Testing for Privilege Escalation (Ayrıcalık Yükseltme Testi)

Summary (Özet)

Bu bölüm, bir aşamadan diğerine artan ayrıcalıklar konusunu açıklar. Bu aşamada, test cihazı, bir kullanıcının ayrıcalıklarını veya rollerini uygulamadaki ayrıcalıklı tırmanma saldırılarına izin verebilecek şekilde değiştirmesinin mümkün olmadığını doğrulamalıdır.

Ayrıcalık artışı, bir kullanıcı normalde izin verilenden daha fazla kaynağa veya işlevselliğe eriştiğinde ortaya çıkar ve bu tür yükselme veya değişiklikler uygulama tarafından engellenmeliydi. Bu genellikle uygulamadaki bir kusurdan kaynaklanır. Sonuç olarak, uygulama geliştirici veya sistem yöneticisi tarafından amaçlananlardan daha fazla ayrıcalıklı eylemler gerçekleştirir.

Esrarengizlik derecesi, saldırganın sahip olmaya ne kadar ayrıcalıklı olduğuna ve başarılı bir istismarda hangi ayrıcalıkların elde edilebileceğine bağlıdır. Örneğin, bir kullanıcının başarılı kimlik
doğrulamadan sonra ekstra ayrıcalık kazanmasını sağlayan bir programlama hatası, tırmanma derecesini sınırlar, çünkü kullanıcı zaten bir miktar ayrıcalık tutma yetkisine sahiptir. Aynı şekilde, herhangi bir kimlik doğrulama olmadan süper kullanıcı ayrıcalığı kazanan bir uzaktan saldırgan daha büyük bir tırmanma derecesi sunar.

Genellikle, insanlar daha *vertical escalation*ayrıcalıklı hesaplara verilen kaynaklara erişmek (örneğin, uygulama için idari ayrıcalıklar edinmek) ve benzer şekilde yapılandırılmış bir hesaba
(örneğin, bir çevrimiçi bankacılık uygulamasında, farklı bir kullanıcıyla ilgili bilgilere erişmek) mümkün olduğunda
yatay tırmanmaya atıfta bulunurlar.

Test Objectives (Test Hedefleri)

- Ayrıcalık manipülasyonu ile ilgili enjeksiyon noktalarını belirleyin.
- Fuzz veya başka türlü güvenlik önlemlerini atlamaya çalışır.

How to Test (Nasıl Test Edilir)

Testing for Role/Privilege Manipulation (Rol/İmtiyaz Manipülasyonunun Test Edilmesi)

Uygulamanın her bölümünde, bir kullanıcının veritabanında bilgi oluşturabileceği (örneğin, bir ödeme yapmak, bir iletişim eklemek veya mesaj göndermek), bilgi (hesap beyanı, sipariş ayrıntıları vb.) alabilir veya bilgileri silebilir (kullanıcıları, mesajları, mesajlar vb.) Alabilir, bu işlevselliği kaydetmek gerekir. Test cihazı, kullanıcının rolü / ayrıcalığı tarafından izin verilmemesi gereken bir işleve erişmenin mümkün olup olmadığını doğrulamak için başka bir kullanıcı gibi işlevlere erişmeye çalışmalıdır (ancak başka bir kullanıcı olarak izin verilebilir).

Manipulation of User Group (Kullanıcı Grubu Manipülasyonu)

Örneğin:
Aşağıdaki HTTP POST, ait olan kullanıcının izin verir
`grp001` Siparişe erişmek için #0001:

```
POST /user/viewOrder.jsp HTTP/1.1
Host: www.example.com
...

groupID=grp001&orderID=0001
```

Ait olmayan bir kullanıcı olup olmadığını doğrulayın `grp001` Parametrelerin değerini değiştirebilir `groupID` ve `orderID` Bu ayrıcalıklı verilere erişmek için.

Manipulation of User Profile (Kullanıcı Profilinin Manipülasyonu)

Örneğin: Aşağıdaki sunucunun cevabı, başarılı bir kimlik doğrulamasından sonra kullanıcıya iade edilen HTML'deki gizli bir alanı gösterir.

```
HTTP/1.1 200 OK
Server: Netscape-Enterprise/6.0
Date: Wed, 1 Apr 2006 13:51:20 GMT
Set-Cookie: USER=aW78ryrGrTWs4MnOd32Fs51yDqp; path=/; domain=www.
example.com
Set-Cookie: SESSION=k+KmKeHXTgDi1J5fT7Zz; path=/; domain= www.exam
ple.com
```

```
Cache-Control: no-cache
Pragma: No-cache
Content-length: 247
Content-Type: text/html
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Connection: close

<form  name="autoriz" method="POST" action = "visual.jsp">
<input type="hidden" name="profile" value="SysAdmin">\

<body onload="document.forms.autoriz.submit()">
</td>
</tr>
```

Ne, test cihazı değişkenin değerini değiştirirse `profile`tot için `SysAdmin`? **Yönetici olmak** mümkün mü?

Manipulation of Condition Value (Koşul Değerinin Manipülasyonu)

Örneğin: Sunucunun, aşağıdaki gibi, bir dizi cevap kodunda belirli bir parametrede bir değer olarak yer alan bir hata mesajı gönderdiği bir ortamda:

```
@0`1`3`3``0`UC`1`Status`OK`SEC`5`1`0`ResultSet`0`PVValid`-1`0`0` Notifications`0
StateExecToolBar`0`0`0`FlagsToolBar`0
```

Sunucu kullanıcıya örtük bir güven verir. Kullanıcının yukarıdaki mesajın oturumu kapatması ile cevap vereceğine inanır.

Bu durumda, parametre değerlerini değiştirerek ayrıcalıkları artırmanın mümkün olmadığını doğrulayın. Bu özel olarak, değiştirerek PVValidDeğerden -1tot için 0(Hata koşulları yok), sunucuya yönetici olarak doğru yapmak mümkün olabilir.

Manipulation of IP Address (IP Adresinin Manipülasyonu)

Bazı web siteleri, erişimin IP adresine dayalı başarısız giriş girişimlerinin sayısını sınırlar veya sayın.

Örneğin:

```
X-Forwarded-For: 8.1.1.1
```

Bu durumda, web sitesi değerini kullanırsa `X-forwarded-For` istemci IP adresi olarak, test cihazı IP değerini değiştirebilir `X-forwarded-For` IP kaynak kimliğinin etrafında çalışmak için HTTP başlığı.

URL Traversal

URL Traversal

Web sitesini geçmeye çalışın ve yetkilendirme kontrolünü kaçırabilecek bazı sayfaların olup olmadığını kontrol edin.

Örneğin:

```
/../.././userInfo.html
```

WhiteBox (BeyazKutu)

URL yetkilendirme kontrolü yalnızca kısmi URL eşleşmesi ile yapılırsa, test cihazlarının veya bilgisayar korsanlarının URL kodlama tekniklerine göre yetkilendirmeyi çözebilmesi muhtemeldir.

Örneğin:

```
startswith(), endswith(), contains(), indexOf()
```

Zayıf SessionD

Zayıf Oturum kimliği algoritmaya sahip, kaba Kuvvet saldırısına karşı savunmasız olabilir. Örneğin, bir web sitesi kullanıyor `MD5(Password + UserID)` Oturumlu olarak. Ardından, testçiler diğer kullanıcılar için oturumID'i tahmin edebilir veya oluşturabilir.

References (Referanslar)

Whitepapers (Beyaz Kağıtlar)

- Wikipedia - Privilege Escalation

Tools (Araçlar)

- OWASP Zed Attack Proxy (ZAP)