Google Hacking
Google Dorks

Estudiante: Kenneth Diaz Gonzalez

Definición

Podemos usar el buscador de Google para encontrar datos interesantes accidentalmente expuestos a internet. Esta simple barra de búsqueda tiene el potencial de ayudarte a protegerte a ti mismo o a tu sitio web contra visitas no deseadas de hackers. De esta manera, si eres un operador o propietario de un sitio web, puedes intentar averiguar qué compartes con el mundo.

Hacking de Google

El hacking de Google, también llamado Google Dorking, es una técnica de “hacking” a veces solo referida como dork, que utiliza la búsqueda avanzada de Google para encontrar agujeros de seguridad en la configuración y el código del sitio web.

Podemos utilizar algunas técnicas para filtrar la información, obtener mejores resultados de búsqueda, pero en este caso, nos centraríamos en la información normalmente no accesible. Como mostrar las imágenes de las cámaras y los documentos.

Todo comenzó en 2002 cuando un hombre llamado Johnny Long comenzó a recopilar consulta que funcionaban en la búsqueda de Google y con las que se podían descubrir vulnerabilidades o revelar información sensible u oculta. Las etiquetó como “tontos de Google”. Mas tarde esto se convirtió en una gran base de datos, eventualmente organizada en la base de datos de Google Hacking.

No puede hackear sitios web directamente usando Google, solo estas haciendo uso de herramientas de búsqueda avanzada disponibles públicamente. Google utiliza capacidades de motor para rastrear internet e indexar los títulos de las paginas, dentro de algunos sitios web poco seguros se puede incluir información sensible. Básicamente, al piratear puedes encontrar vulnerabilidades.

Existen múltiples opciones para definir con mayor precisión tu consulta en https://www.google.com/advanced_search y si te fijas en la parte derecha de esa pagina hay

incluso pistas.

Resumen de operadores de búsqueda

1. La búsqueda en Google distingue entre mayúsculas y minúsculas cuando usamos operadores lógicos. Por tanto, no puede escribir oR, o anD, sino que debes usar mayúsculas o símbolos.

2. OR puede ser reemplazado por el símbolo |

3. NO puede ser reemplazado por el símbolo menos –

4. AND puede ser reemplazado por un solo espacio (pulsando el espacio), pero los resultados pueden diferir si tecleamos AND específicamente entre las palabras.

5. Flights [código IATA ciudad] [código IATA ciudad] muestra los vuelos de una ciudad a otra, incluso si se introduce el código de aeropuerto de IATA como PRG LON

6. Link encuentra sitios que enlazas con su dominio especifico, como “link:ma-no.org”

7. .. Busca dentro de un rango de números, como ‘2002 .. 2020’ o ’25..75’.

8. In convierte las unidades, ejemplo “inches in a foot”

9. site muestra el termino buscad dentro de un sitio especifico, como ‘site:elcorteingles.es watches’ o el dominio especifico ‘site:uk amazon’.

10. Allintitle muestra los resultadoscon la frase buscada en el titulo, ejemplo “intitle”: “salta” .

11. Inblogtitle muestra los resultados de los blogs con la frase buscada en el titulo “inblogtitle: programacion”

12. Inposttitle muestra los resultados con un solo termino con el titulo, como “inposttitle: programacion”

13. Allintext muestra los resultados de las paginas con los términos en el contenido

14. allinanchor - muestra los sitios con su término de búsqueda en los enlaces, ejemplo ‘allinanchor: "ma-no.org" ’

15. allinurl - muestra los resultados a las páginas con los términos en la URL, ejemplo ‘allinurl: virus’

16. inurl - muestra los resultados con el primer término de búsqueda en la URL y el segundo

término es el contenido, 'Inurl: vista de películas'.

17. allinpostauthor - muestra el contenido escrito por el autor buscado, ejemplo 'allinpostauthor': Bukowski'.

18. related - muestra los resultados relacionados con la URL buscada, 'related:NYtimes.com'.

19. info - muestra información sobre el dominio buscado, como 'Info:diariodemallorca.com'.

20. define - 'define:dorking' devolverá la definición de la palabra dada.

21. source - busca menciones de una persona o cosa específica en una determinada fuente de noticias. 'metro source:diario de mallorca'

22. location - muestra artículos basados en una ubicación específica, como "ubicación:playas de Mallorca

23. filetype - Encontrar documentos del tipo especificado, ejemplo 'filetype:pdf gatos'.

24. ext - Muy similar a Filetype pero podemos buscar extensiones poco comunes para obtener resultados más precisos, por ejemplo 'ext:flac mysong'.

25. movie - muestra los tiempos de una película específica en un lugar específico

26. weather - mostrar los resultados del tiempo en un lugar específico, ejemplo "tiempo:palma de mallorca"

27. stocks - muestra el precio de las acciones de una compañía específica. Es decir, "acciones:Starbucks

28. cache - muestra el caché más reciente de una página web específica, ejemplo "cache:ma-no.org

29. map - muestra el mapa de la ubicación especificada, como 'mapa: "sierra de tramuntana"'.

30. equation - calcula los números, por ejemplo "10x4".

31. tip calculator - calculadora de propinas que te ayuda a decidir cuánto dar una propina, ejemplo ".

32. minute timer - muestra un temporizador con su tiempo especificado, como "temporizador de 2 minutos"

33. stopwatch - muestra un cronómetro, ejemplo "cronómetro

34. sunrise | Sunset - muestra la hora del amanecer y del atardecer para un lugar específico,

ejemplo "amanecer palma

35. flight number - muestra el número de vuelo - estado de un vuelo específico, ejemplo 'FR 6363'.

36. sports team - muestra la puntuación de un juego actual "Real Madrid Barcelona".

37. insubject - Encontrar mensajes de grupo con contenido específico, como 'insubordinación: "rastreadores de sitios web" ' '.

38. group - Encuentra mensajes de grupo de una fuente específica, ejemplo "grupo: "google dorks" '

39. numrange - Encuentra el rango de números en una consulta de hasta 5 dígitos

40. daterange - Busca en el rango de fechas, con el uso de fechas julianas, ejemplo 'daterange:2452463.5 2452464'.

41. msgid - Línea de identificación de mensajes utilizada en el correo electrónico y en los grupos de noticias de Usenet.