****

**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 – Arquivo Robots.txt**

O arquivo ***robots.txt*** está disponível publicamente na maioria dos sites da web, este arquivo dá instruções para os mecanismos de busca (web robots ou engine spiders) sobre o que pode e o que não pode ser visível usando o REP (Robots Exclusion Protocol). Ele tem basicamente 3 instruções: User-Agent:, Disallow: e Allow:.

* **User-Agent: <User Agent> 🡪** Informa sobre a política que será aplicada para os clientes que utilizam o browser informado;
* **Disallow: <Path ou File> 🡪** Informa aos mecanismos de busca para não indexar o caminho ou arquivo informado;
* **Allow: <Path ou File> 🡪** Informa aos mecanismos de busca o caminho ou arquivo que pode ser indexado.

Para ver o arquivo robots.txt, podemos acessa-lo a partir do diretório raiz do site alvo. Por exemplo, adicionando o robots.txt na raiz do site do Facebook, nos será mostrado um arquivo parecido com a Figura 01.

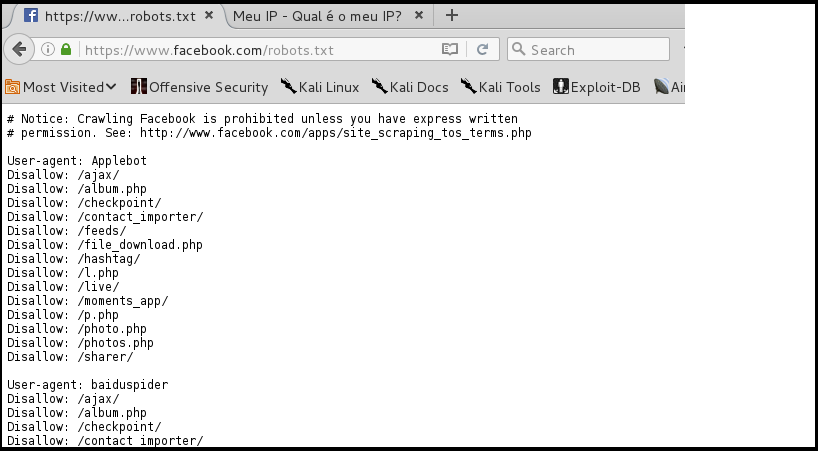


Figura 01 – Arquivo Robots.txt do Facebook

Acumular esses arquivos em sua wordlist de URLs é uma boa prática para aumentar a chances de encontrar arquivos ocultos na hora de levantar arquivos ocultos nos alvos.

**1 – Script Para Gerar Uma Wordlist de Caminhos e Arquivos Através do Robots.txt**

Vamos criar um script para gerar uma wordlist de caminhos e arquivos alimentado pelos arquivos robots.txt.

Primeiramente vamos criar o seguinte arquivo.

root@kali-well:~scripts# vi robots2wordlist.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)"

FILE="wordlist\_url.txt"

banner()

{

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

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

echo -e "$azul# #$fim"

echo -e "$azul# ROBOTS2WORDLIST Version 1.0 - How2Sec Lab #$fim"

echo -e "$azul# #$fim"

echo -e "$azul# Created: 05/11/2016 Updated: 05/11/2016 #$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

# Apagando pesquisas anteriores

rm robots.txt

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

# Isso para fazer bypass de WAF com filtros de Browsers

wget --user-agent="$AGENT" $1/robots.txt

# Laco FOR para fazer a quebra de linha em conteudos compactados

# Enviamos o resultado para um arquivo temporario com o nome PID.robors.1 em /tmp

for FILEs in $(grep "/" robots.txt) ;do

echo $FILEs | grep ^/ >> /tmp/$$.robots.1

done

# Seprarando os caminhos Encontrados

echo "PATH Encontrados"

echo "================"

cat /tmp/$$.robots.1

echo ""\nN de Caminhos|Arquivos encontrados: " `cat /tmp/$$.robots.1 | wc -l`

# Criando o arquivo temporário 2, removendo conteúdo repetido

cat $FILE /tmp/$$.robots.1 | sort -u >> /tmp/$$.robots.2

echo ""\nN Total de Caminhos|Arquivos: " `cat /tmp/$$.robots.2 | wc -l`

cat /tmp/$$.robots.2 > $FILE

# Removendo os Arquivos Temporarios

rm /tmp/$$.robots\*

echo -e "\n"

echo -e "$verde""[+] Search results saved in: wordlist\_url.txt.\n[+]Number of Hits in file: `wc -l $FILE`\n""$fim"

<ESQ>:wq

"robots2wordlist.sh" 75L, 4868C written

root@kali-well:~scripts#

Agora vamos testar em dois sites, o do UOL Diveo e do Facebook para vermos se nosso script se comporta de maneira adequada.

root@kali-well:~scripts# chmod 755 robots2wordlist.sh

root@kali-well:~scripts# ./robots2wordlist.sh http://www.uoldiveo.com.br

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

# By Wellington Luiz da Silva aka w3ll #

# #

# ROBOTS2WORDLIST Version 1.0 - How2Sec Lab #

# #

# Created: 05/11/2016 Updated: 05/11/2016 #

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

--2016-11-05 15:24:42-- http://www.uoldiveo.com.br/robots.txt

Resolving www.uoldiveo.com.br (www.uoldiveo.com.br)... 200.147.68.20, 200.221.64.49, 2804:49c:3103:405:ffff:ffff:ffff:3

Connecting to www.uoldiveo.com.br (www.uoldiveo.com.br)|200.147.68.20|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 217 [text/html]

Saving to: ‘robots.txt’

robots.txt 100%[=======================================>] 217 --.-KB/s in 0s

2016-11-05 15:24:42 (42.2 MB/s) - ‘robots.txt’ saved [217/217]

PATH Encontrados

================

/midia

/parcerias

/solucoes/nota-fiscal-de-servico-eletronica-nfs-e.html

/solucoes/integracao-de-negocios-b2b-supply-chain.html

/OLD

/home.html

N de Caminhos|Arquivos encontrados: 6

N Total de Caminhos|Arquivos: 40

**[+] Search results saved in: wordlist\_url.txt.**

**[+] Number of Hits in file: 40**

root@kali-well:~scripts# ./robots2wordlist.sh http://www.facebook.com

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

# By Wellington Luiz da Silva aka w3ll #

# #

# ROBOTS2WORDLIST Version 1.0 - How2Sec Lab #

# #

# Created: 05/11/2016 Updated: 05/11/2016 #

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

--2016-11-05 15:27:12-- http://www.facebook.com/robots.txt

Resolving www.facebook.com (www.facebook.com)... 31.13.73.36, 2a03:2880:f100:83:face:b00c:0:25de

Connecting to www.facebook.com (www.facebook.com)|31.13.73.36|:80... connected.

HTTP request sent, awaiting response... 302 Found

Location: https://www.facebook.com/robots.txt [following]

--2016-11-05 15:27:13-- https://www.facebook.com/robots.txt

Connecting to www.facebook.com (www.facebook.com)|31.13.73.36|:443... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/plain]

Saving to: ‘robots.txt’

robots.txt [ <=> ] 4.89K --.-KB/s in 0.007s

2016-11-05 15:27:15 (708 KB/s) - ‘robots.txt’ saved [5006]

PATH Encontrados

================

/ajax/

/album.php

/checkpoint/

/contact\_importer/

/feeds/

--==[ Resumido ]==--

/ajax/pagelet/generic.php/PagePostsSectionPagelet

/ajax/pagelet/generic.php/PagePostsSectionPagelet

/ajax/pagelet/generic.php/PagePostsSectionPagelet

/

N de Caminhos|Arquivos encontrados: 186

N Total de Caminhos|Arquivos: 61

**[+] Search results saved in: wordlist\_url.txt.**

**[+] Number of Hits in file: 61**

root@kali-well:~scripts#

Pronto temos um script que pode no ajudar a tornar nossa buscar por caminhos e arquivos ocultos mais efetivas.

**Nota:** Podemos baixar a versão mais recente do script em https://github.com/how2security/robots2wordlist.

**3 – Referências Bibliográficas**

**[1]** MUNIZ, JOSEPH and LAKHANI, AAMIR – Web Penetration Testing with Kali Linux, 2013, Birmingham – Mumbai, Packet 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]** TANENBAUM, Andrew S. – Redes de Computadores, 4º Ed, São Paulo, 2003, Editora Campus.

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

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

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