**Bilgi Sistemleri ve Güvenliği**

**170541052**

**-**

**Muhammed Talha BAYSAL**

**Tarayıcı Sekmelerinde Gezinerek Oltalama**

**(Tabnabbing)**



Netsparker, olası bir tarayıcı sekmelerinde gezinerek oltalama saldırısı belirledi.

Target="\_blank" etiketli normal href'lere sahip açık pencereler, window.opener.location'ı değiştirebilir ve ana web sayfasını farklı bir kaynakta bile olsa başka bir şeyle değiştirebilir.

**TANIM**

Tabnabbing, 2010'dan bu yana denenmiş ve gerçek kimlik avı biçimlerinden biri olmuştur. Saldırgan, birçok insanın meşgul olduğu ve tarayıcılarında açtıkları sekmelere dikkat etmediği gerçeğinden yararlanır. Siber suçlunun güvenilir web sitesi görünümlerini taklit etme yeteneği, kullanıcının kimlik bilgilerini girebilmesi için bir web sayfası gibi görünmelerine olanak tanır. Tabnabbing adı, bir güvenlik araştırmacısı ve tasarım uzmanı Aza Raskin tarafından oluşturulmuştur.

**ETKİ**

Bu güvenlik açığı, komut dosyası yürütülmesine izin vermese de, üst sekmenin sessizce yerini alan oltalama saldırılarına izin verir. Eğer bağlantılar rel=”noopener noreferrer” özelliğinden yoksunsa, üçüncü taraf bir site window.opener.location.assign kullanarak kaynak sekmenin URL’sini değiştirebilir. Bu sayede kullanıcıları hala güvenli bir sitede oldukları yönünde kandırabilir ve hassas verilerini kötü amaçlı websitesine girmelerine sebep olabilir.

**ÇÖZÜM**

* Sayfaların window.opener'ı kötüye kullanmasını önlemek için bağlantılara rel=noopener ekleyin. Bu, sayfanın Chrome ve Opera tarayıcılarında window.opener özelliğine erişememesini sağlar.
* Daha eski tarayıcılar ve Firefox'ta, Referer başlığını ek olarak devre dışı bırakan rel=noreferrer ekleyebilirsiniz.

