Ms SQL Server'ın Gizli Gücü xp_cmdshell

Sql Server dersini alırken sadece kullandığımız belli başlı 3 – 4 komut vardı, SELECT, UPDATE, DELETE… Ama hep dediğimiz bir şey daha vardı "Adamlar bu kadar büyük bir programı sırf SELECT için yazmış olamaz", öyle ya bir yüklüyoruz bilgisayarda neredeyse 10GB yer kaplıyor.

Şimdi Sql Server'ın SELECT dışında yapabildiği binlerce işlemden birini beraber görelim.

xp_cmdshell, SQL Server üzerinden cmd komut satırına komut göndermeyi ve çalıştırmaya imkan sağlayan stored prosedür. Bu özelliği sayesinde cmd ekranında yapabildiğimiz herşeyi:

- Windows Server üzerinde yeni kullanıcı açıpi buna full yetki verilip kuruluşumuzun her türlü gizli verisi ve işlemlerine ulaşılabilir
- "format X" komutunu göndererek Sql Server üzerinden X diskini formatlanabilir
- Windows Server içerisine her hangi bir .exe dosyası atılarak çalıştırılabilir, bu bir keyloger da olabilir

ve daha fazlası kısaca herşeyi.

xp_cmdshell stored prosedürü varsayılan olarak güvenlik politikası olarak devre dışıdır. Prosedürü devreye almak için aşağıdaki kod çalıştırabilir veya arayüz üzerinde de işlem yapılabilir. Sql koduna ve hemen ardından arayüz adımlarına geçelim.

Alternatif olarak arayüz adımları:

xp_cmdshell aktifleştirme

Bu işlemler sonucunda aktifleştirme gerçekleştirilir.

xp_cmdshell komutu çalıştırıldığında dönen sonuş tek kolon ve text şeklinde olur. Çıktı vermeyen komutlar için başarılı olması durumunda 1, başarızı olması durumunda 0 sonucu döner.

Şimdi de bazı örnekler yaparak çalışma şeklini görelim.

- Çıktı Veren Örnek
  Komut satırına 'DIR C:\' komutunu göndererek C:\ diski altında yer alan dosyaları gösterelim.

  
  xp_cmdshell ile C:\ diski altında yer alan dosyaların gösterilmesi

- Çıktı Vermeyen Örnek
  Komut satırın copy komutu göndererek C:\XP\Deneme.txt dosyasını aynı klasör altına Deneme2.txt adıyla kopyalayalım.