

# Penetrasyon Testi Raporu

*Ürün / Sistem: {X} Ürünü*

*Rapor Türü: Penetrasyon Testi Sonuç Raporu*

*Hazırlayan: Subutay Ülgen*

*Tarih: .....*

Penetrasyon Testi Hazır Templateyi

# 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. Enumeration .....	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 zafiyetler tespit edilmiş olup, bulunan bulguların çözülmesi halinde sistem güvenliğinin önemli ölçüde artırılabacağı değerlendirilmektedir. Kritik/Yüksek seviye zafiyet bulunup bulunmadığı burada netleştirilmelidir.

Devamı ...

# Bulgu Özeti

Aşağıdaki tablo, {X} Ürünü üzerinde gerçekleştirilen penetrasyon testi sonucunda tespit edilen tüm güvenlik zafiyetlerinin 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 zafiyetler.	{0}
Yüksek	Yetkisiz erişim veya önemli bilgi sızıntısına neden olabilecek zafiyetler.	{A}
Orta	Kısmi güvenlik riskine yol açan, istismar edilmesi belirli koşullar gerektiren zafiyetler.	{B}
Düşük	Sınırlı etkisi olan ve genellikle yapılandırma iyileştirmesi gerektiren zafiyetler.	{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_ADİ}}/login uç 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 İfadeler (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 zafiyetler.	<b>Hemen Çözülmeli (0-7 gün).</b> İş sürekliliğini doğrudan tehdit eder.
Yüksek	Yetkisiz erişim veya önemli bilgi sızıntısına neden olabilecek zafiyetler.	<b>Acil Çözülmeli (7-30 gün).</b> Veri gizliliği/bütünlüğünü bozar.
Orta	Kısmi güvenlik riskine yol açan, istismar edilmesi belirli koşullar gerektiren zafiyetler.	<b>Planlı Çözülmeli (30-90 gün).</b> Güvenlik duruşunu düşürür.
Düşük	Sınırlı etkisi olan ve genellikle yapılandırma iyileştirmesi gerektiren zafiyetler.	<b>İleride Çözülmeli (90+ gün).</b> En iyi uygulamalar için önemlidir.

Devamı ...

# Kapsam Beyanı

Penetrasyon testi, {Yetkilendirme Türü: Kara Kutu, Gri Kutu, Beyaz Kutu} yaklaşımıyla gerçekleştirilmiştir. 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 gerçekleştirilmiştir. 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, izin taraması yapıldı.
- Zafiyet Değerlendirmesi: {Taranan zafiyet tarayıcı adı: Nessus, OpenVAS} kullanılarak otomatik ve manuel kontroller yapıldı.

Devamı ...

# Bilgi Toplama

Bilgi Toplama ...

# Enumeration

Enumeration ...

# Zafiyet Deęerlendirilmesi

Zafiyet Deęerlendirilmesi ...

# 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 konfigürasyon 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**