5. Reporting (Raporlama)

Reporting (Raporlama)

Değerlendirmenin teknik tarafını gerçekleştirmek genel değerlendirme sürecinin sadece yarısıdır. Nihai ürün, iyi yazılmış ve bilgilendirici bir raporun üretilmesidir. Bir raporun anlaşılması kolay olmalı ve değerlendirme aşamasında bulunan tüm riskleri vurgulamalıdır. Rapor hem yönetici yönetimine hem de teknik personele hitap etmelidir.

About this Section (Bu Bölüm hakkında)

Bu kılavuz, raporlamaya olası bir yaklaşım hakkında yalnızca önerilerde bulunur ve uyulması gereken katı kurallar olarak ele alınmamalıdır. Aşağıdaki önerilerden herhangi birini düşünürken, her zaman önerinin raporunuzu iyileştirip geliştirmeyeceğinizi kendinize sorun.

Raporlama kılavuzu, danışmanlık tabanlı raporlar için en uygun olanıdır. İç veya hata ödül raporları için aşırı olabilir.

Kitleden bağımsız olarak, raporu güvence altına almak ve yalnızca alıcı tarafın onu kullanabileceğinden emin olmak için şifrelemeniz önerilir.

İyi bir rapor, danışınızın bulgularınızı anlamasına yardımcı olur ve teknik testinizin kalitesini vurgular. Teknik testin kalitesi, müşteri bulgularınızı anlayamıyorsa tamamen alakasızdır.

1. Introduction (1. Giriş)

1.1 Version Control (1.1 Sürüm Kontrolü)

Setler, çoğunlukla aşağıdaki gibi bir tablo formatında sunulan değişiklikleri rapor eder.

Versiyon	Açıklama	Tarih	Yazar
1.0	İlk rapor	DD / M / YYYYYYY	J. Doe

1.2 Table of Contents (1.2 İçerik Tablosu)

Belge için bir içerik tablosu sayfası.

1.3 The Team (1.3 Takım)

Uzmanlık ve niteliklerini detaylandıran ekip üyelerinin bir listesi.

1.4 Scope (1.4 Kapsam)

Angajmanın sınırları ve ihtiyaçları örgütle aynı fikirdeydi.

1.5 Limitations (1.5 Sınırlamalar)

Sınırlamalar şunlar olabilir:

- Test ile ilgili olarak sınırların dışında alanlar.
- Kırık işlevsellik.
- İşbirliği eksikliği.
- Zaman eksikliği.
- Erişim eksikliği veya kimlik bilgileri.

1.6 Timeline (1.6 Zaman Çizelgesi)

Nişan süresi.

1.7 Disclaimer (1.7 Feragatname)

Hizmetiniz için bir feragatname vermek isteyebilirsiniz. Yasal olarak bağlayıcı bir belge oluşturmak için her zaman yasal bir profesyonele danışın.

Aşağıdaki örnek sadece açıklayıcı amaçlar içindir. Kanun olarak kullanılmamalı ve yasal tavsiye teşkil etmez.

Bu test "zamanda nokta" bir değerlendirmedir ve bu nedenle test yapıldığından beri ortam değişebilirdi. Tüm olası güvenlik sorunlarının tespit edildiğinin garantisi yoktur ve testler yapıldığından beri yeni güvenlik açıkları keşfedilmiş olabilir. Bu nedenle, bu rapor, raporun
eldeki sistemleri tehdit eden risklerin tam bir temsilini sağladığı bir garanti değil, yol gösterici bir belge olarak hizmet eder.

2. Executive Summary (2. Yönetici Özeti)

Bu, raporun asansör perdesi gibidir, yöneticilere şunları sağlamayı amaçlamaktadır:

- Testin amacı.

    - Güvenlik testinin arkasında iş ihtiyacını açıklayın.
    - Testlerin kuruluşun sistemlerini anlamasına nasıl yardımcı olduğunu açıklayın.
- Olası uyum sorunları, itibar hasarı vb. Gibi bir iş bağlamında temel bulgular. İş etkisine odaklanın ve şimdilik teknik detayları dışarıda bırakın.
- İşletmenin sorunların tekrar yaşanmasını nasıl durdurabileceğine dair stratejik öneriler. Bunları teknik olmayan bir bağlamda tanımlayın ve şimdilik belirli teknik önerileri dışarıda bırakın.

Özet yapıcı ve anlamlı olmalıdır. Jargondan ve olumsuz spekülasyonlardan kaçının. Rakamlar, grafikler veya illüstrasyonlar kullanılırsa, bir mesajı metinden daha net bir şekilde iletmeye yardımcı
olduklarından emin olun.

3. Findings (3. Bulgular)

Bu bölüm teknik takıma yöneliktir. Güvenlik açığını anlamak, çoğaltmak ve çözmek için gerekli tüm bilgileri içermelidir. Mantıksal ayrılık, raporun okunabilirliğini iyileştirmeye yardımcı olabilir.
Örneğin, “Dış Erişim” ve “İç Erişilebilir Erişim” başlıklı ayrı bölümleriniz olabilir.

Bu bir yeniden test ise, önceki testin bulgularını, daha önce tespit edilen güvenlik açıklarının güncellenmiş durumunu ve mevcut testle ilgili çapraz referansları özetleyen bir alt bölüm oluşturabilirsiniz.

3.1 Findings Summary (3.1 Bulgu Özeti)

Risk seviyelerine sahip bulguların bir listesi. Her iki takım tarafından da kullanım kolaylığı için bir tablo kullanılabilir.

Ref. kimlik	Başlık	Risk Seviyesi
1	Kullanıcı Kimlik Doğrulama Bypass	Yüksek

3.2 Findings Details (3.2 Bulgu Detayları)

Her bulgu şu bilgilerle detaylandırılmalıdır:

- Taraflar arasında iletişim ve rapor genelinde çapraz referanslar için kullanılabilecek Referans Kimliği.

- “USer Authentication Bypass” gibi güvenlik açığı.
- Konunun olasılığı veya sömürülebilirliği, aşağıdaki gibi çeşitli faktörlere dayanmaktadır:
    - Sömürmek ne kadar kolay.
    - Bunun için çalışan istismar kodu olup olmadığı.
    - Erişim seviyesi gerekli.
    - Saldırgan onu sömürmek için motivasyon.
- Kırılganlığın sistem üzerindeki etkisi.
- Uygulamadaki güvenlik açığı riski.
    - Önerilen bazı değerler şunlardır: Bilgilendirici, Düşük, Orta, Yüksek ve Kritik. Bir ekte kullanmaya karar verdiğiniz değerleri detaylandırmanızı sağlayın. Bu, okuyucunun her bir puanın nasıl belirlendiğini anlamasını sağlar.
    - Bazı angajmanlarda bir CVSS puanına sahip olmak gerekir. Gerekirse, bazen sahip olmak iyidir ve diğer zamanlarda sadece rapora karmaşıklık katar.
- Güvenlik açığının ne olduğunu, onu nasıl istismar edeceğinize ve sömürüsünden kaynaklanabilecek zararın ayrıntılı bir şekilde tanımlanması. Herhangi bir hassas veri, örneğin şifreler, kişisel bilgiler veya kredi kartı bilgileri maskelenmelidir.
- Güvenlik açığının nasıl düzeltileceğine dair ayrıntılı adımlar, güvenlik duruşunu güçlendirmeye yardımcı olabilecek olası iyileştirmeler ve güvenlik uygulamalarını kaçırmak.
- Okuyucunun bir görüntü, bir video, bir CVE, harici bir rehber vb. Gibi kırılganlığı anlamasına yardımcı olabilecek ek kaynaklar.

Bu bölümü mesajınızı en iyi şekilde iletecek şekilde biçimlendirin.

Açıklamalarınızın, bu raporu okuyan mühendisin buna dayanarak harekete geçmesi için yeterli bilgi sağladığından emin olun. Bulguyu iyice açıklayın ve onu düzeltmek için gerekli olabileceği kadar teknik ayrıntı sağlayın.

Appendices (Aşımlar)

Birden fazla ek eklenebilir, örneğin:

- Test metodolojisi kullanılır.
- Şiddet ve risk değerlendirme açıklamaları.
- Kullanılan aletlerden gelen çıkışla ilgili.
    - Çıktıyı temizlediğinizden emin olun ve sadece çöpe atmayın.
- WSTG kontrol listesi gibi yapılan tüm testlerin bir kontrol listesi. Bunlar rapora ek olarak sağlanabilir.

Referances (Referanslar)

Bu bölüm önerilen rapor formatının bir parçası değildir. Aşağıdaki bağlantılar, raporlarınızı yazmak için daha fazla rehberlik sağlar.

- SANS: Tips for Creating a Strong Cybersecurity Assessment Report
- SANS: Writing a Penetration Testing Report
- Infosec Institute: The Art of Writing Penetration Test Reports
- Dummies: How to Structure a Pen Test Report
- Rhino Security Labs: Four Things Every Penetration Test Report Should Have