Firefox Oturum Geri Yükleme Özelliği

written by Mert SARICA | 13 December 2011

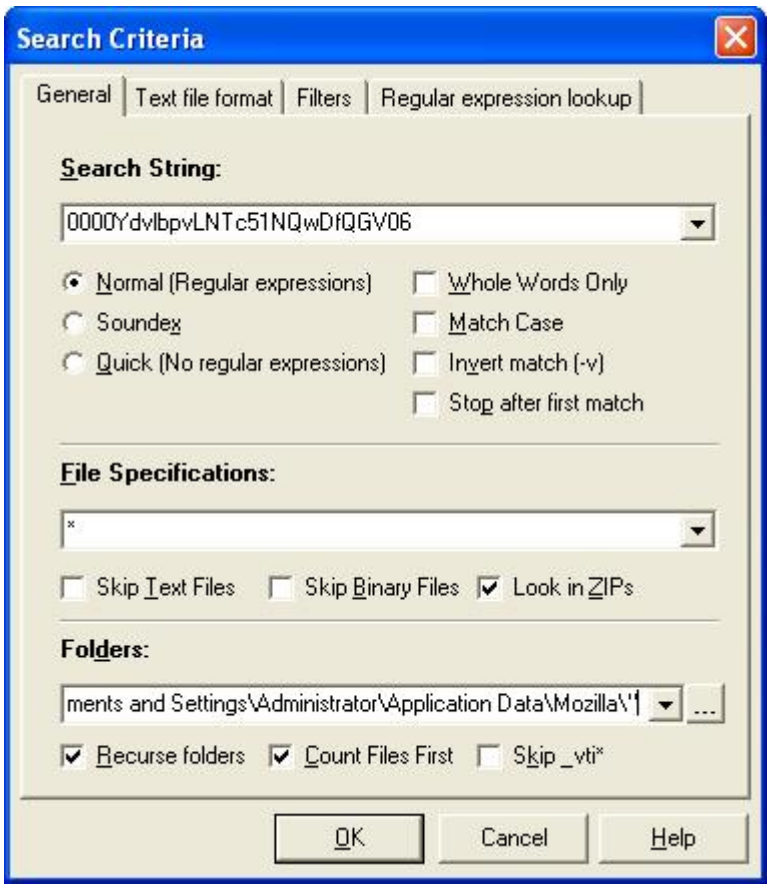
Accuvant firmasının yaptığı araştırmaya göre Chrome internet tarayıcısının rakiplerinden daha güvenli olduğu ortaya çıkmış. Araştırma sonucunda ortaya çıkan sıralamada Firefox internet tarayıcısının üçüncü sırada yer alması kimilerini şaşırtsa da beni pek şaşırtmadı.

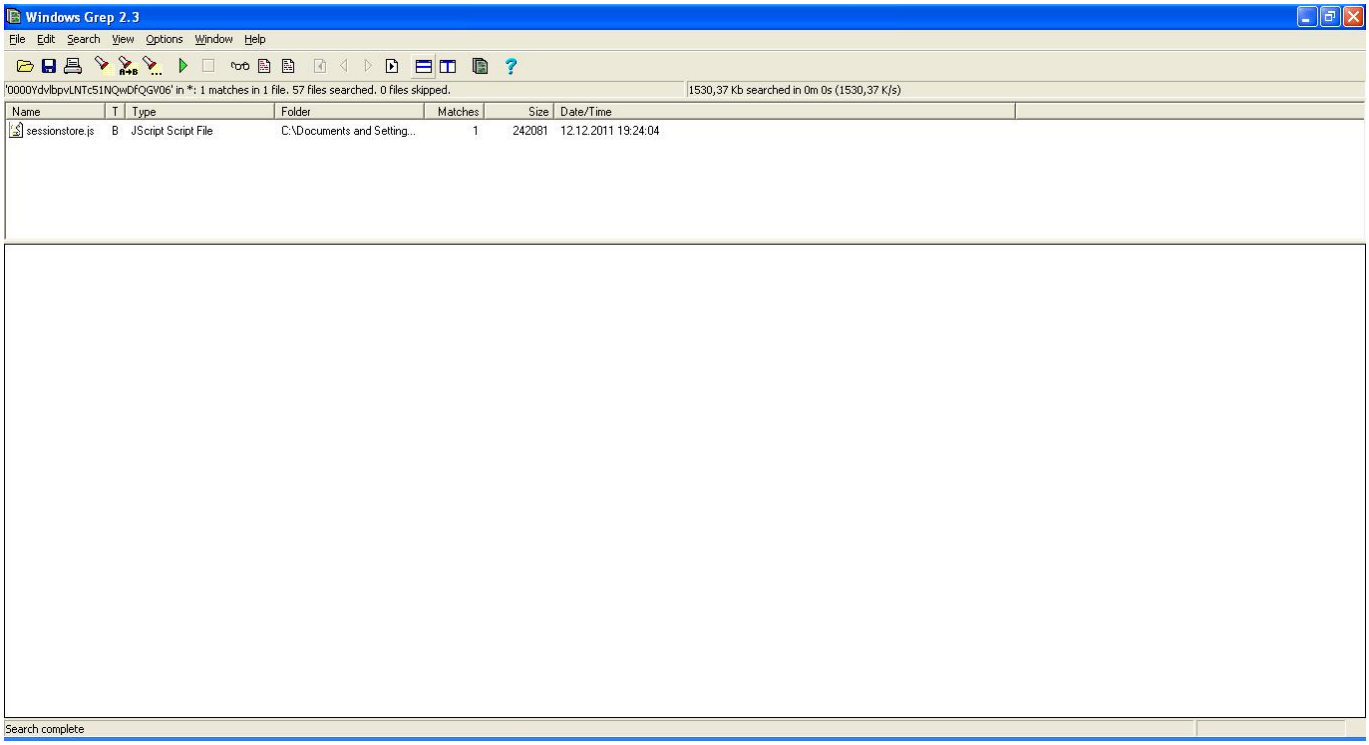
Geçtiğimiz günlerde bir web uygulaması üzerinde penetrasyon testi gerçekleştirirken işlem (transaction) bazlı jeton (token) kullanılmaması durumunda oturum çerezini (session cookie) çalan art niyetli bir kişinin kurbanın oturumunu çaldıktan (session hijack) sonra uygulama üzerinde hangi işlemleri rahatlıkla gerçekleştirebileceğini düşünüyordum. Daha sonra oturum çerezinde HTTPOnly bayrağının kullanılıyor olması nedeniyle bu riskin gerçekleşme ihtimalini düşünmeye başladım. Ardından işletim sistemine bulaşan zararlı bir yazılımın oturum çerezini çalmak için izleyeceği yolları düşünmeye başladım. Oturum çerezi hafızadan (RAM) ne kadar rahatlıkla çalınabilirdi ? Meşhur bankacılık truva atları (zeus, spyeye) gibi internet tarayıcıları ile ilişkili dosyalara kanca (hook) atarak mı çalmak daha kolay olurdu diye düşünürken dosya sistemi üzerinde tutulan normal çerezlerden farklı olan oturum çerezlerinin dosya sistemi üzerinde tutuluyor olma ihtimaline nedense pek ihtimal vermiyordum ancak yine de göz atmaya karar verdim.

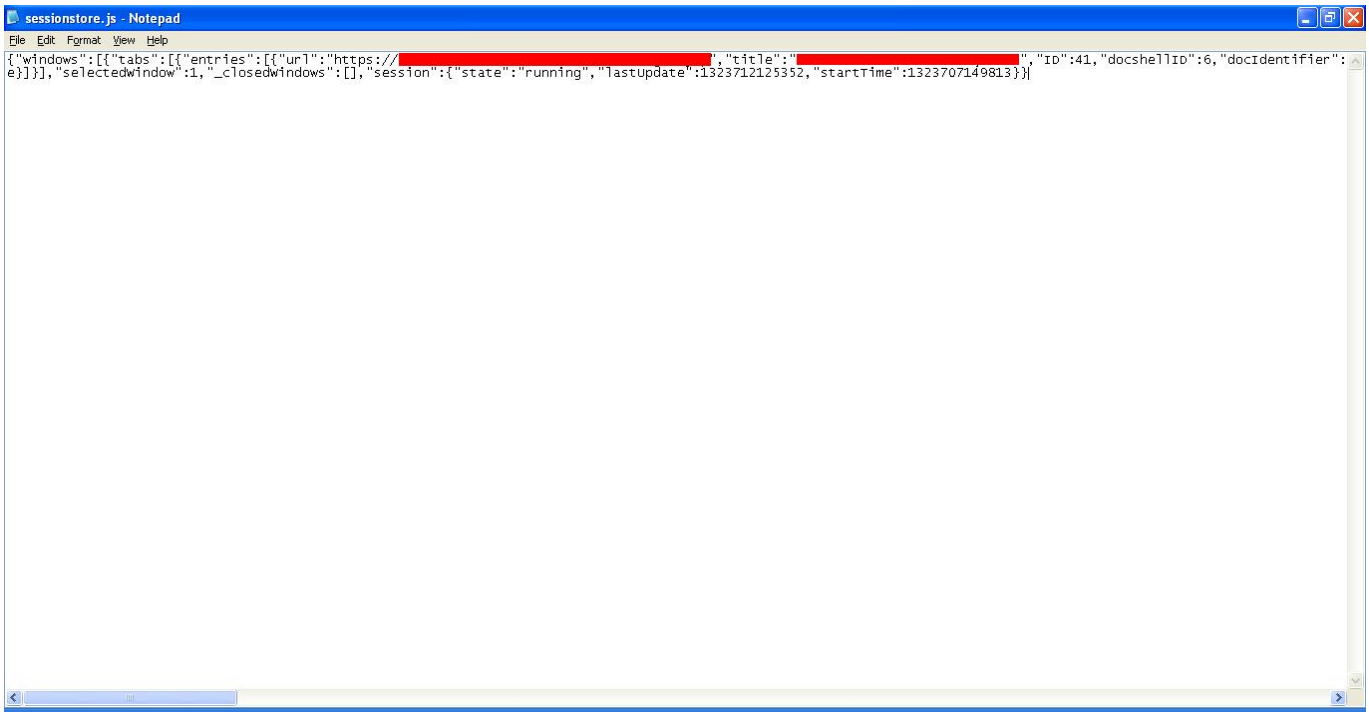
Öncelikle sanal makine üzerine Chrome (15.0.874.121), Firefox (8.0.1) ve Internet Explorer (9.0) internet tarayıcılarının en son sürümlerine kurdum ve üç internet tarayıcısı ile oturum çerezi ile birlikte güvenlik bayrağı (secure flag) ve HTTPOnly bayrağı kullanılan bir web sitesini ziyaret ettim. Ardından web sitesi tarafından her bir internet tarayıcısına gönderilen oturum çerezini not ederek internet tarayıcıları tarafından kullanılan klasörlerde bu çerezleri arattığımda sadece Firefox internet tarayıcısının oturum çerezini dosya sisteminde kayıt altına aldığını gördüm.

NAME	JSESSIONID
VALUE	0000YdvlbpvLNTc51NQwDfQGV06:162u7ac2o
HOST	[redacted]
PATH	/
SECURE	Yes
EXPIRES	At End Of Session

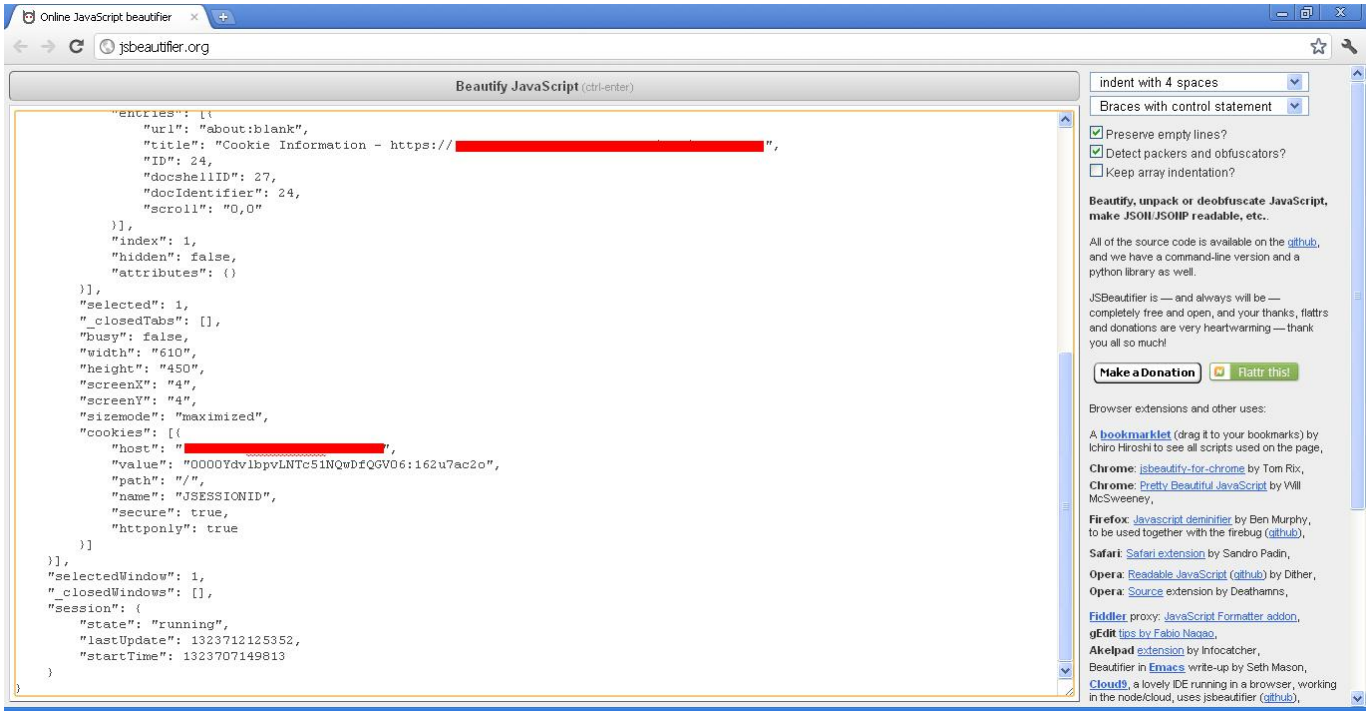
Set-Cookie: JSESSIONID=0000YdvlbpvLNTc51NQwDfQGV06:162u7ac2o; HTTPOnly; Path=/; Secure







Sessionstore.js dosyasında yer alan objeler JavaScript Object Notation (JSON) formatında saklandığı için kolay okunabilmesi adına jsbeautifier.org sitesinde içeriği düzenlettiğimde oturum çerezi okunabilir hale geldi.



Peki ne Chrome, ne Internet Explorer internet tarayıcısı oturum çerezini dosya sistemi üzerinde okunaklı olarak saklamazken Firefox saklıyordu ve saklamasının son kullanıcıya ne tür bir etkisi olabilirdi ?

Web siteleri sizi her oturumda size özel üretilen oturum çerezleri üzerinden takip eder, doğrular ve işleminizi gerçekleştirir. Örnek olarak bir internet bankacılığı uygulaması düşünelim. Uygulamaya giriş yaptıktan sonra uygulama size o oturuma özel bir oturum çerezi göndererek sizin doğrulama adımlarından başarıyla geçtiğinizi kabul eder ve gerçekleştireceğiniz her işlemde (işlem bazlı jeton kullanılmadığı durumlarda) oturum çerezinizi kontrol ederek işleminizi gerçekleştirir.

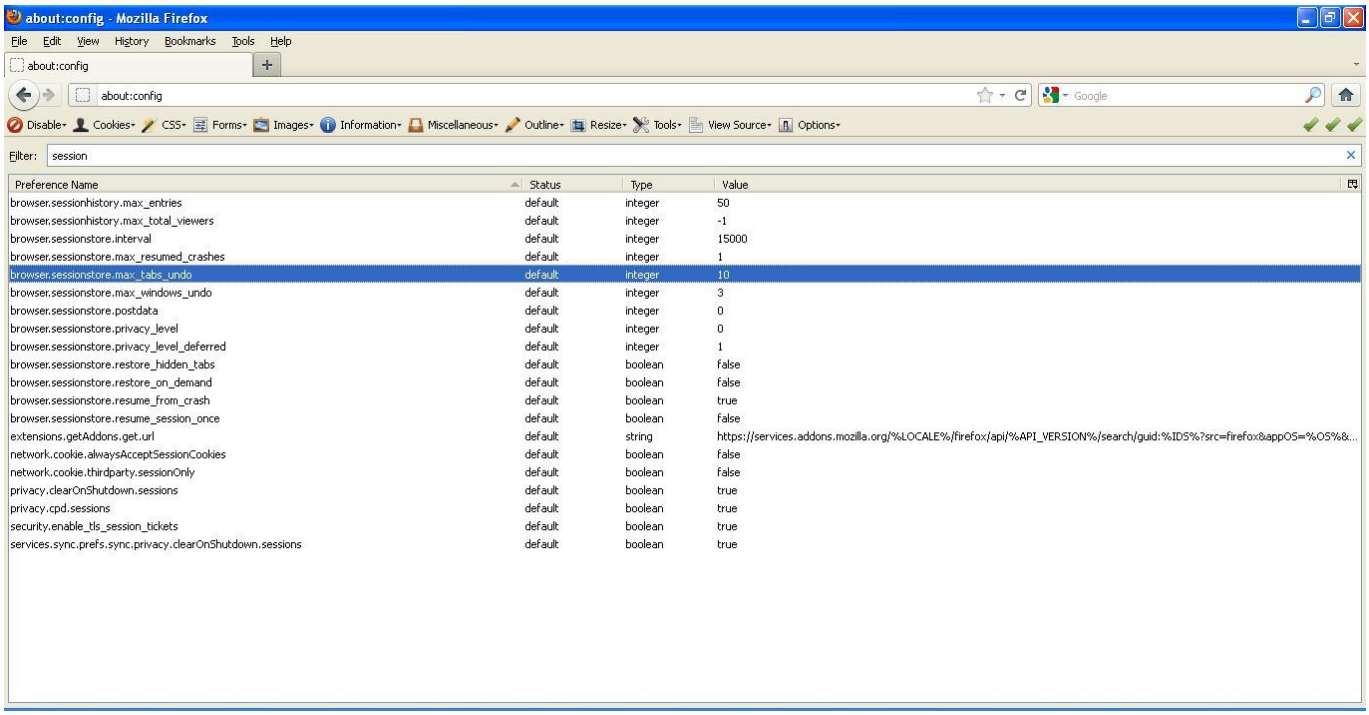
Peki ya bu oturum çereziniz çalınırsa ne olur ? Art niyetli kişi sizin adınıza gerçekleştirmeye yetkili olduğunuz tüm işlemleri (para transferleri, döviz alış/satış vs.) gerçekleştirebilir. İşte bu nedenle oturum çerezlerinin dosya sistemine kayıt edilmesi ve zararlı yazılımlar tarafından kolaylıkla çalınabilir olması tercih edilmez.

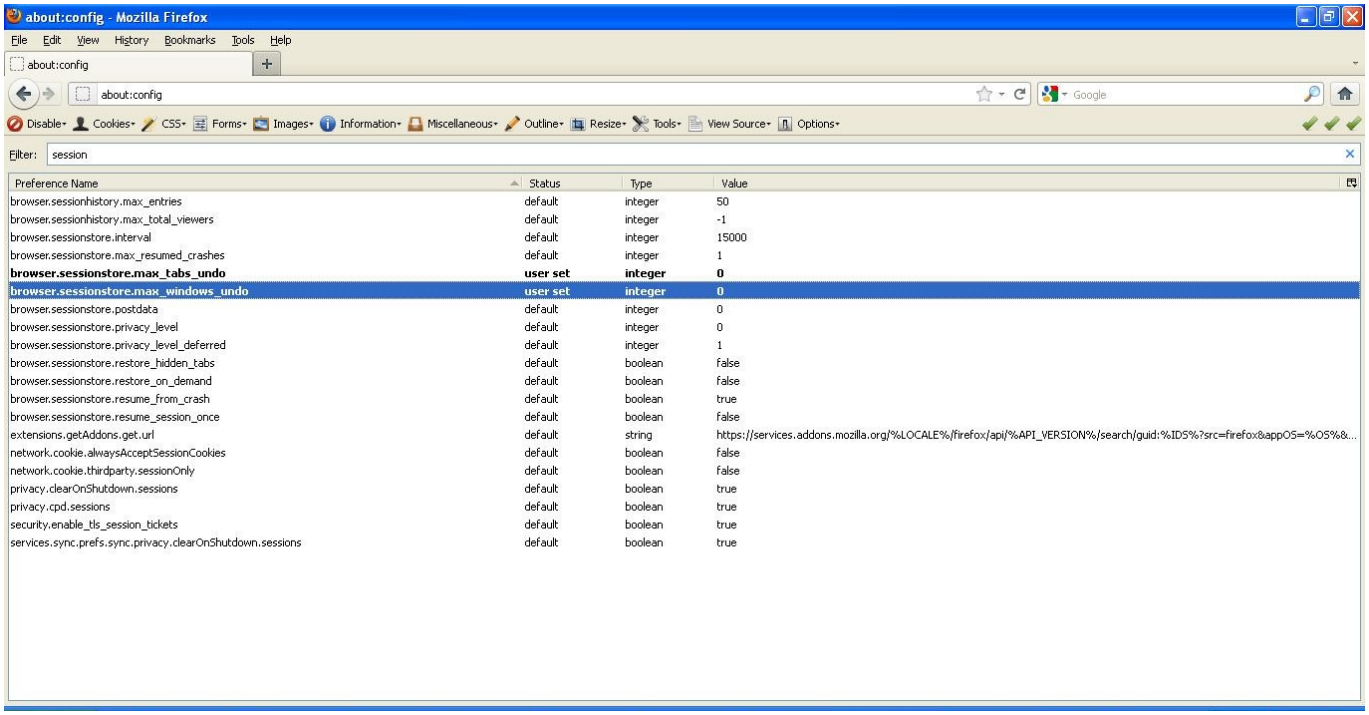
Peki Firefox internet tarayıcısı bunu neden yapıyor ? Beklenmeyen bir durumda (crash), yeni bir eklenti yüklendikten sonra veya otomatik güncelleştirme sonrasında internet tarayıcısının yeniden başlatılması gibi ihtiyaçlar ortaya çıktığı için oturumların kaldığı yerden devam edebilmesi (session restore) amacıyla oturum çerezlerini Sessionstore.js dosyasında saklamaktadır.

Her ne kadar sisteme bulaşmış zararlı bir yazılım günün sonunda hangi internet tarayıcısı olursa olsun bellekten okuma, kanca atma ve diğer

yöntemler ile oturum çerezlerini çalabilse de kullandığınız internet tarayıcınızın art niyetli kişilerin işlerini bu kadar kolaylaştırmıyor olması gerekmektedir.

Güvenliğiniz için oturum geri yükleme (session restore) özelliğini devre dışı bırakmanızı öneririm. Bunun için aşağıdaki iki değeri 0 olarak değiştirmeniz yeterli olacaktır.





Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…