Phishing By Navigating Browser Tabs

Normalde <a> tag'ı target="_blank" ile kullanıldığında bir başka sayfaya sıçrarırız. Fakat target="_blank" ile sıçradığımız sayfalar parent sayfanın window.open nesnesini düzenleyebilme yetkisine sahip olduklarından sıçradığımz sayfa javascript kodlaması ile window.open nesnesini manipule edebilir ve parent sayfayı başka bir sayfaya yönlendirebilir. Böylece kurban parent sayfaya döndüğünde belki de orijinal sayfanın birebir kopyası bir başka sayfayı görüntüleyeceğinden kullanıcı adı, şifre gibi bilgilerini sayfaya verebilir ve hassas bilgilerini böylece kaptırabilir. Bu saldırı türüne phishing with navigating Browsers tabs adı verilmektedir.

Uygulama // Birebir denenmiştir ve başarıyla uygulanmıştır.

Phising By Navigating Browsers Tabs saldırısını localhost'umuzda deneyelim. Öncelikle bu saldırı için bir klasör oluşturalım.

/var/www/Phising By Navigating Browsers Tabs Uygulaması

Ardından içine mevcut sayfa ve temsilen hack yemiş üçüncü parti bir sunucunun sayfasını koyalım.

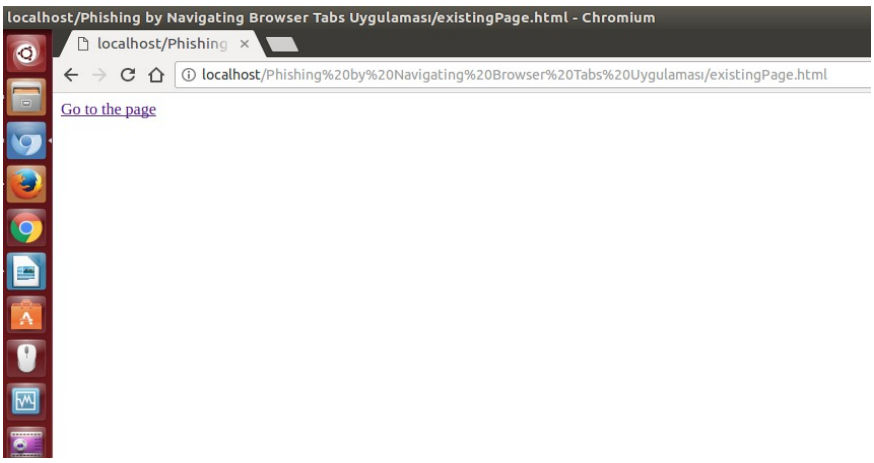
existingPage.html
attackingPage.html

Şimdi mevcut sayfa üçüncü parti sunucunun sayfasına bir link versin.

existingPage.html

```
<a href="attackingPage.html" target="_blank">Go to the page</a>
```

Output:

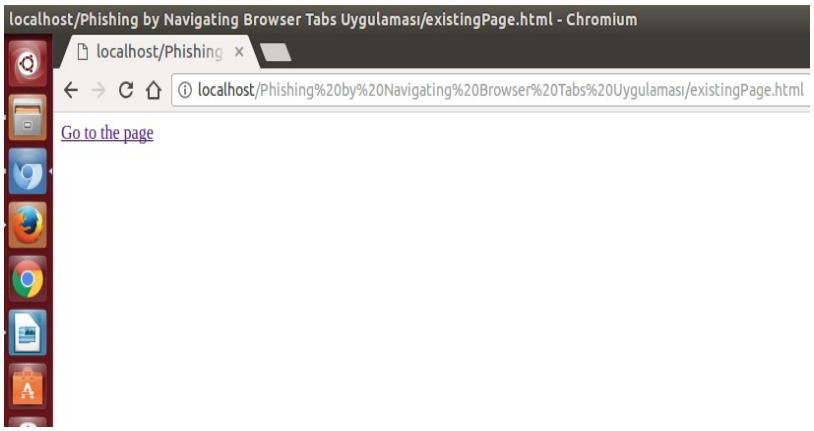


Ardından üçüncü parti sunucu hack yemiş olsun ve saldırgan ilgili sayfaya aşağıdaki javascript kodlarını gömmüş olsun.

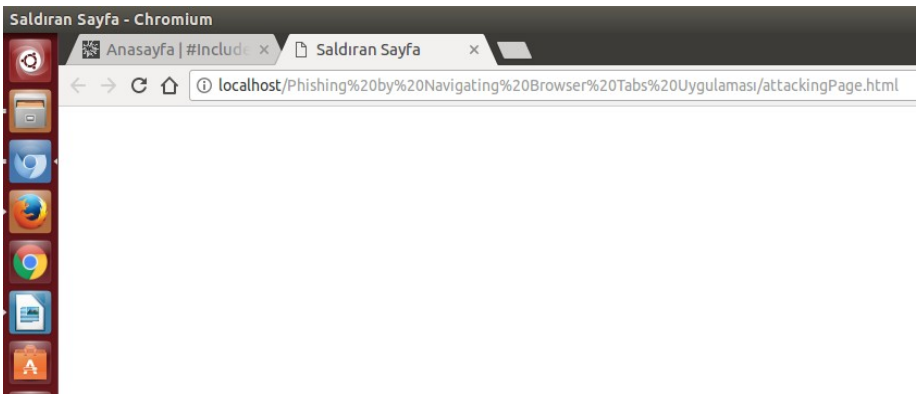
attackingPage.html

```
<html>
  <head>

      <meta charset="UTF-8" />
      <title>Saldıran Sayfa</title>

  </head>
  <body>

      // Üçüncü parti sunucunun normal web sayfa kodları
      // …....
      // …....


      // Saldırganın üçüncü parti sunucudaki sayfaya yerleştirdiği zararlı kodlar

      <script>
          new_page = 'http://www.includekarabuk.com';
          window.opener.location = new_page
      </script>

</body>
</html>
```

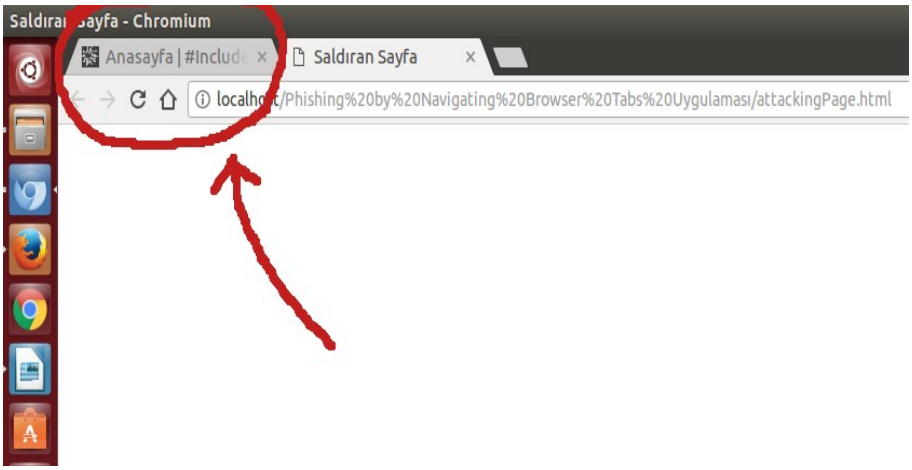
Üçüncü parti sunucudaki web sayfasının <script> tag'ları arasında görüldüğü üzere window.opener nesnesine (yani target="_blank" ile gelindiği için parent'ın window.opener nesnesine) bir url adresi atanmaktadır. Bu atama ile parent sayfa bir anda atanan url adresine gidecektir.



(Parent sayfada linke tıklanır ve yeni sayfaya gidilir)



(Yeni sayfa açılır)



(Parent sayfa belirlenen url'ye otomatikmen gider)

Böylece kurban mevcut sekmede yeni bir sayfayla karşılaşacaktır ve bu sayfa önceki mevcut sayfanın birebir klonu olursa kurban olası bir phishing saldırısına maruz kalacaktır.

Phishing By Navigating Browser Tabs Nasıl Engellenir?

Web uygulamalarında kullanıcıların bu saldırıya maruz kalmamaları için geliştiriciler target="_blank" kullanan linklere rel attribute'unu aşağıdaki gibi koymalıdırlar.

```
<a href="url-address" target="_blank" rel="noopener noreferrer"> some strings </a>
```

noopener : window.opener'ı Chrome 49 ve Opera 36'da null'lar.
noreferrer : window.opener'ı eski tarayıcılarda ve Firefox'da null'lar. Ayrıca http referrer header'ının gönderimini engeller.

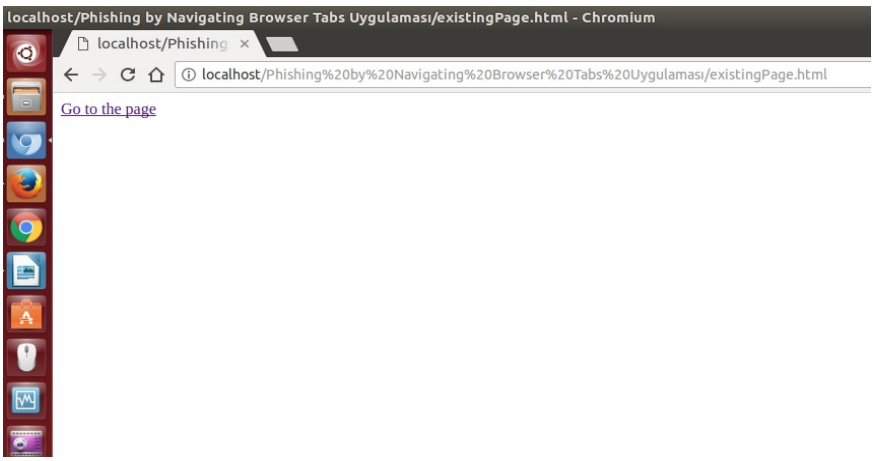
noopener phishing by navigating browser tabs saldırısını önler. noreferrer ise eski tarayıcılarda ve Firefox'da phishing by navigating browser tabs saldırısını önler, ayrıca gidilen sayfaya Referrer header'ının gönderimini engeller. Bu şekilde koyulduğu takdirde sıçranılan üçüncü parti sayfa parent'ın window_opener nesnesini manipule edemeyecektir ve mevcut sayfa farklı sayfalara yönlendirilemeyecektir.

Bunu test etmek için az önce uygulamada yaptığımız sayfaya ilgili rel attribute'unu koyalım ve aynı saldırı işe yaracak mı test edelim.

existingPage.html

```
<a href="attackingPage.html" target="_blank" rel="noopener noreferrer">Go to the page</a>
```

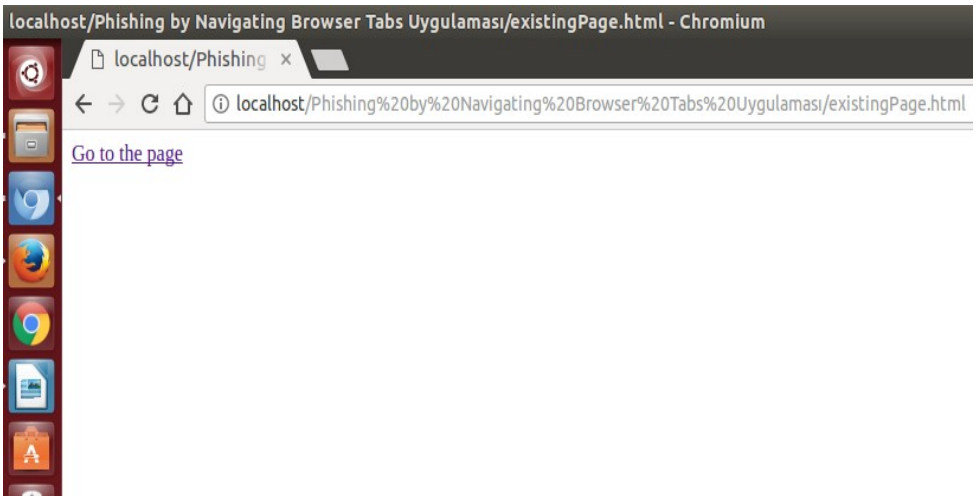
Output:



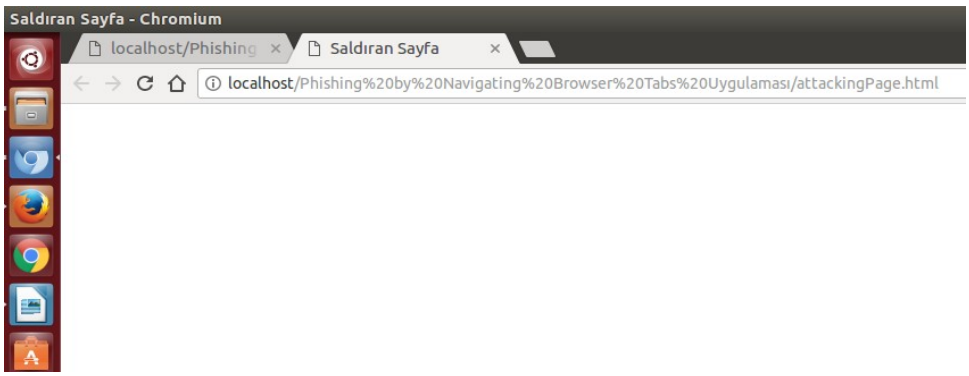
attackingPage.html (Aynı kodlar olduğu gibi kalır)

```
<html>
  <head>

      <meta charset="UTF-8" />
      <title>Saldıran Sayfa</title>

  </head>
  <body>

      // Üçüncü parti sunucunun normal web sayfa kodları
      // …....
      // …....


      // Saldırganın üçüncü parti sunucudaki sayfaya yerleştirdiği zararlı kodlar

      <script>
          new_page = 'http://www.includekarabuk.com';
          window.opener.location = new_page
      </script>

</body>
</html>
```

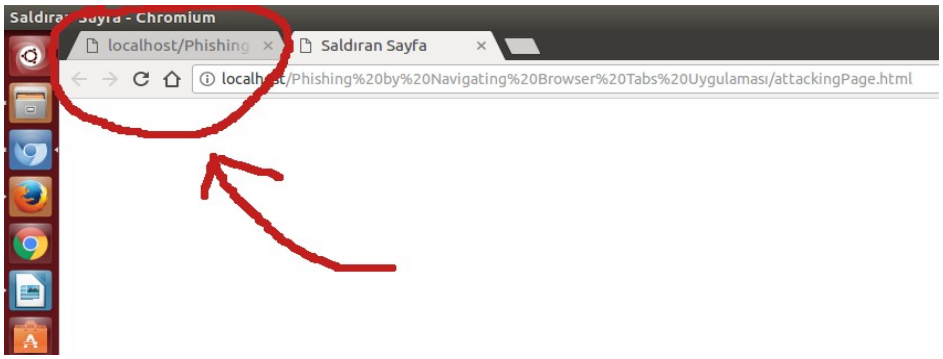
Ardından mevcut sayfada linke tıklanır.



(Parent sayfada linke tıklarız ve üçüncü parti sayfaya sıçrarız)



(Yeni sayfa çalışır)



(Mevcut sayfa aynı kalır)

Görüldüğü üzere *rel="noopener noreferrer"* attribute'u ile mevcut sayfanın window.opener nesnesini manipule edilemez kıldık. Böylece sıçradığımız sayfa manipulasyon işlemini denese de başaramamıştır ve mevcut sayfa olduğu gibi kalmıştır. Sonuç olarak web uygulamamızda üçüncü parti sunuculara <a target="_blank"> ile link veriyorsak üçüncü parti sunucunun hack yiyebileceğini göz önünde bulundurarak oradan gelebilecek olası window.opener manipulasyonlarına karşı <a> tag'ımızda *rel="noopener noreferrer"* attribute'unu kullanmamız gerekir. Böylece kullanıcılar web uygulamamızdan üçüncü parti sunucuya sıçradıklarında üçüncü parti sunucu window.opener nesnesini manipule etme girişiminde bulunsa dahi başaramayacaktır ve web uygulamamızın mevcut sayfasının olası bir phishing sayfasına yönlenmesini engellemiş olacağız.

Web Tarayıcılarda Güncellemeler ile Kapatılan Phishing By Navigating Browser Tabs Açıklığı

(+) Eski versiyon web tarayıcılar Windows 10 işletim sisteminde indirilerek birebir denenmiştir ve başarıyla uygulanmıştır.

Web tarayıcıların güncel son sürümlerinde mimarilerindeki hatadan kaynaklı Phishing By Navigating Browser Tabs açıklığı kapatılmıştır. Ancak önceki sürümlerinde açıklık var olduğundan önceki sürümlerinde sömürülebilmektedir.

Firefox, Chrome, Opera, …. gibi tarayıcılar kendiliğinden otomatik son sürüme güncelleme yapmaktadırlar. Bu noktada son sürüme otomatik güncellenen popüler web tarayıcı kullanıcıları açıklıktan etkilenmeyeceklerdir. Ancak eski işletim sistemlerini kullanan kullanıcılar (örn; eski mac os veya linux) sistem repository'lerinden (depolarından / marketlerinden) popüler web tarayıcılarının o sisteme özgü versiyonlarını (eski sürümlerini) indireceklerinden ve kullanacaklarından açıklıktan etkileneceklerdir. Ayrıca windows sistem güncelleştirmelerini tamamlamayan kullanıcılar Edge web tarayıcının güncel olmayan halini kullanacaklarından açıklıktan etkileneceklerdir.

> Bilgi:
>
> Eski işletim sistemlerine örnek vermek gerekirse örneğin bir linux dağıtımı Ubuntu 14.04 LTS uzun dönem destek süresi bitmiş durumdadır, ancak hatırı sayılır kullanıcısı sistemdeki varlığını uygulamaları, yerleşik düzeni, bağımlılıkları nedeniyle sürdürebilir. Dolayısıyla bu v.b. eski işletim sistemlerinde kalmış kullanıcılar popüler web tarayıcılarının eski sürümlerini (ilgili o dağıtıma özgü sürümlerini) kullanacaklarından açıklıktan etkilenebilir halde kalacaklardır.

Aşağıda popüler web tarayıcıların hangi sürümüne kadar Phishing By Navigating Browser Tabs uygulaması yapılabiliyor (açıklığı sömürülebiliyor) bilgisi web tarayıcıların eski sürümleri açıklık sömürülemeyene kadar indirilmek suretiyle deneme yanılma ile test edilerek not edilmiştir.

a) Firefox

Firefox tarayıcılarda 78.9 ESR versiyonuna (23 Mart 2021 tarihli sürüme) kadar bu açıklık uygulaması çalışmaktadır. 79 ve yukarısı sürümlerde bu açıklık firefox web tarayıcıda kapatılmıştır.

> Eski Mozilla Firefox Setup'ları İçin;
>
> https://ftp.mozilla.org/pub/firefox/releases/
>
> Uyarı;
>
> Firefox Hakkında sayfasına gidildiğinde otomatik son sürüme güncelleme test edilmekte ve son sürüme güncelleme olmakta. Bu nedenle Firefox 78.9 ESR sürümde hakkında sayfasına gidilmeden Phishing By Navigating Browser Tabs uygulaması çalıştırılmıştır ve çalışmıştır. 79 ve yukarısında ise açıklığın kapatıldığı görülmüştür.

b) Opera

Opera tarayıcılarda 73.0 versiyonuna (9 Aralık 2020 tarihli sürüme) kadar bu açıklık uygulaması

çalışmaktadır. 74.0 ve yukarısı sürümlerde bu açıklık opera web tarayıcıda kapatılmıştır.

Eski Opera Setup'ları İçin;

https://get.opera.com/ftp/pub/opera/desktop/

Uyarı;

Opera tarayıcılarda Hakkında sayfasına gidildiğinde otomatik son sürüme güncelleme test edilmekte ve son sürüme güncelleme olmakta. Bu nedenle Opera 73.0 sürümde hakkında sayfasına gidilmeden Phishing By Navigating Browser Tabs uygulaması çalıştırılmıştır ve çalışmıştır. 74.0'de ve yukarısında açıklığın ise kapatıldığı görülmüştür.

c) Chromium

Chromium tarayıcılarda 88.0.4306 versiyonuna (27 Ekim 2020 tarihli sürüme) kadar bu açıklık uygulaması çalışmaktadır. 88.0.4323 ve yukarısı sürümlerde bu açıklık chromium web tarayıcıda kapatılmıştır.

Eski Chromium Setup'ları İçin;

https://chromium.tr.uptodown.com/windows/versions

d) Chrome

Chrome tarayıcılarda tahmini olarak 84.0.4147 versiyonuna (14 Temmuz 2020 tarihli sürüme) kadar bu açıklık uygulaması çalışmaktadır. Chrome tarayıcılar eski sürümlerini güvenlik gereği servis etmemektedir. Daima en son sürüm indirilebilmektedir. Bu nedenle test icabı linux dağıtımı Ubuntu 18.04 LTS'de yüklü eski chrome versiyonu 84.0.4147'ye bakıldığında (14 Temmuz 2020 tarihli sürüme) açıklığın halen çalıştığı gözlemlendi. Dolayısıyla bu sürüm dolaylarına kadar bu açıklık çalışmakta denebilir. Ancak güncel son sürümlerde (örn; şu an ki 2 Mart 2021 tarihli son sürüm chrome 89.0.4389'da) bu açıklık chrome web tarayıcıda kapatılmıştır.

e) Edge

Edge tarayıcılarda bu açıklık windows 10 güncelleştirmeleri tam olana kadar açıktır. Windows 10 güncelleştirmeleri ile edge web tarayıcılarda bu açıklık kapatılmıştır.

Bilgi:

VMWare Workstation'da sıfır kurulum windows 10 kurulmuştur ve Edge tarayıcısında Phishing By Navigating Browser Tabs uygulaması çalışmıştır. Ancak tüm güncelleştirmelerin yüklü olduğu ana makinedeki Windows 10'da Edge tarayıcısında Phishing By Navigating Browser Tabs uygulaması çalışmamıştır. Dolayısıyla windows 10 güncelleştirmeleri tam olduğunda Edge taraycısındaki bu açıklık kapalıdır.

e) Internet Explorer

Internet Explorer tarayıcılar Windows 10'da halen bu açıklığa sahiptirler. Sadece açıklığın sömürülebilmesi için yan sekmeye atlanıldığında "*Internet Explorer bu web sayfasının komut dosyası veya ActiveX denetimi çalıştırmasını kısıtladı.*" durum çubuğuna "*Engellenen içeriğe izin ver*" onayı vermek gerekiyor. Böylece mevcut sekmede yönlendirme gerçekleşmekte ve açıklık sömürülebilmekte.

Sonuç

Bu açıklık 2017 yılında keşfedilen bir açıklıktır (bkz. CWE veritabanına eklenme tarihi 26 Eylül 2017, "Use of Web Link to Untrusted Target with window.opener Access"). Popüler web tarayıcılarının aldıkları 2020-2021 yılı güncellemeleri ile açıklıktan etkilenecek kullanıcı kitlesi azınlığa çekilmiştir, ama azınlık kullanıcı kitlesi üzerinde (yani bulunabilecekleri eski sistem dolayısıyla eski web tarayıcı kullanan veya windows sistem güncelleştirmelerini tamamlamayan kullanıcı kitlesi üzerinde) açıklığın sunduğu risk sürecektir.

Yararlanılan Kaynaklar

https://muhammetdilmac.com.tr/2016/06/target-blank-ile-birlikte-gelen-window-opener-problemi/

https://www.netsparker.com/web-vulnerability-scanner/vulnerability-security-checks-index/phishing-by-navigating-browser-tabs/

https://en.wikipedia.org/wiki/Firefox_version_history

https://en.wikipedia.org/wiki/History_of_the_Opera_web_browser

https://en.wikipedia.org/wiki/Chromium_(web_browser)

https://cwe.mitre.org/data/definitions/1022.html

https://owasp.org/www-community/attacks/Reverse_Tabnabbing#

https://portswigger.net/daily-swig/upcoming-google-chrome-update-will-eradicate-reverse-tabnabbing-attacks#:~:text=Upcoming%20Google%20Chrome%20update%20will%20eradicate%20reverse%20tabnabbing%20attacks,-Charlie%20Osborne%2010&text=An%20upcoming%20update%20to%20the,associated%20with%20reverse%20tabnabbing%20attacks.&text=Chrome%2088%20is%20due%20to,build%20on%20January%2019%2C%202021.

https://portswigger.net/daily-swig/firefox-extension-to-protect-users-from-reverse-tabnabbing