****

**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 – Google Hacking**



Figura 01 – Google Hacking

O Google Hacking é a arte da busca criativa por informações visando atacar ou proteger as informações de uma empresa ou pessoa. As informações disponíveis nos servidores web provavelmente estarão nas bases de dados do Google.

Um servidor mal configurado pode expor diversas informações no Google. Não é difícil conseguir acesso a arquivos de base de dados, número de documentos pessoais, informações internas, entre outras informações de sites através do Google.

O Google possui diversos recursos que podem ser utilizados durante um teste de invasão, e justamente por isso que, é considerada a melhor ferramenta para os pen-test, pois permite acesso a todo e qualquer tipo de informação que se queira.

**1 – Usando os Operadores Booleanos e Caracteres Especiais**

Para realizarmos uma busca avançada é necessário entendermos operadores booleanos **AND**, **OR** e **NOT**. Para segmentar adequadamente as várias partes de uma busca avançada no Google, devemos também explorar as técnicas de agrupamento visual que usam parênteses. Finalmente, combinamos essas técnicas com certos caracteres especiais que podem servir como atalhos para certos operadores, curinga ou termos especiais.

O operador **AND** é redundante para as pesquisas no Google, pois todas as pesquisas que tenha mais de uma palavra ele é incluído entre elas. Por exemplo, a procurar por ***hackers crackers***, será feira como se o operador AND estivesse entre as palavras, ficando assim, ***hackers AND crackers*** e a pesquisa retornaria tanto sites que tenha hackers como sites que tenha crackers.

O símbolo mais **(+)** força a inclusão da palavra que o segue. Não deve haver espaço depois do símbolo de mais. Por exemplo, se fôssemos pesquisar ***justiça para todos*** separadamente, o Google excluiria na busca as palavras mais comuns. Para força-lo a procurar essas palavras, elas deverão ser precedidas do sinal de mais, sendo que não há contraindicações se for usado em excesso. Para realizar essa busca sem a inclusão de todas as palavras, considere-a como ***justiça +para +todos***. Além disso, as palavras podem estar entre aspas. Isso geralmente força o Google a incluir todas as palavras comuns na frase, apresentada como frase, seria ***“justiça para todos”***.

Outro operador é o **NOT**. Funcionalmente, faz o oposto do operador **AND**, excluindo uma palavra da busca. A melhor maneira de usá-lo é preceder a busca com um sinal de menos **(-)**. Assim como no caso anterior, certifique-se de não deixar espaços entre o sinal de menos e o termo da busca. Se fizermos uma busca simples como ***apache***, o Google retornará resultados de todos os tipos, tais como helicóptero apache, servidor web apache, e algum índio que tinha como função em sua tribo ser um apache =] pois essa busca é muito genérica. Para aperfeiçoa a pesquisa podemos incluir mais termos, aos quais o Google faz a exclusão com o NOT. Para remover alguns termos, considere o uso de pesquisas como ***apache -helicóptero -índio***. Isto fará o Google se aproximar do que realmente se desejava com a pesquisa.

Um operador booleano menos comum e às vezes mais confuso é o **OR** (ou). É representado pelo símbolo pipe (|) ou a própria palavra OR em letras maiúsculas e instrui o Google a localizar ou um ou o outro termo de uma pesquisa. Embora pareça fraco, quando consideramos uma pesquisa simples como password ou senha, as coisas podem ficar terrivelmente confusas se utilizarmos muitos AND e ORs e NOTs.

Veja um exemplo complexo, com a exata mecânica que discutimos:

***intext:(password | senha) intext:(user | usuário | userid) filetype:cvs***

Esse exemplo usa operadores avançados combinados como o operador OR para criar uma pesquisa que parece mais uma sentença escrita como um pedido educado. Essa busca diz para o Google: “Localize todas as páginas que tenham password ou senha no texto do documento. Dessas páginas, mostre-me apenas as que contenham as palavras username, usuário ou userid no texto e apenas mostre os documentos que são arquivos CVS”.

**2 – Operadores de Busca Avançados**

Os operadores avançados são muito versáteis, mas lembre-se das regras listadas a seguir. Além disso, devemos também lembrar-nos que nem todos os operadores podem ser usados de qualquer maneira. Alguns só podem ser usados ao realizar uma busca na web, e outros só em buscas de grupos. Se você perceber que a palavra do operador avançado está realçada dentro da pesquisa é que algo está errado. Por exemplo, se a palavra **intitle** está em negrito, provavelmente cometeu um erro no uso do operador **intitle**.

Operadores avançados não são nada mais do que parte de uma pesquisa. Você fornece o operador para o Google como forneceria qualquer outro item de busca. Em contraste com os estilos praticamente livres de buscas básicas, esses operadores têm uma sintaxe altamente rígida e que deve ser seguida. A sintaxe básica de um operador avançado é:

operator:search\_term

Ao usar um desses operadores, lembre-se de que:

1. Não há espaço entre o operador e os dois-pontos **(:)** e o termo de busca. Violar essa sintaxe pode produzir resultados indesejados e manterá o Google longe de entender o operador. Na maioria dos casos, a ferramenta tratará um operador errado como apenas um outro termo de busca. Por exemplo, fornecer o operador **intitle** sem os dois-pontos e sem o termo de busca fará com que o Google retome páginas que contenham a palavra **intitle**.
2. O termo de busca é da mesma sintaxe que os termos que vimos anteriormente. Por exemplo, podemos fornecer um termo único, uma simples palavra ou uma frase dentro de aspas. Se você fornecer uma frase como termo de busca, certifique-se de que não há espaços entre o operador, os dois-pontos e a primeira aspa da frase.
3. Operadores booleanos e caracteres especiais (como OR e +) podem ainda ser aplicados em operadores avançados, mas certifique-se de que não estejam depois dos dois-pontos.
4. Operadores avançados podem ser combinados em uma simples pesquisa desde que você respeite tanto a sintaxe básica de busca do Google quanto o operador avançado. Alguns deles combinam melhor que outros, e alguns simplesmente não podem ser combinados.
5. Os operadores **ALL** (que começam com a palavra ALL) são esquisitos, geralmente usados uma vez por pesquisa, e não se misturam com outros operadores.

**2.1 – intitle: e allintitle: Busca no Título de uma Página**

De um ponto de vista técnico, o título de uma página pode ser descrito como o texto que é encontrado dentro das tags ***<title>...</title>*** de um documento **HTML**. O título é mostrado no topo da maioria dos navegadores quando uma página é exibida, como vemos na figura abaixo. Nesse contexto do Google Grupos, ***intitle*** encontrará o termo no título da mensagem postada.

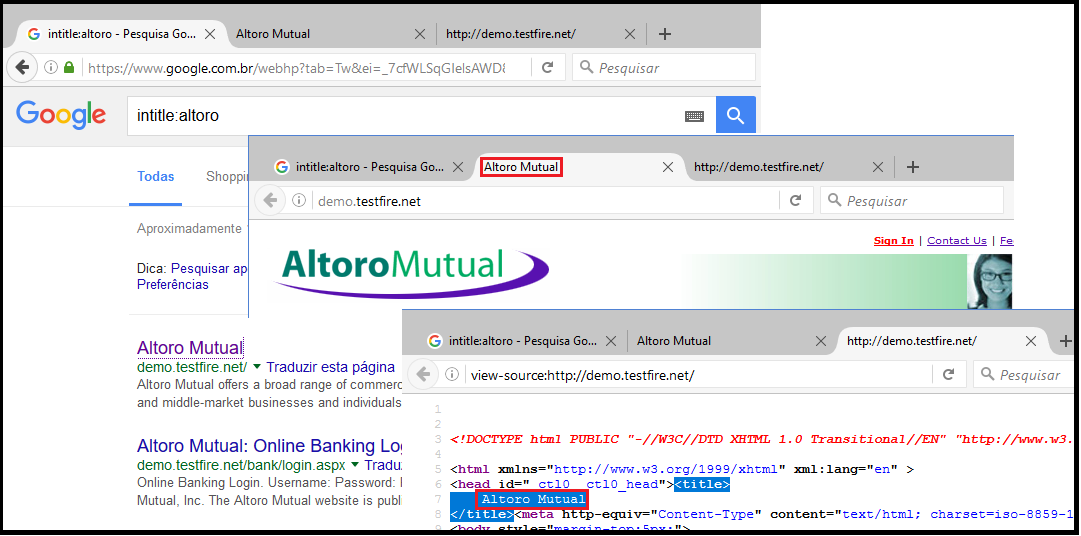


Figura 02 – Operador intitle

Como podemos ver o texto se encontra como título da página da Altoro Mutual. Poderíamos fazer a busca com o ***allintitle*** para o nome completo ficando assim: ***allintitle:”Altoro Mutual”***.

Seja cauteloso ao usar o operador **allintitle**. Ele tende a ser descuidado quando usado com outros operadores e quebra completamente a busca, não retornando resultados. É melhor começar novamente e usar alguns operadores **intitle** do que estragar tudo com as conversões esquisitas do **allintitle**.

Embora não seja completamente exato, lembre-se de que o **allintitle** não pode ser usado como outros operadores ou termos de busca.

**2.2 – allintext: Localiza uma String no Texto de uma Página**

O operador **allintext** é talvez o mais simples a se usar, pois realiza a função pela qual os sistemas de busca são bem conhecidos: localizar uma string dentro do texto de uma página. Embora este operador avançado seja muito genérico para ser de alguma utilidade real, é útil quando você sabe que o texto que procura deve ser encontrado apenas no título, na URL e nos links. Usar **allintext** também serve como um tipo de atalho para “encontrar esta string em qualquer lugar exceto no título, na URL e nos links”. Já que esse operador começa com a palavra all, todo termo de busca fornecido após o operador é considerado parte da busca.

Por essa razão, o **allintext** não deve ser misturado com outros operadores.

**2.3 – inurl: e allinurl: Encontrando Texto em uma URL**

Depois de conhecer os operadores **intitle**, pode parecer uma tarefa um tanto simples começar a preocupar-se com o operador **inurl** precipitadamente. Não são inúteis tais iniciativas de busca, mas lembre-se de que uma URL é algo muito mais complicada que um simples título de página, e as funções do operador **inurl** podem ser igualmente complexas.

Inicialmente, falaremos sobre o que é uma URL. Abreviação de **Uniform Resource Locator (Localizador de Recurso Uniforme)**, uma URL é simplesmente o endereço de uma página. Seu início consiste de um protocolo, seguido de ://, como os mais comuns http:// ou ftp://.

Depois do protocolo, há um endereço seguido de um caminho, tudo separado por barras (/). Após o caminho, vem um nome de arquivo opcional. Uma URL básica, como http://www.how2security.com.br/source/teste.html, pode ser composta de várias partes diferentes. O protocolo, HTTP, indica que se trata, basicamente, de um servidor web. Á no host www.how2security.com.br, e o arquivo requisitado, teste.html, está no diretório /source do servidor.

Resumidamente, é uma lista de parâmetros que serão repassados para o arquivo ou programa de “busca”. Apenas entenda que tudo “isso” é considerado parte da URL, e que o Google pode ser instruído a buscar palavras nas URLs com os operadores **inurl** e **allinurl**.

Até agora não parece ser muito mais complexo do que lidar com o operador **intitle**, mas há algumas complicações. Primeiro, o Google não pode efetivamente procurar a porção de protocolo da URL - http://, por exemplo. Segundo, há uma boa porção de caracteres especiais espalhados pela URL que a ferramenta também terá problemas ao interpretar. A tentativa de ser cada vez mais específico ao incluir esses caracteres especiais em uma busca pode causar resultados inesperados e mesmo limitar sua busca de maneira indesejada. Terceiro, e mais importante, outros operadores avançados (site e filetype, por exemplo) podem buscar em lugares mais específicos dentro da URL e até mesmo com mais qualidade do que o **inurl**. Esses fatores tornam o **inurl** mais cheio de truques efetivos que o **intitle**, que, comparavelmente, é muito simples. Apesar disso, o **inurl** é um dos operadores indispensáveis, sendo talvez o mais importante para usuários avançados.

Como o operador **intitle**, o **inurl** tem um operador companheiro, conhecido como **allinurl**. Considere a página de resultados do **inurl**, que vemos na figura a abaixo.

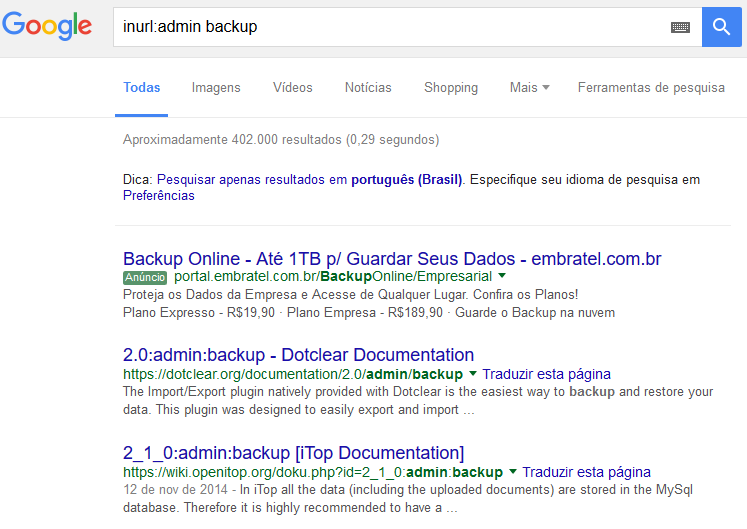


Figura 03 – Operador inurl

Essa busca localiza a palavra **admin** na URL e a palavra **backup** em qualquer parte do documento.

E como em **allintitle**, **allinurl** não se dá bem com outros operadores. Se você precisa encontrar várias palavras ou frases em uma URL, é melhor fornece várias entradas **inurl** do que ser derrotado pelas conversões pouco amigáveis do **allinurl**.

**2.4 – site: Busca Restrita a Página Específicas**

Embora tecnicamente seja uma parte da URL, o endereço (ou nome de domínio) de um servidor pode ser procurado melhor com um operador **site**. Este permite buscar apenas páginas que estejam hospedadas em um servidor ou domínio específico. Embora seja simples, o uso apropriado desse operador pode demorar um pouco para ser compreendido, já que o Google lê nomes de servidores da direita para a esquerda, ao contrário da convenção humana de leitura de páginas, que é da esquerda para a direita.

Por exemplo, para localizar páginas que estejam hospedas em um servidor chamado altoromutual.com uma busca simples do tipo site:altoromutual.com bastará, como vemos na figura abaixo.

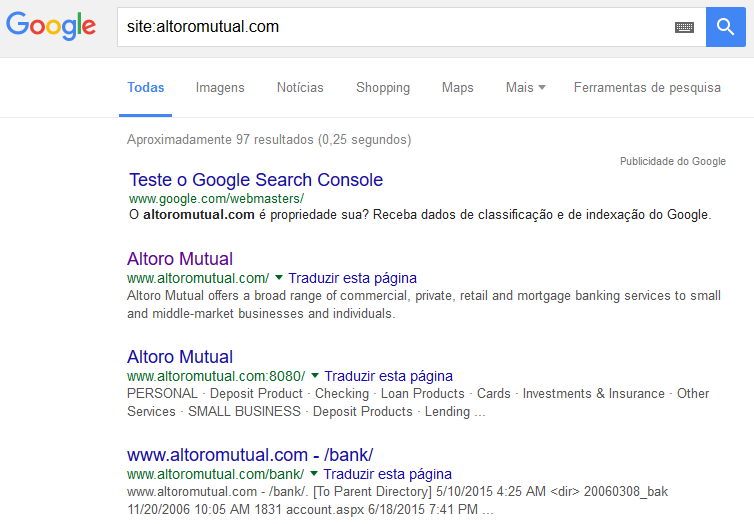


Figura 04 – Operador site

O operador site pode ser facilmente combinado com outros.

**2.5 – filetype: Busca por Arquivos de Tipo Específico**

O Google busca mais que páginas Web. Ele pode procurar diferentes tipos de arquivos, incluindo PDF (Adobe Portable Document Format) e documentos do Microsoft Office. O operador ***filetype*** pode ajudar a localizar esses tipos de arquivos, ou melhor, para ser mais específico, busca por páginas que terminam com uma extensão de arquivo em particular.

Embora nem sempre totalmente exata, a extensão de arquivo pode determinar que tipo de programa o utiliza, uma vez que você use o operador **filetype** para procurar por tipos específicos de arquivos para uma extensão própria.

Para descobrir para que serve algumas extensões desconhecidas você poderá consultar o site http://filext.org, há cerca de oito mil tipos conhecidos de extensões. Isso significa que o Google registra qualquer tipo de página com qualquer tipo de extensão, mas entenda que ele pode não ter a capacidade de buscar um tipo desconhecido.

Vamos pesquisar por arquivos do Microsoft Word (extensão .docx).

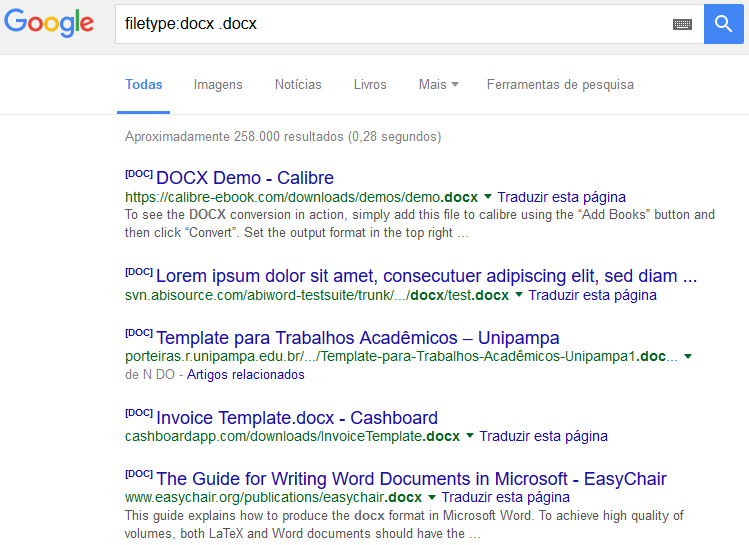


Figura 05 – Operador filetype

Nos primeiros resultados listados, note que há a indicação [DOC] antes do título do documento e um formato de arquivo Microsoft Word, mostrando que o Google reconheceu o arquivo como um documento Microsoft Word.

**2.6 – link: Busca de Links em uma Página**

O operador **link** permite que se busque páginas que tenham links para outras. Em vez de fornecer um termo de busca, o operador requer uma URL ou nome de servidor como argumento. Em sua forma básica, **link** é usado com um nome de servidor, como na figura abaixo.

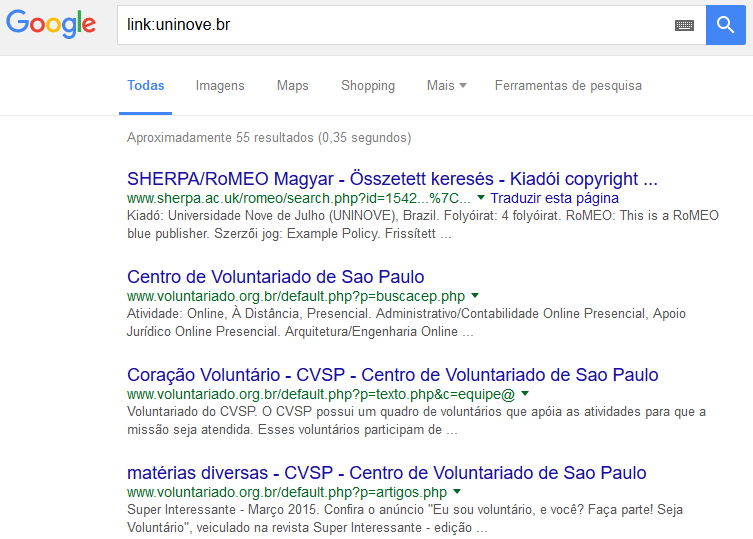


Figura 06 – Operador link

Cada um dos resultados mostrados na figura acima contém links HTML para a página http://www.uninove.br. O operador link pode se estender para incluir não apenas URLs básicas como também completas, que incluem nomes de diretórios, arquivos, parâmetros e outros. Tenha em mente que URLs longas são muito mais específicas e poderiam retomar poucos resultados.

O único lugar em que se visualiza a URL de um **link** é na barra de status de um navegador ou no código fonte da página. Por isso, diferente de outras páginas em cache, a página em cache para a busca de um operador link não destaca o termo de busca, pois este (a página ligada por link) nunca é mostrada. De fato, o banner em cache não faz nenhuma diferença para sua busca.

Quando uma sintaxe inválida de **link**: é fornecida, o Google trata a pesquisa como uma busca de frase.

**2.7 – cache: Mostra a Versão Cache da Página**

Como já discutimos, o Google mantém registros de páginas que podemos acessar via links de cache na página de resultados. Se quiser ir direto para a versão cache de uma página sem primeiro realizar uma busca, simplesmente use o operador avançado cache como em cache:http://www.altoromutual.com. Se não fornecer uma URL completa ou nome de servidor, o Google pode retornar resultados imprevisíveis. Assim como com o operador **link**, passar um nome de servidor ou URL inválidos como parâmetro para o cache irá submeter a busca como uma busca de frase. Uma busca por cache:linux retorna tantos resultados quanto cache linux, indicando que o Google tratou a busca cache como uma busca de frase-padrão.

**2.8 – define: Mostra a Definição de um Termo**

O operador define retoma definições de um termo de busca. Muito simples e direto, seus parâmetros devem ser uma palavra ou frase. Links para a fonte de definições são fornecidos, como vemos na figura abaixo.



Figura 07 – Operador define

O operador define não pode ser usado com outros operadores ou termos de busca.

**2.13 – related: Mostra Site Relacionados**

O operador **related** exibe o que o Google determinou como relacionado a um determinado site. O parâmetro para esse operador é uma URL válida.

Dica: Se você está realizando um pen-test em um site chinês, para que usar um google.com.br? O Google prioriza os resultados para determinados websites. Raramente você vê páginas escritas em japonês, chinês, árabe e outros quando usa o google.com.br, não? Uma boa busca é feita em servidores diferentes, com países diferentes.

Veja na figura abaixo uma pesquisa sobre sites relacionados com a UNINOVE:



Figura 08 – Operador related

**3 – Buscas Interessantes para se Fazer no Alvo**

Nas buscas utilize técnicas avançadas de busca (Google Hacking) para tornar mais eficientes as buscas por informações relevantes:

* **site:domínio-alvo.com** 🡪 Retorna todos os recursos procurado no site alvo;
* **site:domínio-alvo.com login** 🡪 Retorna as ocorrências login no site alvo;
* **link:domínio-alvo.com** 🡪 Retorna todos os sites que contém um link para o domínio alvo;
* **related:domino-alvo.com** 🡪 Retorna páginas similares ao conteúdo do domínio alvo, podemos levantar os concorrentes;
* **filetype:(doc|docx) report site:domínio-alvo.com** 🡪 Retorna documentos com a extensão doc ou docx no site alvo;
* **site:pestebin.com domínio-alvo.com** 🡪 Pesquisar por dados já vazados do alvo.
* **filetype:txt site:domínio-alvo.com** 🡪 Retrona documentos com a extensão txt.
* **site:domínio-alvo.com -www.domínio-alvo.com** 🡪 Retorna outras ocorrências do domínio alvo menos do host www.
* **filetype:rtf site:domínio-alvo.com** 🡪 Retorna documentos com a extensão rtf.
* **filetype:csv site:domínio-alvo.com** 🡪 Retorna documentos com a extensão csv.
* **filetype:xls OR filetype:ppt OR filetype:doc site:domínio-alvo.com** 🡪 Retornam documentos com a extensão xls ou com a extensão ppt ou ainda com a extensão doc.
* **filetype:xlsx OR filetype:pptx OR filetype:docx site:domínio-alvo.com** 🡪 Retornam documentos com a extensão xlsx ou com a extensão pptx ou ainda com a extensão docx.
* **filetype:doc OR filetype:docx site:domínio-alvo.com** 🡪 Retornam documentos com a extensão doc ou ainda com a extensão docx.
* **filetype:ppt OR filetype:pptx site:domínio-alvo.com** 🡪 Retornam documentos com a extensão ppt ou ainda com a extensão pptx.
* **filetype:xls OR filetype:xlsx site:domínio-alvo.com** 🡪 Retornam documentos com a extensão xls ou ainda com a extensão xlsx.
* **filetype:pdf site:domínio-alvo.com** 🡪 Retorna documentos com a extensão pdf.
* "@domínio-alvo.com" -www.domínio-alvo.com 🡪 Retorna ocorrências com possíveis endereços de e-mail.
* **https://groups.google.com/forum/#!search/ domínio-alvo.com** 🡪 Retornam postagens em News Groups do Google.
* **inurl:/etc/passwd%00 intext:root site:domínio-alvo.com** 🡪 Retornam ocorrcncias de LFI no domínio do alvo.
* **inurl:c99 site:domínio-alvo.com** 🡪 Procura por WebShells conhecidas no domínio alvo, isso pode indicar um comprometimento antes mesmo de você tocar no servidor.
* **inurl:r57 site:domínio-alvo.com** 🡪 Idem ao de cima.
* **inurl:pcf vpn site:domínio-alvo.com** 🡪 Arquivos de configuração de VPN.
* **intitle:** **"Index of /" site:domínio-alvo.com** 🡪 Procura por ocorrências de listagem de diretórios no servidor Web.
* **intitle:VNC inurl:5800 site:domínio-alvo.com** 🡪 Procura por acesso a terminais VNC publicados.
* **"VNC desktop" inurl:5800 site:domínio-alvo.com** 🡪 Procura por acesso a terminais VNC publicados.
* **intitle:VNC inurl:5900 site:domínio-alvo.com** 🡪 Procura por acesso a terminais VNC publicados.
* **inurl:ConnectComputer/precheck.htm site:domínio-alvo.com** 🡪 Procura por acesso a terminais TS (Terminal Server)/RDC (Remote Desktop Connection) publicados.
* **inurl:Remote/logon.aspx site:domínio-alvo.com** 🡪 Procura por acesso a terminais TS/RDC publicados.
* **intitle:Remote+Desktop inurl:tsweb site:domínio-alvo.com** 🡪 Procura por acesso a terminais TS/RDC publicados.
* **intitle:Remote+Desktop inurl:tsweb intext:Domain site:domínio-alvo.com** 🡪 Procura por acesso a terminais TS/RDC publicados.
* **filetype:sql site:domínio-alvo.com** 🡪 Procura por arquivos de dump de base de dados no domínio alvo.

**Observação:** Podemos achar várias extensões legais e as aplicações que a utiliza em http://filext.org.

Não limite suas pesquisas a busca padrões, busque assuntos no Google postados em Groups e News, podemos achar coisas interessantes nestes lugares.

As pessoas não têm o mesmo cuidado com as informações de uma empresa onde ele não tem mais vínculo com a empresa. Podendo vazar informações que anteriormente ele não falaria.

Exclua itens que não são relevantes em suas buscas.

Olhe os resultados em cache.

Busque assuntos relacionados ao alvo em fóruns de discussão. Desenvolvedores costumam postar dúvidas em fóruns. Nestas postagens podemos encontrar partes de código fonte, tecnologias utilizadas para suportar as aplicações web, problemas encontrados, bugs e soluções utilizadas nos problemas.

**4 – Google Hacking DataBase (GHDB)**

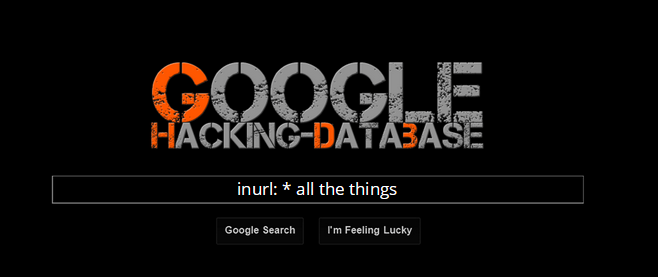


Figura 09 – Google Hacking DataBase

Os atacantes podem usar um tipo especifico de consulta de pesquisa, chamada dork, para localizar problemas de segurança ou dados confidenciais. Os atacantes podem usar dorks para obter logs de firewalls, dados de clientes, para encontrar maneiras de acessar o banco de dados, encontrar erros em web sites, lista de usuários, número de telefones e e-mails, até mesmo senhas, intranets, cartão de crédito entre outras coisas de uma organização.

Profissionais de segurança desenvolvem bibliotecas públicas de dorks. Existem bancos de dados de dorks para vários mecanismos de busca, mas o mais comum é o **Google Hacking DataBase** (também conhecido como GHDB).

O Google Hacking DataBase é um ótimo recurso para localizar dorks que possam auxiliar um atacante. Ele foi criado pelo Johnny Long, e está localizado em http://www.hackersforcharity.org/ghdb/ (você também pode acessar do site http://www.exploit-db.com/google-dorks/).

Para utilizá-lo é fácil basta localizar um tema, por exemplo Error Messages.



Figura 10 – GHDB::Error Messages

Em seguida clique no botão de informação (bolinha azul do lado da explicação).



Figura 11 – GHDB::Error Messages::MySQL

Agora basta clicar no link ou copiar os dados entre aspas duplas e colar no campo de pesquisa do Google.

**5 – 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]** 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