

SEGURIDAD DE DATOS



GOOGLE DORKS

ENCUENTRA EL VALOR QUE
ESTÁ EN TI

4 de febrero, 2021
Diana Aimeé Gutiérrez May
Aimeegtzm



"The quieter you become, the
more you are able to hear..."
- Kali Linux

Índice

¿Qué es Google Dorks?

¿Cómo funciona?

Ejemplos de Google Dorking

Intitle



¿Qué es Google Dork?

Google Hacking o Dorks son técnicas para hackear páginas web o servidores usando la búsqueda avanzada de Google como herramienta.

Básicamente, es una cadena de búsqueda que utiliza una consulta de búsqueda avanzada para encontrar información que no está fácilmente disponible en los sitios web. También se considera una actividad ilegal de piratería de Google que los Hackers informáticos suelen utilizar con fines como el terrorismo y el robo cibernéticos.

Dork

Son como criterios de búsqueda en los que un motor de búsqueda devuelve resultados relacionados con tu dork.

¿Cómo funciona?

Un Dork de Google es un empleado que, sin saberlo, expone información corporativa confidencial en Internet. La palabra idiota es jerga para una persona torpe o inepta.

Los Dorks de Google ponen en riesgo la información corporativa porque, sin saberlo, crean puertas traseras que permiten que un atacante ingrese a una red sin permiso y / o obtenga acceso a información no autorizada. Para localizar información confidencial, los atacantes utilizan búsqueda avanzadas cadenas de llamadas consultas de tontos de Google .

Habitualmente, cuando escribo trucos para ser el 1º en Google, Google es bueno, te ayuda y es tu amigo. Pero aquí verás cómo Google puede ser tu peor enemigo. El proceso que sigue un hacker tiene 7 pasos:

1. Localizar objetivo
2. Recopilar información sobre objetivo
3. Identificar vulnerabilidades
4. Explotar vulnerabilidades y acceder
5. Ataque
6. Borrado de huellas
7. Mantener el acceso, para futuras ocasiones

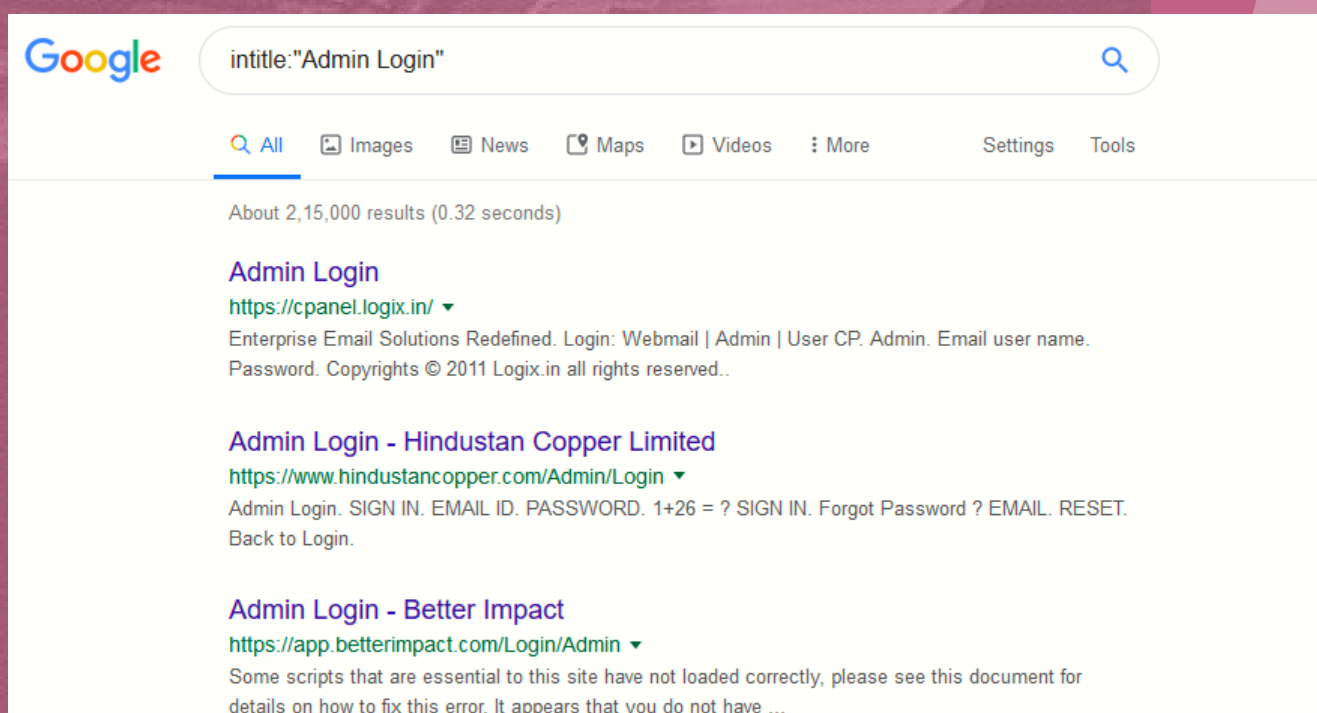
Ejemplos de Google Dorking

- 1.Explora los archivos de registro para obtener credenciales de inicio de sesión.
- 2.Explora configuraciones usando archivos ENV
- 3.Explora las cámaras en vivo
- 4.Para explorar servidores FTP abiertos
- 5.Explora sitios web específicos con dominios específicos
- 6.Ver caché más reciente

| S.No. | Operator | Description | Example |
|-------|-------------------|---|-----------------------------|
| 1 | intitle: | which finds strings in the title of a page | intitle:"Your Text" |
| 2 | allintext: | which finds all terms in the title of a page | allintext:"Contact" |
| 3 | inurl: | which finds strings in the URL of a page | inurl:"news.php?id=" |
| 4 | site: | which restricts a search to a particular site or domain | site:yeahhub.com "Keyword" |
| 5 | filetype: | which finds specific types of files (doc, pdf, mp3 etc) based on file extension | filetype:pdf "Cryptography" |
| 6 | link: | which searches for all links to a site or URL | link:"example.com" |
| 7 | cache: | which displays Google's cached copy of a page | cache:yeahhub.com |
| 8 | info: | which displays summary information about a page | info:www.example.com |

intitle

Este operador indica a Google que busque un término dentro del título de un documento. La mayoría de los navegadores web muestran el título de un documento en la barra de título superior de la ventana del navegador. Este operador no requiere otros argumentos de búsqueda. `intitle:` que es muy similar a `allintitle`, pero solo para la siguiente palabra. “`Intitle: Admin Login`” busca solo páginas con Admin en el título y Login en cualquier lugar de la página.



The screenshot shows a Google search interface with the query "intitle:Admin Login" in the search bar. The results show approximately 2,15,000 results found in 0.32 seconds. Three results are visible:

- Admin Login**
<https://cpanel.logix.in/> ▼
Enterprise Email Solutions Redefined. Login: Webmail | Admin | User CP. Admin. Email user name. Password. Copyrights © 2011 Logix.in all rights reserved..
- Admin Login - Hindustan Copper Limited**
<https://www.hindustancopper.com/Admin/Login> ▼
Admin Login. SIGN IN. EMAIL ID. PASSWORD. 1+26 = ? SIGN IN. Forgot Password ? EMAIL. RESET. Back to Login.
- Admin Login - Better Impact**
<https://app.betterimpact.com/Login/Admin> ▼
Some scripts that are essential to this site have not loaded correctly, please see this document for details on how to fix this error. It appears that you do not have ...

Bibliografía

Implementing Processes. (2021) ¿Qué es Google idiota? – Definición de WhatIs.com. Retrieved February 04, 2021, from <https://whatis.techtarget.com/definition/Google-dork>

Clicking Here. (2021) Google Hacking & Dorks (46 ejemplos): cómo consigue un hacker contraseñas usando sólo Google. Google puede ser tu peor enemigo. | 14 de enero de 2021 Limpiar Reputación Online y SEO Google. Retrieved February 04, 2021, from <https://antoniogonzalezm.es/google-hacking-46-ejemplos-hacker-contrasenas-usando-google-enemigo-peor/>

Antonio Gonzalez . (2021) Google Hacking & Dorks (46 ejemplos): cómo consigue un hacker contraseñas usando sólo Google. Google puede ser tu peor enemigo. | 14 de enero de 2021 Limpiar Reputación Online y SEO Google. Retrieved February 04, 2021, from <https://antoniogonzalezm.es/google-hacking-46-ejemplos-hacker-contrasenas-usando-google-enemigo-peor/>

Yeahhub. (2021) Top 8 Basic Google Search Dorks [Live Examples] – Yeah Hub. Retrieved February 04, 2021, from <https://www.yeahhub.com/top-8-basic-google-search-dorks-live-examples/>