Kırılası Zayıf Şifreler

written by Mert SARICA | 14 August 2010

Kullandığınız şifrenin kırılması, tahmin edilmesi ne kadar zor ise kullandığınız sistem o kadar güvendedir sözünün ne kadar doğru olduğunu zaman geçtikçe anlıyorum. Gerek gerçekleştirdiğim geniş kapsamlı penetrasyon testlerinde olsun gerek yerinde denetimlerde olsun muhakkak raporumda zayıf şifreler ile ilgili bir bulgu yer alıyor.

Kurumunuzun bilgi güvenliği politikası kusursuzda olsa, çalışanlarınız eksiksiz olarak bilgi güvenliği farkındalık eğitimine katılıyorda olsalar, sistemler üzerinde kullanıcılarınız kompleks şifre kullanmaya zorlanıyorda olsalar, insanlar şifre olarak sözlükte yer alan kelimeleri seçmeye devam ediyorlar çünkü gündelik hayatta o telaşla, yoğun iş temposunda hatırlayacak o kadar çok şey dururken sistemler el verdiği sürece o büyük, küçük harflerden, sayılardan ve özel karakterlerden oluşan şifreleri kullanmamak için her yolu deniyorlar. E durum böyle olduğu sürece zayıf şifre kullanılan tüm sistemler bir şekilde istismar edilerek art niyetli kişilerin hedefi olmaya devam ediyor.

Zayıf şifreler sistemlerin vazgeçilmez bir parçası olduğu için penetrasyon testi gerçekleştiren bilişim güvenliği uzmanlarının ellerinin altında bu şifreleri art niyetli kişilerden önce sözlük saldırısı (dictionary attack) ile tespit etmek için özenle hazırlanmış sözlükleri bulunur ve zaman zaman bu sözlükleri güncelleme ihtiyacı duyarlar. İhtiyaç duyarlar çünkü penetrasyon testlerinde ne kadar çok basit şifre tespit ederlerse bunların art niyetli kişilerce tespit edilmelerinin önüne geçtiklerini iyi bilirler.

Yine periyodik bir sözlük güncelleme zamanında sözlüğümde yer alan Türkçe kelimelerin azlığı dikkatimi çekti. Ana dilimiz Türkçe iken sözlüğümde yer alan Türkçe kelimelerin seyrekliği içime pek sinmiyordu. Elektronik ortamda Türkçe kelimeleri nereden bulurumda sözlüğümü kolayca güncelleyebilirim sorusuna yanıt ararken aklıma hemen etrafta yaygın olarak kullanılan Moonstar sözlük geldi.

Moonstar sözlüğü indirip kurduktan sonra kelime veritabanına göz atmaya karar verdim. Kurulum klasörü içinde yer alan Dic.ssm dosyasını Dic.mdb olarak kaydettikten ve MDBViewer programı ile içine göz attıktan sonra içinde toplam 77368 Türkçe kelimenin yer alması sayıca bana yeterli gelmedi.

Başka nereden bulabilirim diye tırmalamaya devam ettiğimde ise aklıma güzel Türkçe'mizi katletmemek için sıkça ziyaret ettiğim Türk Dil Kurumu'nun Büyük Türkçe Sözlüğü geldi.

Ünlü Python programcısı M.S'nin "Aklıma gelen IDE (Integrated development environment)'me gelsin." sözünden yola çıkarak Büyük Türkçe Sözlüğünde yer alan Türkçe kelimelerden online olarak sözlük oluşturan TDK.py adında ufak bir program hazırlamaya karar verdim :)

Program kısaca sorgu sonrasında sunucudan dönen ve içinde kelimelerin yer aldığı html yanıtı diske kaydediyor. Tüm yanıtlar diske kayıt edildikten sonra Search and Replace programı yardımı ile tüm html dosyalarında (*.html) yer alan   ve </td> html taglerini \n ile replace ederek grep'lenebilir formata getirdim ve son olarak aşağıdaki komutlar dizisini çalıştırarak sözlüğü son haline getirmiş oldum.

egrep -e "^[a-z]+[^\n]$" *.html | cut -d " " -f 1 | sort | uniq -i | cut -d ":" -f 2 > sozluk.txt

Sözlük 190774 adet Türkçe kelimeden oluşuyor. Türkçe harflerin kimi sistemde kabul edilmediğini veya soruna yol açabildiğini göz önünde bulundurarak Türkçe harflerden arındırılmış bir kopyasınıda oluşturdum ve her ikisinide zip dosyasının içine koydum.

Her ne kadar sözlüğün kalitesini değerlendirebilmek için yerli bir kaynağa ihtiyaç duymuş olsamda yokluk nedeniyle sözlüğü zamanında hack edilmiş ve internette yayınlanmış, kırılmış yerli ve yabancı şifrelerden oluşan phpbb şifreleri (184389 adet) üzerinde denediğimde 2036 tanesinin sözlüğümde yer aldığını gördüm ve sonuç benim için tatminkar oldu.

Sonuç olarak sizde benim gibi penetrasyon testlerinde sözlük saldırısı gerçekleştirmek için kullanışlı bir Türkçe sözlüğe ihtiyaç duyuyorsanız oluşturduğum sözlüğün kopyasına buradan ulaşabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim.