**Comandos para filtrar as buscas no Google**

Ao fazer uma busca no Google, existem certas palavras-chave e operadores que funcionam como uma linguagem de consulta estruturada e têm um significado especial para este mecanismo de busca. Eles são usados ​​para filtrar os resultados. Isso significa que os usuários podem contar com esses operadores para encontrar resultados relevantes para suas buscas com mais rapidez e precisão, embora, por outro lado, uma pessoa mal-intencionada possa usar essas mesmas técnicas para obter informações sensíveis, e isso é o que se conhece como ” Google Dorks “ou” Google Hacking “.

|  |  |  |  |
| --- | --- | --- | --- |
| **Operador** | **Exemplo** | **Propósito** | **Pode ser combinado com outros operadores** |
| site | site:wikipedia.org | Busca um site específico | sim |
| related | related:wikipedia.org | Busca sites relacionados | sim |
| cache | cache:wikipedia.org | Busca com os sites salvos no cache do Google | sim |
| intitle | intitle:wikipedia | Busca um título de uma página | sim |
| inurl | inurl:wikipedia | Search URL | sim |
|  |  |  |  |
| filetype:env | filetype:pdf | Busca arquivos específicos | sim |
| intext | intext:wiki | Busca apenas no texto da página | sim |
| “” | “Wikipedia” | Busca por uma padrão exato | sim |
| + | jaguar + car | Busca por mais de uma palavra | sim |
| – | jaguar speed -car | Exclui palavras da busca | sim |
| OR | jaguar OR car | Combina duas palavras na busca | sim |
| \* | how to \* Wikipedia | Operador coringa, pode ser tudo ou nada na expressão | sim |
| imagesize | imagesize:320×320 | Busca o tamanho da imagem | não |
| @ | @wikipedia | Busca em redes sociais | sim |
| # | #wiki | Busca para hashtags | sim |
| $ | camera $400 | Busca preços | sim |
| .. | camera $50..$100 | Busca dentro de um leque de preços | sim |

**Google Hacking Database GHDB**

O [Google Hacking Database (GHDB)](https://www.exploit-db.com/google-hacking-database) é um projeto open-source que compila uma imensa coleção de *dorks* conhecidos. Este projeto é a eminência no que diz respeito a este assunto, e é atualizado e mantido pelo grupo [Offensive Security](https://www.offensive-security.com/community-projects/" \t "_blank) (os mesmos criadores do Kali Linux, Backtrack e Exploit-DB).

[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-1.jpg)

Imagem 1. Google Hacking Database.

Esses *dorks*, por sua vez, são classificados em diferentes categorias:

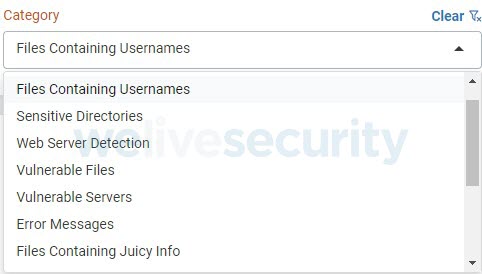
[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-2.jpg)

Imagem 2. Categorias de classificação usadas pelo Google Hacking Database.

A seguir estão alguns exemplos de *dorks* retirados do projeto GHDB e alguns resultados relevantes:

**Exemplo 1:**  
intitle:”webcamXP 5″

Com este *dork*, é possível encontrar webcams modelo “WebcamXP 5” que estão transmitindo ao vivo e que não possuem nenhum tipo de restrição de acesso por IP (whitelist) ou que não requerem autenticação.

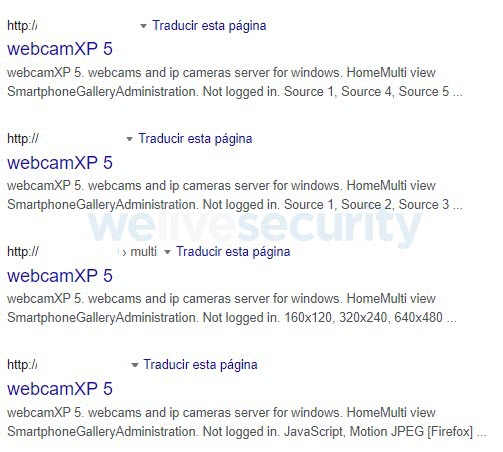
[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-3.jpg)

Imagem 3. Resultados da busca no Google.

[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-4.jpg)

Imagem 4. Exemplo de uma câmera transmitindo ao vivo.

**Exemplo 2:**  
intext:”index of” inurl:ftp

Com o seguinte *dork*, é possível encontrar servidores FTP abertos, que podem estar expondo informações sensíveis e que não requerem nenhum tipo de autenticação.

[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-5.jpg)

Imagem 5. Resultados da busca no Google.

[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-6.jpg)

Imagem 6. Exemplo de um dos resultados.

**Exemplo 3:**  
“Index of” inurl:phpmyadmin

O phpMyAdmin é uma ferramenta do stack do LAMP (Linux, Apache, PHP/Perl/Python, MySQL). Este software é usado para gerenciar um banco de dados MySQL ou MariaDB. Os painéis de login do phpMyAdmin não deve estar acessíveis publicamente e o acesso deve ser restrito por meio de uma lista branca:

[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-7.jpg)

Imagem 7. Resultados da busca no Google.

**Exemplo 4:**inurl:/wp-content/uploads/ ext:txt “username” AND “password” | “pwd” | “pw”

Esta busca permite buscar arquivos txt com as palavras “username”, “password”, “pwd” ou “pw” em sites que usam o popular gerenciador de conteúdo WordPress.

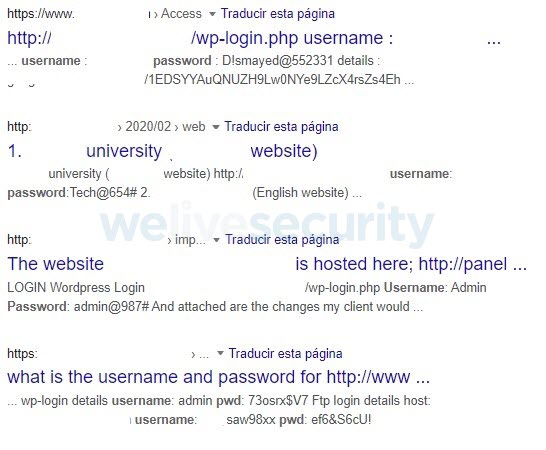
[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-8.jpg)

Imagem 8. Resultados da busca no Google.

[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-9-b.jpg)

Imagem 9. Exemplo de um dos resultados.

**Exemplo 5:**intitle:”index of” “dump.sql”

Essa busca expõe arquivos de backup ou despejos de banco de dados que podem conter informações sensíveis que podem ser acessadas por qualquer pessoa, sem a necessidade de autenticação.

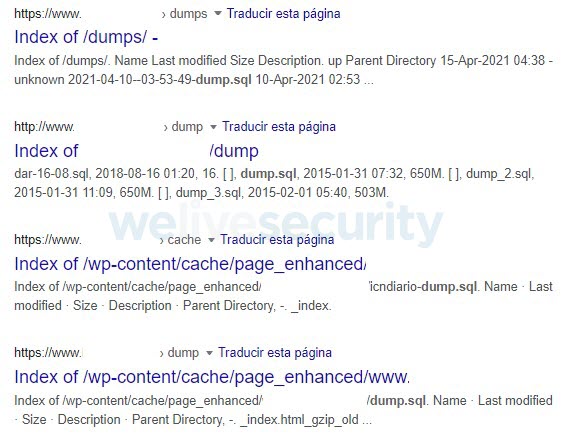
[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-10.jpg)

Imagem 10. Resultados da busca no Google.

[](https://www.welivesecurity.com/wp-content/uploads/2021/07/google-hacking-11-b.jpg)

Imagem 11. Exemplo de um dos resultados.

Depois de destacar alguns exemplos e casos de uso, podemos ver que as possibilidades são muito amplas. Se você tem interesse em saber mais sobre esse assunto, confira os links externos no fim deste post.

Por último, vale a pena refletir sobre essa ferramenta e as opções que ela oferece. É importante configurar a privacidade das contas e serviços expostos na Internet corretamente, a fim de evitar a exposição de informações indevidas que podem ser usadas contra nós por pessoas mal-intencionadas.