Tivibu

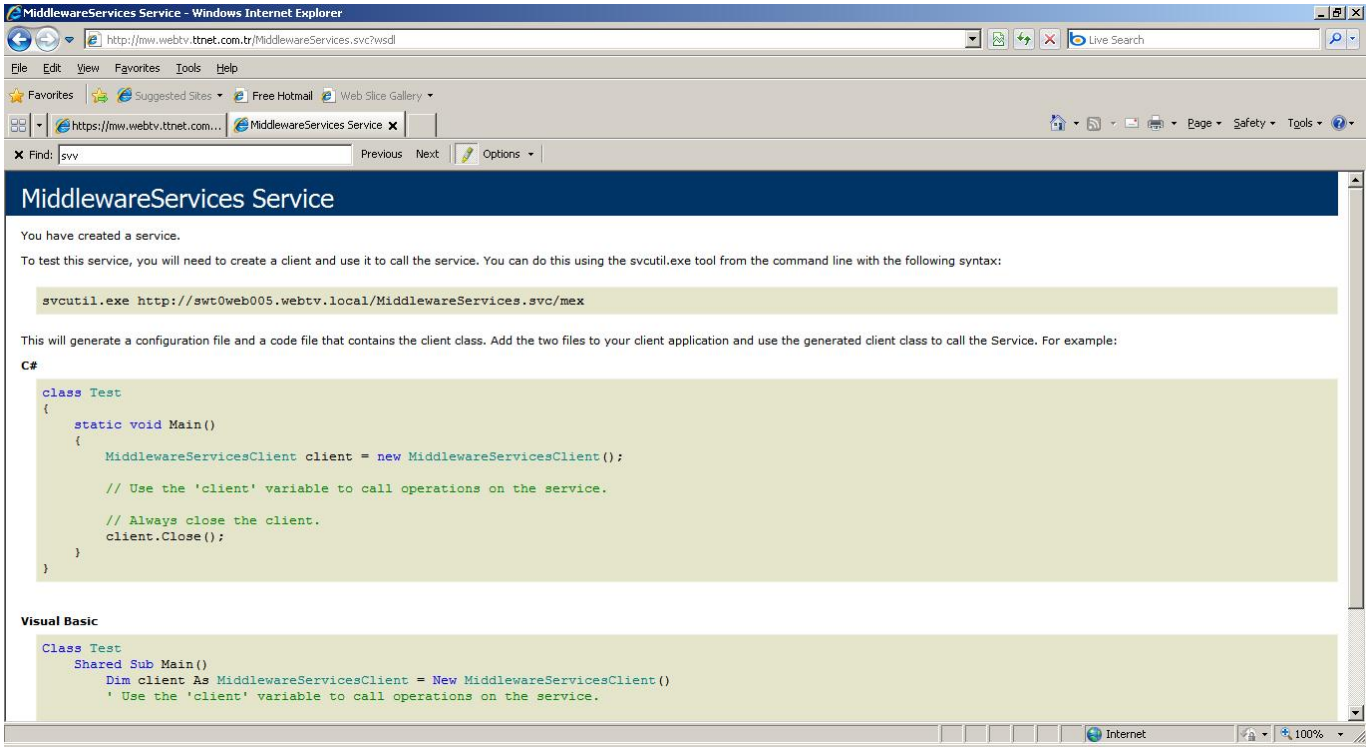
written by Mert SARICA | 7 March 2010

Çocukken meraktan alınan her oyuncağın içini açar bakarmışım ne var ne yok diye. Aradan yıllar geçmesine rağmen huylu huyundan vazgeçmedi sadece oyuncak arabaların, helikopterlerin yerini programlar aldı :)

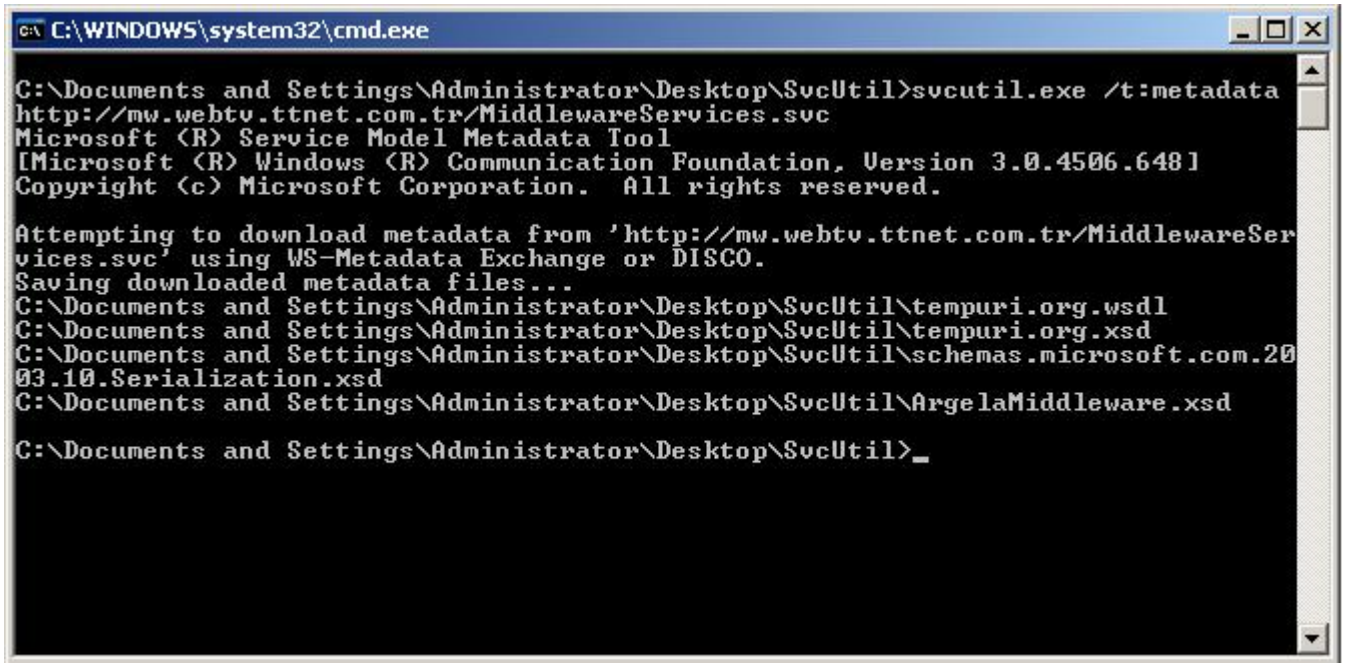
Geçtiğimiz hafta bir web sitesi gezerken TTNet'in Tivibu reklamını gördüm. Nedir bu Tivibu diyecek olursanız internet bağlantısı olan her yerden TV izlemenize imkan tanıyan bir program. Yine bir can sıkıntısı, yine bir merak ile programı kurup incelemeye karar verdim. Bu arada bu hizmetten faydalanabilmek ve programı kullanabilmek için ayda 1 TL ödemeniz gerekiyor. Sadece nasıl çalıştığını merak ettiğim için üye olmak yerine programı kurup incelemeyi tercih ettim.

Kısa süren bir incelemeden sonra Tivibu programının Microsoft Silverlight kullandığını farkettim. Silverlight ile daha önce pek haşır neşir olmadığım için Tivibu sunucusu ile Silverlight client arasındaki şifreli trafiği (SSL) Fiddler programı ile incelemeye karar verdim ancak bir türlü araya giremedim. Laz olmasamda laz damarım tuttu ve biraz kafa patlattıktan sonra sertifikaların uygulamanın içine gömülü olduğunu, bu nedenle araya giremediğimi farkettim. Uygulama içerisine gömülü olan sertifikaları değiştirmeye üşendiğim için Hex editor ile programa göz atmaya karar verdim.

Yine kısa süren bir inceleme sonrasında Tivibu programı içerisinden gerçekleştirilen isteklerin WCF web servisine gittiğini farkettim.



İşin içinde WCF olunca ?wsdl parametresi ile tanımlı web servislerine ait bilgileri görmeniz her zaman mümkün olamayabiliyor bu nedenle Microsoft'un bu iş için geliştirmiş olduğu svcutil uygulaması hemen imdadıma yetişti.



Bu wsdl dosyasından faydalanarak kendi Tivibu programını yazabilir misiniz sorusunun cevabını ve araya neden girilmesini istemediklerinin nedenini bulmayı sizlere bırakıyorum :)

İşin içinde Silverlight oldu mu, cross-domain güvenlik politikaları bir şekilde root klasörü altında yer almak zorunda diye düşündüm, oltamı salladım veeee bingo, Cross domain policy ve Client access policy karşıma çıkıverdi.

Bu politikaların asıl amacı CSRF (cross-site request forgery) saldırılarını önlemektedir. Çoğunlukla program/uygulama (flash/flex/silverlight) geliştiricileri bu politikaların ne işe yaradıklarını pek bilmedikleri için domain adı belirtmeden wildcardı koyuverirler ve ortaya CSRF güvenlik zafiyeti çıkar. Program tarafından veri çekilecek alan adlarına bu politikalarda yer vermez ve wildcard (*) kullanırsanız art niyetli kişiler CSRF saldırısı ile program tarafından kullanılan kullanıcı bilgilerini çalabilirler.

Daha anlaşılabilir olması adına örnek bir senaryo üzerinden gidecek olursak;

1- Sefil kullanıcı Tivibu uygulamasına giriş yapıyor.
2- Art niyetli bir kişi Tivibu sunucusu ile haberleşen Silverlight uygulamasını kendi sitesine koyarak sefil kullanıcının sayfasını ziyaret etmesini bir şekilde sağlıyor. (E-posta, MSN, Facebook)
3- Sefil kullanıcının Silverlight uygulaması art niyetli kişinin sayfasında yer alan Silverlight uygulaması üzerinden Tivibu sunucusu ile haberleşiyor ve art niyetli kişi sefil kullanıcının verilerini çalabiliyor.

Kendi geliştirdiğiniz (flash/flex/silverlight) uygulamalarda/programlarda cross-domain güvenlik politikalarına dikkat etmenizi önerir, bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim…