Test Application Platform Configuration (Test Uygulama Platformu Yapılandırması)

Summary (Özet)

Bir uygulama mimarisi oluşturan tek elemanların düzgün konfigürasyonu, tüm mimarinin güvenliğini tehlikeye atabilecek hataları önlemek için önemlidir.

Yapılandırma incelemesi ve test edilmesi, bir mimari oluşturma ve sürdürmede kritik bir görevdir. Bunun nedeni, birçok farklı sisteme genellikle yüklendikleri belirli sitede gerçekleştirecekleri göreve uygun olmayan jenerik konfigürasyonlar sağlanacağıdır.

Tipik web ve uygulama sunucusu kurulumu çok fazla işlevsellik (uygulama örnekleri, dokümantasyon, test sayfaları gibi) içerecek olsa da, yükleme sonrası sömürüyü önlemek için dağıtımdan önce gerekli olmayan şey kaldırılmalıdır.

Test Objectives (Test Hedefleri)

- Varsayılanların ve bilinen dosyaların kaldırıldığından emin olun.
- Üretim ortamlarında hata ayıklama kodu veya uzantılarının kalmadığını doğrulayın.
- Uygulama için belirlenen oturum mekanizmalarını inceleyin.

How to Test (Nasıl Test Edilir)

Black-Box Testing (Siyah-Kutu Testi)

Sample and Known Files and Directories (Örnek ve Bilinen Dosyalar ve Dizinler)

Birçok web sunucusu ve uygulama sunucusu, varsayılan bir yüklemede, geliştiricinin yararına numune uygulamaları ve dosyaları sunar ve sunucunun kurulumdan hemen sonra düzgün çalıştığını test etmek için kullanılır. Bununla birlikte, birçok varsayılan web sunucusu uygulamasının daha sonra savunmasız olduğu bilinmektedir. Bu, örneğin, CVE-1999-0449 (Exair örnekleme sitesi

kurulduğunda IIS'te Hizmetin Reddi), CAN-2002-1744 (Microsoft IIS 5.0'daki CodeBrws.asp'deki Direktörlük geçidi, CAN-202-1630 (Overtosizi. Oracle 9iAS'ta gönder.jsp kullanın) veya CAN-2003-1172 (Directory traversal

CGI tarayıcıları, farklı web veya uygulama sunucuları tarafından sağlanan bilinen dosyaların ve dizin örneklerinin ayrıntılı bir listesini içerir ve bu dosyaların mevcut olup olmadığını belirlemenin hızlı bir yolu olabilir. Ancak, gerçekten emin olmanın tek yolu, web sunucusunun veya uygulama sunucusunun içeriğinin tam bir incelemesini yapmak ve uygulamanın kendisiyle ilgili olup olmadığını belirlemektir.

Comment Review (Yorum İncelemesi)

Programcıların büyük web tabanlı uygulamalar geliştirirken yorum eklemeleri çok yaygındır. Bununla birlikte, HTML kodunda çevrimiçi olarak yer alan yorumlar, bir saldırganın kullanımına sunulmaması gereken dahili bilgileri ortaya çıkarabilir. Bazen, bir işlevsellik artık gerekli olmadığı için kaynak kodu bile yorumlanır, ancak bu yorum istemeden kullanıcılara iade edilen HTML sayfalarına sızdırılır.

Yorum incelemesi, herhangi bir bilginin yorumlarla sızdırılıp sızdırılmadığını belirlemek için yapılmalıdır. Bu inceleme yalnızca web sunucusu statik ve dinamik içeriğinin analizi ve dosya aramaları yoluyla iyice tamamlanabilir. Siteye otomatik veya rehberli bir şekilde gezinmek ve alınan tüm içeriği saklamak yararlı olabilir. Bu geri alınan içerik daha sonra kodda bulunan HTML yorumlarını analiz etmek için aranabilir.

System Configuration (Sistem Yapılandırma)

BT ve güvenlik uzmanlarına hedef sistemlerin çeşitli yapılandırma temellerine veya kıyaslamalara uygunluğunun ayrıntılı bir değerlendirmesini vermek için çeşitli araçlar, belgeler veya kontrol listeleri kullanılabilir. Bu tür araçlar içerir (ancak bunlarla sınırlı değildir):

- CIS-CAT Lite
- Microsoft'un Saldırı Yüzey Analizörü
- NIST'in Ulusal Kontrol Listesi Programı

Gray-Box Testing (Gri-Kutu Testi)

Configuration Review (Yapılandırma İncelemesi)

Web sunucusu veya uygulama sunucusu yapılandırması, sitenin içeriğini korumada önemli bir rol oynar ve ortak yapılandırma hatalarını tespit etmek için dikkatlice gözden geçirilmelidir. Açıkçası, önerilen yapılandırma site politikasına ve sunucu yazılımı tarafından sağlanması gereken işlevselliğe bağlı olarak değişir. Bununla birlikte, çoğu durumda, sunucunun uygun şekilde güvence altına alınıp alınmadığını belirlemek için yapılandırma yönergeleri (yazıcı satıcı veya harici taraflar tarafından sağlanan) takip edilmelidir.

Bir sunucunun nasıl yapılandırılması gerektiğini genel olarak söylemek imkansızdır, ancak bazı ortak yönergeler dikkate alınmalıdır:

- Uygulama için gerekli olan sunucu modüllerini (IIS durumunda İSAP uzantıları) yalnızca etkinleştirin. Bu, yazılım modülleri devre dışı bırakıldıkça sunucu boyut ve karmaşıklık olarak azaltıldığından saldırı yüzeyini azaltır. Ayrıca, satıcı yazılımında görünebilecek güvenlik
  açıklarının yalnızca zaten devre dışı bırakılmış olan modüllerde mevcutsa siteyi etkilemesini önler.
- Sunucu hatalarını (40x veya 50x) varsayılan web sunucu sayfaları yerine özel yapım sayfalarla ele alın. Özellikle herhangi bir uygulama hatasının son kullanıcıya iade edilmeyeceğinden ve bir saldırgana yardımcı olacağından bu hatalar yoluyla hiçbir kodun sızdırılmadığından emin olun. Bu noktayı unutmak aslında çok yaygındır, çünkü geliştiricilerin üretim öncesi ortamlarda bu bilgilere ihtiyaç duyarlar.
- Sunucu yazılımının işletim sisteminde en aza indirilmiş ayrıcalıklarla çalıştığından emin olun. Bu, sunucu yazılımındaki bir hatanın tüm sistemi doğrudan tehlikeye atmasını önler, ancak bir
  saldırgan web sunucusu olarak kod çalıştırdıktan sonra ayrıcalıkları artırabilir.
- Sunucu yazılımının hem meşru erişim hem de hataları doğru bir şekilde kaydettirdiğinden emin olun.
- Sunucunun aşırı yükleri düzgün bir şekilde ele alacak ve Hizmet Saldırılarının Reddini önlemek için yapılandırıldığından emin olun. Sunucunun düzgün bir şekilde performans ayarlandığından emin olun.
- Asla idari olmayan kimlikler vermeyin (bu istisna dışında `NT SERVICE\WMSvc`) başvuruya erişimHost.config, redirection.config ve admin.config (ya Oku veya Yazma erişimi). Buna dahil `Network Service`, `IIS_IUSRS`, `IUSR`, veya IIS uygulama

havuzları tarafından kullanılan herhangi bir özel kimlik. IIS işçi süreçleri bu dosyalardan herhangi birine doğrudan erişmek anlamına gelmez.

- Uygulamayı asla paylaşın.config, redirection.config ve admin.config ağda. Paylaşılan Yapılandırmayı kullanırken, uygulamaHost.config'i başka bir konuma ihraç etmeyi tercih edin ([Parçalı Yapılandırma için İzinler Ayarlamak) başlıklı bölüme bakın.
- Tüm kullanıcıların okuyabileceğini unutmayın. NET Framework `machine.config` ve kök `web.config` Varsayılan olarak dosyalar. Hassas bilgileri yalnızca yönetici gözleri için olması gerekiyorsa bu dosyalarda saklamayın.
- Sadece IIS işçisi tarafından okunması gereken hassas bilgileri, makinedeki diğer kullanıcılar tarafından değil, şifrelemek.
- Web sunucusunun paylaşılanlara erişmek için kullandığı kimliğe yaz erişimini vermeyin `applicationHost.config`. . Bu kimlik sadece Read erişimi olmalıdır.
- UygulamaHost.config'i paylaşıma yayınlamak için ayrı bir kimlik kullanın. Web sunucularındaki paylaşılan yapılandırmaya erişimi yapılandırmak için bu kimliği kullanmayın.
- Paylaşılan yapılandırma ile kullanılmak üzere şifreleme anahtarlarını ihraç ederken güçlü bir şifre kullanın.
- Paylaşılan yapılandırma ve şifreleme anahtarlarını içeren paya sınırlı erişimi sağlayın. Bu pay ele geçirilirse, bir saldırgan Web sunucularınız için herhangi bir IIS yapılandırmasını okuyup yazabilir, Web sitenizden gelen trafiği kötü amaçlı kaynaklara yönlendirebilir ve bazı durumlarda IIS işçi süreçlerine rastgele kod yükleyerek tüm web sunucularının kontrolünü ele geçirebilir.
- Bu payı yalnızca üye web sunucularının bağlanmasına izin vermek için güvenlik duvarı kuralları ve IPsec politikaları ile korumayı düşünün.

Logging (Kontluk)

Kayıt olmak, bir uygulama mimarisinin güvenliğinin önemli bir varlığıdır, çünkü uygulamalardaki kusurları (sürekli olarak gerçekten var olmayan bir dosyayı almaya çalışan kullanıcılar) ve haydut kullanıcıların sürekli saldırılarını tespit etmek için kullanılabilir. Günlükler genellikle web ve diğer sunucu yazılımları tarafından doğru bir şekilde oluşturulur. Eylemlerini bir kütüğe düzgün bir şekilde kaydeden

uygulamalar bulmak yaygın değildir ve yaptıklarında, uygulama günlüklerinin ana niyeti, programcı tarafından belirli bir hatayı analiz etmek için kullanılabilecek hata ayıklama çıktısı üretmektir.

Her iki durumda da (servis ve uygulama günlükleri) birkaç konu kütük içeriğine göre test edilmeli ve analiz edilmelidir:

1. Günlükler hassas bilgiler içeriyor mu?
2. Günlükler özel bir sunucuda mı saklanıyor?
3. Kayıt kullanımı bir Hizmet İnkarı durumu oluşturabilir mi?
4. Nasıl döndürülürler? Günlükler yeterli süre için tutuluyor mu?
5. Günlükler nasıl incelenir? Yöneticiler bu incelemeleri hedefli saldırıları tespit etmek için kullanabilir mi?
6. Sloganları Nasıl Korur?
7. Verilerin kaydedilmesi, kaydedilmeden önce (min / maksimum uzunluk, köstürler vb.) kaydedilir mi?

Sensitive Information in Logs (Günlüklerde Hassas Bilgiler)

Bazı uygulamalar, örneğin, sunucu kayıtlarında görülecek verileri iletmek için GET isteklerini kullanabilir. Bu, sunucu günlüklerinin hassas bilgiler içerebileceği anlamına gelir (şifreler olarak kullanıcı adları veya banka hesap bilgileri gibi). Bu hassas bilgiler, bir saldırgan tarafından, örneğin idari arayüzler veya bilinen web sunucusu güvenlik açıkları veya yanlış yapılandırma yoluyla (bilinenler gibi) ile kayıtlar elde ettikleri takdirde yanlış kullanılabilir. `server-status` Apache tabanlı HTTP sunucularında yanlış yapılandırma).

Etkinlik günlükleri genellikle bir saldırgan (bilgi sızıntısı) için yararlı olan veya doğrudan istismarlarda kullanılabilen veriler içerecektir:

- Debug bilgileri
- İstif izleri
- Kullanıcı adları
- Sistem bileşeni isimleri
- Dahili IP adresleri

- Daha az hassas kişisel veriler (örneğin e-posta adresleri, posta adresleri ve adı geçen kişilerle ilişkili telefon numaraları)
- İşletme verileri

Ayrıca, bazı yargı bölgelerinde, kişisel veriler gibi bazı hassas bilgileri günlük dosyalarında saklamak, işletmenin dosyaların günlüğünü kaydetmek için arka uç veritabanlarına uygulayacakları veri koruma yasalarını uygulama zorunluluğu getirebilirsiniz. Ve bunu yapmamak, bilmeden bile olsa, geçerli olan veri koruma yasalarına göre cezalar taşıyabilir.

Hassas bilgilerin daha geniş bir listesi şunlardır:

- Uygulama kaynak kodu
- Oturum tanımlama değerleri
- Erişim tokenleri
- Hassas kişisel veriler ve kişisel olarak tanımlanabilir bilgilerin bazı formları (PII)
- Kimlik doğrulama şifreleri
- Veritabanı bağlantı dizeleri
- Şifreleme anahtarları
- Banka hesabı veya ödeme kartı sahibi verileri
- Yetiştirme sisteminin depolanmasına izin verilenden daha yüksek bir güvenlik sınıflandırması verileri
- Ticari olarak hassas bilgiler
- İlgili yargı alanında tahsil etmek yasa dışı olduğu bilgiler
- Bir kullanıcının tahsilattan vazgeçtiği veya örneğin izlememesi için onay vermediği veya izin vermemesi gereken bilgiler veya toplama onayının süresinin dolduğunda

Log Location (Kayıt Konumu)

Tipik olarak sunucular, sunucunun çalıştığı sistemin diskini tüketerek eylemlerinin ve hatalarının yerel günlüklerini oluşturacaktır. Bununla birlikte, sunucu tehlikeye girerse, saldırı ve yöntemlerinin tüm izlerini temizlemek için davetsiz misafir

tarafından silinebilir. Bu olsaydı, sistem yöneticisi saldırının nasıl meydana geldiği veya saldırı kaynağının nerede bulunduğu hakkında hiçbir bilgiye sahip olmayacaktı. Aslında, çoğu saldırgan araç kitleri, verilen bilgileri (saldırganın IP adresi gibi) tutan ve saldırganın sistem düzeyindeki kök kitlerinde rutin olarak kullanılan herhangi bir günlükleri temizleyebilen bir “log zapper” içerir.

Sonuç olarak, günlükleri web sunucusunun kendisinde değil, ayrı bir yerde tutmak daha akıllıcadır. Bu aynı zamanda aynı uygulamayı (bir web sunucusu çiftliğininkiler gibi) ifade eden farklı kaynaklardan günlükleri toplamayı kolaylaştırır ve aynı zamanda sunucunun kendisini etkilemeden günlük analizi yapmayı (CP yoğun olabilir) yapmayı kolaylaştırır.

Log Storage (Log Depolama)

Günlükler, uygun şekilde saklanmadıkları takdirde bir Hizmet İnkarı durumu tanıtabilir. Yeterli kaynağa sahip herhangi bir saldırgan, özellikle bunu yapmaları engellenmediyse, dosya kaydetmek için ayrılan alanı dolduracak yeterli sayıda talep üretebilir. Bununla birlikte, sunucu düzgün yapılandırılmazsa, günlük dosyaları işletim sistemi yazılımı veya uygulamanın kendisi için kullanılan disk bölümünde aynı disk bölümünde saklanacaktır. Bu, diskin çalışma sistemini doldurursa veya uygulamanın diske yazamadığı için başarısız olabileceği anlamına gelir.

Tipik olarak UNIX sistemlerinde günlükler /varda (bazı sunucu kurulumları /opt veya /usr / yerel olarak ikamet edebilir) ve kayıtların depolandığı dizinlerin ayrı bir bölümde olduğundan emin olmak önemlidir. Bazı durumlarda ve sistem kayıtlarının etkilenmesini önlemek için, sunucu yazılımının kendisinin (Apapa web sunucusunda /var / log / apache gibi) özel bir bölümde saklanmalıdır.

Bu, oturum açtıkları dosya sistemini doldurmak için kütüklerin büyümesine izin verilmesi gerektiği anlamına gelmez. Bu koşulu tespit etmek için sunucu günlüklerinin büyümesi, bir saldırının göstergesi olabileceğinden izlenmelidir.

Bu koşulun test edilmesi, üretim ortamlarında, bu taleplerin kaydedilip kaydedilmediğini ve bu isteklerle günlük bölmeyi doldurma olasılığı olup olmadığını görmek için yeterli ve sürekli sayıda talebin ateşlenmesi kadar kolaydır. QUERY_STRING parametrelerinin, GET veya POST istekleri yoluyla üretilip üretilmediğine bakılmaksızın kaydedildiği bazı ortamlarda, günlükleri daha hızlı dolduracak büyük sorgular simüle edilebilir, çünkü tipik olarak, tek bir istek tarih ve

saat, kaynak IP adresi, URI talebi ve sunucu sonucu gibi sadece az miktarda veri kaydedilmesine neden olacaktır.

Log Rotation (Log Rotasyon)

Çoğu sunucu (ancak birkaç özel uygulama), üzerinde ikamet ettikleri dosya sistemini doldurmalarını önlemek için günlükleri döndürür. Kayıtları döndürürken varsayım, içlerindeki bilgilerin yalnızca sınırlı bir süre için gerekli olduğudur.

Bu özellik aşağıdakileri sağlamak için test edilmelidir:

- Lojistikler, daha fazla değil, daha fazla değil, güvenlik politikasında tanımlanan süre için tutulur.
- Günlükler döndürüldükten sonra sıkıştırılır (bu bir kolaylıktır, çünkü aynı mevcut disk alanı için daha fazla kütük saklanacağı anlamına gelir).
- Döndürülmüş günlük dosyalarının dosya sistemi izni, günlük dosyalarının kendisinin aynı (veya daha katı) olmasıdır. Örneğin, web sunucularının kullandıkları günlüklere yazması gerekecektir, ancak aslında dönen günlüklere yazmaları gerekmez, bu da web sunucusu sürecinin bunları değiştirmesini önlemek için dosyaların izinlerinin dönüldüğü anlamına gelir.

Bazı sunucular belirli bir boyuta ulaştıklarında günlükleri döndürebilir. Bu gerçekleşirse, bir saldırganın izlerini gizlemek için kütükleri döndürmeye zorlamaması sağlanmalıdır.

Log Access Control (Log Erişim Kontrolü)

Etkinlik günlüğü bilgileri son kullanıcılar için asla görülememelidir. Web yöneticileri bile görev kontrollerinin ayrılmasını bozduğu için bu tür günlükleri görememelidir. Ham günlüklere erişimi korumak için kullanılan herhangi bir erişim kontrol şemasının ve günlükleri görüntüleme veya arama yetenekleri sağlayan uygulamaların diğer uygulama kullanıcı rolleri için erişim kontrol şemaları ile bağlantılı olmadığından emin olun. Herhangi bir günlük verisi de kimliği belirsiz kullanıcılar tarafından görüntülenebilir olmamalıdır.

Log Review (Log İncelemesi)

Günlüklerin gözden geçirilmesi, web sunucularındaki dosyaların kullanım istatistiklerinin çıkarılmasından daha fazlası için kullanılabilir (bu genellikle çoğu

kayıt tabanlı uygulamanın odaklanacağı şeydir), aynı zamanda saldırıların web sunucusunda gerçekleşip gerçekleşmediğini belirlemek için kullanılabilir.

Web sunucusunun saldırılarını analiz etmek için sunucunun hata günlük dosyalarının analiz edilmesi gerekir. İnceleme:

- 40x (bulut değil) hata mesajları. Aynı kaynaktan gelen bunların büyük bir kısmı, web sunucusuna karşı kullanılan bir CGI tarayıcı aracının göstergesi olabilir.
- 50x (server hata) mesajları. Bunlar, uygulamanın beklenmedik bir şekilde başarısız olan kısımlarını kötüye kullanan bir saldırganın bir göstergesi olabilir. Örneğin, bir SQL enjeksiyon saldırısının ilk aşamaları, SQL sorgusu düzgün bir şekilde oluşturulmadığında ve icrası
  arka uç veritabanında başarısız olduğunda bu hata mesajını üretecektir.

Günlük istatistikleri veya analiz, günlükleri üreten aynı sunucuda oluşturulmamalı veya saklanmamalıdır. Aksi takdirde, bir saldırgan, bir web sunucusu güvenlik açığı veya uygunsuz yapılandırma yoluyla, onlara erişebilir ve günlük dosyaları tarafından açıklanacak gibi benzer bilgileri alabilir.

References (Referanslar)

- Apache
  - Apache Security, Ivan Ristic, O'reilly, Mart 2005.
  - Apache Güvenlik Sırları: Ortaya Çıktı (Tekrar), Mark Cox, Kasım 2003
  - Apache Güvenlik Sırları: Açıklandı, ApacheCon 2002, Las Vegas, Mark J Cox, Ekim 2002
  - Performans Ayarlama
- Lotus Domino'nun
  - Lotus Güvenlik El Kitabı, William Tworek et al., Nisan 2004, IBM Redbooks koleksiyonunda mevcuttur.
  - Lotus Domino Güvenliği, bir X-kuvvet beyaz kağıt, İnternet Güvenlik Sistemleri, Aralık 2002
  - Hackproofing Lotus Domino Web Server, David Litchfield, Ekim 2001
- Microsoft Il'nin

    - IIS 8 için En İyi Güvenlik Uygulamaları
    - CIS Microsoft IIS Benchmarks
    - Web Sunucunuzu Güvence Altına Almak (Patterns and Practices), Microsoft Corporation, Ocak 2004
    - IIS Güvenlik ve Programlama Karşı Önlemleri, Jason Coombs
    - Blueprint'ten Kaleye: IIS 5.0'ı Güvence Altına Kılavuz, John Davis, Microsoft Corporation, Haziran 2001
    - Güvenli İnternet Bilgi Hizmetleri 5 Kontrol Listesi, Michael Howard, Microsoft Corporation, Haziran 2000
- Red Hat's (eski adıyla Netscape) iPlanet
    - IPlanet Web Server'ın Güvenli Konfigülasyonu ve Yönetimi Kılavuzu, Kurumsal Baskı 4.1, James M Hayes, Sistemler ve Ağ Saldırı Merkezi Ağ Uygulamaları Ekibi (SNAC), NSA, Ocak 2001
- WebSphere
    - IBM WebSphere V5.0 Güvenlik, WebSphere El Kitabı Serisi, Peter Kovari ve ark., IBM, Aralık 2002.
    - IBM WebSphere V4.0 Advanced Edition Security, Peter Kovari et al., IBM, Mart 2002.
- Genel
    - Kaydırma Hilesi, OWASP
    - SP 800-92 Bilgisayar Güvenliği Kütüğü Yönetimi Kılavuzu, NIST
    - PCI DSS v3.2.1 Gereklilik 10 ve PA-DSS v3.2 Gereklilik 4, PCI Güvenlik Standartları Konseyi
- Genel:
    - CERT Güvenlik Geliştirme Modülleri: Halka Açık Web Sunucularının Güvencesi
    - Nasıl Yapılır: ISIlockdown.exe'yi Kullanın