Testing for Session Fixation (Oturum Çözünürlüğü için test)

Summary (Özet)

Oturum sabitleme, oturum çerezlerinin kimlik doğrulamadan önce ve sonra aynı değerini korumanın güvensiz uygulaması ile etkinleştirilir. Bu genellikle oturum çerezleri, girişten önce devlet bilgilerini
depolamak için kullanıldığında, örneğin, ödeme için kimlik doğrulamadan önce bir alışveriş sepetine ürün eklemek için kullanılır.

Oturum fiksasyon güvenlik açıklarının genel sömürüsünde, bir saldırgan önce kimlik doğrulamadan hedef web sitesinden bir dizi oturum çerezi elde edebilir. Saldırgan daha sonra bu çerezleri farklı teknikler kullanarak kurbanın tarayıcısına zorlayabilir. Kurban daha sonra hedef web sitesinde doğrularsa ve çerezler oturum açma işleminde yenilenmezse, kurban saldırgan tarafından seçilen oturum çerezleriyle tanımlanacaktır. Saldırgan daha sonra bu bilinen kurabiyelerle kurbanı taklit edebiliyor.

Bu sorun, kimlik doğrulama işleminden sonra oturum çerezlerini yenileyerek giderilebilir. Alternatif olarak, oturum çerezlerinin bütünlüğünü sağlayarak saldırı önlenebilir. Ağ saldırganlarını
düşünürken, yani kurbanın kullandığı ağı kontrol eden saldırganlar, tam HSTS kullanın veya ekleyin
`__Host-` / / `__Secure-` Kurabiye adının önyüklenmesine.

Tam HSTS evlat edinme, bir ev sahibi HSTS'yi kendisi ve tüm alt kıyafetleri için etkinleştirdiğinde ortaya çıkar. Bu, Stefano Calzavara, Alvise Rabitti, Alessio Ragazzo ve Michele Bugliesi tarafından *Web Oturumlarında Dürüstlük Kusurları için Test* adı verilen bir makalede anlatılıyor.

Test Objectives (Test Hedefleri)

- Kimlik doğrulama mekanizmasını ve akışını analiz edin.
- Çerezleri zorlayın ve etkiyi değerlendirin.

How to Test (Nasıl Test Edilir)

Bu bölümde, bir sonraki bölümde gösterilecek test stratejisinin bir açıklamasını veriyoruz.

İlk adım, siteye test edilme talebinde bulunmaktır *(*örneğin. `www.example.com`). Test cihazı aşağıdakileri isterse:

```
GET / HTTP/1.1
Host: www.example.com
```

Aşağıdaki yanıtı elde edecekler:

```
HTTP/1.1 200 OK
Date: Wed, 14 Aug 2008 08:45:11 GMT
Server: IBM_HTTP_Server
Set-Cookie: JSESSIONID=0000d8eyYq3L0z2fgq10m4v-rt4:-1; Path=/; secure
Cache-Control: no-cache="set-cookie,set-cookie2"
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=Cp1254
Content-Language: en-US
```

Uygulama yeni bir oturum tanımlayıcısı belirler, `JSESSIONID=0000d8eyYq3L0z2fgq10m4v-rt4:-1` - Müşteri için.

Daha sonra, test cihazı aşağıdaki POST ile uygulamaya başarılı bir şekilde doğrularsa `https://www.example.com/authentication.php` : :

```
POST /authentication.php HTTP/1.1
Host: www.example.com
[...]
Referer: http://www.example.com
Cookie: JSESSIONID=0000d8eyYq3L0z2fgq10m4v-rt4:-1
Content-Type: application/x-www-form-urlencoded
Content-length: 57

Name=Meucci&wpPassword=secret!&wpLoginattempt=Log+in
```

Test cihazı sunucudan aşağıdaki yanıtı gözlemler:

```
HTTP/1.1 200 OK
Date: Thu, 14 Aug 2008 14:52:58 GMT
Server: Apache/2.2.2 (Fedora)
X-Powered-By: PHP/5.1.6
Content-language: en
Cache-Control: private, must-revalidate, max-age=0
X-Content-Encoding: gzip
Content-length: 4090
Connection: close
Content-Type: text/html; charset=UTF-8
...
HTML data
...
```

Başarılı bir kimlik doğrulaması üzerine yeni bir çerez yayınlanmadığı için, test cihazı oturum çerezinin bütünlüğü sağlanmadıkça oturum kaçırmasının mümkün olduğunu bilir.

Test cihazı, bir kullanıcıya (muhtemelen bir sosyal mühendislik hilesi kullanarak) geçerli bir oturum tanımlayıcısı gönderebilir, kimlik doğrulamalarını bekleyebilir ve daha sonra bu çereze ayrıcalıkların
atandığını doğrulayabilir.

Test with Forced Cookies (Zorla Kurabiye ile test)

Bu test stratejisi ağ saldırganlarını hedef alır, bu nedenle yalnızca tam HSTS benimsemesi olmayan sitelere uygulanması gerekir (tüm çerezlerinin bütünlüğü olduğu için tam HSTS benimsenen siteler
güvenlidir). Test altında web sitesinde iki test hesabı olduğunu varsayıyoruz, biri kurban olarak hareket etmek ve biri saldırgan olarak hareket etmek. Saldırganın kurbanın tarayıcısında girişten sonra yeni yayınlanmayan ve bütünlüğe sahip olmayan tüm çerezlerin güçlendirdiği bir senaryoyu simüle ediyoruz. Kurbanın girişinden sonra, saldırgan kurbanın hesabına erişmek için zorla çerezleri web sitesine sunar: Kurban adına hareket etmek için yeterliyse, oturum fiksasyonu mümkündür.

İşte bu testi yürütme adımları:

1. Web sitesinin giriş sayfasına ulaşın.
2. Kabartmadan önce kurabiye kavanozunun bir anlık görüntüsünü kaydedin, içeren çerezler hariç `__Host-` ya da `__Secure-` Onların adına öne çıkın.
3. Mağdur olarak web sitesine giriş yapın ve kimlik doğrulaması gerektiren güvenli bir işlev sunan herhangi bir sayfaya ulaşın.
4. Kurabiye kavanozu 2'de atılan anlık görüntüye ayarlayın.
5. 3. adımda tanımlanan güvenli işlevi tetikleyin.
6. 5 adımdaki operasyonun başarılı bir şekilde gerçekleştirilip gerçekleştirilmediğini gözlemleyin. Eğer öyleyse, saldırı başarılı oldu.
7. Kurabiye kavanozuyu temizleyin, saldırgan olarak giriş yapın ve 3. adımda sayfaya ulaşın.
8. Kurabiye kavanozuna yazın, tek tek, 2. adımda tasarruf edilen kurabiyeler.
9. 3. adımda tanımlanan güvenli işlevi tekrar tetikleyin.
10. Kurabiye kavanozunu temizleyin ve kurban olarak tekrar giriş yapın.
11. 9 adımdaki operasyonun kurbanın hesabında başarılı bir şekilde gerçekleştirilip gerçekleştirilmediğini gözlemleyin. Eğer öyleyse,saldırı başarılı oldu; aksi takdirde, site oturum fiksasyonuna karşı güvenlidir.

Kurban ve saldırgan için iki farklı makine veya tarayıcı kullanmanızı öneririz. Bu, web uygulaması belirli bir çerezden etkinleştirilen erişimi doğrulamak için parmak izi alırsa yanlış pozitiflerin sayısını
azaltmanıza olanak tanır. Test stratejisinin daha kısa ama daha az kesin bir varyantı sadece bir test hesabı gerektirir. Aynı adımları takip ediyor, ancak 6. adımda duruyor.

Remediation (Düzeltme)

Bir kullanıcı başarılı bir şekilde doğruladıktan sonra bir oturum token yenilemesi uygulayın.

Uygulama, bir kullanıcıyı doğrulamadan önce mevcut oturum kimliğini her zaman geçersiz kılmalı ve kimlik doğrulama başarılı ise başka bir oturum ID sağlamalıdır.

Tools (Araçlar)

- OWASP ZAP

Referance (Referanslar)

- Oturum Düzeltme
- ACRO Güvenliği
- Chris Shiflett'ın