Web Uygulamalarına Yönelik Saldırılar

Onur Yılmaz, Ekim 2009, WGT E-Dergi 2. Sayı

Giriş

Web uygulamaları konusunda yapacağımız bu analiz sonunda ise web uygulamalarına yönelik saldırıların nasıl gerçekleştiği ve nasıl önlenebileceğini dokümante ederek, sizlerin de eklemeleriyle bir saldırı ağacı oluşturacağız ve ismini de 'Temel Bir Web Uygulamasının Deface Edilme Tehdit Modellemesi" koyacağız.

Web Uygulaması Nedir ?

Web uygulaması; kullanıcı etkileşimli veya veriye dayalı web tabanlı yazılımlardır. Kavram olarak basit gözükse de, web uygulamalarına yönelik saldırıları kategorize etmek ve incelemek açısından önem arz etmektedir.

Bir sistemin nasıl çalıştığı bilinmeden o sisteme saldırılamayacağı gibi nasıl saldırıldığı bilinmeden de sistemi korumak güç olacaktır. Bu noktaya istinaden web uygulaması kavramından hareketle, web uygulamalarının nasıl çalıştığını ve web uygulama türlerini inceleyerek uygulamaya gelebilecek saldırıları belirleyebiliriz.

Web Uygulamaları

Web uygulaması tanımına göre sınıflandırma yapacak olursak;

- **Veriye Dayalı Uygulamalar**
  - Statik Web Uygulamaları: Kullanıcının ulaşmak istediği verilerin HTML kaynak kodunda saklanması prensibine dayanan uygulamalardır. Herhangi bir web teknolojisi kullanılmadan ve herhangi bir veri kaynağı olmaksızın salt HTML veya HTML-JavaScript ikilisinin kullanıldığı ve verilerin önceden hazır bulunduğu uygulamalardır. (Örneğin; HTML ile yapılmış internet siteleri)
  - Dinamik Web Uygulamaları: Kullanıcının ulaşmak istediği verilerin, kullanıcı talepleri doğrultusunda veri tabanından (veri kaynağından) çağrılarak gösterilmesi prensibine dayanan uygulamalardır. Kullanıcıdan alınan herhangi bir veri yoktur ve ilgili sorgular önceden belirlenmiştir. (Örneğin; önceden belirlenen kategorilere göre verilerin listelenmesi
- **Kullanıcı Etkileşimli Uygulamalar**
  - İlişkisel Web Uygulamaları olarak da ifade edebileceğimiz bu uygulamalarda kullanıcıdan alınan veriler belirli kriterlere göre işlenerek, ilgili kriterdeki verinin, veri kaynağından çağrılıp kullanıcıya gösterilmesi prensibine dayanmaktadır. (Örneğin; portal veya forum uygulamaları)

Bu üç tür uygulamanın aynı ortamlarda bulunduğunu varsayarsak; web uygulamalarına yönelik saldırılar, yatay eksende, statik web uygulamalarından ilişkisel web uygulamalarına doğru genişleyecektir.

Bir web sitesini tam manasıyla ifade edebilmek için ise,

- Web uygulamasına erişimin sağlanacak bir alan adı (domain)
- Web uygulamasının yayın yapacağı bir sunucu (dedicated / virtual server, reseller, shared hosting, database server vs.)
- Geliştirilmiş olan web uygulaması (statik, dinamik, ilişkisel)
- Uygulama yöneticisi ve kullanıcıları

gereklidir.

Web Uygulamalarına Yönelik Saldırılar

En baştan söylediğimiz gibi web uygulamalarına yönelik saldırıları analiz edebilmek için, bir web uygulamasının bütünleşik yapısını belirledik. Bu yapıya göre saldırılar;

- Alan adı üzerinden (domain)
- Sunucu üzerinden
- Uygulama üzerinden
- Kullanıcılar üzerinden

gerçekleşebilir.

Bu 4 maddeden hareket ile hazırlayacağımız tehdit modellemesi için katkılarınızı bekliyorum (contact-at-onuryilmaz.info). Ayrıca örnek bir tehdit modellemesi için de SSL Thread Model`i (http://blog.ivanristic.com/SSL_Threat_Model.png) inceleyebilirsiniz.