Web Güvenliği Topluluğu – webguvenligi.org

Web Uygulama Güvenliği Kontrol Listesi 2012

Web Uygulama Güvenliği Kontrol Listesi, web uygulamalarında bilgi güvenliği açısından gerçekleştirilmesi, aktif olması gereken kontrolleri içeren ve denetçi bakış açısıyla hazırlanmış olan bir dokümantasyon projesidir.

Kontrol listesinin ilk sürümü 2010 yılında yayınlanmıştır. Şu an elinizdeki doküman, bir çok iyileştirme yapılarak hazırlanan ve Ocak 2012'de tamamlanan ikinci sürümüdür. Bu yeni ikinci sürümde yapılan başlıca değişiklikler aşağıda listelenmiştir;

- Kategorilerde OWASP Testing Guide'ın kategorileri temel alınmıştır.
- Her kontrol maddesi ayrıca ASVS (OWASP Application Security Verification Standard) kategorileri ile de eşlenmiştir.
- Risk seviyesi ve de sorumlular kısmı revize edilmiştir.
- Excel dokümanında kontrollerin aktif olup olmadığına verilecek "Evet" / "Hayır" / "---" cevabına göre farklı risk seviyesindeki ve de toplamdaki güvenlik durumu grafiksel olarak gösterilmektedir. "---" seçeneği ilgili güvenlik kontrolünün denetlenen sistemin kapsamının dışında olduğunu gösterir ve grafiksel gösterimlerde değerlendirmeye alınmaz.
- Kontrol listesi, PDF belgesine ek olarak Excel formatında da sunulmuştur. Bu sayede proje esnasında güvenlik aktivitelerinin durumlarının bir araç yardımı ile takip edilebilmesine olanak sağlanmıştır.

Dokümanın genel yapısı; her kontrol için bir Kategori, Sorumlu, ASVS kategorisi ve Risk Seviyesi şeklinde oluşturulmuştur. Bu bilgiler aşağıdaki değerleri içermektedirler;

Kategori (OWASP Testing Guide)

- Bilgi Toplama
- Yapılandırma Yönetimi
- Kimlik Doğrulama
- Oturum Yönetimi
- Yetkilendirme
- İş Mantığı
- Veri Denetimi
- Hizmet Dışı Bırakma
- Web Servisleri

Sorumlu

- Geliştirici: Uygulamayı geliştirmekten sorumlu kişiler
- Sistem Yöneticisi: Web ve uygulama sunucularının yapılandırma ve yönetiminden sorumlu kişiler
- Veritabanı Yöneticisi: Veritabanı sunucusunun yapılandırma ve yönetiminden sorumlu kişiler

OWASP ASVS Kategorisi

- Veri Koruması Sınama Gereksinimleri
- Hata Yönetimi ve Kayıt Tutma Sınama Gereksinimleri
- Erişim Kontrolü Sınama Gereksinimleri
- Oturum Yönetimi Sınama Gereksinimleri
- Kimlik Sınama Gereksinimleri
- Kriptoloji Sınama Gereksinimleri
- İletişim Güvenliği Sınama Gereksinimleri
- Çıktı Kodlama Sınama Gereksinimleri
- Girdi Denetimi Sınama Gereksinimleri

Risk Seviyesi

- Kritik (4)
- Yüksek (3)
- Orta (2)
- Düşük (1)

Katkıda Bulunanlar

2012 v2 Bünyamin Demir, Emin İslam Tatlı, Onur Yılmaz, Emre Süren, Oğuzhan Topgül

2010 v1 Bedirhan Urgun, Bünyamin Demir, Onur Yılmaz, Kubilay Onur Güngör, A. Kadir Altan, Volkan Altan, Muharrem Aydın, Canberk Bolat

1. Web, uygulama ve veritabanı sunucularının sistem bileşenleri hakkındaki kritik bilgiler (sunucu adı ve sürümü, kullanılan program sürümü v.b.) gizlenmelidir.
   Kategori : Bilgi Toplama **ASVS :** Veri Koruması
   Sorumlu : Sistem Yöneticisi, Veritabanı Yöneticisi **Seviye :** Orta

2. Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajları kullanıcıya detaylı olarak gösterilmemelidir.
   Kategori : Bilgi Toplama **ASVS :** Hata Yönetimi ve Kayıt Tutma
   Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Orta

3. Uygulamaların üzerinde koştukları sunucular, servis verdikleri dizinlerin içeriklerini listelememelidir.
   Kategori : Bilgi Toplama **ASVS :** Erişim Kontrolü
   Sorumlu : Sistem Yöneticisi **Seviye :** Orta

4. Arama motorları tarafından görüntülenmemesi istenen dizinler varsa, bunlar için robots.txt ile önlem alınmalıdır. Yanlız, sayfa içerisinde köprülenmeyen bağlantıların / dizinlerin (örneğin yönetim sayfası) güvenlik sorunu oluşturmaması adına robots.txt dosyasına eklenmemesi gerekmektedir.
   Kategori : Bilgi Toplama **ASVS :** Erişim Kontrolü
   Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Orta

5. Uygulama çatısı, veritabanı, uygulama sunucusu ve web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.
   Kategori : Yapılandırma Yönetimi **ASVS :** Veri Koruması
   Sorumlu : Sistem Yöneticisi **Seviye :** Kritik

6. Gerekmedikçe POST/GET dışındaki HTTP metotlarına izin verilmemelidir.
   Kategori : Yapılandırma Yönetimi **ASVS :** Erişim Kontrolü
   Sorumlu : Sistem Yöneticisi **Seviye :** Orta

7. Ana sistem için gereksiz olan dosyalara (örneğin yedekleme, arşiv, test, geliştirme için kullanılan dosyalar) erişim engellenmeli ve sistemdeki gereksiz uygulamalar (örneğin ön tanımlı sunucu sayfaları, demo uygulamalar) kaldırılmalılar.
   Kategori : Yapılandırma Yönetimi **ASVS :** Erişim Kontrolü
   Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

8. ASP.NET, PHP, STRUTS gibi kullanılan uygulama çatılarının güvenlik özellikleri aktif hale getirilmelidir.
   Kategori : Yapılandırma Yönetimi **ASVS :** Veri Koruması
   Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

9. Ön tanımlı kullanıcı hesapları sistemden, veritabanından ve uygulamadan kaldırılmalıdır.
   Kategori : Yapılandırma Yönetimi **ASVS :** Kimlik Sınama
   Sorumlu : Geliştirici, Sistem / Veritabanı Yöneticisi **Seviye :** Yüksek

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

11. Güvenli web trafiği için (SSL) güçlü şifreleme algoritmaları kullanılmalıdır, güvensiz algoritmalar inaktif hale getirilmelidir.
Kategori : Yapılandırma Yönetimi **ASVS :** Kriptoloji
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

12. Flash uygulamalarında crossdomain.xml ve SilverLight uygulamalarında clientaccesspolicy.xml yapılandırma dosyalarında uygulanan politikaların güvenli olup olmadığı kontrol edilmelidir.
Kategori : Yapılandırma Yönetimi **ASVS :** Erişim Kontrolü
Sorumlu : Sistem Yöneticisi **Seviye :** Orta

13. SSL sunucusunun "renegotiation" özelliği kapatılarak sunucu servis dışı bırakma ve MITM saldırılarına karşı korunaklı hale getirilmelidir.
Kategori : Yapılandırma Yönetimi **ASVS :** Kriptoloji
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

14. Zayıf parolaların kullanımına izin verilmemelidir.
Kategori : Kimlik Doğrulama **ASVS :** Kriptoloji
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Kritik

15. Kullanılan parolalar ve parolamı unuttum kontrol soru ve cevapları gibi diğer hassas veriler açık metin olarak saklanmamalıdır.
Kategori : Kimlik Doğrulama **ASVS :** Veri Koruması
Sorumlu : Geliştirici **Seviye :** Kritik

16. Uygulama ile son kullanıcı arasında aktarılan kullanıcı adı, parola, kredi kartı no, adres gibi hassas veriler HTTPS protokolü üzerinden aktarılmalıdır.
Kategori : Kimlik Doğrulama **ASVS :** İletişim Güvenliği
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Kritik

17. Umumi olmayan bütün kaynaklara ve sayfalara erişim için sunucu tarafında kimlik doğrulaması yapılmalıdır.
Kategori : Kimlik Doğrulama **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

18. Parola hash değerleri oluşturulurken tuz (salt) veriside kullanılmalıdır.
Kategori : Kimlik Doğrulama **ASVS :** Kriptoloji
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

☐ 19. Kullanıcılara (zarf, sözlü, e-posta yoluyla) dağıtılan başlangıç parolalar, kullanıcılar uygulamaya ilk giriş yaptıklarında değiştirilmeye zorlanmalıdır.
Kategori : Kimlik Doğrulama **ASVS :** Kriptoloji
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

☐ 20. Uygulama üzerinden yapılan kritik işlemler hem uygulama seviyesinde hem de sunucu seviyesinde kayıt altına alınmalıdır.
Kategori : Kimlik Doğrulama **ASVS :** Hata Yönetimi ve Kayıt Tutma
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Kritik

☐ 21. Kullanıcı adı ve parola ile kimlik doğrulamasının yapıldığı kontroller tek tip hata mesajı vermek suretiyle kullanıcı adları listeleme saldırılarına engel olmalıdırlar. Örnek bir hata mesajı "Girdiginiz kullanıcı adı ve/veya parola yanlıştır." seklinde olabilir.
Kategori : Kimlik Doğrulama **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 22. Bütün başarılı ve başarısız login işlemleri ve kaynaklara erişim denemeleri kayıt altına alınmalıdır.
Kategori : Kimlik Doğrulama **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

☐ 23. Oturum yönetimi için kullanılan ve uygulamayı kullanan bütün kullanıcılar için tekil olması gereken değerlerin (session id, token v.b.) güçlü bir rastgele veri üretecinden temin edildiği ve tahmin edilemez derecede karmaşık olduğu kontrol edilmelidir.
Kategori : Oturum Yönetimi **ASVS :** Oturum Yönetimi
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Kritik

☐ 24. Oturum bilgisi zaman aşımına uğrayacak şekilde yapılandırılmalıdır.
Kategori : Oturum Yönetimi **ASVS :** Oturum Yönetimi
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

☐ 25. Uygulamalarda başarılı kimlik doğrulama ve tekrarlayan kimlik doğrulama (re-authentication) neticesinde her zaman yeni bir oturum bilgisi oluşturulmalıdır. Çıkış işleminden sonra da var olan oturum bilgisi geçersizleştirilmelidir.
Kategori : Oturum Yönetimi **ASVS :** Oturum Yönetimi
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

☐ 26. Kritik işlemlerde CSRF saldırılarına karşı "token" veya "CAPTCHA" gibi güvenlik önlemleri alınmalıdır.
Kategori : Oturum Yönetimi **ASVS :** Erişim Kontrolü
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 27. Oturum bilgisini iceren cerezlerin (COOKIE) domain ve yol (path) bilgileri ilgili site için en uygun şekilde sınırlandırılmalıdır.
Kategori : Oturum Yönetimi **ASVS :** Oturum Yönetimi
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

28. Kullanılan çerez değerleri için httponly parametresi tanımlı olmalıdır. Buna ek olarak, HTTPS protokolü kullanılan bağlantılarda kullanılan çerez değerleri için secure parametresi tanımlı olmalıdır.
Kategori : Oturum Yönetimi **ASVS :** Oturum Yönetimi
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

29. Başarılı login işlemleri sonrası kullanıcı HTTP 302 ile dahili sayfalara yönlendirilmelidir.
Kategori : Oturum Yönetimi **ASVS :** Oturum Yönetimi
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Orta

30. Başarılı kimlik doğrulaması sonucu erişilen uygulamalarda sistemden tekrar çıkmak (logout) için gerekli linkler sağlanmalıdır.
Kategori : Oturum Yönetimi **ASVS :** Oturum Yönetimi
Sorumlu : Geliştirici **Seviye :** Orta

31. GET ve POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Geliştirici **Seviye :** Kritik

32. Uygulamayı çalıştıran sistem kullanıcısının, hizmet verilen dizin dışındaki yetkileri kaldırılmalıdır.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

33. Veritabanı kullanıcısının sadece uygulamanın kullandığı veritabanı kaynaklarına erişim hakkı olmalıdır.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Sistem Yöneticisi, Veritabanı Yöneticisi **Seviye :** Yüksek

34. Veritabanı kullanıcısının veritabanına sadece uygulama sunucu IP adresinden bağlantı hakkı olmalıdır.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Sistem Yöneticisi, Veritabanı Yöneticisi **Seviye :** Yüksek

35. Race-Condition'lara engel olmak için kritik kaynaklara, objelere, metotlara senkronizasyon sağlanarak eş zamanlı erişime izin verilmemelidir.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Geliştirici **Seviye :** Yüksek

36. Sunucu üzerinde bulunan ve web tabanlı istatistik sağlayan uygulamalara erişim herkese açık olmamalıdır.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Sistem Yöneticisi **Seviye :** Orta

37. Kısıtlı erişim gerektiren bütün URL'lere, fonksiyonlara, obje referanslarına, servislere, uygulama verilerine, kullanıcı bilgilerine, güvenlik yapılandırma dosyalarına erişim denetlenmelidir.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

38. Yetki hakkının artık gerekmediği durumlarda (örneğin şirketi terk etme, projede rol değiştirme gibi) en kısa sürede ilgili haklar iptal edilmelidir.
Kategori : Yetkilendirme **ASVS :** Erişim Kontrolü
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

39. Parola güncelleme işlemleri için eski parola her zaman sorulmalıdır.
Kategori : İş Mantığı **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici **Seviye :** Yüksek

40. Parola unuttum formları, gizli soru ve benzeri ek argümanlarla desteklenmelidir.
Kategori : İş Mantığı **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici **Seviye :** Orta

41. Parola unuttum işlemlerinden sonra kullanıcıya gönderilen eposta, kullanıcı adı ve parola bilgisi içermemelidir. Bunun yerine sınırlı yaşam süresi bulunan bir link gönderilip, o link üzerinden açılan sayfadan parola değiştirme işlemi gerçekleştirilmelidir.
Kategori : İş Mantığı **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici **Seviye :** Yüksek

42. Yönetim paneli gibi kritik dizinlerin isimleri kolay tahmin edilebilir olmamalıdır (admin, yonetici, administrator, yonetim, panel v.b.).
Kategori : İş Mantığı **ASVS :** Erişim Kontrolü
Sorumlu : Geliştirici **Seviye :** Orta

43. Uygulamalar, geliştirme ortamından prodüksiyon ortamına aktarılırken gereksiz olan dosyalar (örneğin test kodlar, demo programlar, yedek dosyalar) silinmeli, şayet gerek yoksa kaynak kod aktarılmamalı ve de aktarılacak olan kaynak kodlardaki yorum satırları silinmelidir. Aktarım esnasında dosyalarda istenmeyen bir değişikliğin olmaması garanti edilmelidir.
Kategori : İş Mantığı **ASVS :** Veri Koruması
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Yüksek

44. Uygulama domain isimlerine ait hassas bilgilerin google/bing gibi arama motorları tarafından indekslenmediği kontrol edilmelidir.
Kategori : İş Mantığı **ASVS :** Oturum Yönetimi
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek

45. Kullanıcıdan gelen tüm girdiler sunucu tarafında pozitif veri kontrolünden geçmelidir. Girdiler veri kontrolünden geçmeden önce „canonicalization" işlemine tabi tutulmalıdırlar.
Kategori : Veri Denetimi **ASVS :** Girdi Denetimi
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 46. Kullanıcıdan gelen veriler işletim sistemi komut satırına girmeden kontrol edilmeli ve düzgünleştirme işleminden (escape) geçirilmelidir.
Kategori : Veri Denetimi **ASVS :** Çıktı Kodlama
Sorumlu : Geliştirici **Seviye :** Kritik

☐ 47. SQL enjeksiyonuna karşı prepared statement/parameterized query/bind variables/pozitif veri kontrolü yöntemlerinden biri veya birkaçı kullanılmalıdır.
Kategori : Veri Denetimi **ASVS :** Çıktı Kodlama
Sorumlu : Geliştirici **Seviye :** Kritik

☐ 48. XSS saldırılarına karşı bütün kullanıcı girdileri dışarı aktarılmadan önce sunucu tarafında özel karakter kodlama (output encoding) işleminden geçirilmelidir. Güvenlik seviyesini artırmak için bu işlem kullanıcı girdilerinin tip, uzunluk, içerik denetlemesi yapılarak desteklenebilir.
Kategori : Veri Denetimi **ASVS :** Çıktı Kodlama
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 49. Güvensiz kaynaklardan veri alarak aritmetik işlem yapan uygulamalar, gerekli tam sayı üst sınır ve alt sınır kontrollerini gerçekleştirmelidirler.
Kategori : Veri Denetimi **ASVS :** Girdi Denetimi
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 50. Kullanıcıdan gelen ve dosya erişim işlemlerinde kullanılan girdiler normalizasyon işlemine tabi tutulmalıdır.
Kategori : Veri Denetimi **ASVS :** Çıktı Kodlama
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 51. Karşıdan dosya yükleme işlemlerinde yüklenilen dosya üzerinde isim, boyut, tip ve içerik kontrolü yapılmalıdır.
Kategori : Veri Denetimi **ASVS :** Girdi Denetimi
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 52. Kullanıcı parametrelerini kullanarak farklı sitelere yönlendirme yapan uygulamalarda ilgili parametrelere pozitif girdi denetimi uygulanmalı ve bu sayede olta saldırılarına engel olunmalıdır.
Kategori : Veri Denetimi **ASVS :** Girdi Denetimi
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 53. Kullanıcıdan veri alarak LDAP'a bağlanan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri LDAP düzgünleştirme işleminden (escape) geçirmelidir.
Kategori : Veri Denetimi **ASVS :** Çıktı Kodlama
Sorumlu : Geliştirici **Seviye :** Yüksek

☐ 54. Güvensiz kaynaklardan veri alarak XPath sorguları yapan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri XPath düzgünleştirme işleminden (escape) geçirmelidir.
Kategori : Veri Denetimi **ASVS :** Çıktı Kodlama
Sorumlu : Geliştirici **Seviye :** Yüksek

55. Kullanıcıdan gelen CR/LF karakterleri uygulama tarafında oldukları gibi HTTP cevap başlıklarında kullanılmamalıdır.
Kategori : Veri Denetimi **ASVS :** Girdi Denetimi
Sorumlu : Geliştirici **Seviye :** Yüksek

56. Uygulamalar, uygun olan her sayfada çerçeve engelleyici önlemleri (frame busting) almalıdırlar.
Kategori : Veri Denetimi **ASVS :** Çıktı Kodlama
Sorumlu : Geliştirici **Seviye :** Orta

57. Uygulama hizmete girmeden önce sızma testleri yapılmalıdır.
Kategori : Veri Denetimi **ASVS :** Girdi Denetimi
Sorumlu : Geliştirici **Seviye :** Yüksek

58. DoS saldırısı barındıracak veya şifre deneme-yanılma gibi kaba kuvvet saldırılarına açık tüm formlara CAPTCHA veya farklı anti-otomasyon güvenlik kontrolleri uygulanmalıdır.
Kategori : Hizmet Dışı Bırakma **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici **Seviye :** Yüksek

59. Genelde uygulamaların arama özelliğini kötüye kullanarak veritabanı üzerinde çok detaylı arama yaptırarak işlemciyi meşgul eden SQL genel arama karakter (%,* v.b.) saldırılarına karşı arama süresini kısıtlamak suretiyle önlem alınmalıdır..
Kategori : Hizmet Dışı Bırakma **ASVS :** Girdi Denetimi
Sorumlu : Geliştirici **Seviye :** Orta

60. SOAP, Restful, XML-RPC gibi teknolojilerle geliştirilmiş web servislerine erişimlerde kimlik doğrulama kontrolü uygulanmalıdır.
Kategori : Web Servisleri **ASVS :** Kimlik Sınama
Sorumlu : Geliştirici, Sistem Yöneticisi **Seviye :** Kritik

61. Web servisleri için kullanılan çatıların klasik XML saldırılarına (örneğin cok büyük XML verileri, çok sık tekrarlanan XML tag'leri) ve parametre manipülasyonları na karşı korunaklı olmaları sağlanmalıdır.
Kategori : Web Servisleri **ASVS :** Çıktı Kodlama
Sorumlu : Sistem Yöneticisi **Seviye :** Yüksek