# Introduction and Objectives (Giriş ve Amaçlar)

Bu bölüm OWASP web uygulama güvenlik test metodolojisini açıklar ve tanımlanmış güvenlik kontrollerine sahip eksiklikler nedeniyle uygulamadaki güvenlik açıklarının kanıtlarının nasıl test edileceğini açıklar.

## What is Web Application Security Testing? (Web Uygulama Güvenliği Testi Nedir?)

Güvenlik testi, uygulama güvenliği kontrollerinin etkinliğini metodik olarak doğrulayarak ve doğrulayarak bir bilgisayar sisteminin veya ağın güvenliğini değerlendirme yöntemidir. Bir web uygulama güvenlik testi yalnızca bir web uygulamasının güvenliğini değerlendirmeye odaklanır. Süreç, herhangi bir zayıflık, teknik kusur veya güvenlik açıkları için uygulamanın aktif bir analizini içerir. Bulunan herhangi bir güvenlik sorunu, etkinin bir değerlendirmesi, hafifletme önerisi veya teknik bir çözüm ile birlikte sistem sahibine sunulacaktır.

## What is a Vulnerability? (Savunmasızlık nedir?)

Bir güvenlik açığı, sistemin güvenlik hedeflerini tehlikeye atmak için yararlanılabilecek bir sistemin tasarımında, uygulamasında, işleyişinde veya yönetiminde bir kusur veya zayıflıktır.

## What is a Threat? (Tehdit nedir?)

Bir tehdit, bir savunmasızlıktan yararlanarak bir uygulamanın (verilemedeki veya dosya sisteminde verim gibi veriler gibi değer kaynaklarına) zarar verebilecek herhangi bir şey (kötü niyetli bir dış saldırgan, dahili bir kullanıcı, sistem istikrarsızlığı vb.) bir şeydir.

## What is a Test? (Test nedir?)

Bir test, bir uygulamanın paydaşlarının güvenlik gereksinimlerini karşıladığını göstermek için bir eylemdir.

### The Approach in Writing this Guide (Bu Kılavuzu Yazmada Yaklaşım)

OWASP yaklaşımı açık ve işbirlikçidir:

- Açık: Her güvenlik uzmanı projedeki deneyimlerine katılabilir. Her şey bedava.
- İşbirlikçi: makaleler yazılmadan önce beyin fırtınası yapılır, böylece ekip fikirleri paylaşabilir ve projenin kolektif bir vizyonunu geliştirebilir. Bu, kaba fikir birliği, daha geniş bir kitle ve artan
  katılım anlamına gelir.

Bu yaklaşım, aşağıdakiler olacak tanımlanmış bir Test Metodolojisi oluşturma eğilimindedir:

- Tutarlı
- Tekrarlanabilir
- Titiz
- Kalite kontrolü altında

Ele alınması gereken sorunlar tamamen belgelenir ve test edilir. Bilinen tüm güvenlik açıklarını test etmek ve tüm güvenlik testi faaliyetlerini belgelemek için bir yöntem kullanmak önemlidir.

## What Is the OWASP Testing Methodology? (OWASP Test Metodolojisi Nedir?)

Güvenlik testi, test edilmesi gereken tüm olası sorunların tam bir listesinin tanımlanabileceği kesin bir bilim olmayacaktır. Gerçekten de, güvenlik testi, belirli koşullar altında web uygulamalarının güvenliğini test etmek için yalnızca uygun bir tekniktir. Bu projenin amacı, olası tüm test tekniklerini toplamak, bu teknikleri açıklamak ve kılavuzu güncel tutmaktır. OWASP Web Uygulama Güvenliği Test yöntemi kara kutu yaklaşımına dayanmaktadır. Test cihazı hiçbir şey bilmiyor ya da test edilecek uygulama hakkında çok az bilgiye sahip.

Test modeli şunlardan oluşur:

- Test Cihazı: Test faaliyetlerini kim gerçekleştiriyor
- Araçlar ve metodoloji: Bu Test Kılavuzu projesinin özü
- Uygulama: Test etmek için kara kutu

Testler pasif veya aktif olarak kategorize edilebilir:

## Passive Testing (Pasif Test)

Pasif testler sırasında, bir test cihazı uygulamanın mantığını anlamaya çalışır ve bir kullanıcı olarak uygulamayı araştırır. Araçlar bilgi toplama için kullanılabilir. Örneğin, tüm HTTP isteklerini ve
yanıtlarını gözlemlemek için bir HTTP proxy kullanılabilir. Bu fazın sonunda, test cihazı genellikle sistemin tüm erişim noktalarını ve işlevselliğini (örneğin, HTTP başlıkları, parametreler, çerezler,
API'ler, teknoloji kullanımı / kalıpları vb.) anlamalıdır. Bilgi Toplama bölümü pasif testin nasıl yapılacağını açıklar.

Örneğin, bir test cihazı aşağıdaki URL'de bir sayfa bulabilir:
`https://www.example.com/login/auth_form`

Bu, uygulamanın kullanıcı adı ve şifre istediği bir kimlik doğrulama formu gösterebilir.

Aşağıdaki parametreler uygulamaya iki erişim noktasını temsil eder:
`https://www.example.com/appx?a=1&b=1`

Bu durumda, uygulama iki erişim noktası gösterir (parametreler `a` ve `b`). Bu aşamada bulunan tüm girdi noktaları test için bir hedef teşkil etmektedir. Uygulamanın dizinin veya arama ağacını takip etmek ve tüm erişim noktaları aktif testler sırasında yararlı olabilir.

## Active Testing (Aktif Test)

Aktif testler sırasında, bir test cihazı aşağıdaki bölümlerde açıklanan metodolojileri kullanmaya başlar.

Aktif test seti 12 kategoriye ayrılmıştır:

- Bilgi Toplaması
- Yapılandırma ve Dağıtım Yönetimi Testi
- Kimlik Yönetimi Testi

- Kimlik Doğrulama Testi
- Yetkilendirme Testi
- Oturum Yönetimi Testi
- Giriş Doğrulama Testi
- Hata Taşıma
- Kriptografi
- İş Mantık Testi
- Müşteri tarafı testi
- API Testi