Güvenli ASP.NET Prodüksiyon Ortamı

Mesut Timur, Ağustos 2009, WGT E-Dergi 1. Sayı

Web Uygulaması Güvenliği

Web uygulaması güvenliği sağlanırken genellikle akıllara ilk gelenler çeşitli kod enjeksiyonu zafiyetleri ve girdi doğrulama temelli yaklaşımlardır. SQL Injection'ı kesmek için parametrik sorgular, XSS'i kesmek için output encoding, LFI & RFI için doğru şekilde girdi doğrulama ve CSRF için de kritik fonksiyonaliteler için token uygulaması.

Oysa dünyanın en güvenli uygulamasını yazmış olsanız dahi, sunucu üzerinde tutulan bir klasörün izinlerini doğru şekilde düzenlemediyseniz , hack'lenmeniz işten bile değil ! Bundan dolayı işin kod kalitesi ile ilgili kısmını düşünürken, konfigürasyonel boyutunu da es geçmemek gerekmektedir.

ASP.NET

Günümüzde web uygulamaları bir çok programlama dili vasıtasıyla yazılabilmekte ve bir çok üretim ortamında çalışabilmektedir. Bu dillerden ve platformlardan önemli bir tanesi ise ASP.NET 'dir.

ASP.NET ortamında geliştirilmiş uygulamaların konfigürasyon bilgileri web.config isimli dosyada tutulur.

Web.config

Söz konusu XML dosyası uygulamanın durum bilgisi, güvenlik konfigürasyonu, derlenme ayarları ve uygulama-spesifik bilgiler yer alır. Bir web sunucu üzerindeki tüm uygulamalar aynı konfigürasyon dosyasını kullanmak zorunda değillerdir. Farklı uygulamalar için farklı Web.config dosyaları tanımlanabilir.

İlgili konfigürasyon dosyasındaki ayarların doğru şekilde belirlenmemesi durumlarında çeşitli güvenlik zafiyetleri ortaya çıkabilmektedir. Kimi güvenlik zafiyeti ise herhangi bir hatalı konfigürasyon beklemeden, varsayılı ayarlarda meydana çıkmaktadır.

Potansiyel zafiyetlerin bir listesi şu şekildedir:

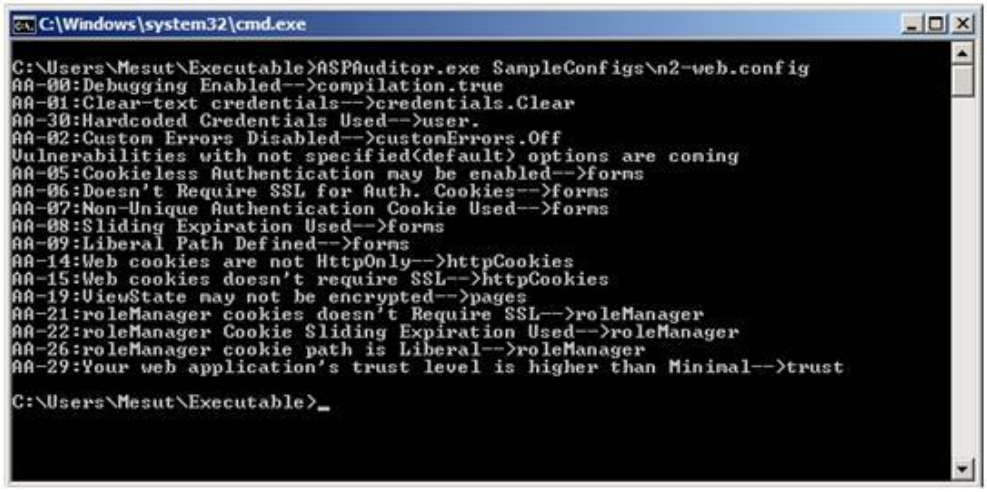
. Hata mesajlarından ve uygulamadan çeşitli şekillerde bilgi sızmaları
. Uygulama ile istemci arasındaki trafiğin ifşası
. Yazılımın saldırganların kontrolüne geçmesi halinde, sunucunun tüm kontrolünün kaybedilmesi
. Oturum ile ilgili konular
  o Oturumun manipüle edilmesi
  o Oturumun çalınması
  o Zaman aşımı olmaması sonucu çalınan çerezin kullanılması
. Web çerezleri ile ilgili konular

o Çerezlerin XSS saldırısı ile çalınması
o Çerezlerin ağ trafiği dinlenilerek çalınması
. İstek hırsızlığı
. Hassas dosyaların ifşası.
. Trafiğin dinlenilmesi
. Web.config içindeki kritik bilgilerin sızdırılması [1]

Web.config dosyasının doğru şekilde konfigüre edilmesiyle söz konusu zafiyetlerin bazılarından sonsuza dek, bazılarından ise bir çok durumda korunmak mümkün olacaktır.

Web.config dosyalarındaki problemlerin otomatik şekilde incelenmesini gerçekleştirmek üzere WCSA (Web.config Security Analyzer) hazırlandı. WCSA kendisine parametre olarak geçilen Web.config dosyalarını inceleyip varolan konfigürasyonel güvenlik problemlerini ortaya çıkarıyor.

Proje'nin ana sayfası http://code.google.com/p/wcsa/ olup, download linklerine de erişebilirsiniz.



Çıktı olarak verdiği HTML raporda güvenlik zafiyetleri, zafiyetlerin tanımları, yapılması gereken güvenli konfigürasyon ve referanslar veriliyor.

Sonuç

Güvenlik bir bütün olarak düşünülmelidir. Güvenli web uygulamaları geliştirirken, güvenli kod pratiklerinin uygulanmasının yanında sürecin konfigürasyonel boyutu da göz önünde bulundurulmalıdır.

Referanslar

[1] http://www.onuryilmaz.info/Icerik/61-web-config-dosyasinin-icerigini-sifrelemek.aspx