Insecure Frame Usage (External)

a. Insecure Frame Usage (External) Nedir?

Insecure Frame Usage (External) zafiyeti harici bir içeriğin iframe ile güvensiz bir şekilde web uygulamasına yerleştirilmesine denir.

b. Insecure Frame Usage zafiyeti nasıl kapatılır?

Insecure Frame Usage zafiyeti iFrame'e sandbox attribute'unu koyarak kapatılır. Sandbox attribute'u konulduğunda iframe'in getirdiği içeriğe verdiği izinler tamamen kapatılmış olur. Sandbox'a konulacak izinler ile de iframe getirdiği içeriğe belirli izinler verebilir.

iframe'in getirdiği içeriğe verdiği tüm izinleri kapatmak için sandbox şu şekilde kullanılır:

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

Böylece üçüncü parti konumdan gelen içeriğin tüm izinleri engellenmiş olur. iframe'in getirdiği içeriğe izinler vermek için ise sandbox attribute'una aşağıdaki değerler konabilir:

allow-top-navigate	:	iframe içerisindeki içeriğin parent'ına gitme iznini verir.
allow-forms	:	iframe içerisinde form varsa submit'lenmesi iznini verir.
allow-popups	:	iframe içerisinden popup fırlatılabilmesi iznini verir.
allow-scripts	:	iframe içerisindeki javascript kodlarının çalışabilmesi iznini verir (ancak halen popup oluşturulmasına izin vermez)

Örn;

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

Böylece iframe'in getirdiği içeriğe kendi içindeki javascript kodlarını çalıştırma izni ve ayrıca popup çıkarabilme izni vermiş olduk.

Sonuç olarak web uygulamamızdaki iframe üçüncü parti konumdan bir içerik getirmektedir. Üçüncü parti konum ise hack'lenirse iframe güvenilmez bir içerik getirebilir ve web uygulamamız bu durumdan etkilenebilir. Dolayısıyla iframe güvensiz kullanıldığında web uygulamamız üçüncü parti konumun güvenliğine bağımlı hale gelecektir ve üçüncü parti konum düştüğünde bizim web uygulamamız da düşecektir. Bu nedenle web uygulamamızdaki iframe tag'ı ve getirdiği içerik sandbox attribute'u ile izin denetimi altına alınmalıdır.

Ekstra

Twittter'ın tweet butonu bir iframe'dir:

```
<iframe src="https://platform.twitter.com/widgets/tweet_button.html" style="border: 0; width:130px; height:20px;"></iframe>
```

Bu tweet butonu çeşitli web sitelerine konulur ve basıldığında submit'leme işlemi yapar, bazı javascript kodları çalıştırır ve bir de popup çıkarır. Dolayısıyla principle of least privilege (yani en az izin verme prosedürünü) uygulayacak olursak biz bu iframe'in tüm izinlerini kapatıp sadece submit'leme, javascript kodu çalıştırma ve popup çıkarabilme izinlerini vermemiz gerekir.

```
<iframe sandbox="allow-forms allow-scripts allow-popups allow-same-origin" src="https://platform.twitter.com/widgets/tweet_button.html" style="border: 0; width:130px; height:20px;"></iframe>
```

Not: allow-same-origin ile twitter sunucusu dışında başka sunuculara bağlantı isteği gönderme ve alma demiş oluyoruz. Yani XmlHttpRequest ve XmlHttpResponse sadece twitter sunucusuyla yapılabilsin demiş oluyoruz.

Böylece en az izinleri vererek güvenli bir iframe kullanımı görmüş olduk.

Kaynaklar

https://www.netsparker.com/web-vulnerability-scanner/vulnerability-security-checks-index/insecure-frame-external/

https://www.html5rocks.com/en/tutorials/security/sandboxed-iframes/

https://www.w3schools.com/TagS/att_iframe_sandbox.asp