**Web Uygulamalarında Sekmeli Tarayıcılar için Oturum Yönetimi Zafiyeti**

Sekmeli tarayıcılar günümüzün vazgeçilmez unsurlarından biri haline gelmiştir. Yakın bir tarihe kadar tarayıcı pencereleri birbirinden bağımsız kontroller halinde kullanılırken, sekmeli tarayıcılar bu ayrık modeli daha merkezi ve kullanışlı bir halde, tek pencere altında toplayıp, kullanılabilirliği daha yüksek bir çözüm şeklinde kullanıcılara sunmuştur. Bu durumun bir sonucu olarak söz konusu bilgi güvenliği bakış açısından kullanılabilirliğin yorumlanmasına geldiğinde ise sonuç şaşırtıcı olmamaktadır…

Bilgi güvenliğinin temel kavramları arasında yer alan konulardan biri kullanılabilirlik-güvenlik dengesidir. Bu denge terazinin iki kefesine konmuş ağırlıklara veya matematikteki ters orantıya benzetilebilir. Kullanılabilirliğin arttığı her senaryoda güvenliğin bir tehdit altında bulunması durumu ortaya çıkabilir.

Kullanılabilirlik ve güvenlik dengesinin anlaşılması için bir örnekle konuyu somutlaştırmak yerinde olacaktır:

Günümüzde İnternet'ten bankacılık işlemleri gerçekleştirilirken oturum açmak için birçok doğrulama adımından geçmek gerekmektedir. Bu doğrulama adımlarından birçoğu çok faktörlü doğrulama (Multi Factor Authentication) ile (kullanıcının bildiği bir şeye, kendisine ve/veya sahip olduğu bir faktöre dayandırılması ile) gerçekleştirilirken, birçoğu da sadece kullanıcının bildiği (PIN, parola, gizli soru cevabı, vs.) faktörlere dayanmaktadır. Sadece bir kullanıcı adı ve parola kullanılarak giriş yapılabilen bir İnternet bankacılığı uygulaması günümüzde bulunmamaktadır. En az 2 adet parolanın ve/veya cep telefonuna gelen bir de PIN kodunun sorulduğu uygulamalar ağırlıktadır. Bu durum, İnternet bankacılığına giriş yapabilmek için sarf edilen çabayı arttırmakta, oturum açma işini zahmetli bir hale getirmektedir ancak zahmetli hale gelerek kullanılabilirliği düşen sistem daha güvenli hale gelmiş olmaktadır.

Ayrık pencere yapısındaki tarayıcılarla sekmeli tarayıcılar kıyaslandığında da durum kullanılabilirlik-güvenlik dengesi bakımından güvenlik kefesinin zayıflamasıyla sonuçlanabilmektedir. Ayrık pencere yapısındaki tarayıcılarda açılan bir oturum pencere kapanana kadar devam eder. Tarayıcı penceresi kapandığı anda ise oturuma ait kimlik bilgisi (Cookie, Session ID) istemci tarafında silinir. Sunucu tarafında ise bu bilginin silinip silinmemesi konusu Web uygulamasındaki oturum açma tasarımına bağlıdır.

İstemci tarafında silinen oturum açma kimliği sayesinde sonradan açılan yeni tarayıcı pencereleri, kapatılan pencere ile silinen istemci tarafındaki oturum için bir tehlike arz edemez. Söz konusu sekmeli tarayıcılara geldiğinde ise durum farklıdır.

Sekmeli tarayıcılarda açılan oturumlar, sekmelerin kapanmasıyla beraber istemci tarafında silinmezler ve sunucu tarafındaki zaman aşımı süresi kadar istemci tarafında da aktif olmaya devam ederler. Sekmeli tarayıcılardaki oturumlar ancak tarayıcı penceresinin (yani sekmelerinin tümünün) kapanmasıyla veya Web uygulamasının oturumu sonlandırmasıyla silinir. Tarayıcı penceresini kapatmak oturumu sonlandırmak için Web uygulamasına bir istek yollamıyorsa, bu durum genellikle (kayıtlı çerez yoksa) sadece istemci tarafındaki oturumun silinmesiyle sonuçlanır. Sekmeli tarayıcılarda sadece sekmeyi kapatmak ise yine oturumu sonlandırmak için Web uygulamasına bir istek yollamıyorsa hem sunucu hem de istemci tarafındaki oturumun devam etmesiyle sonuçlanır ve sekmeyi kapatan kullanıcı arka planda devam eden oturumu fark edemez. Hem teknik hem de sosyal mühendislik saldırılarına zemin hazırlayan açık ise tam da burada başlamaktır.

Sadece sekmesinin kapatıldığı, sonlandırılmamış bir oturum CSRF (Cross Site Request Forgery – Çapraz Site İstek Sahtekârlığı) veya XSS (Cross Site Scripting – Çapraz Site Komut Çalıştırma) gibi teknik saldırılarda ek saldırı yüzeyi rolü oynayacaktır. Benzer şekilde ortak kullanım alanlarındaki bilgisayarlar için bu açık, sosyal mühendislik saldırılarına zemin oluşturabilir.

Bu tarz saldırılardan kaçınmak için sistem tasarımı uygun olan Web uygulamalarında oturumları sadece tarayıcı pencereleri ile tetiklenerek değil, sekmelerin de tetiklemesiyle sonlandırmak gerekir. Günümüzde birçok bankanın İnternet şubesi, tarayıcı pencerelerinin kapanmasıyla beraber oturumlarını otomatik sonlandırmaktadır. Bu kullanıcının çıkış yapma işlemini unuttuğu durumlar için kabul görmüş bir bilgi güvenliği pratiğidir. Ancak söz konusu aynı uygulamanın bir Pop-up penceresi yerine sekme içinde açılmasına geldiğinde ise durum farklı olmaktadır. Sekme içinde açıldığının farkına varamayan Web uygulaması, oturumunu sekme kapansa dahi zaman aşımı süresi kadar devam ettirmektedir.

Teknik bir saldırı örneği için aşağıdaki adımlar izlendiğinde bu zafiyetin saldırı yüzeyini arttırdığını görmek mümkündür.

Teknik örnek için CSRF ve XSS saldırılarına zafiyeti olan hayali ACME sitesi seçilecektir:

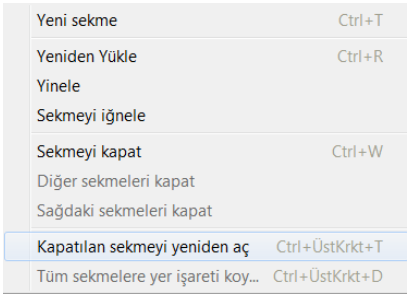
- Kullanıcı sekmeli tarayıcısı ile ACME sitesinde oturum açar,
- Kullanıcı bu oturum dışında birkaç sekme daha açarak başka sayfalarda gezintiye başlar,
- Başka sayfalardaki gezintisi sırasında ilk açtığı ACME sitesinin sekmesini kapatır (çıkış işlemi yapmaz),
- Yeni açtığı sekmelerde saldırgan bir Web sayfasını ziyaret eder,
- Saldırgan Web sayfası, ACME sayfasındaki açığı sömüren bir kod çalıştırmaktadır,
- Saldırgan Web sayfası ACME sitesindeki CSRF ve XSS saldırılarına izin veren açığı sömüren kodu kullanıcı üstünde çalıştırır,
- Oturumu arka planda devam eden kullanıcı saldırıya maruz kalır.

Saldırı senaryolarını çeşitlendirmek mümkündür. Burada bahsi geçen zafiyet, oturumun yönetilmesinden kaynaklıdır. Sekmeli tarayıcılarda açılan oturumların yönetilmesi sırasında kullanıcının çıkış yapmadan sadece sekmeyi kapatacağı senaryolar da göz önünde bulundurulmalıdır.

Teknik olmayan bir sosyal mühendislik senaryosu ise aşağıdaki adımlarla örneklenebilir.

Sosyal mühendislik örneği için yerel güvenlik politikaları ve güvenlik yazılımlarıyla sadece tarayıcı kullanılacak şekilde yapılandırılmış ortak KIOSK tipi bir istemci seçilecektir:

- A kullanıcısı sekmeli tarayıcıda birçok pencere açar ve gezintiye başlar,
- B kullanıcısı bankasının İnternet şubesine girmek ister,
- A kullanıcısı İnternet şubesini açar ve çıkan Pop-up içindeki URL'i sekme içinde açar,
- A kullanıcısı istemciyi B kullanıcısına teslim eder,
- B kullanıcısı A kullanıcısının hazırladığı sekmeden İnternet şubesine giriş yapar,
- B kullanıcısı çıkış işlemi yapmadan sekmeyi kapatır,
- A kullanıcısı "kapatılan sekmeyi yeniden aç" komutuyla oturuma devam eder.




Başta İnternet şubeleri olmak üzere oturum güvenliğini öncelikli bir konu olarak gören Web uygulamaları, penceresi çıkış işlemi yapılmadan kapatılan sayfalar için çıkış işlemini otomatik olarak yapmaktadır. Bu bilgi güvenliği pratiğinin sekmeler için de hayata geçirilmesi saldırı yüzeyini azaltmaya yardımcı olacaktır.

Unutulmaması gereken noktalardan biri de "açık" kavramı ile "saldırı" kavramının farklı iki öğe olduğudur. Açıklar saldırılara olanak sağlayan zayıflıklardır. XSS saldırısı için "HTML karakterlerin filtrelenmemesi" bir açık iken, saldırı yüzeyinin artmasına sebep olan sekmeli tarayıcılardaki bu zayıflık aslında oturum tasarımındaki bir açıktır. Teorik olarak açık ve saldırı arasındaki ilişki bu şekilde olsa da güncel hayatta açıkların olanak verdiği saldırı türleri ile de anıldığı bilinmektedir.

**Konuyla ilgili makaleler:**

- Oturum Açma Sistemleri Tasarımında Güvenlik
  https://www.bilgiguvenligi.gov.tr/siniflandirilmamis/oturum-acma-sistemleri-tasariminda-guvenlik.html
- Oturum Öncesi Tanımlı Oturum Kimliği Çerezi Açığı
  http://www.iosec.org/oturum_oncesi_tanimli_cerez.pdf

Gökhan Muharremoğlu
Bilgi Güvenliği Uzmanı
gokhan.muharremoglu@iosec.org