1.1.1 Kabuk Hata Mesajı Yoluyla Bilgi Sızıntısı (Information Leak Through Shell Error Message) (CWE-535)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Bilgi İfşası

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Geliştiricilerin bazı zamanlar hata ayıklama veya geçici günlük kaydı tutmak için kullandıkları konsol çıktıları sıklıkla güvenli çıktı akışı açısından yanlış bir tercih olarak öne çıkmaktadır. Konsol çıktıları beklenmeyen çıktı akışlarına yönlendirilebilir. Örneğin konsol çıktısı esas konsola yazdırılabilir, fakat eşzamanlı olarak bir dosyaya da yazdırılabilir (log'lanabilir). Ayrıca konsol içerikleri ve konsol geçmişi başka programlar (process'ler) ile okunabilir. Sonuç olarak bu gibi bir konsol, çıktının ifşa edildiği bir tür olarak değerlendirilmelidir ve hassas veri yazdırılmamalıdır.

Java - Güvensiz Kod Bloğu:

```
protected void doGet(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException
{
    HttpSession session = request.getSession();
    String sessionId = session.getId();
    System.out.println("SessionId: " + sessionId);
}
```

Güvensiz kod bloğunda oturum ID'sinin konsola çıktı olarak yazdırıldığı gösterilmiştir. Bu kullanım tavsiye edilen bir kullanım değildir. Konsola yazdırılan hassas veriler log'lara, hata mesajlarına ve dahasına sızdırılabilir.

Kurum uygulamada Kabuk Hata Mesajı Yoluyla Bilgi Sızıntısı (CWE-535) açıklığı tespit edilmiştir.

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

Açıklığın Önlemi:

Konsola hassas veri yazdırmaktan sakınılmalıdır. Çünkü bir konsolun içerikleri başka bir yere sızdırılabilir.

Referanslar:

1. https://cwe.mitre.org/data/definitions/535.html