1.1.1 Dizin Görüntüleme (Directory Browse) (CWE-548)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Hassas Dosyaların İfşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Bir web uygulama dizin listelemeye izin verdiğinde bu durum kullanıcılara uygulama içerisindeki listelenen klasörleri ve dosyaları denetleme imkanı verir. Dizin listelemeyi aktifleştirmek geliştirici ortamında kabul edilebilir olsa da prod ortamda çoğunlukla kabul edilebilir değildir. Çünkü dizin listeleme sunucuda depolanan veriler veya kaynak kodlar gibi hassas bilgileri içerebilen klasörleri, dosyaları ve dosya adlarını ifşa eder.

Dizin listeleme ifşası ifşa edilen dizinlere göre çeşitli türlerde saldırılara dönüşebilir. Örneğin uygulama yedekleme işlevi veritabanı yedeklerini uygulama kök dizini altında depoluyorsa saldırganlar dizin listeleme ile yedek sql dosysını görüntüleyebilirler, yedek dosyadan web uygulama parolasını elde edebilirler ve web uygulamayı ele geçirerek defacement (“Hacked by Hackers” şeklinde arayüz tahrifi) uygulayabilirler. İfşa edilen klasör ve dosyalara göre bu v.b. çeşitli sayıda saldırı gerçekleştirilebilir.

Bu açıklık ASP.NET web uygulamalar ile örneklenmiştir.

ASP.NET - Web.Config - Güvensiz Kod:

```
 <!-- Güvensiz Yapılandırma -->

<?xml version="1.0" encoding="utf-8" ?>
<configuration>

    <directoryBrowse enable="true"/>
    <!--
        ...
    -->
</configuration>
```

ASP.NET - Web.Config - Güvenli Kod:

```
 <!-- Güvenli Yapılandırma -->

<?xml version="1.0" encoding="utf-8" ?>
<configuration>

    <directoryBrowse enable="false"/>
    <!--
        ...
    -->
</configuration>
```

Kurum web uygulamada “Dizin Görüntüleme (CWE-548)” açıklığı tespit edilmiştir.

::::::::::::::::BULGU::::::::::::::::::::

Açıklığın Önlemi:

Eğer dizin listeleme gerekli değilse kullanımından **daima** kaçınılmalıdır.

Referanslar:

1. http://cwe.mitre.org/data/definitions/548.html