

Table of Contents (İçindekiler)

0. Foreword by Eoin Keary (Önsöz: Eoin Keary)

1. Frontispiece (Önsöz)

2. Introduction (Giriş)

2.1 The OWASP Testing Project (OWASP Test Projesi)

2.2 Principles of Testing (Test Prensipleri)

2.3 Testing Techniques Explained (Açıklanan Test Teknikleri)

2.4 Manual Inspections and Reviews (Manuel Denetimler ve İncelemeler)

2.5 Threat Modeling (Tehdit Modellemesi)

2.6 Source Code Review (Kaynak Kod İncelemesi)

2.7 Penetration Testing (Sızma Testi)

2.8 The Need for a Balanced Approach (Dengeli Bir Yaklaşım İhtiyacı)

2.9 Deriving Security Test Requirements (Güvenlik Testi Gereksinimlerinin Türetilmesi)

2.10 Security Tests Integrated in Development and Testing Workflows (Geliştirme ve Test İş Akışlarına Entegre Edilmiş Güvenlik Testleri)

2.11 Security Test Data Analysis and Reporting (Güvenlik Testi Veri Analizi ve Raporlama)

3. The OWASP Testing Framework (OWASP Test Çerçevesi)

3.1 The Web Security Testing Framework (Web Güvenliği Test Çerçevesi)

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

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

3.4 Phase 3 During Development (Geliştirme Sırasında 3. Aşama)

3.5 Phase 4 During Deployment (Geliştirme Sırasında 4. Aşama)

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

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

3.8 Penetration Testing Methodologies (Sızma Testi Metodolojileri)

4. Web Application Security Testing (Web Uygulaması Güvenlik Testi)

4.0 Introduction and Objectives (Giriş ve Hedefler)

4.1 Information Gathering (Bilgi Toplama)

4.1.1 Conduct Search Engine Discovery Reconnaissance for Information Leakage (Bilgi Sızıntısı için Arama Motoru Keşfi Yapın)

4.1.2 Fingerprint Web Server (Web Sunucusunun Parmak İzini Alın)

4.1.3 Review Webserver Metafiles for Information Leakage (Bilgi Sızıntısı için Web Sunucusu Meta Dosyalarını İnceleyin)

4.1.4 Enumerate Applications on Webserver (Web Sunucusundaki Uygulamaları Numaralandırın)

4.1.5 Review Webpage Content for Information Leakage (Bilgi Sızıntısı için Web Sayfası İçeriğini İnceleyin)

4.1.6 Identify Application Entry Points (Uygulama Giriş Noktalarını Belirleyin)

4.1.7 Map Execution Paths Through Application (Uygulama Üzerinden Yürütme Yollarını Haritalayın)

4.1.8 Fingerprint Web Application Framework (Web Uygulama Çerçevesinin Parmak İzini Alın)

4.1.9 Fingerprint Web Application (Web Uygulamasının Parmak İzini Alın)

4.1.10 Map Application Architecture (Uygulama Mimarisini Haritalayın)

4.2 Configuration and Deployment Management Testing (Konfigürasyon ve Dağıtım Yönetimi Testi)

4.2.1 Test Network Infrastructure Configuration (Ağ Altyapısı Yapılandırmasını Test Edin)

4.2.2 Test Application Platform Configuration (Uygulama Platformu Yapılandırmasını Test Edin)

4.2.3 Test File Extensions Handling for Sensitive Information (Hassas Bilgiler için Dosya Uzantılarının İşlenmesini Test Edin)

4.2.4 Review Old Backup and Unreferenced Files for Sensitive Information (Hassas Bilgiler için Eski Yedekleme ve Referanslanmamış Dosyaları İnceleyin)

4.2.5 Enumerate Infrastructure and Application Admin Interfaces (Altyapı ve Uygulama Yönetici Arayüzlerini Numaralandırın)

4.2.6 Test HTTP Methods (HTTP Yöntemlerini Test Edin)

4.2.7 Test HTTP Strict Transport Security (HTTP Sıkı Aktarım Güvenliğini Test Edin)

4.2.8 Test RIA Cross Domain Policy (RIA Çapraz Etki Alanı İlkesini Test Edin)

4.2.9 Test File Permission (Dosya İznini Test Edin)

4.2.10 Test for Subdomain Takeover (Alt Alan Devralmayı Test Edin)

4.2.11 Test Cloud Storage (Bulut Depolamayı Test Edin)

4.3 Identity Management Testing (Kimlik Yönetimi Testi)

4.3.1 Test Role Definitions (Rol Tanımlarını Test Edin)

4.3.2 Test User Registration Process (Kullanıcı Kayıt Sürecini Test Edin)

4.3.3 Test Account Provisioning Process (Hesap Sağlama Sürecini Test Edin)

4.3.4 Testing for Account Enumeration and Guessable User Account (Hesap Numaralandırma ve Tahmin Edilebilir Kullanıcı Hesabı Testi)

4.3.5 Testing for Weak or Unenforced Username Policy (Zayıf veya Uygulanmayan Kullanıcı Adı Politikasını Test Edin)

4.4 Authentication Testing (Kimlik Doğrulama Testi)

4.4.1 Testing for Credentials Transported over an Encrypted Channel (Şifrelenmiş Bir Kanal Üzerinden Taşınan Kimlik Bilgilerinin Test Edilmesi)

4.4.2 Testing for Default Credentials (Varsayılan Kimlik Bilgilerinin Test Edilmesi)

4.4.3 Testing for Weak Lock Out Mechanism (Zayıf Kilitleme Mekanizmasının Test Edilmesi)

4.4.4 Testing for Bypassing Authentication Schema (Kimlik Doğrulama Şemasının Atlanmasının Test Edilmesi)

4.4.5 Testing for Vulnerable Remember Password (Güvenlik Açığı Bulunan Parolayı Hatırlama Durumunun Test Edilmesi)

4.4.6 Testing for Browser Cache Weaknesses (Tarayıcı Önbelleği Zayıflıklarının Test Edilmesi)

4.4.7 Testing for Weak Password Policy (Zayıf Parola İlkesinin Test Edilmesi)

4.4.8 Testing for Weak Security Question Answer (Zayıf Güvenlik Sorusu Yanıtının Test Edilmesi)

4.4.9 Testing for Weak Password Change or Reset Functionalities (Zayıf Parola Değiştirme veya Sıfırlama İşlevlerinin Test Edilmesi)

4.4.10 Testing for Weaker Authentication in Alternative Channel (Alternatif Kanalda Zayıf Kimlik Doğrulamanın Test Edilmesi)

4.5 Authorization Testing (Yetkilendirme Testi)

4.5.1 Testing Directory Traversal File Include (Dizin Çaprazlama Dosya Ekleme Testi)

4.5.2 Testing for Bypassing Authorization Schema (Yetkilendirme Şemasını Atlama Testi)

4.5.3 Testing for Privilege Escalation (Ayrıcalık Yükseltme Testi)

4.5.4 Testing for Insecure Direct Object References (Güvensiz Doğrudan Nesne Referansları Testi)

4.6 Session Management Testing (Oturum Yönetimi Testi)

4.6.1 Testing for Session Management Schema (Oturum Yönetimi Şeması Testi)

4.6.2 Testing for Cookies Attributes (Çerez Öznitelikleri Testi)

4.6.3 Testing for Session Fixation (Oturum Sabitleme Testi)

4.6.4 Testing for Exposed Session Variables (Açık Oturum Değişkenleri Testi)

4.6.5 Testing for Cross Site Request Forgery (Siteler Arası İstek Sahteciliği Testi)

4.6.6 Testing for Logout Functionality (Oturumu Kapatma İşlevselliği Testi)

4.6.7 Testing Session Timeout (Oturum Zaman Aşımı Testi)

4.6.8 Testing for Session Puzzling (Oturum Şaşırtma Testi)

4.6.9 Testing for Session Hijacking (Oturum Korsanlığı Testi)

4.7 Input Validation Testing (Girdi Doğrulama Testi)

4.7.1 Testing for Reflected Cross Site Scripting (Yansıtılmış Çapraz Site Komut Dosyası Testi)

4.7.2 Testing for Stored Cross Site Scripting (Depolanmış Çapraz Site Komut Dosyası Testi)

4.7.3 Testing for HTTP Verb Tampering (HTTP Fiil Kurcalama Testi)

4.7.4 Testing for HTTP Parameter Pollution (HTTP Parametre Kirliliği Testi)

4.7.5 Testing for SQL Injection (SQL Enjeksiyonu Testi)

4.7.5.1 Testing for Oracle (Oracle için Test)

4.7.5.2 Testing for MySQL (MySQL için Test)

4.7.5.3 Testing for SQL Server (SQL Server için Test)

- 4.7.5.4 Testing PostgreSQL (PostgreSQL için Test)**
- 4.7.5.5 Testing for MS Access (MS Access için Test)**
- 4.7.5.6 Testing for NoSQL Injection (NoSQL Enjeksiyonu için Test)**
- 4.7.5.7 Testing for ORM Injection (ORM Enjeksiyonu için Test)**
- 4.7.5.8 Testing for Client-side (İstemci Tarafı için Test)**
- 4.7.6 Testing for LDAP Injection (LDAP Enjeksiyonu için Test)**
- 4.7.7 Testing for XML Injection (XML Enjeksiyonu için Test)**
- 4.7.8 Testing for SSI Injection (SSI Enjeksiyonu için Test)**
- 4.7.9 Testing for XPath Injection (XPath Enjeksiyonu için Test)**
- 4.7.10 Testing for IMAP SMTP Injection (IMAP SMTP Enjeksiyonu için Test)**
- 4.7.11 Testing for Code Injection (Kod Enjeksiyonu için Test)**
 - 4.7.11.1 Testing for Local File Inclusion (Yerel Dosya Ekleme Testi)**
 - 4.7.11.2 Testing for Remote File Inclusion (Uzak Dosya Ekleme Testi)**
- 4.7.12 Testing for Command Injection (Komut Enjeksiyonu Testi)**
- 4.7.13 Testing for Format String Injection (Biçim Dizesi Enjeksiyonu Testi)**
- 4.7.14 Testing for Incubated Vulnerability (Kuluçkalanmış Güvenlik Açığı Testi)**

4.7.15 Testing for HTTP Splitting Smuggling (HTTP Bölme Kaçakçılığı Testi)

4.7.16 Testing for HTTP Incoming Requests (HTTP Gelen İstekleri Testi)

4.7.17 Testing for Host Header Injection (Ana Bilgisayar Başlığı Enjeksiyonu Testi)

4.7.18 Testing for Server-side Template Injection (Sunucu Tarafı Şablon Enjeksiyonu Testi)

4.7.19 Testing for Server-Side Request Forgery (Sunucu Tarafı İstek Sahteciliği Testi)

4.8 Testing for Error Handling (Hata İşleme Testi)

4.8.1 Testing for Improper Error Handling (Uygunsuz Hata İşleme Testi)

4.8.2 Testing for Stack Traces (Yığın İzlerinin Test Edilmesi)

4.9 Testing for Weak Cryptography (Zayıf Kriptografi Testi)

4.9.1 Testing for Weak Transport Layer Security (Zayıf Aktarım Katmanı Güvenliği Testi)

4.9.2 Testing for Padding Oracle (Oracle Dolgu Testi)

4.9.3 Testing for Sensitive Information Sent via Unencrypted Channels (Şifrlenmemiş Kanallar Üzerinden Gönderilen Hassas Bilgilerin Testi)

4.9.4 Testing for Weak Encryption (Zayıf Şifreleme Testi)

4.10 Business Logic Testing (İş Mantığı Testi)

4.10.0 Introduction to Business Logic (İş Mantığına Giriş)

- 4.10.1 Test Business Logic Data Validation (İş Mantığı Veri Doğrulamasını Test Edin)**
- 4.10.2 Test Ability to Forge Requests (İstekleri Taklit Edebilme Yeteneğini Test Edin)**
- 4.10.3 Test Integrity Checks (Bütünlük Kontrollerini Test Edin)**
- 4.10.4 Test for Process Timing (İşlem Zamanlamasını Test Edin)**
- 4.10.5 Test Number of Times a Function Can Be Used Limits (Bir Fonksiyonun Kullanılabileceği Kez Sayısı Sınırlarını Test Edin)**
- 4.10.6 Testing for the Circumvention of Work Flows (İş Akışlarının Atlanmasını Test Edin)**
- 4.10.7 Test Defenses Against Application Misuse (Uygulamanın Kötüye Kullanımına Karşı Savunmaları Test Edin)**
- 4.10.8 Test Upload of Unexpected File Types (Beklenmeyen Dosya Türlerinin Yüklenmesini Test Edin)**
- 4.10.9 Test Upload of Malicious Files (Kötü Amaçlı Dosyaların Yüklenmesini Test Edin)**
- 4.11 Client-side Testing (İstemci Tarafı Testleri)**
 - 4.11.1 Testing for DOM-Based Cross Site Scripting (DOM Tabanlı Çapraz Site Komut Dosyası Oluşturma Testi)**
 - 4.11.2 Testing for JavaScript Execution (JavaScript Yürütme Testi)**
 - 4.11.3 Testing for HTML Injection (HTML Enjeksiyonu Testi)**
 - 4.11.4 Testing for Client-side URL Redirect (İstemci Tarafı URL Yönlendirme Testi)**

4.11.5 Testing for CSS Injection (CSS Enjeksiyonu Testi)

4.11.6 Testing for Client-side Resource Manipulation (İstemci Tarafı Kaynak Manipülasyonu Testi)

4.11.7 Testing Cross Origin Resource Sharing (Çapraz Kaynak Paylaşımının Test Edilmesi)

4.11.8 Testing for Cross Site Flashing (Siteler Arası Yanıp Sönme Testi)

4.11.9 Testing for Clickjacking (Clickjacking Testi)

4.11.10 Testing WebSockets (WebSockets Testi)

4.11.11 Testing Web Messaging (Web Mesajlaşmasının Test Edilmesi)

4.11.12 Testing Browser Storage (Tarayıcı Depolamasının Test Edilmesi)

4.11.13 Testing for Cross Site Script Inclusion (Siteler Arası Betik Ekleme Testi)

4.12 API Testing (API Testi)

4.12.1 Testing GraphQL (GraphQL'i Test Etme)

5. Reporting (Raporlama)

Appendix A. Testing Tools Resource (Ek A. Test Araçları Kaynağı)

Appendix B. Suggested Reading (Ek B. Önerilen Okuma)

Appendix C. Fuzz Vectors (Ek C. Fuzz Vektörleri)

Appendix D. Encoded Injection (Ek D. Kodlanmış Enjeksiyon)

Appendix E. History (Ek E. Tarihçe)

Appendix F. Leveraging Dev Tools (Ek F. Geliştirme Araçlarından Yararlanma)