2021

Google Dorking

EL HACKING DE GOOGLE

ISAAC PERALTA

UNIVERSIDAD DEL CARIBE | PRIMAVERA 2021

Introducción

El *Google Dorking* es una técnica de "hacking" que utiliza la búsqueda avanzada de Google para poder encontrar agujeros de seguridad en la configuración del sitio.

Estás técnicas pueden ser usadas para filtrar información, obteniendo mejores resultados, pero lo interesante es que gracias a la búsqueda avanzada podemos acceder a información que normalmente oculta.

El primero en utilizar estás técnicas fue Johny Long quien encontró que se podían hacer consultas que funcionaban con la búsqueda de Google con las que se podían descubrir vulnerabilidades o revelar información o documentos ocultos.

¿Cómo funciona?

Cómo tal no se está haciendo hacking desde Google. Se pueden utilizar las herramientas de búsqueda avanzada para rastrear Internet en busca de los títulos de las páginas dentro de sitios web poco seguros y en algunas ocasiones se podrá encontrar información sensible. El objetivo del Google Dorking es encontrar vulnerabilidades.

La búsqueda avanzada de Google permite usar operadores lógicos como OR, NO y AND; el buscador avanzado distingue entre mayúsculas y minúsculas por lo que es necesario escribir estos operadores siempre con mayúsculas.

Otros comandos de búsqueda son los siguientes:

- flights [código IATA ciudad] [código IATA ciudad], sirve para mostrar los vuelos de una ciudad a otra.
- link, encuentra sitios con un dominio específico.
- *..*, donde * es un número, sirve para hacer búsquedas con rangos numéricos.
- in, que convierte unidades de un tipo a otro (inches in foot)
- site, busca el término buscado en un sitio en específico o dominio específico
- allintitle, muestra resultados con la frase especificado en el título
- intitle, muestra resultados con el término especificado en el título.
- inbogtitle, muestra resultados de blogs con el término en el título
- inposttitle, muestra resultados con un solo término en el título
- allintext, resultados con los términos especificados en el contenido
- allinanchor, muestra los sitios con su término de búsqueda en los enlaces
- allinurl, resultados con el término en el url
- inurl, muestra los sitios con un primer término en el url y un segundo en el contenido
- allinpostauthor, muestra contenido con el autor buscado
- related, muestra resultados relacionados a una url especificada
- info, muestra información sobre el dominio buscado
- define, devuelve la definición de una palabra
- source, busca menciones de un término (que puede ser una persona) en una fuente de noticias específica
- location, muestra artículos de la locación n especificada

- filetype, encuentra documentos del tipo especificado
- ext, archivos de la extensión especificada
- movie, muestra los tiempos en cartelera de una película específica
- weather, resultados sobre el tiempo de un lugar especificado
- stocks, muestra información sobre las acciones de una empresa especificada
- cache, muestra el cache de más reciente de una página
- map, muestra el mapa de una ubicación especificada
- equation, calcula una operación
- tip calculator, ayuda a calcular la propina
- minute timer, muestra un temporizador con el tiempo especificado
- sinrise | Sunset muestra la hora del próximo amanecer para un lugar específico
- flight numbrer, muestra el número de vuelo o estado de vuelo de un vuelo en específico
- sports team, muestra la puntuación de un juego actual
- insubject, encuentra mensajes de grupo con el contenido especificado
- group, encuentra mensajes de un grupo desde una fuente específica
- numrange, encuentra el rango de número en una consulta de hasta 5 digitos
- daterange, busca el rango de fechas con el uso de fechas julianas
- msgid, línea para identificar mensajes en correos electrónicos o grupos de noticias de Usenet

Evitar que te hagan Dorking

Para poder evitar el dorking en nuestro sistema es necesario que tenga al día las actualizaciones del sistema operativo, de los servicios y aplicaciones. Asegurarse de tener un antivirus y no almacenar información sensible en lugares públicos.

Si eres propietario de un sitio web necesitas configurar un archivo llamado robots.txt para evitar que Google Dorks acceda a datos importantes.