3. The OWASP Testing Framework (OWASP Test Çerçevesi)

Overview (Genel Bakış)

Bu bölüm, bir organizasyon içinde geliştirilebilecek tipik bir test çerçevesini açıklar. Yazılım geliştirme yaşam döngüsünün (SDLC) çeşitli aşamalarında uygun olan teknik ve görevlerden oluşan bir referans çerçevesi olarak görülebilir. Şirketler ve proje ekipleri bu modeli kendi test çerçevelerini geliştirmek ve satıcılardan gelen test hizmetlerini kapsayacak şekilde kullanabilirler. Bu çerçeve kuralcı olarak değil, bir kuruluşun gelişim sürecine ve kültürüne uyacak şekilde genişletilebilen ve şekillendirilebilecek esnek bir yaklaşım olarak görülmelidir.

Bu bölüm, kuruluşların tam bir stratejik test süreci oluşturmasına yardımcı olmayı amaçlamaktadır ve daha taktiksel, belirli test alanlarına girme eğiliminde olan danışmanlara veya yüklenicilere yönelik değildir.

Bir uçtan uca test çerçevesi oluşturmanın neden yazılım güvenliğini değerlendirmek ve geliştirmek için çok önemli olduğunu anlamak kritik öneme sahiptir. *Güvenli* Kod *Yazarı olarak*, Howard ve LeBlanc, bir güvenlik bülteni yayınlamanın Microsoft'a en az 100.000 dolara mal olduğunu ve müşterilerine güvenlik yamalarını uygulamak için toplu olarak çok daha pahalıya mal olduğunu belirtiyor. Ayrıca, ABD hükümetinin CyberCrime web sitesinin son ceza davalarını ve kuruluşlara verilen zararı detaylandırdığını da belirtiyorlar. Tipik kayıplar 100.000 ABD dolarını aşmaktadır.

Bunun gibi ekonomi ile, yazılım satıcılarının neden yalnızca daha önce geliştirilmiş uygulamalarda gerçekleştirilebilen, yalnızca tanım, tasarım ve geliştirme gibi uygulama geliştirmenin erken döngülerinde testlere odaklanabilecek kara kutu güvenlik testlerinden neden çok az şaşırtıcıdır.

Birçok güvenlik uygulayıcısı hala penetrasyon testi alanında güvenlik testi görüyor. Önceki bölümde tartışıldığı gibi, penetrasyon testinin oynaması gereken bir rol olsa da, genellikle hata bulmada verimsizdir ve test cihazının becerisine aşırı derecede dayanır. Sadece bir uygulama tekniği olarak düşünülmeli veya üretim sorunları hakkında farkındalık yaratmak gerekir. Uygulamaların güvenliğini artırmak için yazılımın güvenlik kalitesinin iyileştirilmesi gerekir. Bu, tanım, tasarım, geliştirme, dağıtım ve bakım aşamalarında güvenliğin test edilmesi ve kod tamamen inşa edilene kadar beklemenin maliyetli stratejisine güvenmemek anlamına gelir.

Bu belgenin tanıtımında tartışıldığı gibi, Rasyonel Birleşik Süreç, eKretrem ve Çevik geliştirme ve geleneksel şelale metodolojileri gibi birçok geliştirme metodolojisi vardır. Bu kılavuzun amacı, ne belirli bir gelişim metodolojisi önermek ne de belirli bir metodolojiye bağlı olan belirli bir rehberlik sağlamaktır. Bunun yerine, jenerik bir geliştirme modeli sunuyoruz ve okuyucu bunu şirket süreçlerine göre takip etmelidir.

Bu test çerçevesi, gerçekleşmesi gereken faaliyetlerden oluşur:

- Gelişim başlamadan önce,
- Tanım ve tasarım sırasında,
- Gelişim sırasında,
- Dağıtım sırasında ve
- Bakım ve operasyonlar sırasında.

Phase 1 Before Development Begins (Geliştirme Başlamadan Önce 1. Aşama)

Phase 1.1 Define a SDLC (Aşama 1.1 Bir SDLC tanımlayın)

Uygulama geliştirme başlamadan önce, güvenliğin her aşamada bulunduğu yerde yeterli bir SDLC tanımlanmalıdır.

(Faz 1.2 İnceleme Politikaları ve Standartları)

Uygun politikalar, standartlar ve belgeler olduğundan emin olun. Dokümantasyon, geliştirme ekiplerine izleyebilecekleri yönergeler ve politikalar verdiği için son derece önemlidir. İnsanlar doğru olanı ancak doğru şeyin ne olduğunu bilirlerse yapabilirler.

Uygulama Java'da geliştirilecekse, Java güvenli kodlama standardı olması esastır. Uygulama kriptografi kullanmaksa, bir kriptografi standardı olması esastır. Hiçbir politika veya standart, geliştirme ekibinin karşılaşacağı her durumu karşılayamaz. Ortak ve öngörülebilir konuları belgeleyerek, geliştirme sürecinde yapılması gereken daha az karar olacaktır.

(Faz 1.3 Ölçüm ve Metrik Kriterlerini Geliştirin ve İzlenebilirliği Sağlayın)

Gelişim başlamadan önce, ölçüm programını planlayın. Ölçülmesi gereken kriterleri tanımlayarak, hem süreçte hem de üründeki kusurlara görünürlük sağlar. Gelişme başlamadan önce metrikleri tanımlamak esastır, çünkü verileri yakalamak için süreci değiştirmeye ihtiyaç duyabilir.

Phase 2 During Definition and Design (Tanımlama ve Tasarım Sırasında 2. Aşama)

Phase 2.1 Review Security Requirements (Aşama 2.1 Güvenlik Gereksinimlerini Gözden Geçirin)

Güvenlik gereksinimleri, bir uygulamanın güvenlik perspektifinden nasıl çalıştığını tanımlar. Güvenlik gereksinimlerinin test edilmesi çok önemlidir. Bu durumda test etmek, gereksinimlerde yapılan varsayımların test edilmesi ve gereksinim tanımlarında boşluklar olup olmadığının test edilmesi anlamına gelir.

Örneğin, kullanıcıların bir web sitesinin whitepapers bölümüne erişmeden önce kaydedilmesi gerektiğini belirten bir güvenlik şartı varsa, bu, kullanıcının sisteme kayıtlı olması gerektiği veya kullanıcının doğrulanması gerektiği anlamına mı geliyor? Gereksinimlerin mümkün olduğunca açık olduğundan emin olun.

Gereksinim boşluklarını ararken, aşağıdaki gibi güvenlik mekanizmalarına bakmayı düşünün:

- Kullanıcı yönetimi

- Kimlik doğrulaması
- Yetkilendirme
- Veri gizliliği
- Dürüstlük
- Hesap verebilirlik
- Oturum yönetimi
- Ulaştırma güvenliği
- Kademeli sistem ayrışması
- Yasama ve standartlar uyumluluğu (gizlilik, hükümet ve endüstri standartları dahil)

Phase 2.2 Review Design and Architecture (Aşama 2.2 Tasarım ve Mimarinin Gözden Geçirilmesi)

Uygulamalar belgelenmiş bir tasarım ve mimariye sahip olmalıdır. Bu dokümantasyon modelleri, metinsel belgeleri ve diğer benzer eserleri içerebilir. Tasarım ve mimarinin gereksinimlerde tanımlandığı gibi uygun güvenlik seviyesini zorlamasını sağlamak için bu eserleri test etmek esastır.

Tasarım aşamasındaki güvenlik kusurlarını tanımlamak sadece kusurları tanımlamak için en uygun maliyetli yerlerden biri değildir, aynı zamanda değişiklik yapmak için en etkili yerlerden biri olabilir. Örneğin, tasarımın birden fazla yerde yetkilendirme kararları alınması gerektiği tespit edilirse, merkezi bir yetkilendirme bileşenini göz önünde bulundurmak uygun olabilir. Uygulama birden fazla yerde veri doğrulaması yapıyorsa, merkezi bir doğrulama çerçevesi geliştirmek uygun olabilir (yani, giriş doğrulamasını yüzlerce yerde değil, tek bir yerde sabitlemek çok daha ucuzdur).

Zayıflıklar keşfedilirse, alternatif yaklaşımlar için sistem mimarına verilmelidir.

Phase 2.3 Create and Review UML Models (Aşama 2.3 UML Modellerinin Oluşturulması ve Gözden Geçirilmesi)

Tasarım ve mimari tamamlandıktan sonra, uygulamanın nasıl çalıştığını tanımlayan Birleşik Modelleme Dili (UML) modelleri oluşturun. Bazı durumlarda, bunlar zaten mevcut olabilir. Bu modelleri, sistem tasarımcılarıyla uygulamanın nasıl çalıştığını tam olarak anlamak için kullanın. Zayıflıklar keşfedilirse, alternatif yaklaşımlar için sistem mimarına verilmelidir.

Phase 2.4 Create and Review Threat Models (Aşama 2.4 Tehdit Modellerinin Oluşturulması ve Gözden Geçirilmesi)

Sistemin tam olarak nasıl çalıştığını açıklayan UML modelleri ile donanmış, bir tehdit modelleme egzersizi gerçekleştiriyor. Gerçekçi tehdit senaryoları geliştirin. Bu tehditlerin hafifletilmesini, işletme tarafından kabul edilmesini veya bir sigorta firması gibi üçüncü bir tarafa atanmasını sağlamak için tasarımı ve mimariyi analiz edin. Tehditlerin tespit edildiğinde, tasarımı değiştirmek için sistem mimarı ile tasarımı ve mimariyi yeniden ziyaret edin.

Phase 3 During Development (Geliştirme Sırasında 3. Aşama)

Teorik olarak, geliştirme bir tasarımın uygulanmasıdır. Bununla birlikte, gerçek dünyada, kod geliştirme sırasında birçok tasarım kararı verilir. Bunlar genellikle tasarımda açıklanamayacak kadar ayrıntılı olan daha küçük kararlar veya hiçbir politika veya standart rehberliğin sunulmadığı konulardır. Tasarım ve mimari yeterli değilse, geliştirici birçok kararla karşılaşacak. Yetersiz politika ve standartlar varsa, geliştirici daha da fazla kararla karşılaşacaktır.

Phase 3.1 Code Walkthrough (Aşama 3.1 Kod İzleme)

Güvenlik ekibi, geliştiricilerle ve bazı durumlarda sistem mimarlarıyla bir kod yapmalıdır. Bir kod yürüyüşü, geliştiricilerin uygulanan kodun mantığını ve akışını açıklayabilecekleri koda yüksek düzeyde bir bakıştır. Kod inceleme ekibinin kodun genel bir anlayışını elde etmesini sağlar ve geliştiricilerin neden belirli şeylerin olduğu gibi geliştirildiğini açıklamalarını sağlar.

Amaç bir kod incelemesi yapmak değil, uygulamayı oluşturan kodun akışını, düzenini ve yapısını yüksek düzeyde anlamaktır.

Phase 3.2 Code Reviews (Aşama 3.2 Kod İncelemeleri)

Kodun nasıl yapılandırıldığını ve bazı şeylerin neden olduğu gibi kodlandığını iyi anlayarak, test cihazı artık güvenlik kusurları için gerçek kodu inceleyebilir.

Statik kod incelemeleri, kodu aşağıdakiler dahil olmak üzere bir dizi kontrol listesine karşı onaylar.

- kullanılabilirlik, gizlilik ve bütünlük için iş gereksinimleri;
- Teknik pozlamalar için OWASP Kılavuzu veya En İyi 10 Kontrol Listesi (incelemenin derinliğine bağlı olarak);
- PHP için Scarlet kağıdı veya ASP.NET için Microsoft Güvenli Kodlama kontrol listeleri gibi kullanımdaki dil veya çerçeve ile ilgili özel konular; ve
- Sarbanes-Oxley 404, COPPA, ISO / IEC 27002, APRA, HIPAA, Visa Tüccar yönergeleri veya diğer düzenleyici rejimler gibi endüstriye özgü gereksinimler.

Yatırım yapılan kaynakların geri dönüşü (çoğunlukla zaman), statik kod incelemeleri, diğer güvenlik inceleme yöntemlerinden çok daha yüksek kaliteli getiri sağlar ve en az gözden geçirenin becerisine güvenir. Bununla birlikte, gümüş bir mermi değildirler ve tam spektrumlu bir test rejimi içinde dikkatlice düşünülmelidir.

OWASP kontrol listeleri hakkında daha fazla bilgi için lütfen OWASP Top 10'un en son sürümüne bakın.

Phase 4 During Deployment (Dağıtım Sırasında 4. Aşama)

Phase 4.1 Application Penetration Testing (Aşama 4.1 Uygulama Sızma Testi)

Gereksinimleri test ettikten, tasarımı analiz ettikten ve kod incelemesini yaptıktan sonra, tüm sorunların yakalandığı varsayılabilir. Umarım durum böyledir, ancak konuşlandırıldıktan sonra uygulamayı test eden penetrasyon, hiçbir şeyin kaçırılmadığından emin olmak için ek bir kontrol sağlar.

Phase 4.2 Configuration Management Testing (Aşama 4.2 Konfigürasyon Yönetimi Testi)

Başvuru penetrasyon testi, altyapının nasıl konuşlandırıldığının ve güvence altına alındığına dair bir incelemeyi içermelidir. Ne kadar küçük olursa olsun, hiçbirinin sömürüye karşı savunmasız olabilecek varsayılan bir ortamda bırakılmamasını sağlamak için yapılandırma yönlerini gözden geçirmek önemlidir.

Phase 5 During Maintenance and Operations (5. Aşama Bakım ve İşletme Sırasında)

Phase 5.1 Conduct Operational Management Reviews (Aşama 5.1 Operasyonel Yönetim İncelemelerinin Yürütülmesi)

Hem uygulamanın hem de altyapının operasyonel tarafının nasıl yönetildiğini detaylandıran bir süreç olması gerekiyor.

Phase 5.2 Conduct Periodic Health Checks (Aşama 5.2 Periyodik Sağlık Kontrollerinin Yapılması)

Yeni güvenlik riskinin uygulanmamasını ve güvenlik seviyesinin hala sağlam olmasını sağlamak için hem uygulama hem de altyapıda aylık veya üç aylık sağlık kontrolleri yapılmalıdır.

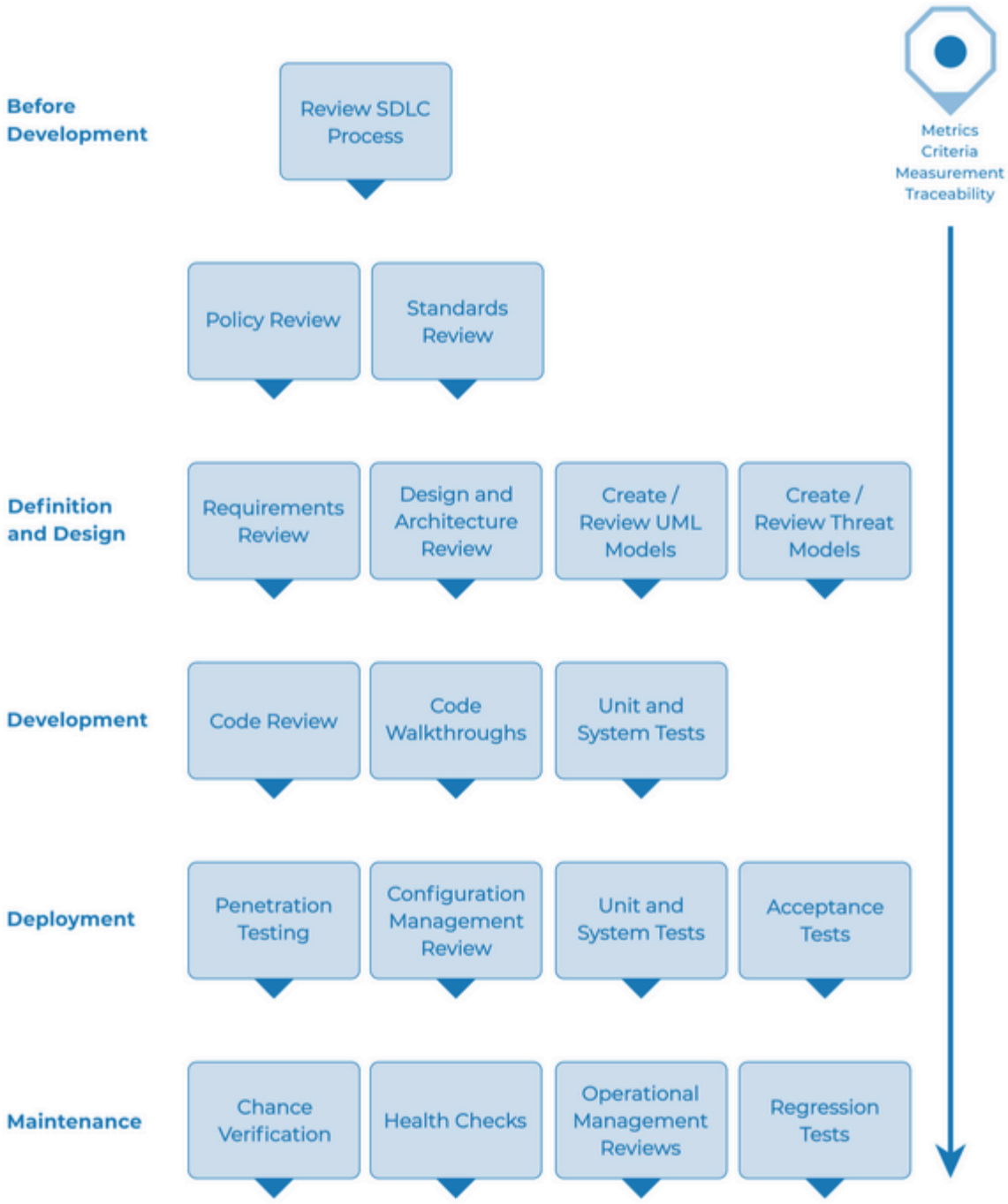
Phase 5.3 Ensure Change Verification (Aşama 5.3 Değişiklik Doğrulamasının Sağlanması)

Her değişiklik QA ortamında onaylandıktan ve test edildikten ve üretim ortamına yerleştirildikten sonra, güvenlik seviyesinin değişiklikten etkilenmemesini sağlamak

için değişikliğin kontrol edilmesi hayati önem taşımaktadır. Bu, değişim yönetimi sürecine entegre edilmelidir.

A Typical SDLC Testing Workflow (Tipik Bir SDLC Test İş Akışı)

Aşağıdaki şekilde tipik bir SDLC Test İş Akışı gösterilmektedir.



Şekil 3-1: Tipik SDLC test iş akışı

Penetration Testing Methodologies (Sızma Testi Metodolojileri)

Summary (Özet)

- OWASP Testing Guides (OWASP Test Kılavuzları)
  - Web Security Testing Guide (WSTG) (Web Güvenlik Test Kılavuzu (WSTG))
  - Mobile Security Testing Guide (MSTG) (Mobil Güvenlik Test Kılavuzu (MSTG))
  - Firmware Security Testing Methodology (Firmware Güvenlik Test Metodolojisi)
- Penetration Testing Execution Standard (Penetrasyon Testi Yürütme Standardı)
- PCI Penetration Testing Guide (PCI Penetrasyon Test Kılavuzu)
  - PCI DSS Penetration Testing Guidance (PCI DSS Penetrasyon Test Rehberliği)
  - PCI DSS Penetration Testing Requirements (PCI DSS Penetrasyon Test Gereksinimleri)
- Penetration Testing Framework (Penetrasyon Test Çerçevesi)
- Technical Guide to Information Security Testing and Assessment (Bilgi Güvenliği Testi ve Değerlendirme Teknik Kılavuzu)
- Open Source Security Testing Methodology Manual (Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu)
- References (Referanslar)

OWASP Testing Guides (OWASP Test Kılavuzları)

Teknik güvenlik testi uygulaması açısından, OWASP test kılavuzları şiddetle tavsiye edilir. Uygulama türlerine bağlı olarak, test kılavuzları sırasıyla web / bulut hizmetleri, Mobil uygulama (Android / iOS) veya IoT firmware için aşağıda listelenir.

- OWASP Web Security Testing Guide (OWASP Web Güvenlik Test Kılavuzu)
- OWASP Mobile Security Testing Guide (OWASP Mobil Güvenlik Test Kılavuzu)
- OWASP Firmware Security Testing Methodology (OWASP Firmware Güvenlik Test Metodolojisi)

Penetration Testing Execution Standard (Penetrasyon Testi Yürütme Standardı)

Penetration Testing Execution Standard (PTES), penetrasyon testini 7 faz olarak tanımlar. Özellikle, PTES Teknik Yönergeleri, test prosedürleri ve güvenlik test araçları için tavsiyeler hakkında uygulamalı öneriler sunar.

- Pre-engagement Interactions (Katılım öncesi etkileşimler)
- Intelligence Gathering (İstihbarat Toplantısı)
- Threat Modeling (Tehdit Modellemesi)
- Vulnerability Analysis (Güvenlik Açığı Analizi)
- Exploitation (İstismar)
- Post Exploitation (Post Exploitation)
- Reporting (Raporlama)

PTES Technical Guidelines (PTES Teknik Kılavuzları)

PCI Penetration Testing Guide (PCI Penetrasyon Test Kılavuzu)

Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS) Gerekliliği 11.3 penetrasyon testini tanımlar. PCI ayrıca Penetrasyon Testi Rehberliğini de tanımlar.

PCI DSS Penetration Testing Guidance (PCI DSS Penetrasyon Test Rehberliği)

PCI DSS Penetrasyon test kılavuzu aşağıdakiler hakkında rehberlik sağlar:

- Penetration Testing Components (Penetrasyon Test Bileşenleri)
- Qualifications of a Penetration Tester (Bir Penetrasyon Test Cihazının Nitelikleri)
- Penetration Testing Methodologies (Penetrasyon Test Metodolojileri)
- Penetration Testing Reporting Guidelines (Penetrasyon Testi Raporlama Kılavuzları)

PCI DSS Penetration Testing Requirements (PCI DSS Penetrasyon Test Gereksinimleri)

PCI DSS gereksinimi, Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS) Gereksinimini ifade eder 11.3

- Based on industry-accepted approaches (Endüstri tarafından kabul edilen yaklaşımlara dayanarak)
- Coverage for CDE and critical systems (CDE ve kritik sistemler için teminat)
- Includes external and internal testing (Dış ve iç test içerir)
- Test to validate scope reduction (Kapsam azaltımını doğrulamak için test)
- Application-layer testing (Uygulama katmanlı test)
- Network-layer tests for network and OS (Ağ ve işletim sistemi için ağ katman testleri)

PCI DSS Penetration Test Guidance (PCI DSS Penetrasyon Test Rehberliği)

Penetration Testing Framework (Penetrasyon Test Çerçevesi)

Penetrasyon Test Çerçevesi (PTF), kapsamlı uygulamalı penetrasyon test kılavuzu sağlar. Ayrıca her test kategorisindeki güvenlik test araçlarının kullanımlarını listeler. Penettrasyon testinin ana alanı şunları içerir:

- Network Footprinting (Reconnaissance) (Ağ Ayak Izi (Keşif))
- Discovery & Probing (Keşif ve Anlaşıntı)
- Enumeration (Sayım)
- Password cracking (Şifre çatlatma)
- Vulnerability Assessment (Güvenlik Açığı Değerlendirmesi)
- AS/400 Auditing (AS/400 Denetim)
- Bluetooth Specific Testing (Bluetooth Özel Test)
- Cisco Specific Testing (Cisco Özel Test)
- Citrix Specific Testing (Citrix Spesifik Test)

- Network Backbone (Ağ Omurga)
- Server Specific Tests (Sunucuya Özel Testler)
- VoIP Security (VoIP Güvenlik)
- Wireless Penetration (Kablosuz Penetrasyon)
- Physical Security (Fiziksel güvenlik)
- Final Report - template (Nihai Rapor - şablon)

Penetration Testing Framework (Penetrasyon Test Çerçevesi)

Technical Guide to Information Security Testing and Assessment (Bilgi Güvenliği Testi ve Değerlendirme Teknik Kılavuzu)

Bilgi Güvenliği Testi ve Değerlendirme Teknik Kılavuzu (NIST 800-115) NIST tarafından yayınlandı, aşağıda listelenen bazı değerlendirme tekniklerini içerir.

- Review Techniques (İnceleme Teknikleri)
- Target Identification and Analysis Techniques (Hedef Tanımlama ve Analiz Teknikleri)
- Target Vulnerability Validation Techniques (Hedef Güvenlik Açığı Doğrulama Teknikleri)
- Security Assessment Planning (Güvenlik Değerlendirme Planlaması)
- Security Assessment Execution (Güvenlik Değerlendirmesi Yürütme)
- Post-Testing Activities (Test Sonrası Etkinlikler)

NIST 800-115'e buradan erişilebilir

Open Source Security Testing Methodology Manual (Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu)

Açık Kaynak Güvenlik Test Metodolojisi Manuel (OSSTMM), fiziksel konumların, iş akışının, insan güvenliği testinin, fiziksel güvenlik testinin, kablosuz güvenliğin, telekomünikasyon güvenliği testinin, veri ağlarının güvenlik testinin ve uyumluluğunun operasyonel güvenliğini test etmek için bir metodolojidir.

OSSMMS, uygulamalı veya teknik uygulama penetrasyon test kılavuzu yerine ISO 27001 referansını destekleyebilir.

OSSMM aşağıdaki temel bölümleri içerir:

- Security Analysis (Güvenlik Analizi)
- Operational Security Metrics (Operasyonel Güvenlik Metrikleri)
- Trust Analysis (Güven Analizi)
- Work Flow (İş Akışı)
- Human Security Testing (İnsan Güvenliği Testi)
- Physical Security Testing (Fiziksel güvenlik testi)
- Wireless Security Testing (Kablosuz Güvenlik Testi)
- Telecommunications Security Testing (Telekomünikasyon Güvenlik Testi)
- Data Networks Security Testing (Veri Ağları Güvenlik Testi)
- Compliance Regulations (Uyum Düzenlemeleri)
- Reporting with the STAR (Security Test Audit Report) (STAR ile Raporlama (Güvenlik Test Denetim Raporu))

Open Source Security Testing Methodology Manual (Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu)

References (Referanslar)

- PCI Data Security Standard - Penetration TestingGuidance (PCI Veri Güvenliği Standardı - Sızma Testi Kılavuzu)
- PTES Standard (PTES Standard)
- Open Source Security Testing Methodology Manual (OSSTMM) (Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu (OSSTMM))
- Technical Guide to Information Security Testing and Assessment NIST SP 800-115 (Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu (OSSTMM))
- HIPAA Security Testing Assessment 2012 (Bilgi Güvenliği Test ve Değerlendirme Teknik Kılavuzu NIST SP 800-115)

- Penetration Testing Framework 0.59 (Sızma Testi Çerçevesi 0.59)
- OWASP Mobile Security Testing Guide (OWASP Mobil Güvenlik Test Kılavuzu)
- Security Testing Guidelines for Mobile Apps (Mobil Uygulamalar için Güvenlik Testi Yönergeleri)
- Kali Linux
- Information Supplement: Requirement 11.3 Penetration Testing (Bilgi Eki: Gereksinim 11.3 Sızma Testi)