

Web Servis Güvenliđine Dair

written by Mert SARICA | 23 March 2011

Ađırlıklı 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.

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

Web servis denilince çođu 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, parametre manipölasyonu, WSDL taraması ve daha birçok tehdit gelmektedir.

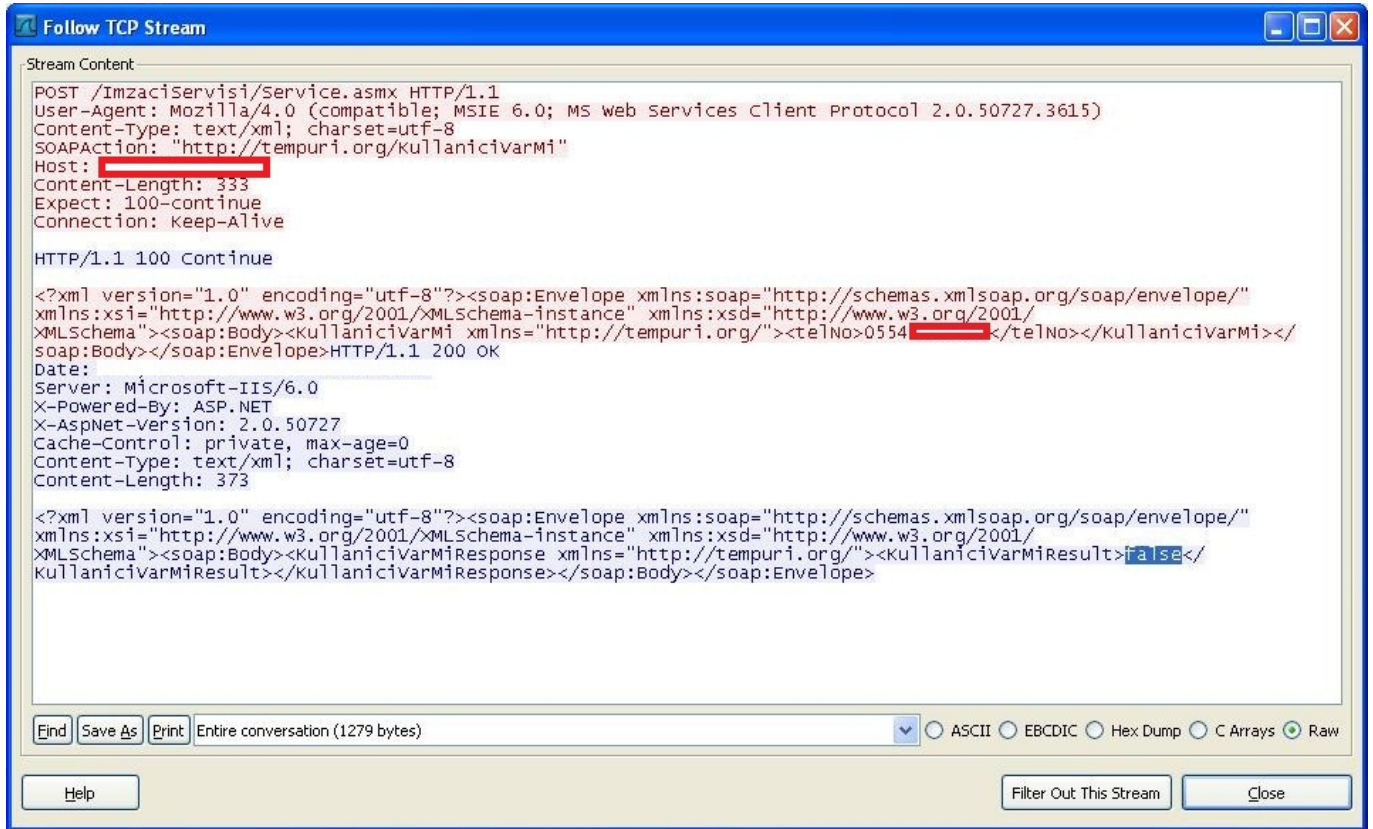
Web Services Description Language (WSDL), bir web servis ile iletişim kurulabilmesi için gerekli parametreleri, metodları içerir. WSDL'i dış dünyaya açık olan bir web servis üzerinde yer alan servis yukarda bahsi geçen tehditlere mağruz kalabildiđi gibi servisin ve hizmetin kötüye kullanımını da yol 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 aracılıđıyla elektronik olarak imzalamalarını ve kendilerine gelen elektronik imzalanmış dosyaları dođrulamalarını

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.



```
Stream Content
POST /ImzaciServisi/Service.asmx HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol 2.0.50727.3615)
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/kullaniciVarMi"
Host: [REDACTED]
Content-Length: 333
Expect: 100-continue
Connection: keep-alive

HTTP/1.1 100 Continue

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/
/XMLSchema"><soap:Body><kullaniciVarMi xmlns="http://tempuri.org/"><telNo>0554 [REDACTED]</telNo></kullaniciVarMi></
soap:Body></soap:Envelope>HTTP/1.1 200 OK
Date:
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 373

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/
/XMLSchema"><soap:Body><kullaniciVarMiResponse xmlns="http://tempuri.org/"><kullaniciVarMiResult>false</
kullaniciVarMiResult></kullaniciVarMiResponse></soap:Body></soap:Envelope>
```

WSDL dosyasına baktığımda KullanıcıVarMi, ImzaIleLisansAl, VarOlanLisansGetir servisleri ilgimi çekti. Normal şartlarda imzalama uygulaması kullanılarak çağrılacak bu servisler, WSDL'den elde edilen bilgiler ile istenildiği takdirde 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.

```
http://[redacted]/ImzaciServisi/Service.asmx?wsdl - Windows Internet Explorer
http://[redacted]/ImzaciServisi/Service.asmx?wsdl
File Edit View Favorites Tools Help
Favorites Suggested Sites Web Slice Gallery
http://[redacted]/ImzaciServisi/Service.asmx?wsdl
- <s:element name="KullanciVarMi">
- <s:complexType>
- <s:sequence>
  <s:element minOccurs="0" maxOccurs="1" name="telNo" type="s:string" />
</s:sequence>
</s:complexType>
</s:element>
- <s:element name="KullanciVarMiResponse">
- <s:complexType>
- <s:sequence>
  <s:element minOccurs="1" maxOccurs="1" name="KullanciVarMiResult" type="s:boolean" />
</s:sequence>
</s:complexType>
</s:element>
- <s:element name="ImzaIleLisansAl">
- <s:complexType>
- <s:sequence>
  <s:element minOccurs="0" maxOccurs="1" name="signedData" type="s:string" />
  <s:element minOccurs="0" maxOccurs="1" name="telno" type="s:string" />
  <s:element minOccurs="0" maxOccurs="1" name="serial" type="s:string" />
</s:sequence>
</s:complexType>
</s:element>
- <s:element name="ImzaIleLisansAlResponse">
- <s:complexType>
- <s:sequence>
  <s:element minOccurs="0" maxOccurs="1" name="ImzaIleLisansAlResult" type="s:string" />
</s:sequence>
</s:complexType>
</s:element>
- <s:element name="VarOlanLisansGetir">
```

Aklıma gelen ilk soru art niyetli bir kişi başkasına ait olan bir lisansı VarOlanLisansGetir 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 çağırılması 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.



```
request
raw params headers hex xml
Host: [redacted]
Expect: 100-continue
Connection: Keep-Alive
Content-Length: 337
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><KullaniciVarMi
xmlns="http://tempuri.org/"><telNo>0505 [redacted] </telNo></KullaniciVarMi></soap:Body></soap:Envelope>

response
raw headers hex xml
HTTP/1.1 200 OK
Date:
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 372
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><KullaniciVarMiResponse
xmlns="http://tempuri.org/"><KullaniciVarMiResult>true</KullaniciVarMiResult></KullaniciVarMiResponse></soap:Body></soap:Envelope>

done length: 602 (1.458 mi)
```

Servisin bu şekilde isteyen herkes tarafından kullanılabilir olmasının art niyetli kişiler tarafından nasıl istismar edilebileceğini düşünmeye koyduğumda 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 kurbanına ait olan cep telefonu numarasına SMS şifresini çalan trojan göndermek yerine öncelikle bu servisi çağırarak mobil imza kullanıcısı olup olmadığını teyit edebilir ve yanıtı 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 itibarıyla 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.