DokümanKontr	
Belge referans:	
Sorun durumu:	
Tarih:	22.08.2021
Yazar:	M.Semih uslukılıç

Versiyon	Tarih	Yazar	Tanım
1.0	22.08.2021	M.Semih uslukılıç	Sızma testi raporu

Müşteri iletişim bilgileri	
Kişi Adı:	Mustafa
Telefon:	Xxxxxxxx8505
E-posta:	
Şirket Adı:	
Posta kodu:	

Danışman Bilgileri	
Şirket Adı:	MSU
Kişi Adı:	M.semih USLUKILIÇ
Başlık:	Pentest
Telefon	Xxxxxxxxx8505
E-posta	usxxxxxx@gmail.com
İşletme Adresi:	
Şehir:	
URL:	

1. Giriş

Siber Güvenlik her büyüklükteki işletmeler ve kamu sektörü kuruluşları için güvenlik çözümleri ve hizmetleri sağlar. Devlet, sağlık, eğitim, kurumsal ve hayır kurumlarındaki özel ekiplerimizle, ihtiyaçlarınıza göre hazırlanmış derinlemesine, sektöre özel tavsiyeler ve çözümler alacağınızdan emin olabilirsiniz.

1.1. Bu belgenin amacı

Ağ Güvenliği Değerlendirmesinden elde edilen bulguları özetlemek için.

1.2. Ağ Güvenliği Değerlendirmelerine Giriş

Ağ Güvenlik Değerlendirmeleri (NSA'lar), kuruluşunuzun bilgi güvenliğinin kapsamlı bir incelemesini sağlar. Danışmanımız, endüstri standardı metodolojileri kullanarak altyapınız, prosedürleriniz ve politikalarınızdaki endişe verici alanları keşfetmek için tasarlanmış bir dizi değerlendirme gerçekleştirecektir.

Ağ Güvenliği Değerlendirmesi (NSA), bir saldırgan tarafından istismar edilebilecek sistemlerdeki ve uygulamalardaki kusurları belirleme sürecidir. Kullanılabilecek herhangi bir kusur bir güvenlik açığı olarak kabul edilir ve her bir güvenlik açığının ciddiyeti CVSS sistemi kullanılarak ölçülür. Güvenlik açıkları, yanlış yapılandırmadan güncel olmayan yazılımlara veya zayıf kimlik doğrulama kullanımına kadar herhangi bir şeyden kaynaklanabilir. Teknik güvenlik açıklarının belirlenmesinin yanı sıra, çalışma uygulamalarının diğer saldırı biçimlerine karşı savunmasız olmadığından emin olmak için yazılı politikalar ve prosedürler gözden geçirilebilir. Örneğin, başarılı bir saldırıyla sonuçlanabilecek veya bu saldırıya yardımcı olabilecek, zayıf parola kullanımını veya fiziksel güvenlikteki gecikmeleri belirleyebiliriz.

Saldırganın bakış açısından olası saldırı vektörlerini belirleyerek ve her bir güvenlik açığının ciddiyetini derecelendirerek, bu kişilerin büyük olasılıkla erişiminize nasıl yetkisiz erişim elde etmeye çalışacaklarını raporlayabiliyoruz.

1.3. Güvenlik Açığı Puanlaması

Bu raporda listelenen tüm güvenlik açıkları, bir puanlama sistemi kullanılarak derecelendirilir. Ortak Güvenlik Açığı Puanlama Sistemini (CVSSv3) kullanır. CVSS, yazılım/donanım platformundan veya hizmetin işlevinden bağımsız olarak güvenlik açıklarının ciddiyetinin ölçülebildiği bir sistem sağlar. Her güvenlik açığına sıfır ile on arasında bir puan verilir; sıfır risk yok ve on ciddi bir riski temsil eder. Keşfedilen her güvenlik açığına bir puan atamak, en savunmasız sistemleri belirlemeye ve her soruna verilen yanıtlara öncelik vermeye yardımcı olur.

NVD, bir puan sağlamanın yanı sıra, bir önem derecesi sıralaması da sağlar:

Puan	önem
0.0	Yok/Bilgilendirme
0.1-3.9	Düşük
4.0-6.9	Orta
7.0-8.9	Yüksek
8.0-10.0	Kritik

2. Metodoloji

Penetration test metodolojisi, sistem güvenliğini doğru bir şekilde değerlendirmek için büyük bir dikkatle ele alınması gereken pratik fikirler ve kanıtlanmış uygulamalar içeren bir yol haritası tanımlar.

2.1. Keşif/OSINT

Bir değerlendirme yapmak için siteye katılmadan önce güvenlik mühendisi bazı bilgi toplama görevlerini yerine getirir. Bunların amacı, müşteri hakkında mümkün olduğunca fazla bilgi ve içgörü kazanmaktır. Bu bilgiler hassas olarak kabul edilmese de bir saldırgan, kuruluşunuza yönelik saldırılarını hassaslaştırmak için kullanabilir.

Bilgi kaynakları şunları içerebilir;

Web Sitelerinin IP Adresleri ve MX Kayıtları

E-posta adreslerinin ayrıntıları

Sosyal ağlar

İnsan arama

İş Arama Web Siteleri

Araçlardan bazıları şunları içererir; nmap, unicornscan

2.2. Hizmet Tanımlaması

Aktif olarak değerlendirecek ve olası güvenlik açıklarını belirleyecektir. Bu değerlendirme, ağınız hakkında önceden bilgisi olmayan bir saldırganın bakış açısından gerçekleştirilir ve böyle bir kişinin keşfedebileceği güvenlik açıklarını vurgulamak için tasarlanmıştır.

Kullanımdaki hizmetleri ve altında yatan İşletim sistemlerini belirleme. Araçlar şunları içererir; nmap, Nessus, Metasploit, unicornscan

2.3. Sömürü

Saldırı planı, sürüm ve imza tabanlı güvenlik açıklarından, manuel olarak tanımlanan ve zincirleme saldırılardan ve ayrıca test ediciler tarafından belirlenen diğer saldırılardan oluşacaktır. Ayrıca, saldırı planı ve yürütme, kuruluşa özgü tehdit ajanlarını hesaba katacak şekilde uyarlanabilir. Saldırı planı daha sonra sistemlere ve verilere erişim sağlamaya odaklanarak yürütülür.

İlk erişim sağlandığında, hedef, saldırıyı daha yaygın hale getirmek ve hassas varlıklara ve bilgilere erişim sağlamak için ayrıcalıkları artırmaya kayar.

Araçlar şunları içererir; : Kali Linux ,Nmap, Metasploit

2.4. Şifre saldırıları

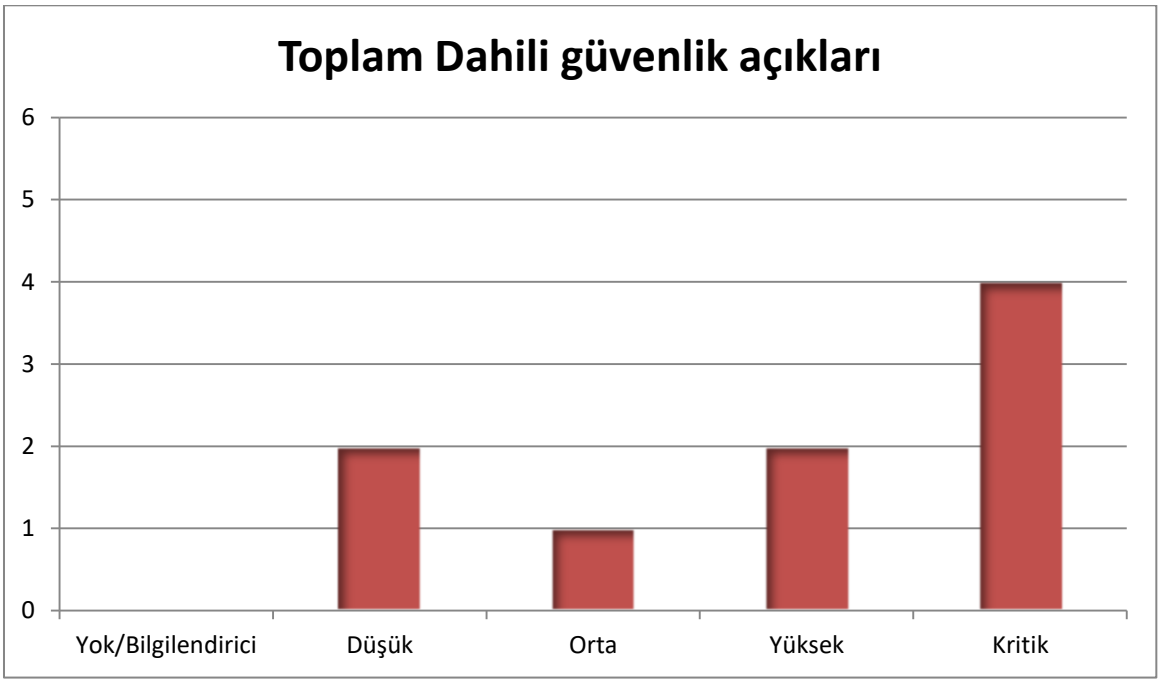
Tipik olarak yararlanma aşamasının bir parçası olarak dahil edilen, kimliği doğrulanmış oturum açmalarla tanımlanan hizmetler, önceki aşamalardan toplanan bilgilere dayanarak kuruluşa göre uyarlanabilecek statik/dinamik kelime listelerine karşı test edilir. Sömürü sırasında elde edilen herhangi bir şifre karmaları, bilinen kelime listelerine karşı kontrol edilecektir.

Araçlar şunları içererir: Hydra, Kali linux

3. Sınırlamalar ve kısıtlamalar

Müşteri tarafından herhangi bir özel sınırlama ve/veya kısıtlama getirilmemiştir. Zaman kısıtlamaları nedeniyle, verilen aralıklarda bulunan masaüstlerine ve sunuculara odaklandık. belirtilen aralıklar içinde alınan diğer cihazlara da bakıldı.

İsim Bulma
Doğrudan Nesne Referansı
XML Harici Varlık(XXE)işleme
Kimlik Avı Saldırısı
Güvensiz Java RMI Uç Noktası



4. Öneriler

Uygun bir parola politikası uygulayın. Yetersiz bir parola politikasına sahip olmak, bir ortamda uzlaşma riskini büyük ölçüde artırır. uygun bir parolanın uygulanmasını ve ardından kuruluşa dağıtılmasını önerir. Aşağıdakileri kılavuz olarak kullanabilirsiniz.

En az 12 alfasayısal karakter

Büyük harf küçük harf

En az 1 numara

En az 1 Özel Karakter

Ayrıca, "L33t 5p34K" IE: A'ları 4;s ile ve E'leri 3'ler ile değiştirmek ve tek sözlük kelimeleri kullanmak gibi şeylerden kaçınmak için kullanıcılara parola oluşturma konusunda brifing vermeyi unutmayın. Cümleleri ve veya birden fazla kelimeyi kırmak çok daha zordur.

İşletim sistemleri, yazılım paketleri ve ağ altyapısı için uygun bir yama politikası ve rejimi uygulayın. Yetersiz bir yama politikasına sahip olmak, bir ortamda uzlaşma riskini büyük ölçüde artırır. hem işletim sistemleri hem de yazılım paketleri için uygun bir yama politikası ve rejiminin uygulanmasını önerir.

Güvenlik yamaları, ortamın altyapısındaki güvenlik açıklarını giderir ve bireysel olarak gözden geçirilmelidir. Gereksiz kesinti sürelerini önlemek için işletmenin ihtiyaçları ile sistem güvenliği arasında dikkatli bir denge sağlanmalıdır.

5. Azaltma

Bazı eski uygulamalar gerektirdiğinden her zaman bir seçenek değildir, ancak bunları desteklemek için herhangi bir gereklilik yoksa güvenli bir şekilde devre dışı bırakılabilirler.

Etki Alanları Arası SMB İmzalamayı Etkinleştirme

SMB İmzalama, SMB kullanan iletişimlerin paket düzeyinde dijital olarak imzalanabileceği bir özelliktir.

Paketleri dijital olarak imzalamak, paketlerin alıcısının, başlangıç noktalarını ve orijinalliklerini doğrulamasını sağlar. SMB protokolündeki bu güvenlik mekanizması, paketlerin kurcalanması ve "ortadaki adam" saldırıları gibi sorunlardan kaçınmaya yardımcı olur.

Güçlü şifre politikası

Zayıf şifreler oldukları için birkaç kullanıcı şifresini çok kolay bir şekilde kırabildim, eğer kullanıcılar daha güçlü şifreler oluşturmaya zorlanırsa ve şifre oluşturma konusunda eğitilirse, bu güvenliği büyük ölçüde artıracaktır.

Birçoğu ağla ilgili olan bir dizi güvenli olmayan veya gereksiz hizmet de tespit edildi.

6. Bulgular

6.1. Bulgular Tablosu

Siteler Arası Komut Dosyası Çalıştırma (XSS)
Doğrudan Nesne Referansları
Kimlik avı Saldırısı
Güvensiz Java RMI Uç Noktası
SSQL'de Zayıf SA Parolası sunucu
Varsayılan veya Boş Şifreler
Dahili IP Adresi Açıklaması
Açık Posta Aktarımı Tanımlandı
Sabit Kodlu Şifreler Kullanımda

6.2. Kritik Bulgular Detay

Aşağıdakiler, değerlendirmeden elde edilen tüm Kritik Bulgulardır.

Siteler Arası Komut Dosyası Çalıştırma (XSS)

Özet:

OWASP kılavuzu Siteler Arası Komut Dosyası Oluşturma için aşağıdaki açıklamayı verir:

Siteler Arası Komut Dosyası Çalıştırma (XSS) saldırıları, kötü amaçlı komut dosyalarının normalde zararsız ve güvenilir web sitelerine enjekte edildiği bir tür enjeksiyondur. XSS saldırıları, bir saldırgan, genellikle tarayıcı tarafı komut dosyası biçiminde kötü amaçlı kodu farklı bir son kullanıcıya göndermek için bir web uygulaması kullandığında meydana gelir. Bu saldırıların başarılı olmasına izin veren kusurlar oldukça yaygındır ve bir web uygulamasının, doğrulamadan veya kodlamadan ürettiği çıktı içinde bir kullanıcıdan gelen girdiyi kullandığı her yerde ortaya çıkar.

Saldırgan, şüphelenmeyen bir kullanıcıya kötü amaçlı bir komut dosyası göndermek için XSS kullanabilir. Son kullanıcının tarayıcısının, komut dosyasına güvenilmemesi gerektiğini bilmesinin hiçbir yolu yoktur ve komut dosyasını yürütür. Komut dosyasının güvenilir bir kaynaktan geldiğini düşündüğünden, kötü amaçlı komut dosyası, tarayıcı tarafından tutulan ve o siteyle kullanılan tüm tanımlama bilgilerine, oturum belirteçlerine veya diğer hassas bilgilere erişebilir. Bu komut dosyaları, HTML sayfasının içeriğini bile yeniden yazabilir.

İyileştirme

XSS güvenlik açıklarını gidermek için aşağıdakiler önerilir: Kullanıcı girdisine asla güvenmeyin İzin verilen konumlar dışında asla güvenilmeyen verileri ekleme HTML öğesi içeriğine güvenilmeyen verileri eklemeden önce HTML kaçışı Girdi filtreleme için Kara listeler için yerinde beyaz listeleri kullanın

Doğrudan Nesne Referansları

Özet

OWASP kılavuzu [1], Güvenli Olmayan Doğrudan Nesne Başvurusu için aşağıdaki açıklamayı verir:

Uygulamalar, web sayfaları oluştururken sıklıkla bir nesnenin gerçek adını veya anahtarını kullanır. Uygulamalar, kullanıcının hedef nesne için yetkilendirildiğini her zaman doğrulamaz. Bu, güvenli olmayan bir doğrudan nesne referans hatasıyla sonuçlanır.

Test cihazları, bu tür kusurları tespit etmek için parametre değerlerini kolayca değiştirebilir ve kod analizi, yetkilendirmenin doğru şekilde doğrulanıp doğrulanmadığını hızla gösterir.

İyileştirme

Kullanıcı veya oturum başına dolaylı nesne referansları kullanın. Bu, saldırganların yetkisiz kaynakları doğrudan hedeflemesini önler. Örneğin, kaynağın veritabanı anahtarını kullanmak yerine, geçerli kullanıcı için yetkilendirilmiş altı kaynağın bir açılır listesi, kullanıcının hangi değeri seçtiğini belirtmek için 1'den 6'ya kadar olan sayıları kullanabilir. Uygulamanın, kullanıcı başına dolaylı referansı sunucudaki gerçek veritabanı anahtarına geri eşlemesi gerekir. Erişimi kontrol edin. Güvenilmeyen bir kaynaktan doğrudan nesne başvurusunun her kullanımı, kullanıcının istenen nesne için yetkilendirildiğinden emin olmak için bir erişim denetimi denetimi içermelidir.

Kimlik avı saldırısı

Kimlik avı, suçlunun güvenilir bir kimlik gibi görünmek için sosyal mühendisliği kullandığı yanlış beyandır. Değerli bilgiler elde etmek için güvenden yararlanırlar; genellikle hesap detayları veya e-ticaret siteleri aracılığıyla hesap açmak, kredi almak veya mal satın almak için yeterli bilgi.

Kimlik avı, suçlunun güvenilir bir kimlik gibi görünmek için sosyal mühendisliği kullandığı yanlış beyandır. Değerli bilgiler elde etmek için güvenden yararlanırlar; genellikle hesap detayları veya e-ticaret siteleri aracılığıyla hesap açmak, kredi almak veya mal satın almak için yeterli bilgi.

İyileştirme

Düzenli son kullanıcı eğitimi

Güvensiz Java RMI Uç Noktası

Risk KRİTİK

Özet

Herhangi bir uzak (HTTP) URL'den sınıfların yüklenmesine izin veren RMI Kayıt ve RMI Etkinleştirme hizmetlerinin varsayılan yapılandırması olan [1]'den yararlanma tartışmasından alıntı. Her RMI uç noktasında mevcut olan RMI Dağıtılmış Çöp Toplayıcıda bir yöntemi çağırdığı için, hem rmiregistry ve rmid'e hem de diğer (özel) RMI uç noktalarının çoğuna karşı kullanılabilir. Aynı Java'da başka bir RMI uç noktası etkin olmadığı sürece, uzaktan sınıf yüklemeyi desteklemediğinden Java Yönetim Uzantısı (JMX) bağlantı noktalarına karşı çalışmadığını unutmayın.

RMI yöntem çağrıları, herhangi bir kimlik doğrulamayı desteklemez veya gerektirmez.

Yelleştirme

Java RMI yöntem çağrılarını devre dışı bırakın.

6.3. YÜKSEK RİSKLİ BULGULAR DETAYLAR

Risk	YÜKSEK

SSQL'de Zayıf SA Parolası sunucu

Özet

Microsoft SQL sunucusu, yerleşik bir Sistem Yöneticisi (SA) hesabıyla birlikte gelir. Varsayılan olarak SA hesabının tüm ayrıcalıkları vardır. Değerlendirme sırasında SA hesabının varsayılan bir SA parolasına sahip olduğu veya boş olduğu tespit edildi. Bir saldırgan, veritabanına yönetici düzeyinde erişim sağlamak için bu hesabı kullanabilir.

İyileştirme

Varsayılan SA hesabı devre dışı bırakılmalıdır. Windows Kimlik Doğrulaması kullanılması önerilir. Ticari nedenlerle bu mümkün değilse, SA hesabı güçlü bir parola ile yapılandırılmalıdır. Güçlü bir parola oluşturmak için aşağıdaki kılavuz satırları kullanılabilir: Alfanümerik, özel karakterler ve boşluklar kullanın En az 32 karakter uzunluğunda bir parola kullanın Parolayı sık sık değiştirin Önceki parolaları yeniden kullanmayın

Varsayılan veya Boş Şifreler

Risk	YÜKSEK

Özet

${ACCOUNT_NAME_HERE} Tomcat hesabının boş veya varsayılan bir şifreyle yapılandırıldığı bulundu. Bir saldırgan, yönetim arayüzüne erişmek ve kötü amaçlı bir web arşiv dosyası (WAR) dosyasını dağıtmak ve sistemi oluşturmak için bu hesabı kullanabilir.

İyileştirme

Varsayılan Tomcat hesabı parolaları, güçlü bir parola ifadesi ile yapılandırılmalıdır. Parola oluşturmak için aşağıdaki kılavuz satırları kullanılabilir: Parola oluşturmak için alfasayısal, özel karakterler ve boşluklar kullanın En az 32 karakter uzunluğunda parolalar kullanın Parolayı sık sık değiştirin Parolaları yeniden kullanmayın

6.4. DİĞER BULGULAR DETAYLAR

Risk	ILIMAN

Dahili IP Adresi Açıklaması

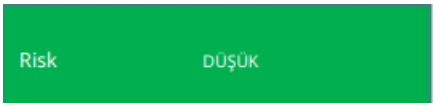
Özet

<<Müşteri>>'nin web sunucusunu incelerken, web sunucularının, İçerik-Konum başlığı aracılığıyla sistemin dahili IP adresini ifşa ettiği keşfedildi. Sistemlerin dahili IP adresinin ifşa edilmesi, bir düşmana dahili ağın nasıl adresleneceğine dair bir gösterge verir.

İyileştirme

<<Müşteri>>'nin, sistemlerin tam nitelikli etki alanı adını (FQDN) kullanmak için web sunucularını yeniden yapılandırması önerilir.

Açık Posta Aktarımı Tanımlandı



ÖzetAçık posta geçişi, yalnızca bilinen kullanıcılara gönderilen veya bu kullanıcılardan gelen postaları değil, İnternet'teki herkesin e-posta göndermesine izin verecek şekilde yapılandırılmış bir SMTP sunucusudur . <Müşteri> için risk kurumsal bütünlük şeklindedir. Ayrıca, < Müşteri > IP'leri bir SPAM ana bilgisayarı veya kötü niyetli kaynak olarak kara listeye alınmış olabilir.

Yileştirme

Açık posta geçişini devre dışı bırakın.

Sabit Kodlu Şifreler Kullanımda

Risk	DÜŞÜK

Özet

Sabit kodlanmış bir parola kullanan bir dizi hizmet tespit edildi. Bu sorunun riski, bir saldırganın sabit kodlanmış bir paroladan bir hesapla oturum açabilmesidir.

İyileştirme

Sabit kodlanmış şifreleri kaldırın.