Gaarrkkk

written by Mert SARICA | 21 October 2010

Bir kaç gün önce geceleri rahat uyku uyumanıza yardımcı olan binlerce dolarlık web uygulama güvenlik tarayıcılarının basit bir güvenlik zafiyetini tespit etmekte ne kadar başarısız olduğuna ve bir kurum için 3. parti penetrasyon testlerinin, 3. bir gözün ne kadar değerli olduğuna bir kez daha tanık oldum.

Bir web uygulaması düşünün bu zamana dek web uygulama güvenlik tarama araçlarının ağır topları (HP Webinspect, IBM Appscan, Acunetix ve ~~Netsparker~~) ile taranmış ve sql injection güvenlik zafiyeti adına bir tane bulgu ortaya çıkmamış. Uygulama oldukça büyük, ister istemez zaman ve kaynak kısıtlarından ötürü manual olarak siteyi baştan aşağıya test etmek mümkün değil. Durum böyle oluncada iş testi gerçekleştiren bilişim güvenlik uzmanlarının Jedi sezgisine ve kullanmış olduğu araçların becerisine kalıyor.

Gerçekleştirilen bu testlerde de olabildiğince fazla araç kullanmakta her zaman fayda var çünkü bir aracın bulamadığı bir güvenlik zafiyeti diğer bir araç, diğer iki aracın bulamadığı bir güvenlik zafiyetini ise diğer araç bulabiliyor. Tabii ki hiç bir araç manual testlerin yerini alamıyor ve yakın gelecektede almasını beklemiyorum.

Gün geliyor bu uygulama, yerli bir firmadan alınan penetrasyon testi hizmetinin kapsamına alınıyor. Tüm güvenlik mekanizmaları devre dışı bırakıldıktan sonra whitebox penetrasyon testi başlıyor ve çok geçmeden bu uygulama üzerinde zaman tabanlı blind sql injection güvenlik zafiyeti tespit ediliyor. Her ne kadar manual testlerin yerini hiç bir araç alamıyor olsada bu kadar üst düzey araçlar ile taranan bir uygulamada nasıl oluyorsa bu zafiyet keşfediliyor sorusu akıllara gelen ilk soru oluyor. Sorunun cevabı ise deyim yerindeyse samanlıkta iğne bulan bilişim güvenlik uzmanının Jedi sezgisi ve bu güvenlik zafiyetini tespit etmesini sağlayan 149 Pound değerindeki Burp Suite PRO aracı oluyor.

Bu anekdottan kurumlar ve bilişim güvenlik uzmanları kendileri için şu dersleri çıkarabilirler;

- 3. parti penetrasyon testlerinin önemi
- Binlerce dolarlık ticari araçlara çok fazla güvenmemek gerektiği

- Manual testlerin önemi
- Güvenlik testlerinde olduğunca fazla araçtan faydalanmak gerektiği

Bir sonraki yazıda görüşmek dileğiyle şimdiden herkese iyi haftasonları dilerim.

Not: Yazının başlığı neden mi Gaarrkkk ? İşte yanıtı :)

Güncelleme (27.10.2010): Netsparker dışındaki ürünler ile gerçekleştirilen testleri bizzat doğrulama imkanım olmuştu fakat Netsparker lisansım olmadığı için testi denetçi gerçekleştirmiş ve bulamadığını iletmişti bende buna istisneden listeye Netsparker ürününüde eklemiştim. Ferruh ile yaptığım görüşmeler neticesinde Netsparker ürünü ile aynı testi bizzat gerçekleştirme imkanım oldu ve ürünün bu zafiyeti tespit edebildiğine tanık oldum.
Denetçi ile yaptığım son görüşmede ise siteyi baştan sona Netsparker ile taratmadığını proxy modunda zafiyete sahip olan bölümü tarattığını öğrendim ve proxy modunda uygulamayı test ettiğimde bu zafiyeti bulamadığını teyit ettim.
Son durumda Netsparker'ın bu zafiyeti tam tarama seçeneği ile başarıyla tespit edebildiğini, proxy modundayken tespit edemediğini söylemek isterim, kullananlara duyurulur.