

# Test Defenses Against Application Misuse (Uygulamanın Kötüye Kullanımına Karşı Savunmaları Test Edin)


## Summary (Özet)

Geçerli işlevselliğin kötüye kullanımı ve geçersiz kullanımı, web uygulamasını belirlemeye, zayıflıkları belirlemeye ve güvenlik açıklarından yararlanmaya çalışan saldırıları tanımlayabilir. Uygulamayı korumak için uygulama katmanlı savunma mekanizmalarının mevcut olup olmadığını belirlemek için testler yapılmalıdır.

Aktif savunma eksikliği, bir saldırganın herhangi bir rücu olmadan güvenlik açıklarını avlamasına izin verir. Böylece başvuru sahibinin başvurusunun saldırı altında olduğunu bilmeyecektir.

## Example (Örnek)

Doğrulanmış bir kullanıcı aşağıdaki (muhtemelen) eylem dizisini üstlenir:

1. Bir dosya kimliğine erişme girişiminin rollerinin indirilmesine izin verilmez
2. Tek bir keneyi yedekler  Dosya kimlik numarası yerine
3. Bir POSTA'ya bir alma isteğini değiştirir
4. Ekstra bir parametre ekler
5. Bir parametre adı / değer çiftini çoğaltın

Uygulama, kötüye kullanımı izliyor ve 5. olaydan sonra kullanıcı bir saldırgan olduğuna dair son derece yüksek güvenle yanıt veriyor. Örneğin uygulama:

- Kritik işlevselliği devre dışı bırakır
- Kalan işlevselliğe ek kimlik doğrulama adımları sağlar

- Her istek-yanıt döngüsüne zaman gecikmeleri ekler
- Kullanıcının etkileşimleri hakkında ek verileri kaydetmeye başlar (örneğin sanitize HTTP istek başlıkları, bedenleri ve yanıt organları)

Başvuru herhangi bir şekilde yanıt vermezse ve saldırgan işlevselliği kötüye kullanmaya devam edebilir ve uygulamada açıkça kötü amaçlı içerik gönderebilirse, uygulama bu test davasında başarısız oldu. Pratikte, yukarıdaki örnekteki ayırık örnek eylemlerin böyle gerçekleşmesi pek olası değildir. Her parametredeki zayıflıkları tanımlamak için bir bulanık bir aletin kullanılması çok daha olasıdır. Bir güvenlik test cihazının da üstlendiği şey budur.

## Test Objectives (Test Hedefleri)

- Sisteme karşı yapılan tüm testlerden notlar alın.
- Hangi testlerin agresif girdiye dayalı farklı bir işlevselliğe sahip olduğunu gözden geçirin.
- Savunmaları yerinde anlayın ve sistemi atlama tekniklerine karşı korumak için yeterli olup olmadıklarını doğrulayın.

## How To Test (Nasıl Test Edilir)

Bu test, sonucun web uygulamasına karşı yapılan diğer tüm testlerden çekilebilmesi açısından olağandışıdır. Diğer tüm testleri yaparken, uygulamanın yerleşik bir meşru müdafaa olduğunu gösterebilecek önlemleri not edin:

- Değişen yanıtlar
- Engellenen talepler
- Bir kullanıcıyı kaydeden veya hesaplarını kilitleyen eylemler

Bunlar sadece yerelleştirilmiş olabilir. Yaygın yerelleştirilmiş (işlev başına) savunmalar şunlardır:

- Belirli karakterleri içeren girişleri reddetmek
- Bir dizi kimlik doğrulama arızasından sonra bir hesabı geçici olarak kilitlemek

Yerel güvenlik kontrolleri yeterli değildir. Genellikle genel yanlış kullanıma karşı savunma yoktur:

- Zorla tarama
- Sunum katmanı giriş doğrulamasını atlama
- Çoklu erişim kontrol hataları
- Ek, çoğaltılmış veya eksik parametre isimleri
- Kullanıcı hataları veya yazım hataları olmayan değerler ile çoklu girdi doğrulama veya iş mantığı doğrulama başarısızlıkları
- Yapılandırılmış veriler (örneğin. JSON, XML) geçersiz bir formatın alınması
- Blatant çapraz site komut dosyası veya SQL enjeksiyon yükleri alınır
- Uygulamayı otomasyon araçları olmadan mümkün olandan daha hızlı kullanmak
- Bir kullanıcının kıtasal coğrafi konumundaki değişiklik
- Kullanıcı temsilcisinin değiştirilmesi
- Çok aşamalı bir iş sürecine yanlış sırayla erişim
- Uygulamaya özel işlevselliğin çok sayıda veya yüksek kullanım oranı (örneğin kupon kodu gönderimi, başarısız kredi kartı ödemeleri, dosya yüklemeleri, dosya indirmeleri, çıkışlar vb.)

Bu savunmalar, uygulamanın doğrulanmış bölümlerinde en iyi şekilde çalışır, ancak yeni hesapların oluşturulması veya içeriğe erişim oranı (örneğin bilgi sıyırmak için) kamuya açık alanlarda kullanılabilir.

Yukarıdakilerin hepsi uygulama tarafından izlenmelidir, ancak hiçbirisi değilse bir sorun vardır. Web uygulamasını test ederek, yukarıdaki eylem türünü yaparak, testçiye karşı herhangi bir yanıt alındı mı? Değilse, test cihazı uygulamanın kötüye kullanıma karşı uygulama çapında aktif savunması olmadığını bildirmelidir. Bazen saldırı tespitine verilen tüm yanıtların kullanıcıya sessiz kalması mümkündür (örneğin, kayıt değişiklikleri, yöneticilere yönelik uyarılar ve vekillik talep etmek), bu nedenle bu bulguya güvenin garanti edilemez. Pratikte, çok az uygulama (veya web uygulaması güvenlik duvarı gibi ilgili altyapı) bu tür kötüye kullanımı tespit etmektedir.

## **Related Test Cases (İlgili Test Vakaları)**

Diğer tüm test vakaları önemlidir.

## **Remediation (Düzeltilme)**

Başvurular, saldırganları ve istismarcıları savuşturmak için aktif savunma uygulamalıdır.

## **Referances (Referanslar)**

- Esnek Yazılım, Yazılım Güvencesi, ABD Departman İç Güvenlik
- IR 7684 Ortak Yanlış Kullanım Puanlama Sistemi (CMSS), NIST
- Common Attack Pattern Enumeration and Classification (CAPEC), The Mitre Corporation
- OWASP AppSensor Projesi
- AppSensor Guide v2, OWASP
- Watson C, Coates M, Melton J ve Groves G, Gerçek Zamanlı Savunmalarla Saldırı Yazılımı Uygulamaları Oluşturuyor, CrossTalk The Journal of Defense Software Engineering, Vol. 24, Hayır. 5, Eylül 2011