1.1.1 Sorgu String'leri Yoluyla Bilgi İfşası (Information Exposure Through Query String) (CWE-598)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi ifşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Web uygulamalarda URL'nin GET parametresi üzerinden hassas bilgi göndermek bu bilgilerin potansiyel olarak şu konumlarda yer almasıyla sonuçlanır:

- son kullanıcı bilgisayarındaki web tarayıcı önbelleğinde (cache'inde),
- son kullanıcı yerel ağındaki proxy sunucusunda,
- hedef web uygulama sunucusundaki access log'larında (erişim log'larında) ve
- hedef web uygulama eğer dış (external) linklere sahipse Referrer http başlığı yoluyla diğer web uygulamaların sunucularındaki access log'larında (erişim log'larında)

Bir saldırgan yukarıdaki konumlardan herhangi birine erişim sağladığında ise hassas bilgileri elde edebilir. Örneğin bir parola bilgisinin URL ile birleştirilmesi yoluyla veya URL'de sorgu parametresi olarak eklenmesi yoluyla GET isteğinde gönderildiğini ele aldığımızda saldırganların yukarıda bahsedilen 4 lokasyona olası başarılı sızma girişimlerinde parola bilgisinin ele geçebileceği söylenebilir.

Örneğin Java dilinde bu açıklığa şöyle bir örnek verilebilir:

Java - Güvensiz Kod Bloğu:

```
// GET Metot Yoluyla Access Token'ı Alma

protected void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {

    PrintWriter out = response.getWriter();

    String temp = request.getParameter("secret_token");

    if (temp==null) {
        out.print("Unauthorized");
    }
    else{
        out.print("<html><body><h1 align='center'>" + new Date().toString() +
"</h1></body></html>");
    }
}
```

Bu örnekte access token (erişim jetonu) hassas bilgisi GET parametresi üzerinden gönderildiğinden GET parametresinin çekilmesi suretiyle kaynak kodda kullanılmaktadır. Bu yaşanan http trafiğinde GET parametresi olan access token (erişim jetonu) hassas bilgisi GET parametresi üzerinden gittiğinden web tarayıcı önbelleğinde, Proxy sunucuda, hedef web uygulama access log'da (erişim log'unda) veya diğer ziyaret edilen web uygulama access log'da kayıtlara düşecektir. Bu ise bir güvenlik riski doğuracaktır. Bu doğan riske "Sorgu String'i Yoluyla Bilgi İfşası (CWE-598)" açıklığı adı verilir. Bu kodun güvenli versiyonu olarak GET yerine POST kullanılması tercih edilmelidir.

Kurum uygulamada "Sorgu String'i Yoluyla Bilgi İfşası (CWE-598)" açıklığı tespit edilmiştir:

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

Açıklığın Önlemi:

Hassas bilgilere örnek olarak;

- Hesap bilgileri (Credentials)
- Oturum veya erişim jetonları (Session or access tokens)
- Kişisel Bilgiler (Personel Information) // Örn; Tel No, Eposta, TC No, v.b.

verilebilir.

Bu hassas bilgiler asla URL'de gönderilmemelidir.

Referanslar:

1. https://cwe.mitre.org/data/definitions/598.html
2. https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/password-transmitted-over-query-string/
3.