

Cos'è Google Dorks? - Guida agli operatori di ricerca

Redazione | 03/04/2025 | Open source intelligence

Google Hacking

Il Google dorking, noto anche come Google hacking, può restituire informazioni difficili da trovare con semplici query di ricerca. Utilizzando questa tecnica, è possibile scoprire informazioni non destinate all'accesso pubblico.

Il Google Hacking Database (GHDB) è una fonte autorevole per interrogare l'ampia portata del motore di ricerca Google. I suoi contenuti sono termini di ricerca che permettono di trovare nomi utente, password e persino file contenenti informazioni sensibili. Il GHDB si trova qui:

<https://www.exploit-db.com/google-hacking-database/>

Operatori di Ricerca di Google e Bing

Operatore	Descrizione
"Search Term"	Cerca la frase esatta tra ""
-	Rimuove le pagine che menzionano un dato termine dai risultati della ricerca
+	Forza Google a restituire parole comuni che potrebbero essere scartate normalmente
OR	Cerca un dato termine di ricerca OR un altro termine
site:	Cerca all'interno di un dato dominio
filetype:	Cerca un certo tipo di file
intitle:	Cerca siti con le parole date nel titolo della pagina
inurl:	Cerca siti con le parole date nell'URL
intext:	Cerca siti con le parole date nel testo della pagina
inanchor:	Cerca siti che hanno le parole date nei link che puntano ad essi
cache:	Mostra la cache più recente di una pagina web
IP:	Solo Bing: Trova risultati basati su un dato indirizzo IP
linkfromdomain:	Solo Bing: Cerca link sul dominio dato

Funzionalità Aggiuntive di Google

- Strumenti di Ricerca: Il pulsante "Strumenti" presenta una nuova riga di opzioni, che consente di restringere i risultati della ricerca. Una delle opzioni più interessanti di questa funzionalità è "Intervallo Personalizzato", che può essere utilizzato per cercare entro un determinato intervallo di tempo.
- Google Immagini: Il servizio di ricerca inversa di immagini più potente. <https://images.google.com/>

Ricerca di Informazioni Archivate

- Google e Bing: entrambi i motori di ricerca offrono una vista memorizzata nella cache dei risultati.
- The Wayback Machine: <http://archive.org/web/>
- Archive Today: <http://archive.is/>

Yandex

Yandex gestisce il motore di ricerca più grande in Russia con circa il 65% delle quote di mercato.

Operatori di Ricerca Yandex

Esempio	Descrizione
"* music"	Trova tutti i risultati con qualsiasi parola dove si trova l'asterisco (*)
Cheshire cat \ hatter \ Alice	Cerca qualsiasi parola nella query. Questa query funziona anche per Google
croquet+flamingo	Questa query richiederebbe che la pagina abbia la parola "flamingo", ma non "croquet"
rhost:org.wikipedia.*	Ricerca inversa dell'host
mime:pdf	Cerca un tipo di file specifico
!Curiouser!and!curiouser	Cerca parole identiche multiple
Twinkle twinkle little-star	Esclude "star" dai risultati della ricerca
lang:en	Restringe la ricerca per lingua
date:200712*,date:20071215..20080101,date:>20091231	Restringe la ricerca per data o intervallo di date

Motori di Ricerca: Altre Alternative

- carrot2.org: Carrot2 è un motore di ricerca cluster che raggruppa i risultati della ricerca in insiemi di argomenti
- www.exalead.com/search: Exalead funziona bene nel trovare documenti che contengono il termine di ricerca
- millionshort.com: Million Short consente di rimuovere i risultati che collegano ai siti web più popolari
- globalfilesearch.com: il sito afferma di aver indicizzato 243 terabyte di file memorizzati su server FTP pubblici
- Shodan: Shodan è un motore di ricerca per trovare dispositivi connessi a Internet e tipi di dispositivi. Consente di cercare webcam, router, dispositivi IoT/SCADA e altro.

Filtri Shodan

Filtro	Descrizione
city:	Cerca risultati in una data città
country:	Cerca risultati in un dato paese (codice a 2 lettere)
port:	Cerca una porta specifica o porte
hostname:	Cerca valori che corrispondono al nome host
net:	Cerca un dato IP o subnet (es.: 192.168.1.0/24)
product:	Cerca il nome del software identificato nel banner
version:	Cerca la versione del prodotto
os:	Cerca un nome di sistema operativo specifico
title:	Cerca nel contenuto estratto dal tag HTML
html:	Cerca nel contenuto HTML completo della pagina restituita

Social Networks

Facebook

- Barra di ricerca: consente di cercare tutti i profili creati utilizzando un dato indirizzo email o numero di telefono.
- ID Facebook: l'UserID di Facebook può essere trovato utilizzando <https://findmyfbid.com>. In alternativa, mentre si è loggati su Facebook, l'UserID può essere trovato nel codice sorgente HTML dopo il tag `fb://profile/`.

Facebook Graph Search

Risultato	Query
Luoghi visitati / Luoghi visitati recentemente / Luoghi in cui si è effettuato il check-in / Luoghi piaciuti	<code>/search/UserID/places /search/UserID/places-visited /search/UserID/recent-places-visited /search/UserID/places-checked-in /search/UserID/places-liked</code>
Pagine piaciute	<code>/search/UserID/pages-liked</code>
Foto di / Foto di / Foto piaciute / Foto commentate	<code>/search/UserID/photos /search/UserID/photos-of /search/UserID/photos-by /search/UserID/photos-liked /search/UserID/photos-commented</code>
App usate	<code>/search/UserID/apps</code>
Video di / Video di / Video piaciuti / Video commentati	<code>/search/UserID/videos /search/UserID/videos-of /search/UserID/videos-by /search/UserID/videos-liked /search/UserID/videos-commented</code>
Eventi a cui si è partecipato nel 2010	<code>/search/UserID/events /search/str/UserID/events-joined/2010/date/ events/intersect/</code>
Post contrassegnati / Post piaciuti / Post per anno	<code>/search/UserID/stories-by /search/UserID/stories-tagged /search/UserID/stories-liked /search/UserID/stories-by/2010/date/ stories/intersect</code>
Amici / Parenti / Follower / Gruppi / Datori di lavoro / Colleghi	<code>/search/UserID/friends /search/UserID/relatives /search/UserID/followers /search/UserID/groups /search/UserID/employers /search/UserID/employees</code>
Persone che hanno messo mi piace a una pagina	<code>/likers</code>

Operatori di Ricerca Twitter

Operatore	Trova Tweet...
<code>twitter search</code>	Contenenti sia "twitter" che "search". Questo è l'operatore predefinito
<code>"happy hour"</code>	Contenenti la frase esatta "happy hour"
<code>love OR hate</code>	Contenenti "love" o "hate" (o entrambi)
<code>beer -root</code>	Contenenti "beer" ma non "root"
<code>#haiku</code>	Contenenti l'hashtag "haiku"
<code>from:alexiskold</code>	Inviati dall'utente "alexiskold"
<code>to:techcrunch</code>	Inviati all'utente "techcrunch"
<code>@mashable</code>	Referenzianti l'utente "mashable"
<code>"happy hour" near:"san francisco"</code>	Contenenti la frase esatta "happy hour" e inviati da "San Francisco"
<code>near:NYC within:15mi</code>	Inviati entro 15 miglia da "NYC"
<code>superhero since:2010-12-27</code>	Contenenti "superhero" e inviati dalla data "2010-12-27"
<code>ftw until:2010-12-27</code>	Contenenti "ftw" e inviati fino alla data "2010-12-27"
<code>hilarious filter:links</code>	Contenenti "hilarious" e colleganti a URL
<code>news source:"Twitter Lite"</code>	Contenenti "news" e inseriti tramite Twitter Lite
<code>geocode:47.37,8.541,10km</code>	Inviati entro 10 km da Zurigo

Google Dorks: Guida approfondita e suggerimenti per ricerche avanzate

01

Che cosa sono i Google Dorks e come funzionano

I Google Dorks sono tecniche di ricerca avanzate che utilizzano operatori specializzati per trovare informazioni specifiche e spesso nascoste su Internet. Sfruttano operatori come 'site:', 'inurl:', 'intitle:', 'intext:' e 'filetype:' per ottenere risultati mirati e accedere a contenuti altrimenti difficili da trovare.

02

Utilizzo responsabile dei Google Dorks ed aspetti legali

L'uso responsabile dei Google Dorks è fondamentale. Devono essere utilizzati per scopi autorizzati, ad esempio valutazioni di sicurezza con il permesso. Azioni come l'aggirare paywall o pagine di autorizzazione possono essere illegali. L'uso etico implica buone intenzioni, evitare accessi non autorizzati e seguire i Termini di Servizio di Google.

03

Misure di sicurezza per proteggere il tuo sito web dai Google Dorks

E' essenziale implementare diverse misure di sicurezza, tra cui: utilizzare web application firewall, impostare meccanismi di autenticazione robusti, limitare le informazioni mostrate nei messaggi di errore, proteggere i file tramite il file robots.txt, aggiornare regolarmente il software e disabilitare l'indicizzazione delle directory con .htaccess.

04

Applicazioni pratiche dei Google Dorks in SEO, marketing e analisi della concorrenza

I Google Dorks offrono un supporto significativo in attività SEO, marketing e analisi della concorrenza. Permettono di ottimizzare i contenuti, scoprire i concorrenti, valutare le strategie di marketing e recuperare dati preziosi per migliorare le campagne.



Google Hacking

Il Google dorking, noto anche come Google hacking, può restituire informazioni difficili da trovare con semplici query di ricerca. Utilizzando questa tecnica, è possibile scoprire informazioni non destinate all'accesso pubblico.

Il Google Hacking Database (GHDB) è una fonte autorevole per interrogare l'ampia portata del motore di ricerca Google. I suoi contenuti sono termini di ricerca che permettono di trovare nomi utente, password e persino file contenenti informazioni sensibili. Il GHDB si trova qui: <https://www.exploit-db.com/google-hacking-database/>

Operatori di Ricerca di Google e Bing

Operatore	Descrizione
"Search Term"	Cerca la frase esatta tra ""
-	Rimuove le pagine che menzionano un dato termine dai risultati della ricerca
+	Forza Google a restituire parole comuni che potrebbero essere scartate normalmente
OR	Cerca un dato termine di ricerca OR un altro termine
site:	Cerca all'interno di un dato dominio
filetype:	Cerca un certo tipo di file
intitle:	Cerca siti con le parole date nel titolo della pagina
inurl:	Cerca siti con le parole date nell'URL
intext:	Cerca siti con le parole date nel testo della pagina
inanchor:	Cerca siti che hanno le parole date nei link che puntano ad essi
cache:	Mostra la cache più recente di una pagina web
IP:	Solo Bing: Trova risultati basati su un dato indirizzo IP
linkfromdomain:	Solo Bing: Cerca link sul dominio dato

Funzionalità Aggiuntive di Google

- Strumenti di Ricerca: Il pulsante "Strumenti" presenta una nuova riga di opzioni, che consente di restringere i risultati della ricerca. Una delle opzioni più interessanti di questa funzionalità è "Intervallo Personalizzato", che può essere utilizzato per cercare entro un determinato intervallo di tempo.
- Google Immagini: Il servizio di ricerca inversa di immagini più potente. <https://images.google.com/>

Ricerca di Informazioni Archivate

- Google e Bing: entrambi i motori di ricerca offrono una vista memorizzata nella cache dei risultati.
- The Wayback Machine: <http://archive.org/web/>
- Archive Today: <http://archive.is/>

Yandex

Yandex gestisce il motore di ricerca più grande in Russia con circa il 65% delle quote di mercato.

Operatori di Ricerca Yandex

Esempio	Descrizione
"I* music"	Trova tutti i risultati con qualsiasi parola dove si trova l'asterisco (*)
Cheshire cat \\\ hatter \\\ Alice	Cerca qualsiasi parola nella query. Questa query funziona anche per Google
croquet+flamingo	Questa query richiederebbe che la pagina abbia la parola "flamingo", ma non "croquet"
rhost:org.wikipedia.*	Ricerca inversa dell'host
mime:pdf	Cerca un tipo di file specifico

!Curiouser!and!curiouser
Twinkle twinkle little-star
lang:en
date:200712*,date:20071215..20080101,date:>20091231

Cerca parole identiche multiple
Esclude "star" dai risultati della ricerca
Restringe la ricerca per lingua
Restringe la ricerca per data o intervallo di date

Motori di Ricerca: Altre Alternative

- carrot2.org: Carrot2 è un motore di ricerca cluster che raggruppa i risultati della ricerca in insiemi di argomenti
- www.exalead.com/search: Exalead funziona bene nel trovare documenti che contengono il termine di ricerca
- millionshort.com: Million Short consente di rimuovere i risultati che collegano ai siti web più popolari
- globalfilesearch.com: il sito afferma di aver indicizzato 243 terabyte di file memorizzati su server FTP pubblici
- Shodan: Shodan è un motore di ricerca per trovare dispositivi connessi a Internet e tipi di dispositivi. Consente di cercare webcam, router, dispositivi IoT/SCADA e altro.

Filtri Shodan

Filtro	Descrizione
city:	Cerca risultati in una data città
country:	Cerca risultati in un dato paese (codice a 2 lettere)
port:	Cerca una porta specifica o porte
hostname:	Cerca valori che corrispondono al nome host
net:	Cerca un dato IP o subnet (es.: 192.168.1.0/24)
product:	Cerca il nome del software identificato nel banner
version:	Cerca la versione del prodotto
os:	Cerca un nome di sistema operativo specifico
title:	Cerca nel contenuto estratto dal tag HTML
html:	Cerca nel contenuto HTML completo della pagina restituita

Social Networks

Facebook

- Barra di ricerca: consente di cercare tutti i profili creati utilizzando un dato indirizzo email o numero di telefono.
- ID Facebook: l'UserID di Facebook può essere trovato utilizzando <https://findmyfbid.com>. In alternativa, mentre si è loggati su Facebook, l'UserID può essere trovato nel codice sorgente HTML dopo il tag `fb://profile/`.

Facebook Graph Search

Risultato	Query
Luoghi visitati / Luoghi visitati recentemente / Luoghi in cui si è effettuato il check-in / Luoghi piaciuti	<code>/search/UserID/places /search/UserID/places-visited /search/UserID/recent-places-visited /search/UserID/places-checked-in /search/UserID/places-liked /search/UserID/pages-liked</code>
Pagine piaciute	<code>/search/UserID/photos /search/UserID/photos-of /search/UserID/photos-by /search/UserID/photos-liked /search/UserID/photos-commented</code>
Foto di / Foto di / Foto piaciute / Foto commentate	<code>/search/UserID/apps</code>
App usate	

Video di / Video di / Video piaciuti / Video commentati

Eventi a cui si è partecipato nel 2010

Post contrassegnati / Post piaciuti / Post per anno

Amici / Parenti / Follower / Gruppi / Datori di lavoro / Colleghi

Persone che hanno messo mi piace a una pagina

/search/UserID/videos /search/UserID/videos-of
/search/UserID/videos-by /search/UserID/videos-liked
/search/UserID/videos-commented /search/UserID/events
/search/str/UserID/events-joined/2010/date/ events/intersect/
/search/UserID/stories-by /search/UserID/stories-tagged
/search/UserID/stories-liked /search/UserID/stories-by/2010/date/
stories/intersect
/search/UserID/friends /search/UserID/relatives
/search/UserID/followers /search/UserID/groups
/search/UserID/employers /search/UserID/employees
/likers

Operatori di Ricerca Twitter

Operatore
twitter search

"happy hour"
love OR hate
beer -root
#haiku
from:alexiskold
to:techcrunch
@mashable
"happy hour" near:"san francisco"

near:NYC within:15mi
superhero since:2010-12-27

ftw until:2010-12-27

hilarious filter:links
news source:"Twitter Lite"
geocode:47.37,8.541,10km

Trova Tweet...

Contenenti sia "twitter" che "search". Questo è l'operatore predefinito

Contenenti la frase esatta "happy hour"

Contenenti "love" o "hate" (o entrambi)

Contenenti "beer" ma non "root"

Contenenti l'hashtag "haiku"

Inviati dall'utente "alexiskold"

Inviati all'utente "techcrunch"

Referenzianti l'utente "mashable"

Contenenti la frase esatta "happy hour" e inviati da "San Francisco"

Inviati entro 15 miglia da "NYC"

Contenenti "superhero" e inviati dalla data "2010-12-27"

Contenenti "ftw" e inviati fino alla data "2010-12-27"

Contenenti "hilarious" e colleganti a URL

Contenenti "news" e inseriti tramite Twitter Lite

Inviati entro 10 km da Zurigo

Google Dorks: Guida approfondita e suggerimenti per ricerche avanzate

01

Che cosa sono i Google Dorks e come funzionano

I Google Dorks sono tecniche di ricerca avanzate che utilizzano operatori specializzati per trovare informazioni specifiche e spesso nascoste su Internet. Sfruttano operatori come 'site:', 'inurl:', 'intitle:', 'intext:' e 'filetype:' per ottenere risultati mirati e accedere a contenuti altrimenti difficili da trovare.

02

Utilizzo responsabile dei Google Dorks ed aspetti legali

L'uso responsabile dei Google Dorks è fondamentale. Devono essere utilizzati per scopi autorizzati, ad esempio valutazioni di sicurezza con il permesso. Azioni come l'aggirare paywall o pagine di autorizzazione possono essere illegali. L'uso etico implica buone intenzioni, evitare accessi non autorizzati e seguire i Termini di Servizio di Google.

03

Misure di sicurezza per proteggere il tuo sito web dai Google Dorks

E' essenziale implementare diverse misure di sicurezza, tra cui: utilizzare web application firewall, impostare meccanismi di autenticazione robusti, limitare le informazioni mostrate nei messaggi di errore, proteggere i file tramite il file robots.txt, aggiornare regolarmente il software e disabilitare l'indicizzazione delle directory con .htaccess.

04

Applicazioni pratiche dei Google Dorks in SEO, marketing e analisi della concorrenza

I Google Dorks offrono un supporto significativo in attività SEO, marketing e analisi della concorrenza. Permettono di ottimizzare i contenuti, scoprire i concorrenti, valutare le strategie di marketing e recuperare dati preziosi per migliorare le campagne.

