1.1.1 Güvensiz Target Blank Kullanılması (Unsafe Use of Target Blank) (CWE-1022)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Oltalama saldırılarıyla karşı karşıya kalma

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Web uygulamalarda html'deki <a> etiketi target="_blank" ile kullanıldığında link tıklaması sonucu açılan sayfa yeni sekmede açılır. Fakat target="_blank" ile açılan sayfalar bir önceki sayfanın window opener nesnesini düzenleyebilme yetkisine sahip olduklarından yeni sayfa javascript kodlaması ile bir önceki sekmedeki sayfanın window.opener nesnesini manipüle edebilir ve bir önceki sekmedeki sayfayı başka bir sayfaya yönlendirebilir. Böylece kurban yan sekmede görüntülediği sayfadan bir önceki sekmedeki sayfaya geri döndüğünde belki de mevcut orijinal sayfanın birebir kopyası bir başka siteyi (oltalama sitesini) görüntüleyebilir ve kullanıcı adı, şifre gibi hassas bilgilerini kandırılma neticesinde yönlendirildiği sayfaya kaptırabilir.

Bu açıklığı göstermek adına ilgili dillerde güvensiz kod blokları ve güvenli halleri verilmiştir:

HTML Güvensiz Kod Bloğu:

```
<a href="untrustedURL" target="_blank">Link 1</a>
```

HTML Güvenli Kod Bloğu:

```
<a href="untrustedURL" target="_blank" rel="noopener noreferrer">Link 1</a>
```

Bu açıklığın görüldüğü en yaygın iki yoldan birincisi html'de <a> etiketinin target="_blank" ile kullanılması şeklindedir. Bu kullanımda saldırganlarca yeni sekmeden önceki sekmenin oltalama sayfasına yönlendirilmesi sağlanabilir. Bunu önlemek için <a> etiketine rel attribute (özellik) ve değeri eklenerek bu açıklık kapatılmalıdır. Böylece ikinci sekme ilk sekmeyi olası saldırı durumunda yönlendiremez.

Javascript Güvensiz Kod Bloğu - 1:

```
// Güvensiz Window.Open() Kullanılması

function newWindowOpener(untrustedURL) {
    var newWindow=window.open(untrustedURL, "_blank");
}
```

Javascript Güvenli Kod Bloğu - 1:

```
// Güvenli Window.Open() Kullanılması

function newWindowOpenerSafe(untrustedURL) {
    var newWindow=window.open(untrustedURL, "_blank");
    newWindow.opener=null;
}
```

Bu açıklığın görüldüğü en yaygın iki yoldan ikincisi window.open() javascript metodunun target attribute'u (özelliği) _blank şeklinde ayarlanarak çağırılmasıdır. Bu kullanımda saldırganlarca yeni sekmeden önceki sekmenin oltalama sayfasına yönlendirilmesi sağlanabilir. Bunu önlemek için window.open() javascript metodu çağırıldıktan sonra opener nesnesi null'lanarak bu açıklık kapatılmalıdır. Böylece ikinci sekme ilk sekmeyi olası saldırı durumunda yönlendiremez.

Javascript Güvensiz Kod Bloğu - 2:

```
// Güvensiz Window.Open() Kullanılması

function newWindowOpener(untrustedURL) {
    var newWindow=window.open();
    newWindow.location=untrustedURL;
}
```

Javascript Güvenli Kod Bloğu - 2:

```
// Güvenli Window.Open() Kullanılması

function newWindowOpenerSafe(untrustedURL) {
    var newWindow=window.open();
    newWindow.opener=null;
    newWindow.location=untrustedURL;
}
```

Bu açıklığın görüldüğü bir başka yol da window.open() javascript metodunun çağırılması sonrası sayfayı yönlendirmedir. Bu kullanımda da saldırganlarca yeni sekmeden önceki sekmenin oltalama sayfasına yönlendirilmesi sağlanabilir. Bunu önlemek için window.open() javascript metodu çağırıldıktan sonra opener nesnesi null'lanarak bu açıklık kapatılmalıdır. Böylece ikinci sekme ilk sekmeyi olası saldırı durumunda yönlendiremez.

Kurum web uygulamada güvensiz / tehlikeli link kullanımları tespit edilmiştir:

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

Bulgularda gösterildiği üzere kurum web uygulamasında yer alan linkler target="_blank" ile kullanılmışlardır. Dışarıya target="_blank" ile götüren linkler güvenilir web sunucularına götürüyorlar olarak kabul edilse bile gidilen yeni sekmedeki üçüncü taraf web sitelerin hack'lenebileceği (ele geçirilebileceği) ve kaynak kodlarına zararlı javascript kodlarının eklenebileceği, böylece kurum web uygulaması takipçisi kullanıcıların olası ciddi bir sosyal mühendislik saldırısına maruz kalabileceği göz önünde bulundurulmalıdır.

Açıklığın Önlemi:

Bu açıklığı kapatmanın yolu genel manasıyla şu şekildedir:

HTML Tarafında;

- Gerekmedikçe kullanıcılar için oluşturulan linklerde target attribute'unu (özelliğini) - herhangi bir değerle - kullanmayın.
- Eğer gerekiyorsa target attribute'una (özelliğine) ek olarak rel attribute'unu (özelliğini) "noopener noreferrer" değeriyle beraber ekleyin.
    - "noopener" değeri Chrome ve Opera web tarayıcıları içindir.
    - "noreferrer" değeri Firefox ve eski web tarayıcılar içindir.
    - Safari web tarayıcılar için benzer bir çözüm yoktur.

Javascript Tarafında;

- "var newWindow = windows.open()" ile güvenilmeyen bir yeni pencere / sekme çağıracakken "newWindow.location"a potansiyel olarak güvenilmeyen yeni pencereyi / sekmeyi atamadan önce "newWindow.opener=null" ataması yapılmalıdır. Böylece yeni site yeni pencerede / sekmede açıldığında bu pencerenin / sekmenin bir önceki sayfadaki "opener" attribute'una erişimi olmayacaktır ve oltalama yönlendirmesi yapılamayacaktır.

Referanslar:

1. https://www.netsparker.com/web-vulnerability-scanner/vulnerability-security-checks-index/phishing-by-navigating-browser-tabs/
2. https://cwe.mitre.org/data/definitions/1022.html