda aklıma gelen ilk senaryo şu şekilde oldu. Bildiğiniz gibi man in the mobile saldırısı gerçekleştiren Zeus bankacılık trojanı, kullanıcının cep telefonuna SMS şifresini çalmak için bir trojan göndermektedir. Böyle bir servisin halka açık olarak hizmet vermesi durumunda bu servisten faydalanan zararlı bir yazılım körü körüne kurbana ait olan cep telefonu numarasına SMS şifresini çalan trojan göndermek yerine öncelikle bu servisi çağırarak mobil imza kullanıcısı olup olmadığını teyit edebilir ve yanıta göre mobil imza uygulamasını hedef alan zararlı bir yazılım gönderebilir. Bu servisin bu şekli ile kullanılmasının bir gsm firmasına ait mobil imza kullanan banka müşterilerinin ve bankaların doğru bulmayacağını düşünerek konuyu hemen X firmasına bildirmek için sayfalarında yer alan e-posta adresine bir e-posta gönderdim. Bu adrese gönderilen e-postaları kontrol etmeyeceklerini düşünerek (Türkiye gerçeği) biraz araştırma yaparak genel müdürün e-posta adresini bularak kendisine konu ile ilgili iletişim kurabileceğim bir yetkilinin bilgisini öğrenmek için ayrı bir e-posta gönderdim. Ancak iki hafta içinde tarafıma herhangi bir geri dönüş yapılmadığı için bu servisin art niyetli kişiler tarafından bu şekilde kullanılmasını en kısa sürede engelleyebilmek adına bu yazıyı yazma ve ilgilileri göreve çağırma misyonunu üstlendim.

Yazının giriş kısmında da belirttiğim üzere web servislerin sadece uygulamalar arasında kullanılıyor olması ve son kullanıcı kullanımına kısıtlanıyor olması bu tür tehditleri berteraf edilmesine yardımcı olacaktır.

Bir sonraki yazıda görüşmek dileğiyle…

[28-03-2011] Güncelleme: Firma genel müdürünün bugün itibariyle tarafımla

iletişime geçmesi ve firma isimlerinin yazıda geçmesinden ötürü duyduğu rahatsızlığı dile getirmesi üzerine yazıda geçen firma isimleri sansürlenmiştir. Gerekli görülmesi durumunda ilerleyen zamanlarda kendileri ile gerçekleştirilen yazışmalara yer verilebilir.