1.1.1 iFrame'de Sandbox Kullanılmaması (Client Use of iFrame Without Sandbox) (CWE-829)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: XSS, oltalama ve clickjacking saldırılarına karşı savunmasız kalma

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

iFrame ile güvenilmeyen, uzak bir kaynaktan bir web sayfaya sayfa gömmek genellikle bir mesuliyet gerektirir. Çünkü iframe ile hangi web sayfasına sayfa gömülmüşse o web sayfanın güvenliği harici ve potansiyel olarak güvenilmez bir kaynağa dayandırılmış olur. Bu durum özellikle üçüncü taraf sağlayıcılardan reklamlar göstermek için iframe'ler kullanıldığında yaygınlık teşkil eder. Eğer gömülen kaynağın güvenliği zararlı içerik servis edecek şekilde ihlal olursa bu durumda gömülen sayfa ile beraber esas web uygulama sayfasının da güvenliği olumsuz etkilenir. Bu amaçla iframe'lerde yer alan sandbox özelliği kullanılmalıdır. Sandbox ile iFrame yetenekleri iptal edilebilir veya kısıtlanabilir. Bu şekilde harici içeriği gömerken oluşan risk limitlenmiş olur.

Uzak bir kaynaktan gelen içeriklere sahip, düzgün sandbox uygulanmamış bir iFrame kullanımı Cross-Site Scripting (XSS) ile sonuçlanabilecek zararlı script çalıştırmaya, oltalama saldırılarıyla sonuçlanacak zararlı bir web sitesine yönlendirmeye veya daha fazla işleme izin verebilir. Bir iFrame'de sandbox kullanılmadığında web uygulamada iFrame'de Sandbox Kullanılmaması (CWE-829) açıklığı vardır denir.

Güvensiz ve güvenli iframe kullanımlarına örnekler verilmiştir:

HTML / JS - Güvensiz iFrame:

```
<!-- GÜVENSİZ IFRAME -->

<iframe src="https://untrusted.example.com/content.html"></iframe>
```

HTML / JS - Güvenli iFrame:

```
<!-- GÜVENLİ IFRAME -->

<iframe src="https://untrusted.example.com/content.html" sandbox ></iframe>
```

Kurum web uygulamada iFrame'de Sandbox Kullanılmaması (CWE-829) açıklığı tespit edilmiştir:

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

Şekil XXX. iFrame'de Sandbox Kullanılmaması

Açıklığın Önlemi:

Bu açıklığı kapamak için tavsiye edilen öneriler şu şekildedir:

- Web sayfada uzak içerik dahil etme ihtiyacını gözden geçirin ve mümkün olan yerlerde bu fonksiyonelliği saldırı yüzeyini azaltmak için kaldırın.
- İframe'ler uzak bir içeriği görüntülemek için kullanıldığında daima sandbox ile denetim altına alın.
- Uzak güvensiz kaynaklardan gelebilecek script'lerin çalışmasına izin vermekten kaçının.

Güvensiz iFrame kullanımı zafiyeti iFrame'e sandbox özelliği konularak kapatılır. Sandbox özelliği konulduğunda iframe'in getirdiği içeriğe verilen izinler tamamen kapatılmış olur. Sandbox'a konulacak belirli izinler ile de iframe'in getirdiği içerik kontrollü şekilde uygulamada çalışır.

iframe'in getirdiği içeriğe verdiği tüm izinleri kapatmak için sandbox gösterildiği gibi kullanılmalıdır:

```
<iframe sandbox src="framed-page-url"></iframe>
```

Şekil XXX. Güvenli iFrame

Böylece üçüncü taraf konumdan gelen içeriğin tüm izinleri kapatılmış olur. iframe'in getirdiği içeriğe belirli izinler vermek için ise sandbox özelliğine gösterilen şu değerler konulabilir:

Sandbox Argümanları	Açıklamalar
allow-top-navigate	iframe içerisindeki içeriğin parent'ına gitme iznini verir.
allow-forms	iframe içerisinde form varsa submit'lenmesi iznini verir.

Sandbox Argümanları	Açıklamalar
allow-popups	iframe içerisinden popup fırlatılabilmesi iznini verir.
allow-scripts	iframe içerisindeki javascript kodlarının çalışabilmesi iznini verir (ancak halen popup oluşturulmasına izin vermez)

Tablo XXX. iFrame Sandbox Tanımlanabilen İzinler

Bu şekildeki güvenlik seviyesi ayarlı örnek bir kullanım verilmiştir:

```
<iframe sandbox="allow-scripts  allow-popups" src="framed-page-url"></iframe>
```

Şekil XXX. iFrame'de Çeşitli İzinlerin Verildiği Sandbox Kullanılması

Bu örnek kullanım ile iframe'in getirdiği içeriğe kendi içindeki javascript kodlarını çalıştırma izni ve ayrıca popup çıkarabilme izni verilmektedir. Kurum web uygulama geliştiricileri de kullandıkları iframe'lerin ihtiyaç duydukları izinlerini tespit edip sandbox ile sadece o izinleri vererek iframe'lerini kullanmalıdırlar. Böylece iframe ile gelen içeriği kontrollü bir şekilde uygulamalarında çalıştırmış olacaklardır.

Referanslar:

1. http://cwe.mitre.org/data/definitions/829.html
2. https://www.html5rocks.com/en/tutorials/security/sandboxed-iframes/
3. https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-frame-external/