

Penetrasyon Testi Raporu

Ürün / Sistem: {X} Ürünü

Rapor Türü: Penetrasyon Testi Sonuç Raporu

Hazırlayan: Subutay Ülgen

Tarih:

Penetrasyon Testi Hazır Templeyti

İÇİNDEKİLER

- █ TEKNİK BİLGİSİ OLANLAR İÇİN YAZILMISTIR
- █ TEKNİK BİLGİSİ OLMAYANLAR İÇİN YAZILMISTIR
- █ HER İKİ GRUPTA OKUYABİLİR

| | |
|-------------------------------------|----|
| 1. Yönetici özeti | 3 |
| 2. Bulgu özeti | 4 |
| 3. Öneri ve Tavsiyeler | 5 |
| 4. Ciddiyet Skalası | 6 |
| 5. Kapsam Beyanı | 7 |
| 6. Final Raporu | 8 |
| 7. Metodoloji | 8 |
| 8. Bilgi Toplama | 9 |
| 9. Enumetion | 10 |
| 10. Zafiyet Değerlendirilmesi | 11 |
| 11. Exploiting | 12 |
| 12. Home cleaning beyanı | 13 |

Yönetici Özeti

Bu rapor, {Müşteri/Kurum Adı} şirketine ait {Hedef Sistem/Ürün Adı} ürününde gerçekleştirilen penetrasyon testi çalışmasının sonuçlarını içermektedir. Test, {Başlangıç Tarihi} ile {Bitiş Tarihi} tarihleri arasında gerçekleştirilmiştir.

Yapılan analizler sonucunda {X} Kritik, {Y} Yüksek, {Z} Orta ve {W} Düşük seviye zayıflıkları tespit edilmiş olup, bulunan bulguların çözülmesi halinde sistem güvenliğinin önemli ölçüde artırılacağı değerlendirilmektedir. Kritik/Yüksek seviye zayıfı bulunup bulunmadığı burada netleştirilmelidir.

Devamı ...

Bulgu Özeti

Aşağıdaki tablo, {X} Ürünü üzerinde gerçekleştirilen penetrasyon testi sonucunda tespit edilen tüm güvenlik zayıflığının risk seviyelerine göre özetini sunmaktadır. Bulgular, risk seviyesine göre azalan sırada listelenmiştir.

| Risk Seviyesi | Tanım | Tespit Edilen Bulgu Sayısı |
|---------------|---|----------------------------|
| Kritik | Sistemin tamamen ele geçirilmesine neden olabilecek zayıflıklar. | {0} |
| Yüksek | Yetkisiz erişim veya önemli bilgi sızıntısına neden olabilecek zayıflıklar. | {A} |
| Orta | Kısmi güvenlik riskine yol açan, istismar edilmesi belirli koşullar gerektiren zayıflıklar. | {B} |
| Düşük | Sınırlı etkisi olan ve genellikle yapılandırma iyileştirmesi gerektiren zayıflıklar. | {C} |
| Bilgilendirme | Risk oluşturmayan, ancak iyileştirme önerilen durumlar. | {D} |
| Toplam | | {A+B+C+D} |

Bu bölümde, tespit edilen en yüksek riskli (Yüksek/Kritik) bulgulara odaklanılır ve yöneticinin dikkatini en acil konulara çekmek amaçlanır.

| Bulgu Adı | Risk Seviyesi | Etkilenen Sistem | Çözüm Önceliği |
|-----------------------------|---------------|-----------------------------|----------------|
| SQL Injection (Olası) | Yüksek | /{API_ADI}/login üç noktası | Acil |
| Eski Kütüphane Kullanımı | Orta | Web Uygulaması Frontend | Planlı |
| Zayıf Parola Politikası | Orta | Kimlik Doğrulama Servisi | Planlı |

Öneri ve Tavsiye

Bu bölüm, tespit edilen zafiyetlerin giderilmesi için gerekli olan spesifik aksiyonları ve sistemin genel güvenlik duruşunu güçlendirmeye yönelik uzun vadeli stratejik önerileri içermektedir.

Aşağıdaki tablo, Bulgu Özeti'nde listelenen her bir zafiyet için atılması gereken adımları özetlemektedir. Her bir bulgu, risk seviyesine uygun önceliklendirme ile ele alınmalıdır.

| Bulgu Adı | Risk Seviyesi | Önerilen Aksiyon (Örnek) | Çözüm Maliyeti Tahmini |
|-----------------------------|---------------|--|------------------------|
| 1. SQL Injection (Olası) | Yüksek | Giriş Doğrulaması (Input Validation): Veritabanı sorgularının Hazırlanmış ifadeler (Prepared Statements) kullanılarak oluşturulması ve kullanıcı girişlerinin kesinlikle doğrulanması. | Düşük/Orta |
| 2. Eski Kütüphane Kullanımı | Orta | Yama Yönetimi: Kullanılan {Kütüphane Adı} kütüphanesinin en son kararlı ve güvenli sürümüne güncellenmesi. | Düşük |
| 3. Zayıf Parola Politikası | Orta | Güçlendirilmiş Parola Politikası: Minimum parola uzunluğunun artırılması (Örn: 12 karakter) ve zorunlu çok faktörlü kimlik doğrulama (MFA) uygulanması. | Orta |

Ciddiyet Skalası

| Seviye | Tanım (Mevcut) | Önerilen Ek Bilgi (Temel) |
|--------|---|--|
| Kritik | Sistemin tamamen ele geçirilmesine neden olabilecek zayıflıklar. | Hemen Çözülmeli (0-7 gün). İş sürekliliğini doğrudan tehdit eder. |
| Yüksek | Yetkisiz erişim veya önemli bilgi sızıntısına neden olabilecek zayıflıklar. | Acil Çözülmeli (7-30 gün). Veri gizliliği/bütünlüğünü bozar. |
| Orta | Kısmi güvenlik riskine yol açan, istismar edilmesi belirli koşullar gerektiren zayıflıklar. | Planlı Çözülmeli (30-90 gün). Güvenlik duruşunu düşürür. |
| Düşük | Sınırlı etkisi olan ve genellikle yapılandırma iyileştirmesi gerektiren zayıflıklar. | İleride Çözülmeli (90+ gün). En iyi uygulamalar için önemlidir. |

Devamı ...

Kapsam Beyanı

Penetrasyon testi, {Yetkilendirme Türü: Kara Kutu, Gri Kutu, Beyaz Kutu} yaklaşımıyla gerçekleştirılmıştır. Test kapsamına giren sistemler ve uygulamalar aşağıda listelenmiştir:

- Hedef 1 (IP/URL): {Açıklama: Web Uygulaması, Harici Ağ vb.}
- Hedef 2 (IP/URL): {Açıklama: Mobil Uygulama API'ları vb.}

Kapsam Dışı Öğeler:

- {Hariç Tutulan Sistemler/IP'ler/Özellikler}
- {Sosyal Mühendislik, DDoS Simülasyonu gibi test edilmeyen aktiviteler}

Not: Test sırasında {X} kullanıcısı/erişim seviyesi ile çalışılmıştır.

Devamı ...

Final Raporu

Metodoloji

Bu penetrasyon testi, {OWASP Testing Guide v4.0 / PTES / NIST SP 800-115} metodolojileri referans alınarak gerçekleştirılmıştır. Test süreci temel olarak aşağıdaki aşamaları takip etmiştir:

- Bilgi Toplama: {Nmap, Shodan, Google Dorking} gibi araçlar kullanıldı.
- Keşif: {Dirbuster, Burp Suite} gibi araçlarla port taraması, dizin taraması yapıldı.
- Zafiyet Değerlendirmesi: {Taranan zafiyet tarayıcı adı: Nessus, OpenVAS} kullanılarak otomatik ve manuel kontroller yapıldı.

Devamı ...

Bilgi Toplama

Bilgi Toplama ...

Enumetion

Enumetion ...

Zafiyet Değerlendirilmesi

Zafiyet Değerlendirilmesi ...

Exploit

Exploit ...

Home Clearing

Bu çalışma kapsamında gerçekleştirilen tüm penetrasyon testi faaliyetleri sonrasında, test süreci boyunca kullanılan araçlar, oluşturulan geçici dosyalar, bırakılan payload'lar, test amaçlı oluşturulan kullanıcı hesapları, yapılan konfigurasyon değişiklikleri ve benzeri tüm unsurlar sistemler üzerinde kalıcı etki bırakmayacak şekilde temizlenmiştir.

Test sırasında üretilen log, komut geçmişi ve operasyonel izler, test tamamlandıktan sonra hedef sistemlerin bütünlüğünü ve iş sürekliliğini korumak amacıyla kaldırılmış veya eski haline döndürülmüştür. Hiçbir kalıcı erişim yöntemi, arka kapı veya test dışı bir mekanizma sistemlerde bırakılmamıştır.

Bu beyan, gerçekleştirilen penetrasyon testinin güvenli, kontrollü ve müşteri ortamına zarar vermeyecek şekilde tamamlandığını ifade eder.

Subutay Ülgen