Testing for Logout Functionality (Lokavt Fonksiyonelliği için Test)

Summary (Özet)

Oturum sonlandırma, oturum yaşam döngüsünün önemli bir parçasıdır. Oturum tokenlerinin
ömrünü minimumda azaltmak, başarılı bir oturum kaçırma saldırısı olasılığını azaltır. Bu, Cross Site Scripting ve Cross Site İstek Sahteciliği gibi diğer saldırıları önlemeye karşı bir kontrol olarak
görülebilir. Bu tür saldırıların, doğrulanmış bir oturuma sahip bir kullanıcıya dayandığı bilinmektedir. Güvenli bir oturum sonu geçirmemek sadece bu saldırıların hiçbirinde saldırı yüzeyini arttırır.

Güvenli bir oturum fesih en azından aşağıdaki bileşenleri gerektirir:

- Kullanıcının manuel olarak çıkış yapmasını sağlayan kullanıcı arayüzü kontrollerinin kullanılabilirliği.
- Aktivite olmadan belirli bir süre sonra seans fesih (oturum zaman aşımı).
- Sunucu tarafı oturum durumunun uygun şekilde geçersiz kılınması.

Bir oturumun etkili bir şekilde sonlandırılmasını önleyebilecek birden fazla konu vardır. İdeal güvenli web uygulaması için, bir kullanıcı kullanıcı arayüzü aracılığıyla herhangi bir zamanda sonlandırabilmelidir. Her sayfa doğrudan görülebildiği bir yerde bir kayıt çıkış düğmesi içermelidir. Belirsiz veya belirsiz günlük fonksiyonları, kullanıcının bu tür işlevlere güvenmemesine neden
olabilir.

Oturum feshindeki bir diğer yaygın hata, istemci tarafı oturum belirtecinin yeni bir değere ayarlanması, sunucu tarafı durumunun aktif kalması ve oturum çerezini önceki değere geri döndürerek yeniden kullanılabilmesidir. Bazen başka bir işlem yapmadan kullanıcıya sadece bir onay mesajı gösterilir. Bundan kaçınılmalıdır.

Bazı web uygulama çerçeveleri, oturum açma kullanıcısını tanımlamak için yalnızca oturum çerezine dayanır. Kullanıcının kimliği (şifreli) çerez değerine gömülüdür. Uygulama sunucusu oturumun sunucu tarafında herhangi bir izleme yapmaz. Çıkış yaparken, oturum çerezi tarayıcıdan
kaldırılır. Ancak, uygulama herhangi bir izleme yapmadığından, bir oturumun kaydedilip kaydedilmediğini bilmez. Bu nedenle, bir oturum çerezini yeniden kullanarak, doğrulanmış oturuma erişim sağlamak mümkündür. Bunun iyi bilinen bir örneği, ASP.NET'teki Formlar Kimlik
Doğrulama işlevselliğidir.

Web tarayıcılarının kullanıcıları genellikle bir uygulamanın hala açık olduğunu ve tarayıcıyı veya bir sekmeyi kapatmasını umursamıyor. Bir web uygulaması bu davranışın farkında olmalı ve belirli bir süre sonra oturumu sunucu tarafında otomatik olarak sonlandırmalıdır.

Uygulamaya özgü bir kimlik doğrulama şeması yerine tek bir oturum açma (SSO) sisteminin kullanılması genellikle ayrı olarak feshedilmesi gereken birden fazla oturumun bir arada yaşamasına neden olur. Örneğin, uygulamaya özel oturumun feshedilmesi, SSO sistemindeki oturumu
sonlandırmaz. SSO portalına geri dönmek, kullanıcıya daha önce günlüğün yapıldığı uygulamaya geri dönme imkanı sunar. Diğer tarafta, bir SSO sistemindeki bir kayıt çıkışı işlevi, bağlantılı uygulamalarda oturum sonlandırmasına neden olmaz.

Test Objectives (Test Hedefleri)

- Logout UI'yi değerlendirin.
- Oturum zaman aşımını analiz edin ve oturumun logouttan sonra düzgün bir şekilde öldürüldüğünü analiz edin.

How to Test (Nasıl Test Edilir)

Testing for Log Out User Interface (Kullanıcı arayüzünü açmak için test)

Kullanıcı arayüzündeki oturum açma işlevselliğinin görünümünü ve görünürlüğünü doğrulayın. Bu amaçla, her sayfayı web uygulamasından çıkış yapma niyeti olan bir kullanıcının bakış açısından görüntüleyin.

> İyi bir kayıt kullanıcı arayüzünü gösteren bazı özellikler vardır:
>
> - Web uygulamasının tüm sayfalarında bir kayıt çıkışı düğmesi bulunur.
> - Kayıt dışı düğmesi, web uygulamasından çıkış yapmak isteyen bir kullanıcı tarafından hızlı bir şekilde tanımlanmalıdır.
> - Bir sayfayı yükledikten sonra, çıkış düğmesi kaydırmadan görünür olmalıdır.
> - İdeal olarak, kayıt çıkış düğmesi, tarayıcının görüntülenmesinde sabit olan ve içeriğin kaydırılmasından etkilenmeyen sayfanın bir alanına yerleştirilir.

Testing for Server-Side Session Termination (Sunucu-Yardöndürme Oturum Sonlandırması için Test)

İlk olarak, bir oturumu tanımlamak için kullanılan çerezlerin değerlerini saklayın. Günlük işlevini çağırın ve özellikle oturum çerezleriyle ilgili olarak uygulamanın davranışını gözlemleyin.
Tarayıcının arka düğmesinin kullanılmasıyla yalnızca doğrulanmış bir oturumda görülebilen bir sayfaya geçmeye çalışın. Sayfanın önbelleğe alınmış bir sürümü görüntülenirse, sayfayı sunucudan yenilemek için yeniden yükleme düğmesini kullanın. Kayıt dışı fonksiyon, oturum çerezlerinin yeni bir değere ayarlanmasına neden oluyorsa, oturum çerezlerinin eski değerini geri yükleyin ve uygulamanın doğrulanmış alanından bir sayfayı yeniden yükleyin. Bu testler belirli bir sayfada herhangi bir güvenlik açığı göstermezse, oturum sonlandırmasının başvurunun bu alanları tarafından uygun şekilde tanınmasını sağlamak için güvenlik açısından kritik olarak kabul edilen başvurunun en azından bir başka sayfasını deneyin.

> Sadece doğrulanmış kullanıcılar tarafından görülebilmesi gereken hiçbir veri, testleri gerçekleştirirken incelenen sayfalarda görülemez. İdeal olarak, uygulama, oturumun

> sonlandırılmasından sonra doğrulanmış alanlara erişirken halka açık bir alana veya formdaki bir kütüğe yönlendirir. Uygulamanın güvenliği için gerekli olmamalıdır, ancak oturum çerezlerini oturum çerezlerini oturum çıkıştan sonra yeni değerlere ayarlamak genellikle iyi bir uygulama olarak kabul edilir.

Testing for Session Timeout (Oturum Zamana Dayanıklılık Testi)

Artan gecikmelerle web uygulamasının doğrulanmış alanında bir sayfaya taleplerde bulunarak bir oturum zaman aşımı belirlemeye çalışın. Kayıt davranışı ortaya çıkarsa, kullanılan gecikme yaklaşık oturum zaman aşımı değeri ile eşleşir.

> Daha önce açıklanan sunucu tarafı oturumu sonlandırma testi ile aynı sonuçlar, bir hareketsizlik zaman aşımından kaynaklanan bir günlük tarafından hariçtir.
>
> Oturum zaman aşımı için uygun değer, uygulamanın amacına bağlıdır ve güvenlik ve kullanılabilirlik dengesi olmalıdır. Bir bankacılık uygulamalarında, aktif olmayan bir oturumun 15 dakikadan fazla tutulmasının bir anlamı yoktur. Öte yandan, bir wiki veya forumda kısa bir süre, isteklerde gereksiz kayıtlarla uzun makaleler yazan kullanıcıları rahatsız edebilir. Bir saat ve daha fazla zaman aşımı kabul edilebilir.

Testing for Session Termination in Single Sign-On Environments (Single Sign-Off) (Tek İşaretli Ortamlarda Oturum Sonlandırması için Test (Tek İşaretli Çıkarma)

Test edilen uygulamada bir günlüğü yapın. Kullanıcının kimlik doğrulama olmadan uygulamaya geri giriş yapmasına izin veren merkezi bir portal veya uygulama dizini varsa doğrulayın. Uygulamanın kullanıcının doğrulanmasını talep edip etmediğini, uygulamaya bir giriş noktasının URL'si istenirse test edin. Test uygulamasında

oturum açarken, SSO sisteminde bir gün ileri kayıt yapın. Daha sonra test edilen uygulamanın doğrulanmış bir alanına erişmeye çalışın.

> Bir SSO sistemine bağlı bir web uygulamasında veya SSO sisteminde bir günlük bırakma işlevinin uygulanmasının tüm oturumların küresel olarak sona ermesine neden olması beklenmektedir. Kullanıcının bir kimlik doğrulaması, SSO sisteminde ve bağlı uygulamada oturum açtıktan sonra uygulamaya erişmesi istenmelidir.

Tools (Araçlar)

- Burp Suite - Tekrarlayan

Referances (Referanslar)

Whitepapers (Beyaz kağıtlar)

- Formlar kimlik doğrulama kullanırken ASP.NET'te çerez tekrarı saldırıları