****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.



Caso você pense que com a leitura dos materiais da How2Security, você irá se tornar um Cracker capaz de invadir sistemas, se você espera encontrar aqui scripts infalíveis para invasão e, a partir deles, sair por aí invadindo computadores, essa não é a leitura indicada. Indicamos, sim a leitura do Código Penal (Lei 2.848/1940), principalmente a Lei Carolina Dickmann (Lei 12.737/2012), nos Artigos 154-A e 154-B.

*154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

*Pena – Detenção, de 3 meses a 1 ano, e multa*

Este material é um conjunto de informações compiladas de documentos e ferramentas do Mundo Underground testadas em ambiente de laboratório na nossa intranet. Desta forma, todo conhecimento aqui condensado é tangível, assim como as orientações das contramedidas.

Dessa forma, esperamos ter sido bem claros que, em momento algum, estamos com a pretensão de ensinar a você como se tornar um invasor. Estaremos sim, mostrando muitas das técnicas utilizadas pelos crackers e, em alguns casos, pelos scripts kiddies, para que você, como administrador de redes, seja capaz de identificá-las em tempo hábil para se defender, antes que alguém com desejos menos nobres ô faça por você.

Assim sendo, todo o conteúdo dessa literatura tem apenas o objetivo didático de informar e preparar os administradores de redes dos novos tempos. Em momento algum nos responsabilizamos pelo mau uso desse conhecimento ou por danos causados em seu equipamento ou de terceiros, assim como também não somos responsáveis pelos códigos e ferramentas aqui citados.

Sandro Melo

Adaptado por Wellington Silva aka Well

**0 – Espelhando o Site**

Podemos espelhar o website para fazermos uma análise off-line. A cópia do site nos permite verificar todo o conteúdo do site, todas as páginas, os arquivos, os comentários e os scripts. Além disso, podemos usar a cópia para fazer ataques de engenharia social.

Ter uma cópia de um site serve para desenvolvemos bons phishing, os quais podem ser incorporados em outras ferramentas como o SET (Social Engineering Tolkit).

**1 – Usando a Tool HTTrack**

Para utilizarmos o utilitário HTTrack vamos primeiro criar um diretório para acomodar nosso clone e entrar no diretório.

root@kali-well:~# mkdir -p altoromutual

root@kali-well:~# cd altoromutual

root@kali-well:~altoromutual#

root@kali-wellx64:~/altoromutual# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.48-20

Copyright (C) 1998-2014 Xavier Roche and other contributors

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

Enter project name :

Para iniciar o HTTrack, basta digitar o nome do utilitário, onde devemos dar um nome ao projeto.

root@kali-well:~altoromutual# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.48-20

Copyright (C) 1998-2014 Xavier Roche and other contributors

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

Enter project name :**AltoroMutual**

O próximo passo é selecionar o diretório para salvar o site (no nosso caso ***/root/altoromutual***). Em seguida devemos informar a URL que desejamos clonar (**www.altoromutual.com**).

As próximas opções são apresentadas no formato de menu, para nosso exemplo vamos escolher a opção **2 (Mirror Web Site{s} with Wizard)**.

Em seguida ele nos questiona se queremos configurar algum proxy, por padrão não é configurado. Depois pergunta se queremos escolher algum tipo de arquivo para ser copiado (utilizamos o wirdcard /\* para baixar todos os arquivos do site em questão).

Por fim ele questiona se queremos adicionar mais alguma opção (no nosso caso não iremos colocar mais opções). Ele nos mostra a linha de comando que ele executará e questiona se estamos prontos para espelhar o site (escolha **Y**).

root@kali-well:~altoromutual# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.48-20

Copyright (C) 1998-2014 Xavier Roche and other contributors

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

Enter project name :**AltoroMutual**

Base path (return=/root/websites/) :/root/altoromutual

Enter URLs (separated by commas or blank spaces) :www.altoromutual.com

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>), separed by blank spaces

To see the option list, type help

Additional options (return=none) :

---> Wizard command line: httrack www.altoromutual.com -W -O "/root/altoromutual/AltoroMutual" -%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 Sat, 12 Nov 2016 21:22:40 by HTTrack Website Copier/3.48-20 [XR&CO'2014]

mirroring www.altoromutual.com /\* with the wizard help..

Done.

Thanks for using HTTrack!

\*

root@kali-well:~altoromutual#

Quando finalizar podemos navegar off-line pelo site do alvo.

root@kali-well:~altoromutual# ls AltoroMutual/www.altoromutual.com/

**admin** default5788.html defaultaea6.html disclaimer93a8.html

**altoro** default58e2.html defaultaf95.html feedback.html

**bank** default59f5.html defaultb374.html high\_yield\_investments.html

cgi.exe default61b9.html defaultb42f.html **images**

comments.txt default6349.html defaultb7e6.html index.html

default0064.html default6c68.html defaultbae8.html inside\_points\_of\_interest.html

default0aa1.html default6c8b.html defaultc193.html notfounda9ac.html

default0b4d.html default7114.html defaultc207.html **pr**

default14e5.html default7bb7.html defaultca85.html retirement.html

default1cb5.html default86eb.html defaultdb9a.html security.html

default2345.html default8fcf.html defaulte9b5.html style.css

default2a12.html default9055.html defaulteb20.html subscribe.swf

default2a69.html default90d8.html defaulted9a.html survey\_questions79e8.html

default2db7.html default97c5.html defaultf172.html survey\_questions.html

default49df.html defaultac2e.html defaultfadf.html

default4a61.html defaultad11.html default.html

default5453.html defaultad36.html disclaimer2900.html

root@kali-well:~altoromutual#

Depois de terminar o espelhamento do site, navegue nos diretórios onde você salvou. Também navegue pelo browser.

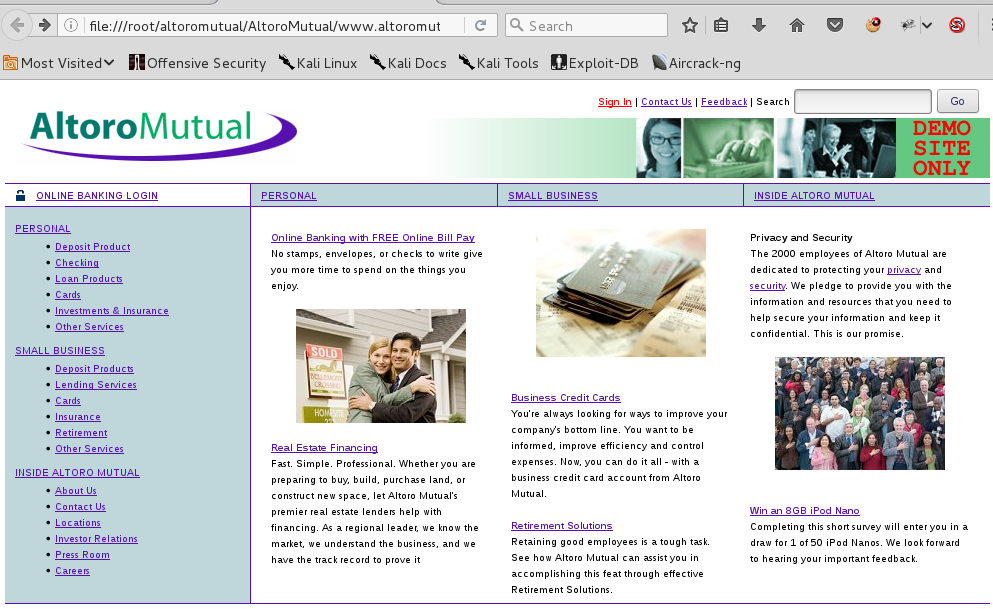


Figura 01 – Navegando Off-Line Pelo Site Espelhado do Alvo

**2 – Criando Nosso Próprio Script de Espelhamento com WGET**

Bom vamos desenvolver nosso script de espelhamento de sites, utilizando utilitários como o **wget**.

As opções que podemos utilizar do wget para clonar sites são:

* **-c** 🡪 Continua o download caso ele tenha sido interrompido;
* **-r** 🡪 Solicita um recurso de forma recursiva. Por padrão, realiza a busca em até cinco níveis de pronfundidade;
* **-m** 🡪 Opção de mirror. Usada para realizar o espelhamento do site para arquivos locais (realizaro download do site). Equivale a usar as opções –r –N –l inf –no-remove-listing.
* **-e robots=off** 🡪 De acordo com as configurações do arquivorobots.txt, o wget solicitará ou não recursos. Essa opção desabilita a checagem do conteúdo do arquivo robots.txt;
* **--load-cookie=cookie.txt** 🡪 Utiliza um cookie. O conteúdo do cookie deve estar presente no arquivo cookie.txt;
* **--save-cookie=cookie.txt** 🡪 Salva os cookie no arquivo cookie.txt. Por padrão, não salva cookie de sessão;
* **--keep-session-cookie** 🡪 Salva cookies de seesão. Usado com a opção –save-cookie.
* **--user-agent=”Mozila...”** 🡪 Configura o campo User-Agent do protocolo HTTP. Alguns sites são bloqueados para determinados User-Agent, então podemos alterá-lo aqui.

root@kali-well:~scripts# vi clone\_site.sh

#!/bin/bash

### CORES

amarelo="\e[33;1m"

azul="\e[34;1m"

verde="\e[32;1m"

vermelho="\e[31;1m"

fim="\e[m"

# BROWSER AGENT

AGENT="Mozilla/5.0 (Windows NT 10.0; WOW64)"

banner()

{

echo -e "$azul##############################################################$fim"

echo -e "$azul# By Wellington Luiz da Silva aka w3ll #$fim"

echo -e "$azul# #$fim"

echo -e "$azul# CLONE SITE Version 1.0 - How2Sec Lab #$fim"

echo -e "$azul# #$fim"

echo -e "$azul# Created: 12/11/2016 Updated: 12/11/2016 #$fim"

echo -e "$azul##############################################################$fim"

echo -e "\n"

}

banner

# Validando se o usuario passou a URL

if [ "$1" == "" ] ;then

echo -e "$vermelho""[-] ERROR: You need to specify a URL$fim"

echo -e "$verde""[+] Use: $0 http://www.exemplo.com.br\n$fim"

exit 1

fi

# Criando o diretorio onde serao salvo os arquivos do servidor

DIR=`echo "$1" | cut -f3 -d"/"`

mkdir -p "mirrot.$DIR"

cd "mirrot.$DIR"

# Fazendo o download passando como parametro o User-Agent do Browser

# Isso para fazer bypass de WAF com filtros de Browsers

# As opcoes -m => de mirror (espelho) para espelhar o site, -k => para converter

# os links o conteúdo dinâmico, por fim a opção -w => para esperar X segundos

# antes de fazer a próxima requisição, fazendo o menos barulho possível no alvo

wget --user-agent="$AGENT" -mk -w 20 $1

cd -

echo -e "\n"

echo -e "$verde""[+] Search results saved in: mirror.$DIR""$fim"

<ESQ>:wq

"clone\_site.sh" 60L, 4295C written

root@kali-well:~scripts#

Depois de criarmos o script podemos execute-lo para clonar/espelhar o site alvo para um diretório local.

root@kali-well:~altoromutual# ./clone\_site.sh http://www.altoromutual.com

#################################################################################

# By Wellington Luiz da Silva aka w3ll #

# #

# CLONE SITE Version 1.0 - How2Sec Lab #

# #

# Created: 12/11/2016 Updated: 12/11/2016 #

#################################################################################

--2016-11-12 22:16:06-- http://www.altoromutual.com/

Resolving www.altoromutual.com (www.altoromutual.com)... 65.61.137.117

Connecting to www.altoromutual.com (www.altoromutual.com)|65.61.137.117|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 9605 (9.4K) [text/html]

Saving to: ‘www.altoromutual.com/index.html’

www.altoromutual.co 100% [=========================>] 9.38K 7.90KB/s in 1.2s

Last-modified header missing -- time-stamps turned off.

2016-11-12 22:16:10 (7.90 KB/s) - ‘www.altoromutual.com/index.html’ saved [9605/9605]

--==[ Resumido ]==--

--2016-11-12 22:49:14-- http://www.altoromutual.com/default.aspx?content=jobs/20061024.htm

Reusing existing connection to www.altoromutual.com:80.

HTTP request sent, awaiting response... 200 OK

Length: 8005 (7.8K) [text/html]

Saving to: ‘www.altoromutual.com/default.aspx?content=jobs%2F20061024.htm’

www.altoromutual.com/defaul 100%[=================>] 7.82K --.-KB/s in 0.01s

Last-modified header missing -- time-stamps turned off.

2016-11-12 22:49:14 (595 KB/s) - ‘www.altoromutual.com/default.aspx?content=jobs%2F20061024.htm’ saved [8005/8005]

FINISHED --2016-11-12 22:49:14--

Total wall clock time: 33m 7s

Downloaded: 92 files, 933K in 13s (72.1 KB/s)

--==[ Resumido ]==--

Converting www.altoromutual.com/default.aspx?content=business\_cards.htm... 38-1

Converting www.altoromutual.com/style.css... nothing to do.

Converted 55 files in 0.02 seconds.

/root/scripts

[+] Search results saved in: mirrir.www.altoromutual.com

root@kali-well:~altoromutual#

Pronto podemos buscar dados como JavaScripts, por form HTML, campos ocultos em form HTML e comentários nas páginas de forma Off-Line.

**2.1 – Cookies com WGET**

Há situações em que é necessário realizar o download de arquivos protegidos por mecanismos de autenticação, como sistemas de login. Para imular esse ambiente será utilizado o DVWA (Dann Vulnerable Web pplication).

Ao acessar o endereço IP do servidor DVWA, é exibida uma tela de login.

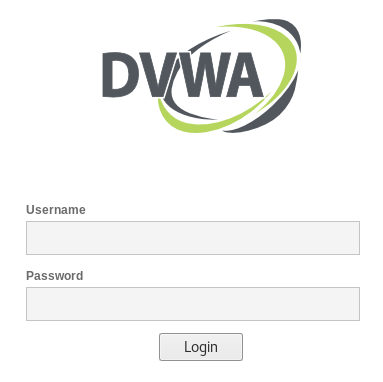


Figura 02 – DVWA

Ao realizar o login (admin/password), exibe a página administrativa. É justamente essa página que deverá ser clonada.

Para isso, será necessário configurar o wget apara realizar uma requisição com o cookie de sessão do administrador (opção –load-cokkie). Para saber como deve ser o formato do arquivo de cookie, realize uma requisição, salvando os cookies no arquivo cookies.txt:

root@kali-well:~# mkdir DVWA

root@kali-well:~# cd DVWA/

root@kali-well:~DVWA# wget --keep-session-cookies --save-cookies=cookies.txt http://192.168.0.108/DVWA/DVWA-1.9/

--=[ Resumido ]==--

Saving to: ‘index.html’

index.html 100%[==============================================================>] 1.53K --.-KB/s in 0s

2018-04-08 02:33:49 (57.6 MB/s) - ‘index.html’ saved [1567/1567]

root@kali-well:~DVWA#

O cookie salvo pela wget apresenta a seguinte estrutura:

root@kali-well:~DVWA# ls

cookies.txt index.html

root@kali-well:~DVWA# cat cookies.txt

# HTTP cookie file.

# Generated by Wget on 2018-04-08 02:33:49.

# Edit at your own risk.

192.168.0.108 FALSE /DVWA/DVWA-1.9/ FALSE 0 security impossible

192.168.0.108 FALSE / FALSE 0 PHPSESSID qvlm0abh8uksjcj6b0cipojq25

root@kali-2k17-x64:~/tools/DVWA#

root@kali-well:~DVWA#

O valor do cookie PHPSESSID pode ser trocado para o PHPSESSID do administrador. Uma maneira de descobrir esse PHPSESSID é logando como administrador pelo Firefox, e nas opções de privacidade, visualizar o seu conteúdo. Outra forma é por meio de Add-nos como Edit Cookies. Lembre-se de um cookie de sessão é perdido caso o browser seja fechado, portanto, para realizar a o mirror é necessário manter a aba do Firefox aberta.

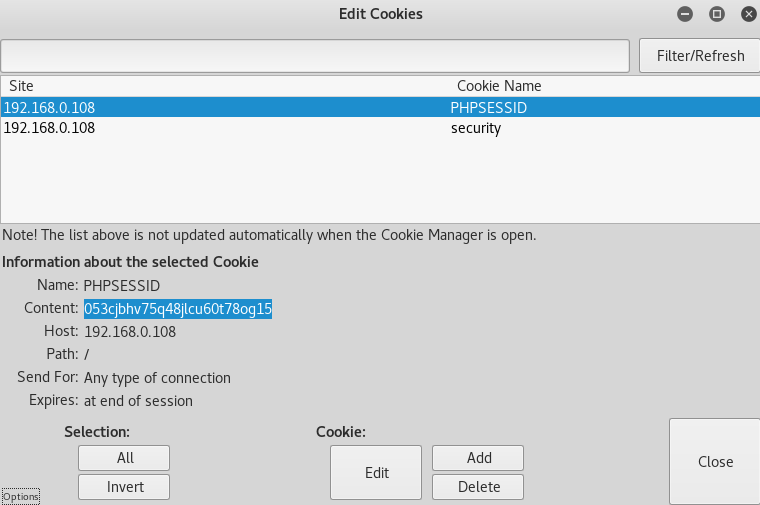


Figura 03 – Edit Cookie

root@kali-well:~DVWA# cat cookies.txt

# HTTP cookie file.

# Generated by Wget on 2018-04-08 02:33:49.

# Edit at your own risk.

192.168.0.108 FALSE /DVWA/DVWA-1.9/ FALSE 0 security impossible

192.168.0.108 FALSE / FALSE 0 PHPSESSID **053cjbhv75q48jlcu60t78og15**

root@kali-2k17-x64:~/tools/DVWA#

root@kali-well:~DVWA#

Agora vamos fazer a requisição com o wget utilizando dessa vez o arquivo contendo o cookie de sessão do administrador.

root@kali-well:~DVWA# wget --keep-session-cookies --save-cookies=cookies.txt http://192.168.0.108/DVWA/DVWA-1.9/

--==[ Resumido ]==--

root@kali-well:~DVWA#

ls 192.168.0.108/DVWA/DVWA-1.9/

about.php logout.php

docs phpinfo.php

--==[ Resumido ]==--

root@kali-well:~DVWA#

O espelhamento do site foi feito e podemos navegar off-line.

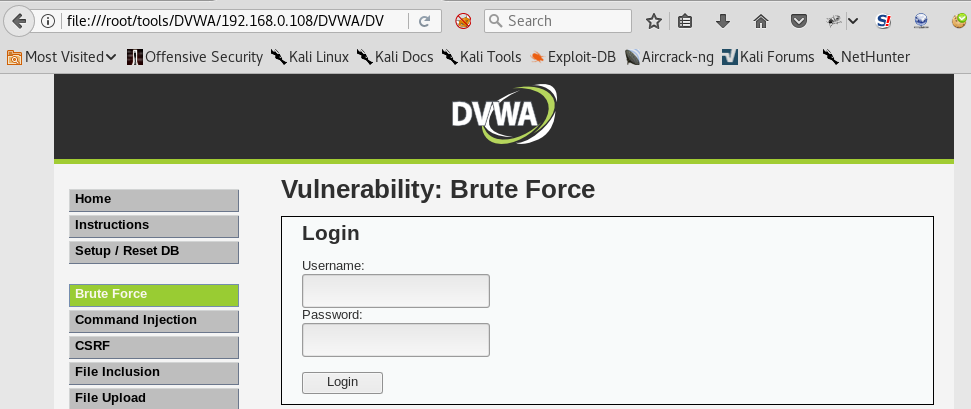


Figura 04 – Site DVWA

**4 – Referências Bibliográficas**

**[1]** MUNIZ, JOSEPH and LAKHANI, AAMIR – Web Penetration Testing with Kali Linux, 2013, Birmingham – Mumbai, Packt Publishing

**[2]** GRAVES, KIMBERLY – CEH – Official Ethical Hacker Review Guide, Indianapolis - Indiana, 2007, Wiley Publishing Inc.

**[3]** STUTTARD, DAFYDD and PINTO, MARCUS – The Web Application Hacker’s Handbook, Indianapolis - Indiana, 2º Edition, Wiley Publishing Inc.

**[4]** SCAMBRAY, JOEL, McCLURE, STUART and KURTZ, GEORGE – Hackers Expostos Segredos e Soluções para a Segurança de Redes, São Paulo, 2001, MAKRON Books Ltda.

**[5]** LONG, JOHNNY - GOOGLE HACKING - Para Teste de Invasão [tradução Sérgio Pereira Couto] 2005, DIGERATI (BOOKS)

**[6]** MELO, Sandro – Estudo de Técnicas para Exploração de Vulnerabilidades em Redes TCP/IP, 2º Ed, Rio de Janeiro, 2006, Editora Alta Books Ltda.

**[7]** AHARONI, Mati; Offensive Security Lab Exercises - Curso de Pen-Test oferecido pela Offensive Security, 2007

**[8]** SCAMBRAY, Joel; LIU, Vicent; SIMA, Caleb - Hacking Exposed Web Application: Web Application Security Secrets And Solutions – 3ª Edition, New York – 2011, McGraw-Hill

**[9]** DHANJANI, Nitesh; RIOS, Billy; HARDIN, Brett - Hacking A Próxima Geração – Rio de Janeiro – 2011, Alta Books

**[10]** MORENO, Daniel – Penest em Aplicações Web – São Paulo – 2017, Novatec