1.1.1 Web Uygulamaya Özel Hata Sayfası Eksikliği (CustomError) (CWE-756)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi İfşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Web uygulamalar 404 Not Found, 400 Bad Request v.b. hata sayfalarında varsayılan hata sayfalarını yansıtmaktadırlar. Bu tarz varsayılan hata sayfalarında uygulamayla alakalı hassas veriler ifşa edilebilmektedir. Bir saldırgan bir istisnayı (exception'ı) kasıtlı olarak tetikleyebilir ve bu yolla uygulama ve sistem hakkında değerli bilgiler elde edebilir. Örn; işletim sistemi türü ve/veya versiyonu, web sunucu yazılımı ismi ve/veya versiyonu, framework ismi ve/veya versiyonu, veritabanı ismi, veritabanı tablosu ismi, veritabanı tablosunun kolon ismi, veritabanı bağlantı string'i (kullanıcı adı ve parola) v.b.

Web uygulamalar kişisel (geliştiricinin oluşturduğu) hata sayfaları tanımlamadıklarında ve kullanmadıklarında "Web Uygulamaya Özel Hata Sayfası Eksikliği (CWE-12)" açıklığı vardır denir. Web uygulamalarda bu açıklık örneğin şöyle örneklenebilir:

ASP.NET - Web.config - Güvensiz Örnek:

```
<!-- GÜVENSİZ YAPILANDIRMA -->

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

        <customErrors mode="Off"/>

        ...
    </system.web>
</configuration>
```

ASP.NET - Web.config - Güvenli Örnek (Alternatif #1):

```
<!-- GÜVENLİ YAPILANDIRMA -->

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

        <!-- Local ve Remote Kullanıcıların Her İkisi İçin -->
        <CustomErrors mode="On" defaultRedirect="global_hata_sayfasi.aspx">

        ...
    </system.web>
</configuration>
```

ASP.NET - Web.config - Güvenli Örnek (Alternatif #2):

```
<!-- GÜVENLİ YAPILANDIRMA -->

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

        <!-- Yalnızca Remote Kullanıcılar İçin -->
         <CustomErrors mode="RemoteOnly"
defaultRedirect="global_hata_sayfasi.aspx">

        ...
    </system.web>
</configuration>
```

Ayar “off” olarak kaldığında hata durumlarında IIS varsayılan hata sayfasını son kullanıcıya dönecektir. Bu güvensiz durumdur. Ayar “on” veya “RemoteOnly” olarak güncellendiğinde ise hata durumlarında “defaultRedirect”teki geliştiricinin belirlediği / tasarladığı uygulamaya has hata sayfası son kullanıcıya dönecektir. Bu güvenli durumdur.

Kurum web uygulamada “Web Uygulamaya Özel Hata Sayfası Eksikliği (CWE-12)” açıklığı tespit edilmiştir.

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

Açıklığın Önlemi:

ASP.NET web uygulamalarda web.config dosyası <system.web> etiketleri arasında şu alternatif iki ayardan biri eklenmelidir ve defaultRedirect özelliğinde belirtilen hata sayfası dosyası oluşturulmalıdır.

Yöntem #1

```
<!-- Local ve Remote Kullanıcıların Her İkisi İçin -->
<CustomErrors mode="On" defaultRedirect="global_hata_sayfasi.aspx">
```

Yöntem #2

```
<!-- Yalnızca Remote Kullanıcılar İçin -->
<CustomErrors mode="RemoteOnly" defaultRedirect="global_hata_sayfasi.aspx">
```

Referanslar:

1. https://cwe.mitre.org/data/definitions/756.html
2. https://cwe.mitre.org/data/definitions/12.html
3. https://www.codeproject.com/Articles/2345/Custom-Errors-in-ASP-NET
4. https://learn.microsoft.com/en-us/archive/msdn-technet-forums/038bf178-1de5-4a95-96e4-f4d90401ad23