1.1.1 X- ile Başlayan Başlıklar Yoluyla Bilgi İfşası (Information Exposure via X- Headers) (CWE-200)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi İfşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

İsimler ve versiyon numaraları sıklıkla belirli bir teknoloji parçasının yaşam döngüsündeki belirli bir noktayı gösterir. Belirli teknolojilerin isimlerinin ve versiyon numaralarının harici kimselere ifşa edilmesi saldırganların bilinen güvenlik açıklıklar ve mevcut zararlılar (exploit'ler) kullanarak sunucuyu nasıl daha iyi hedef tahtasına koyabileceğini öğrenmesine neden olabilir, saldırganların bu belirli teknolojileri araştırabilmelerine ve arzu edilen hedefe uygun yeni exploit'ler geliştirebilmelerine neden olabilir veya saldırganların bu belirli teknolojileri belirli bir konumda not altına alma ve anında saldırmak için bu belirli teknolojilerde yeni bir güvenlik açığının duyurulmasını beklemesi ile sonuçlanabilir. Bu v.b. nedenlerle oluşan riskleri yok etmek için dahili bilgiler ve sistem bilgilerinin ifşasının azaltılması tavsiye edilmektedir.

Bir uygulama yanıt başlıklarında (response headers) sistem bilgisi ifşa edecek şekilde X- ile başlayan başlıklarda yapılandırma ayarına sahip olduğunda "X- ile Başlayan Başlıklar Yoluyla Bilgi İfşası (CWE-200)" açıklığına sahiptir denir. Saldırganlar bu açıklık yoluyla sistem hakkında kendi açılarından değerli bilgiler elde edebilirler. X- başlıklarına örnek olarak

- X-Powered-By,
- X-AspNetMvc-Version,
- X-AspNet-Version,…
- v.b.

verilebilir.

Kurum uygulamada “X- ile Başlayan Başlıklar Yoluyla Bilgi İfşası (CWE-200)” açıklığı olduğu tespit edilmiştir:

:::::BULGU:::::

Açıklığın Önlemi:

Bu açıklığın kapatılabilmesi için tavsiye edilen öneriler şu şekildedir:

- Ortamların ilgili yazılım, işletim sistemi ve diğer kullanılan teknolojilerle ilgili bilgi – örn; isimlerini, versiyonlarını, ayarlarını, … - sızdırmadığından daima emin olun.
- Özellikle IIS ve .NET sunuculardaki başlıklar söz konusu olduğunda web.config dosyası elzemdir. Eğer bir web.config dosyası yoksa sırf bu amaç için oluşturulmak zorundadır.

a) IIS Web Sunucular

IIS sunucularda x-powered-by başlığı şu web.config yapılandırması ile kaldırılabilir:

```
<!-- GÜVENLİ YAPILANDIRMA -->

<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.webServer>
        <security>
            ...
        </security>
        <httpProtocol>
            <customHeaders>
                <remove name="X-Powered-By" />
            </customHeaders>
        </httpProtocol>
    </system.webServer>
</configuration>
```

IIS sunucularda X-AspNetMvc-Version ve X-AspNet-Version başlıkları Global.asax.cs dosyasındaki Application_Start() event’ine şu satır eklenerek kaldırılabilir.

```
MvcHandler.DisableMvcResponseHeader = true;
```

b) Apache Web Sunucular

Apache PHP web sunucularda X-Powered-By başlığını kaldırmak için php.ini dosyası açılmalıdır ve açılan konfigürasyon dosyasındaki expose_php satırı Off yapılmalıdır. Örneğin;

```
> sudo su
> gedit /etc/php5/apache2/php.ini

Çıktı:

      expose_php = Off

> service apache2 restart
```

Referanslar:

1. https://cwe.mitre.org/data/definitions/200.html
2. https://bilisim.io/2018/10/19/nedir-bu-kestrel-web-sunucusu-artisi-eksisi-ve-daha-fazlasi/
3. https://www.zaproxy.org/docs/alerts/10061/
4. https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/
5. https://stackoverflow.com/questions/3418557/how-to-remove-asp-net-mvc-default-http-headers
6. https://ict.ken.be/removing-x-powered-by-aspnet-and-other-version-headers
7. http://ask.xmodulo.com/turn-off-server-signature-apache-web-server.html
8. https://scotthelme.co.uk/hardening-your-http-response-headers/
9.