1.1.1 Link ve Parametre Gizliliğinin Sağlanmaması (Missing Referrer-Policy Header) (CWE-16)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi İfşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Kurum web uygulaması arayüzündeki bir linkten farklı bir web uygulama sunucusuna gidildiğinde kullanıcının mevcut kurum web uygulamasındaki link ve paremetreleri farklı web uygulama sunucusuna Referrer başlığı ile gönderilmektedir. Bu durum Kişisel Verileri Koruma Kanunu'na (KVKK'ya) aykırı bir durum teşkil etmektedir. Çünkü kullanıcının gizli kalması gereken kurum web uygulama bilgileri farklı bir web uygulama sunucusuna gitmektedir ve ifşa olmaktadır.

Kurum web uygulamasında kullanıcıların link ve parametre gizliliğinin korunmadığı (cwe-346) açıklığı tespit edilmiştir.

:::::BULGU:::::

Açıklığın Önlemi:

a) IIS Web Sunucular

IIS sunucularda konfigürasyon dosyası Web.config açılmalıdır ve httpprotocol etiketi içerisindeki customheaders etiketi içerisine gösterilen satır eklenmelidir.

```
<!-- GÜVENLİ YAPILANDIRMA -->

<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <system.webServer>
        <security>
            ...
        </security>
        <httpProtocol>
            <customHeaders>
                <add name="Referrer-Policy" value="no-referrer">
                </add>
            </customHeaders>
        </httpProtocol>
    </system.webServer>
</configuration>
```

b) Apache Web Sunucular

Debian / Ubuntu tabanlı linux işletim sistemlerinde yer alan apache web sunucularda apache2.conf, RedHat / Centos tabanlı linux işletim sistemlerinde yer alan apache web sunucularda httpd.conf dosyası açılmalıdır ve dosya içeriğinin en altına belirtilen satır eklenmelidir.

```
Header set Referrer-Policy "no-referrer"
```

c) Nginx Web Sunucular

Nginx web sunucularda nginx.conf konfigürasyon dosyası açılmalıdır ve dosya içeriğindeki http { ... } bloğu içerisine belirtilen satır eklenmelidir

```
add_header Referrer-Policy "no-referrer";
```

d) Tomcat v.b. Java Web Sunucular

Tomcat gibi hafif java uygulamalarını taşıyabilen servlet container'larda ya da GlashFish, JBoss, WebLogic gibi kompleks java uygulamalarını taşıyabilen servlet container'larda spring framework'ünü kullanan web uygulamalarının src/main/java/hello/ dizininde WebSecurityConfig.java adlı bir dosyasısı bulunur. Bu java dosyasında gösterilen java kod bloğuna "Eklenecek Kodlar Başlıyor" yorum satırı ile "Eklenecek Kodlar Bitti" yorum satırı arasındaki satırlar eklenmelidir:

```
public class WebSecurityConfig extends WebSecurityConfigurerAdapter {
    @Override
    protected void configure(HttpSecurity http) throws Exception {

        // Eklenecek Kodlar Başlıyor

        http
        .headers()
        .referrerPolicy(ReferrerPolicy.SAME_ORIGIN);

        // Eklenecek Kodlar Bitti

    }
}
```

Sonuç

En nihayetinde yapılandırma dosyasında yapılan değişiklik sonrası web sunucusu yazılımı yeniden başlatılmalıdır. Böylelikle kullanıcıların gönderdiği http / https taleplerine karşılık web sunucudan dönen http / https yanıtlarında Referrer-Policy önlemi yer alır duruma gelecektir.

Referanslar:

1. http://www.insiderattack.net/2014/04/configuring-secure-iis-response-headers.html
2. https://www.ryadel.com/en/iis-web-config-secure-http-response-headers-pass-securityheaders-io-scan/
3. https://stackoverflow.com/questions/16385541/content-security-policy-invalid-command
4. https://www.keycdn.com/blog/http-security-headers/
5. https://stackoverflow.com/questions/39502968/apache-difference-between-header-always-set-and-header-set
6. https://scotthelme.co.uk/a-new-security-header-referrer-policy/
7. https://blog.qualys.com/securitylabs/2016/01/07/open-redirection-a-simple-vulnerability-threatens-your-web-applications
8. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3175
9. https://blog.appcanary.com/2017/http-security-headers.html
10. https://www.netsparker.com.tr/blog/web-guvenligi/turkiyede-http-guvenlik-headerlerinin-kullanimi/