Testing for Default Credentials (Varsayılan Kimlik Bilgileri için Test)

Summary (Özet)

Günümüzde web uygulamaları genellikle sunucu yöneticisi tarafından minimum yapılandırma veya özelleştirme ile sunuculara yüklenebilen popüler Açık Kaynak veya ticari yazılımlardan yararlanmaktadır. Ayrıca, birçok donanım cihazı (yani ağ yönlendiricileri ve veritabanı sunucuları) web tabanlı yapılandırma veya idari arayüzler sunar.

Genellikle bu uygulamalar, bir kez kurulduktan sonra, uygun şekilde yapılandırılmamıştır ve ilk kimlik doğrulama ve yapılandırma için sağlanan varsayılan kimlik bilgileri asla değişmez. Bu varsayılan kimlik bilgileri penetrasyon test cihazları ve ne yazık ki, çeşitli uygulamalara erişmek için kullanabilen kötü niyetli saldırganlar tarafından da iyi bilinmektedir.

Ayrıca, birçok durumda, bir uygulamada yeni bir hesap oluşturulduğunda, varsayılan bir şifre (bazı standart özelliklere sahip) oluşturulur. Bu şifre öngörülebilirse ve kullanıcı ilk erişimde değiştirmezse, bu bir saldırganın uygulamaya yetkisiz erişim kazanmasına neden olabilir.

Bu sorunun temel nedeni şu şekilde tanımlanabilir:

- Yüklü altyapı bileşenlerinde varsayılan şifrelerin değiştirilmesinin öneminden habersiz olan veya şifreyi “bakım kolaylığı” için varsayılan olarak bırakan deneyimsiz BT personeli.
- Başvurularına kolayca erişmek ve test etmek için arka kapı bırakan ve daha sonra bunları kaldırmayı unutan programcılar.
- Önceden belirlenmiş bir kullanıcı adı ve şifre ile yerleşik çıkarılabilir olmayan varsayılan hesaplara sahip uygulamalar.

- Kullanıcıyı ilk girişten sonra varsayılan kimlik bilgilerini değiştirmeye zorlamayan uygulamalar.

Test Objectives (Test Hedefleri)

- Varsayılan kimlik bilgileri için başvuruları numaralandırın ve hala varsa doğrulayın.
- Yeni kullanıcı hesaplarını gözden geçirin ve değerlendirin ve herhangi bir varsayılan veya tanımlanabilir kalıplarla oluşturulduğunda.

How to Test (Nasıl Test Edilir.)

Testing for Default Credentials of Common Applications (Ortak Uygulamaların Varsayılan Kimlik Bilgileri İçin Test)

Kara kutu testinde test cihazı uygulama ve altta yatan altyapısı hakkında hiçbir şey bilmiyor. Gerçekte bu genellikle doğru değildir ve uygulama hakkında bazı bilgiler bilinmektedir. Bu Test Kılavuzunda açıklanan tekniklerin, Bilgi Toplama bölümü kapsamında, erişilebilir idari arayüzler içerebilecek en az bir veya daha yaygın uygulamada tanımladığınızı varsayıyoruz.

Bir uygulama arayüzünü, örneğin bir Cisco yönlendirici web arayüzü veya bir WebLogic yönetici portalı belirledikten sonra, bu cihazlar için bilinen kullanıcı adlarının ve şifrelerin başarılı bir kimlik doğrulama ile sonuçlanmadığını kontrol edin. Bunu yapmak için üreticinin belgelerine danışabilir veya çok daha basit bir şekilde, bir arama motoru kullanarak veya Referans bölümünde listelenen sitelerden veya araçlardan birini kullanarak ortak kimlik bilgilerini bulabilirsiniz.

Varsayılan ve ortak kullanıcı hesaplarının bir listesi olmadığımız uygulamalarla karşılaştığımızda (örneğin, uygulamanın geniş yayılmadığı için) geçerli varsayılan kimlik bilgilerini tahmin etmeye çalışabiliriz. Test edilen uygulamanın bir hesap kilitleme politikasına sahip olabileceğini ve bilinen bir kullanıcı adı ile birden fazla şifre tahmin girişiminin hesabın kilitlenmesine neden olabileceğini unutmayın. Yönetici hesabını kilitlemek mümkünse, sistem yöneticisinin sıfırlaması sıkıntılı olabilir.

Birçok uygulama, site kullanıcılarını içeri giren kullanıcı adlarının geçerliliği konusunda bilgilendiren sözlü hata mesajlarına sahiptir. Bu bilgiler varsayılan veya tahmin edilebilir kullanıcı hesapları için

test yaparken yararlı olacaktır. Bu tür işlevsellikler, örneğin sayfadaki günlükte bulunabilir, şifre sıfırlama ve unutulmuş şifre sayfası ve oturum açma ve sayfayı kaydedilebilir. Varsayılan bir
kullanıcı adı bulduktan sonra, bu hesap için şifreleri tahmin etmeye de başlayabilirsiniz.

Bu prosedür hakkında daha fazla bilgiyi aşağıdaki bölümlerde bulabilirsiniz:

- Kullanıcı Sayısı ve Tahmini Kullanıcı Hesabı için Test
- Zayıf şifre politikası için test.

Bu tür temerrüt kimlik bilgileri genellikle idari hesaplara bağlı olduğundan, bu şekilde ilerleyebilirsiniz:

- Aşağıdaki kullanıcı adlarını deneyin - “admin”, “yönetici”, “kök”, “sis”, “konuşma”, “operatör” veya “süper”. Bunlar sistem yöneticileri arasında popülerdir ve sıklıkla kullanılır. Ek olarak “kadet”, “test1”, “test1” ve benzeri isimleri deneyebilirsiniz. Yukarıdakilerin herhangi bir kombinasyonunu hem kullanıcı adı hem de şifre alanlarında deneyin. Uygulama kullanıcı adı numaralandırmasına karşı savunmasızsa ve yukarıdaki kullanıcı adlarından herhangi birini başarılı bir şekilde tanımlamayı başarırsanız, şifreleri benzer şekilde deneyin. Ayrıca boş bir şifre veya aşağıdaki “şifreden”, “password123”, “password123”, “admin” veya “konuk” yukarıda hesaplar veya diğer numaralandırılmış hesaplardan birini deneyin. Yukarıdakilerin daha fazla permütasyonları da denenebilir. Bu şifreler başarısız olursa, ortak bir kullanıcı adı ve şifre listesi kullanmaya ve uygulamaya karşı birden fazla istek denemesi yapmaya değer olabilir. Bu, elbette, zamandan tasarruf etmek için yazılabilir.
- Uygulama yöneticisi kullanıcılar genellikle başvuru veya kuruluştan sonra adlandırılmıştır. Bu, “Belirsizlik” adlı bir uygulamayı test ediyorsanız, bilinmezlik / belirsizlik veya kullanıcı adı ve şifre ile benzer bir kombinasyon kullanmayı deneyin.
- Bir müşteri için bir test yaparken, herhangi bir yaygın şifre ile kullanıcı adları olarak aldığınız kişilerin adlarını kullanmaya çalışın. Müşteri e-posta adresleri posta, kullanıcı hesapları adlandırma sözleşmesini ortaya çıkarır: çalışan “John Doe” e-posta adresine sahipse `jdoe@example.com`, sistem yöneticilerinin isimlerini sosyal medyada bulmaya ve aynı

adlandırma sözleşmesini adlarına uygulayarak kullanıcı adlarını tahmin etmeye çalışabilirsiniz.

- Boş şifrelerle yukarıdaki tüm kullanıcı adlarını kullanmaya çalışın.
- Sayfa kaynağını ve JavaScript'i bir proxy aracılığıyla veya kaynağı görüntüleyerek gözden geçirin. Kaynaktaki kullanıcılara ve şifrelere yapılan herhangi bir referansı arayın. Örneğin `If username='admin' then starturl=/admin.asp else /index.asp` (Başarılı bir giriş için başarısız bir girişe karşı). Ayrıca, geçerli bir hesabınız varsa, o zaman giriş yapın ve geçerli bir gün için geçerli bir kayıt için yanıtı görüntüleyin, ek gizli parametreler, ilginç GET talebi (login = evet) vb.
- Kaynak kodundaki yorumlarda yazılı hesap adlarını ve şifreleri arayın. Ayrıca, ilginç yorumlar ve kod içerebilecek kaynak kodu (veya kaynak kodu yedeklemeleri) için yedekleme dizinlerine bakın.

Testing for Default Password of New Accounts (Yeni Hesapların Varsayılan Şifresi için Test)

Bir uygulamada yeni bir hesap oluşturulduğunda, hesabın varsayılan bir şifre atandığı da ortaya çıkabilir. Bu şifre, öngörülebilir hale getiren bazı standart özelliklere sahip olabilir. Kullanıcı ilk
kullanımda değiştirmezse (bu genellikle kullanıcı değiştirmeye zorlanmazsa olur) veya kullanıcı henüz uygulamaya girişmediyse, bu bir saldırganın uygulamaya yetkisiz erişim sağlamasına neden olabilir.

Muhtemel bir lokavt politikası ve fiili hata mesajları hakkında daha önce verilen tavsiyeler, varsayılan şifreler için test yaparken burada da geçerlidir.

Bu tür varsayılan kimlik bilgileri için test için aşağıdaki adımlar uygulanabilir:

- Kullanıcı Kayıt sayfasına bakmak, uygulama kullanıcı adlarının ve şifrelerinin beklenen biçimini ve minimum veya maksimum uzunluğunu belirlemeye yardımcı olabilir. Bir kullanıcı kayıt sayfası yoksa, kuruluşun e-posta adresi veya adı önceden adlandırılan ad gibi kullanıcı adları için standart bir adlandırma sözleşmesi kullanıp kullanmadığını belirleyin `@` E-postada.
- Kullanıcıların nasıl oluşturulduğunu uygulamadan tahmin etmeye çalışın. Örneğin, bir kullanıcı kendi kullanıcı adını seçebilir mi yoksa sistem bazı kişisel bilgilere dayanarak veya öngörülebilir bir dizi kullanarak kullanıcı için bir hesap adı oluşturur mu? Başvuru, hesap adlarını öngörülebilir bir sıra halinde

oluşturursa, örneğin `user7811`, olası tüm hesapları tekrarlayan bir şekilde karıştırmayı deneyin. Geçerli bir kullanıcı adı ve yanlış bir şifre kullanırken uygulamadan
farklı bir yanıtı tanımlayabilirseniz, geçerli kullanıcı adına kaba bir kuvvet saldırısı deneyebilir (veya yukarıda veya referans bölümünde tespit edilen ortak şifrelerden herhangi birini hızlı bir şekilde deneyebilirsiniz).

- Sistem tarafından oluşturulan şifrenin öngörülebilir olup olmadığını belirlemeye çalışın. Bunu yapmak için birbiri ardına çok sayıda yeni hesap oluşturun, böylece şifrelerin öngörülebilir olup
olmadığını karşılaştırabilir ve belirleyebilirsiniz. Öngörülebilir durumda, bunları kullanıcı adları veya numaralandırılmış hesaplarla ilişkilendirmeye çalışın ve bunları kaba bir kuvvet saldırısı için bir temel olarak kullanın.
- Kullanıcı adı için doğru adlandırma sözleşmesini belirlediyseniz, örneğin doğum tarihleri gibi bazı yaygın öngörülebilir dizilişe sahip şifreleri "kırmaya zorlamaya" çalışın.
- Yukarıdaki tüm kullanıcı adlarını boş şifrelerle kullanmaya veya kullanıcı adını şifre değeri olarak kullanmaya çalışın.

Gray-Box Testing (Gri Kutu Testi)

Aşağıdaki adımlar tamamen gri kutulu bir yaklaşıma dayanır. Bu bilgilerin sadece bir kısmı sizin için mevcutsa, boşlukları doldurmak için kara kutu testine bakın.

- İdari erişim için hangi şifreleri kullandıklarını ve uygulamanın nasıl uygulandığını belirlemek için BT personeli ile konuşun.
- BT personeline varsayılan şifrelerin değiştirilip değiştirilmediğini ve varsayılan kullanıcı hesaplarının devre dışı bırakılıp bırakılmadığını sorun.
- Kara kutu test bölümünde açıklandığı gibi varsayılan kimlik bilgileri için kullanıcı veritabanını inceleyin. Ayrıca boş şifre alanlarını kontrol edin.
- Sert kodlanmış kullanıcı adları ve şifreler için kodu inceleyin.
- Kullanıcı adları ve şifreler içeren yapılandırma dosyalarını kontrol edin.
- Şifre politikasını inceleyin ve uygulama yeni kullanıcılar için kendi şifrelerini oluşturursa, bu prosedür için kullanılan politikayı kontrol edin.

Tools (Araçlar)

- Burp Intruder
- THC Hydra
- Nikto 2

References (Referanslar)

CIRT