Web Uygulama Güvenliği Kontrol Listesi 2010

Web uygulama güvenliği kontrol listesi 2010, OWASP-Türkiye ve Web Güvenliği Topluluğu tarafından güvenli web uygulamalarında aktif olması gereken denetim adımlarını içeren bir dokümantasyon projesidir. Projedeki her kontrole dört nitelik atanmıştır. Kategorilere ayrılmış kontrollerin uygulama sorumluları belirlenmiştir. Ayrıca eksikliklerinde sistemlere genel etkileri belirtilen kontroller doğru önceliklendirmek için risk seviyelerine sınıflandırılmışlardır.

1. Kategoriler
    a. Hata Yönetimi
    b. Girdi Denetimi
    c. Oturum Yönetimi
    d. Yetkilendirme
    e. Kayıt Tutma
    f. Kimlik Doğrulama
    g. Bağlantı Güvenliği
    h. Web Servisleri
    i. İş Mantığı
    j. Veri Güvenliği
    k. Yapılandırma Yönetimi

2. Sorumlular
    a. Sistem Yöneticisi: İşletim sistemi ve uygulama sunucusunu yöneten ilgili.
    b. Veritabanı Yöneticisi: Veritabanı sunucusunu yöneten ilgili.
    c. Geliştirici: Uygulamayı geliştiren ilgili.

3. Etkiler
    a. Bilgi Toplama
    b. SQL Enjeksiyonu
    c. XSS
    d. Bilgi Hırsızlığı
    e. Hizmet Dışı Bırakma
    f. Komut Çalıştırma

4. Seviyeler
    a. Acil (5)
    b. Kritik (4)
    c. Yüksek (3)
    d. Orta (2)
    e. Düşük (1)

Not: Sıralama seviye bazlı yapılmıştır.

1. Uygulama ile son kullanıcı arasındaki kullanıcı adı, parola, kredi kartı no, adres gibi hassas veriler HTTPS protokolü üzerinden aktarılmalıdır.
   Kategori : Bağlantı Güvenliği **Etki :** Bilgi Hırsızlığı
   Sorumlu : Sistem Yöneticisi **Seviye :** Acil

2. Kullanılan parolalar ve parolamı unuttum kontrol soru cevapları gibi diğer hassas veriler açıkmetin olarak saklanmamalıdır.
   Kategori : Veri Güvenliği **Etki :** Bilgi Hırsızlığı
   Sorumlu : Geliştirici **Seviye :** Acil

3. SQL enjeksiyonuna karşı prepared statement/parameterized query/bind variables/pozitif veri kontrolü yöntemlerinden biri veya bir kaçı kullanılmalıdır.
   Kategori : Girdi Denetimi **Etki :** SQL Enjeksiyonu
   Sorumlu : Geliştirici **Seviye :** Acil

4. Kullanıcıdan gelen tüm girdilere sunucu tarafında pozitif veri kontrolü uygulanmalıdır.
   Kategori : Girdi Denetimi **Etki :** Hepsi
   Sorumlu : Geliştirici **Seviye :** Acil

5. Kullanıcıdan gelen verilerin işletim sistemi komut satırına girmeden kontrol edilmesi ve düzgünleştirme işleminden (escape) geçirilmesi gerekmektedir.
   Kategori : Girdi Denetimi **Etki :** İşletim Sistemi Komut Enjeksiyonu
   Sorumlu : Geliştirici **Seviye :** Acil

6. Kullanıcıdan gelen ve dosya erişim işlemlerinde kullanılan girdiler normalizasyon işlemine tabi tutulmalıdır.
   Kategori : Girdi Denetimi **Etki :** Dizin Gezinimi
   Sorumlu : Geliştirici **Seviye :** Acil

7. GET veya POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.
   Kategori : Yetkilendirme **Etki :** Bilgi Hırsızlığı, Hak Yükseltme
   Sorumlu : Geliştirici **Seviye :** Acil

8. SOAP, Restful, XML-RPC gibi teknolojilerle geliştirilmiş web servislerine erişimlerde kimlik doğrulama kontrolü uygulanmalıdır.
   Kategori : Web Servisleri **Etki :** Bilgi Hırsızlığı
   Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Acil

9. Kullanıcıdan veri alarak LDAP'a bağlanan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri LDAP düzgünleştirme işleminden (escape) geçirmelidirler.
   Kategori : Girdi Denetimi **Etki :** LDAP Enjeksiyonu
   Sorumlu : Geliştirici **Seviye :** Acil

10. Güvensiz kaynaklardan veri alarak XPath sorguları yapan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri XPath düzgünleştirme işleminden (escape) geçirmelidirler.
    Kategori : Girdi Denetimi **Etki :** XPath Enjeksiyonu
    Sorumlu : Geliştirici **Seviye :** Acil

☐ 11. Karşıdan dosya yükleme işlemlerinde yüklenilen dosya üzerinde isim, boyut, tip ve içerik kontrolü yapılmalıdır.
Kategori : Girdi Denetimi **Etki :** XSS, Dosya Çalıştırma
Sorumlu : Geliştirici **Seviye :** Kritik

☐ 12. DoS saldırısı barındıracak veya şifre deneme-yanılma gibi kaba kuvvet saldırılarına açık tüm formlara CAPTHCA veya farklı anti-otomasyon güvenlik kontrolleri uygulanmalıdır.
Kategori : Girdi Denetimi **Etki :** Hizmet Dışı Bırakma, Kaba Kuvvet
Sorumlu : Geliştirici **Seviye :** Kritik

☐ 13. Güvenli web trafiği için (SSL) güçlü şifreleme algoritmaları kullanılmalıdır, güçsüz algoritmalar inaktif hale getirilmelidir.
Kategori : Bağlantı Güvenliği **Etki :** Bilgi Hırsızlığı
Sorumlu : Sistem Yöneticisi **Seviye :** Kritik

☐ 14. Uygulama çatısı/veritabanı/uygulama sunucusu/web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.
Kategori : Yapılandırma Yönetimi **Etki :** Hepsi
Sorumlu : Sistem Yöneticisi **Seviye :** Kritik

☐ 15. Kritik işlemlerde CSRF saldırılarına karşı güvenlik önlemleri alınmalıdır.
Kategori : Oturum Yönetimi **Etki :** CSRF
Sorumlu : Geliştirici **Seviye :** Kritik

☐ 16. Uygulama üzerinden yapılan hassas işlemler hem uygulama seviyesinde hem de sunucu seviyesinde kayıt altına alınmalıdır.
Kategori : Kayıt Tutma **Etki :** Non repudiation
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Kritik

☐ 17. Kullanıcıdan gelen CR/LF karakterleri uygulama tarafında oldukları gibi HTTP cevap başlıklarında kullanılmamalıdır.
Kategori : Girdi Denetimi **Etki :** HRS
Sorumlu : Geliştirici **Seviye :** Kritik

☐ 18. Uygulamaların üzerinde koştukları sunucuları, servis verdikleri dizinlerin içeriklerini listelememelidir.
Kategori : Yapılandırma Yönetimi **Etki :** Dizin Listeleme
Sorumlu : Sistem Yöneticisi **Seviye :** Kritik

☐ 19. Güvensiz kaynaklardan veri alarak aritimetik işlem yapan uygulamalar, gerekli tam sayı üst sınır ve alt sınır kontrollerini gerçekleştirmelidirler.
Kategori : Girdi Denetimi **Etki :** Tamsayı Taşması
Sorumlu : Geliştirici **Seviye :** Kritik

☐ 20. Web servisleri için kullanılan çatıların klasik XML saldırılarına karşı bağışık olup olmadıkları kontrol edilmelidir.
Kategori : Web Servisleri **Etki :** Hizmet Dışı Bırakma
Sorumlu : Sistem Yöneticisi **Seviye :** Kritik

21. Uygulamalarda başarılı kimlik doğrulama ve çıkış işlemleri sonrası oturum bilgisinin değiştirilmesi gerekmektedir.
Kategori : Oturum Yönetimi **Etki :** Session Fixation
Sorumlu : Geliştirici **Seviye :** Kritik

22. Oturum yönetimi için kullanılan ve uygulamayı kullanan bütün kullanıcılar için tekil olması gereken değerlerin tahmin edilemez derecede karmaşık olduğu ve güçlü bir rastgele veri üretecinden temin edildiği kontrol edilmelidir.
Kategori : Oturum Yönetimi **Etki :** Hak Yükseltme
Sorumlu : Geliştirici **Seviye :** Kritik

23. Uygulamayı çalıştıran sistem kullanıcısının, hizmet verilen dizin dışındaki yetkileri kaldırılmalıdır.
Kategori : Yetkilendirme **Etki :** Hepsi
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

24. ASP.NET, PHP, STRUTS gibi kullanılan uygulama çatılarının güvenlik özellikleri aktif hale getirilmelidir.
Kategori : Yapılandırma Yönetimi **Etki :** Hepsi
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

25. Veritabanı kullanıcısının sadece uygulamanın kullandığı veritabanı kaynaklarına erişim hakkı olmalıdır.
Kategori : Yetkilendirme **Etki :** Bilgi Hırsızlığı, Komut Çalıştırma
Sorumlu : Veritabanı Yöneticisi **Seviye :** Yüksek

26. Hassas bilgiler içeren web sayfalarının tarayıcılarda belleğe alınmaması için autocomplete, cache-control, pragma gibi gerekli HTTP/HTML başlıkları kullanılmalıdır.
Kategori : Yapılandırma Yönetimi **Etki :** Bilgi Hırsızlığı
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

27. Arama motorları tarafından görüntülenmemesi istenen dizinler varsa, bunlar için robots.txt ile önlem alınmalıdır.
Kategori : Yapılandırma Yönetimi **Etki :** Bilgi Toplama
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

28. Yedekleme, arşiv, test, geliştirme için kullanılan gereksiz hiçbir dosya İnternet üzerinden erişilebilir dizinlerde bulunmamalıdır.
Kategori : Yapılandırma Yönetimi **Etki :** Bilgi Toplama
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

29. Ön tanımlı kullanıcı hesapları sistemden veya uygulamadan kaldırılmalıdır.
Kategori : Yapılandırma Yönetimi **Etki :** Hepsi
Sorumlu : Geliştirici, Sistem Ynt., Veritabanı Ynt. **Seviye :** Yüksek

30. Uygulama domain isimlerine ait hassas bilgilerin google/bing gibi arama motorları tarafından indexlenmediği kontrol edilmelidir.
Kategori : İş Mantığı **Etki :** Bilgi Toplama
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

31. Parola güncelleme işlemleri için eski şifre her zaman sorulmalıdır.
Kategori : Yetkilendirme **Etki :** Bilgi Hırsızlığı
Sorumlu : Geliştirici **Seviye :** Orta

32. Parola unuttum formları, gizli soru, doğum tarihi gibi birden fazla parametre ile desteklenmelidir .
Kategori : İş Mantığı **Etki :** Hizmet Dışı Bırakma
Sorumlu : Geliştirici **Seviye :** Orta

33. Veritabanı kullanıcısının veritabanına sadece uygulama sunucu IP`sinden bağlantı hakkı olmalıdır.
Kategori : Yetkilendirme **Etki :** Bilgi Hırsızlığı
Sorumlu : Veritabanı Yöneticisi **Seviye :** Orta

34. Başarılı login işlemleri sonrası HTTP 302 ile kullanıcı dahili sayfalara yönlendirilmelidir.
Kategori : Oturum Yönetimi **Etki :** Bilgi Hırsızlığı
Sorumlu : Geliştirici **Seviye :** Orta

35. Gerekmedikçe POST/GET dışındaki HTTP metotlarına izin verilmemelidir.
Kategori : Yapılandırma Yönetimi **Etki :** XSS, Dosya Çalıştırma, Bilgi Toplama
Sorumlu : Sistem Yöneticisi **Seviye :** Orta

36. Yönetim paneli, arayüzü gibi kritik dizinlerin isimleri kolay tahmin edilebilir olmamalıdır (admin, yonetici, administrator, yonetim, panel, etc...)
Kategori : İş Mantığı **Etki :** Bilgi Toplama
Sorumlu : Geliştirici **Seviye :** Orta

37. Sunucu üzerinde bulunan ve web tabanlı istatistik sağlayan uygulamalara erişim herkese açık olmamalıdır.
Kategori : Yetkilendirme **Etki :** Bilgi Toplama
Sorumlu : Sistem Yöneticisi **Seviye :** Orta

38. Uygulamaların, uygun olan her sayfada çerçeve engelleyici önlemleri (frame busting) almaları gerekmektedir.
Kategori : Girdi Denetimi **Etki :** ClickJacking / Leeching
Sorumlu : Geliştirici **Seviye :** Orta

39. HTTPS protokolü kullanılan bağlantılarda kullanılan COOKIE değerleri için Secure parametresinin tanımlı olduğu kontrol edilmelidir.
Kategori : Oturum Yönetimi **Etki :** Bilgi Hırsızlığı
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Orta

☐ 40. Uygulamada oluşan hatalar veya uygulama sunucu varsayılı hata mesajları kullanıcıya detaylı olarak gösterilmemelidir.
Kategori : Hata Yönetimi **Etki :** Bilgi Toplama
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Orta

☐ 41. Kullanılan COOKIE değerleri için HTTPOnly parametresinin tanımlı olduğu kontrol edilmelidir.
Kategori : Oturum Yönetimi **Etki :** Bilgi Hırsızlığı
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Orta

☐ 42. Flash uygulamalarında crossdomain.xml yapılandırma dosyası uygulanan politikanın güvenli olduğu kontrol edilmelidir.
Kategori : Yapılandırma Yönetimi **Etki :** Bilgi Hırsızlığı
Sorumlu : Sistem Yöneticisi **Seviye :** Orta