****

**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 – Levantando informações com o WhatWeb**

Esta ferramenta faz o levantamento das tecnologias envolvidas na aplicação web, desde a versão do sistema operacional até as linguagens utilizadas da aplicação.

Vamos levantar informações de duas aplicações:

root@kali-wellx64:~tools# whatweb 192.168.0.102

http://192.168.0.102 [200 OK] Apache[2.2.14], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.14 (Ubuntu)], IP[192.168.0.102], Index-Of, Title[Index of /]

root@kali-wellx64:~tools# whatweb www.altoromutual.com

http://www.altoromutual.com [200 OK] ASP\_NET[2.0.50727], Cookies[ASP.NET\_SessionId,amSessionId], Country[UNITED STATES][US], HTTPServer[Microsoft-IIS/8.0], HttpOnly[ASP.NET\_SessionId], IP[65.61.137.117], Microsoft-IIS[8.0], Title[Altoro Mutual][Title element contains newline(s)!], X-Powered-By[ASP.NET]

root@kali-wellx64:~tools#

Agora vamos fazer de forma que nos traga o máximo de informações possível utilizando a opção **–v** (verbose).

root@kali-wellx64:~tools# whatweb 192.168.0.102 -v

WhatWeb report for http://192.168.0.102

Status : 200 OK

Title : Index of /

IP : 192.168.0.102

Country : RESERVED, ZZ

Summary : Index-Of, Apache[2.2.14], HTTPServer[Ubuntu Linux][Apache/2.2.14 (Ubuntu)]

Detected Plugins:

[ Apache ]

The Apache HTTP Server Project is an effort to develop and

maintain an open-source HTTP server for modern operating

systems including UNIX and Windows NT. The goal of this

project is to provide a secure, efficient and extensible

server that provides HTTP services in sync with the current

HTTP standards.

Version : 2.2.14 (from HTTP Server Header)

Google Dorks: (3)

Website : http://httpd.apache.org/

[ HTTPServer ]

HTTP server header string. This plugin also attempts to

identify the operating system from the server header.

OS : Ubuntu Linux

String : Apache/2.2.14 (Ubuntu) (from server string)

[ Index-Of ]

Index of

Google Dorks: (1)

HTTP Headers:

HTTP/1.1 200 OK

Date: Wed, 11 Apr 2018 04:44:08 GMT

Server: Apache/2.2.14 (Ubuntu)

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 692

Connection: close

Content-Type: text/html;charset=UTF-8

root@kali-wellx64:~tools# whatweb www.altoromutual.com -v

WhatWeb report for http://www.altoromutual.com

Status : 200 OK

Title : ,Altoro Mutual

IP : 65.61.137.117

Country : UNITED STATES, US

Summary : HttpOnly[ASP.NET\_SessionId], ASP\_NET[2.0.50727], Microsoft-IIS[8.0], Cookies[ASP.NET\_SessionId,amSessionId], HTTPServer[Microsoft-IIS/8.0], X-Powered-By[ASP.NET]

Detected Plugins:

[ ASP\_NET ]

ASP.NET is a free web framework that enables great Web

applications. Used by millions of developers, it runs some

of the biggest sites in the world.

Version : 2.0.50727 (from X-AspNet-Version HTTP header)

Google Dorks: (2)

Website : http://www.asp.net/

[ Cookies ]

Display the names of cookies in the HTTP headers. The

values are not returned to save on space.

String : ASP.NET\_SessionId

String : amSessionId

[ HTTPServer ]

HTTP server header string. This plugin also attempts to

identify the operating system from the server header.

String : Microsoft-IIS/8.0 (from server string)

[ HttpOnly ]

If the HttpOnly flag is included in the HTTP set-cookie

response header and the browser supports it then the cookie

cannot be accessed through client side script - More Info:

http://en.wikipedia.org/wiki/HTTP\_cookie

String : ASP.NET\_SessionId

[ Microsoft-IIS ]

Microsoft Internet Information Services (IIS) for Windows

Server is a flexible, secure and easy-to-manage Web server

for hosting anything on the Web. From media streaming to

web application hosting, IIS's scalable and open

architecture is ready to handle the most demanding tasks.

Version : 8.0

Website : http://www.iis.net/

[ X-Powered-By ]

X-Powered-By HTTP header

String : ASP.NET (from x-powered-by string)

HTTP Headers:

HTTP/1.1 200 OK

Cache-Control: no-cache

Pragma: no-cache

Content-Length: 9550

Content-Type: text/html; charset=utf-8

Expires: -1

Server: Microsoft-IIS/8.0

X-AspNet-Version: 2.0.50727

Set-Cookie: ASP.NET\_SessionId=nzfc4bmzhvjmfhyzwjurtv55; path=/; HttpOnly

Set-Cookie: amSessionId=02342265009; path=/

X-Powered-By: ASP.NET

Date: Wed, 11 Apr 2018 05:23:41 GMT

Connection: close

root@kali-wellx64:~tools#

Desta forma podemos levantar as versões de aplicações utilizadas e procurar por exploits públicos para as falhas já encontradas nas versões de aplicações plug-ins em uso.

Podemos baixar essa ferramenta em: http://www.morningstarsecurity.com/research/whatweb.

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