

- **Archive.org**

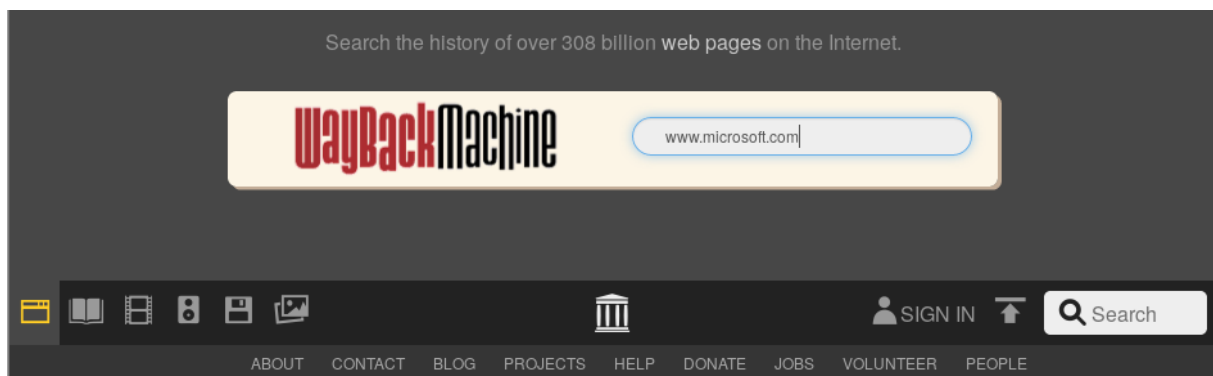
Le 1^{er} outil Web utilisé sera le site www.archive.org, qui garde une base de données de tous les sites web à une date précise.

Dans notre cas, nous effectuons une recherche passive sur la société Microsoft.

A partir de votre machine linux, ouvrez le navigateur Web et saisissez le site www.microsoft.com

Vous êtes sur la page de Microsoft actuellement présente sur les serveurs web de Microsoft.

Maintenant rendez-vous sur le site www.archive.org et saisissez dans la section « search » votre site en question, dans notre cas <http://www.microsoft.com>



Une fois la recherche effectuée, un calendrier s'offre à vous. Sélectionnez une date et « archive » affiche l'image de ce site à cette date précise. Ceci permet de voir si la société a mis des informations vis-à-vis de sa sécurité, ou d'autres informations, sur d'anciennes pages.

- **Google Hacking**

Voici un autre outil, le Google Hack. Cette technique se base sur le moteur de recherche Google et sur les filtres à appliquer sur nos recherches. Cela permet d'essayer de récupérer des données vraiment spécifiques.

1. Toujours dans le contexte de recherche d'informations sur Microsoft.

Dans notre recherche Google, il suffit de rajouter la fonction **site :ledomaine.com/fr/etc...**


Effectuez une recherche **site:microsoft.com**

Google

site:microsoft.com

Tous Images Actualités Shopping Maps Plus Paramètres Outils

Environ 31 500 000 résultats (0,35 secondes)

**Rappel concernant les règles de confidentialité de Google**
[ME LE RAPPELER PLUS TARD](#) [LIRE](#)

Microsoft - Official Home Page
<https://www.microsoft.com/> ▼ Traduire cette page
At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.

Microsoft Virtual Academy – Free Online Training for Developers, IT ...
<https://mva.microsoft.com/> ▼ Traduire cette page
Build your skills and advance your career. Microsoft Virtual Academy (MVA) offers free IT training for Developers, IT Pros, Data Scientists, and students.

Student Developer Tools, Resources and Experiences | Imagine
<https://imagine.microsoft.com/> ▼ Traduire cette page
Bring your ideas to life. Find out how student developers can join Microsoft Imagine, and elevate their skills with developer tools and resources.

Microsoft Exchange, Secure Enterprise Email Solutions for Business
<https://www.microsoft.com/exchange/> ▼ Traduire cette page

Comme vous pouvez le constater, le résultat de la recherche ne sort que des URL appartenant au site de microsoft.com

La fonction **site:'lesite'.com** permet donc de retourner des recherches appartenant seulement au site saisi.

Autre test :

Site :offensive-security.com

Offensive Security Training and Professional Services

<https://www.offensive-security.com/> ▼ Traduire cette page

Check out our **Offensive Security** testimonials and reviews [page](#). The OSCP is a certification that has already gained a very solid recognition and I only hope and expect that to continue. I've taken a couple of other **security** related certifications including the CEH, Security+, CISSP and the TigerScheme QSTM. If I had to ...

[Offensive Security Certified ...](#) · [Offensive Security Exploitation ...](#) · [Virtual Images](#)

Kali Linux Custom Image Downloads - Offensive Security

<https://www.offensive-security.com/kali-linux-vmware-virtualbox-...> ▼ Traduire cette page

Want to download Kali Linux custom images? We have generated several Kali Linux VMware, VirtualBox and ARM images which we would like to share with the community. Note that the images provided below are maintained on a "best effort" basis and all future updates will be listed on this [page](#). Furthermore, **Offensive** ...

Offensive Security Online Training & Pentesting Blog

<https://www.offensive-security.com/blog/> ▼ Traduire cette page

5 juil. 2017 - The customised Kali ISO would undergo an unattended autoinstall in a remote client [site](#), and automatically connect back to our OpenVPN server over TCP port 443. The OpenVPN connection would then bridge the remote and local networks, allowing us full "layer 3" access to the internal network from our ...

Penetration Testing with Kali - Online Security ... - Offensive Security

<https://www.offensive-security.com/...security.../penetration-testing...> ▼ Traduire cette page

On your assigned course start date, you'll be provided access to download all your course materials, including the 8-hour **Offensive Security** PWK course video series in HTML/Flash format and the 350-[page](#) PWK lab guide. You will also receive instructions on how to connect to our virtual penetration testing labs. **Offensive** ...

Information Security Training Online - Offensive Security

<https://www.offensive-security.com/information-security-training/> ▼ Traduire cette page

The **Offensive Security** Advanced Windows Exploitation InfoSec Training Course is particularly intense and demanding and for this reason, is only available in a live training environment, with current dates displayed on the Advanced Windows Exploitation course [page](#). For students who complete the course and wish to put ...

Tous les sites qui en ressortent font partie de offensive-security.com

2. La fonction **inurl:'larecherche'**, qui permet de renvoyer juste des liens qui ont dans leur URL la recherche saisie.

Saisissez : **inurl:test**

Tests gratuits, Test en ligne - Psychologies.com

test.psychologies.com/ ▼

Test gratuit avec Psychologie.com. Plus de 600 tests gratuits, autour de la relation famille enfant, la santé, le travail, le couple et la sexualité - Test et vous ! par Psychologies.com.

[Test de QI 5](#) [Ce test de QI ...](#) · [Test lâcher prise](#) · [Test de QI 2](#) · [Tests de personnalité](#)

Test de QI de 123test.fr

<https://www.123test.fr/test-de-qi/> ▼

Test QI gratuit de 123test.fr. Ce test de QI contient tous les composants communs à la plupart des tests de QI standard.

test — Wiktionnaire

<https://fr.wiktionary.org/wiki/test> ▼

Français[modifier]. Étymologie[modifier]. (Nom 1) (XII^e siècle) Forme collatérale de têt, du latin testum (« pot »). (Nom 2) (1686) De l'anglais test emprunté à l'ancien français test (« pot ») de même origine que le précédent. Voir le mot anglais ci-dessous pour l'évolution sémantique qui conduit de « pot » à « examen ».

[Tester](#) · [Testage](#) · [Testologie](#)

Test & quiz - Gratuit - Doctissimo

test.doctissimo.fr/ ▼

Test santé, test sexualité, test nutrition, test psycho, test grossesse, test forme... Doctissimo vous propose près de 300 tests gratuits !

Tous les sites ont bien « test » dans leur URL

3. Encore une autre fonction **intitle:larecherche** qui permet de sortir tous les liens avec la recherche dans le titre.

Intitle:microsoft

Compte Microsoft | Connectez-vous ou créez votre compte dès ...

<https://account.microsoft.com/account?lang=fr-be> ▼

Connectez-vous avec votre compte Microsoft pour travailler et vous amuser encore plus. La création et l'utilisation d'un compte Microsoft vous permettent d'accéder facilement à tous les éléments numériques.

Support Microsoft

<https://support.microsoft.com/fr-fr> ▼

Ce site utilise des cookies pour l'analyse, ainsi que pour les contenus et publicités personnalisés. En continuant à naviguer sur ce site, vous acceptez cette utilisation. En savoir plus. Passer directement au contenu principal. Microsoft. Support Microsoft. Office · Windows · Surface · Xbox · Offres spéciales · Support technique.

Microsoft Store en ligne - Bienvenue

<https://www.microsoft.com/fr-fr/store/b/home> ▼

Offrez-vous les derniers logiciels et produits technologiques sur le Microsoft Store. Découvrez le meilleur de Microsoft avec un commerce en ligne facile.

Microsoft — Wikipédia

<https://fr.wikipedia.org/wiki/Microsoft> ▼

Microsoft Corporation est une multinationale informatique et micro-informatique américaine, fondée en 1975 par Bill Gates et Paul Allen. Son activité principale consiste à développer et vendre des systèmes d'exploitation, des logiciels et des produits matériels dérivés. En 2013, le chiffre d'affaires s'élevait à 77,85 milliards ...

Office 365 Login | Microsoft Office

<https://www.office.com/> ▼ Traduire cette page

Collaborate for free with online versions of Microsoft Word, PowerPoint, Excel, and OneNote. Save documents, spreadsheets, and presentations online, in OneDrive. Share them with others and work together at the same time.

Microsoft est bien présent dans tous les titres.

4. Il existe aussi une fonction qui permet de faire sortir tous les liens avec un PDF ou n'importe quel format de fichier, la fonction est **ext:'leformat'**
ext:pdf

Le résultat de la recherche pointe bien sur des pdf.

Si vous voulez, par exemple, faire une recherche sur le hack en format pdf. Il faut saisir : **ext:pdf Hack**

[\[PDF\] Lesson 1: Being a Hacker - Hacker Highschool](#)

www.hackerhighschool.org/.../HHS_en1_Being_a_Hacker.v2.pdf ▼ [Traduire cette page](#)

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons ...

[\[PDF\] Hack A Fond', le 1er hackathon qui met en compétition 5 association...](#)

<https://www.theragora.fr/communiqués/CP-B-Braun717.pdf> ▼

6 juil. 2017 - **Hack A Fond'**, le 1er hackathon qui met en compétition. 5 associations de patients pour améliorer la qualité de vie de jeunes malades. 13 et 14 octobre 2017. Pour la 5ème édition de son Prix, la Fondation d'entreprise B. Braun lance le premier « **Hack A Fond'** ». L'AFA, vaincre la maladie de Crohn et.

[\[PDF\] Nuit du Hack 2017 : pourquoi nous aimons les Bug ... - DenyAll.com](#)

<https://www.denyall.com/uploads/2017/07/Press-Release-NDH-17-Final-FR.pdf> ▼

DenyAll a participé une nouvelle fois à l'événement de La Nuit du **Hack** qui a eu lieu à Paris le. 24 et 25 juin dernier. Pour son second "Bug Bounty", DenyAll a vu 2 500 experts tester ses parefeux applicatifs Web et parefeux pour Services Web, afin d'atteindre les quatre sites web et. APIs vulnérables. Les données ...

[\[PDF\] Nuit du Hack Kids : l'ESIEA met les nouvelles technologies à la porté...](#)

<https://www.esiea.fr/wp-content/.../CP-ESIEA-NUIT-DU-HACK-KIDS-2017-VD.pdf> ▼

Paris, 08 juin 2017. C'est en 2003 que l'équipe Hackerz Voice, inspirée par la célèbre conférence DEFCON crée la « **Nuit du. Hack** », l'une des manifestations les plus importantes dédiée à la sécurité informatique. Chaque année, elle accueille le grand public à Paris pendant 24 heures autour de conférences, d'ateliers et ...

5. Il existe une fonction qui est utile si l'objet de votre recherche existe sous plusieurs aspects.

Exemple : Vous souhaitez effectuer une recherche sur un blender, qui est un appareil de cuisine, mais aussi un logiciel de 3D. Si vous entrez « **blender** » sur Google, les résultats seront mitigés. Il est possible de faire un tri.

Pour exemple, je veux retirer tous les résultats qui pointent sur le mot 3D pour cela la fonction est : **recherche -intext :mot**

Exemple : **blender -intext:3D**

Google

blender -intext:3D

Tous Shopping Images Vidéos Actualités Plus Paramètres Outils

Environ 76 800 000 résultats (0,49 secondes)



Rappel concernant les règles de confidentialité de Google

[ME LE RAPPELER PLUS TARD](#) [LIRE](#)

Blender - Retrait 1h en magasin* | Boulanger
<https://www.boulanger.com/c/tous-les-blenders> ▼
Découvrez notre sélection de **Blender** avec Boulanger. Profitez de la livraison offerte* ou du retrait 1h en magasin*. Garantie 2 ans Boulanger.

Blender - Achat Blender pas cher - Rue du Commerce
<https://www.rueducommerce.fr> > [Electroménager](#) > [Préparation culinaire](#) > [Blender](#) ▼
Retrouvez notre offre **Blender** au meilleur prix sur Rue du Commerce avec du stock des services et la livraison rapide.

Blender, blender chauffant, soup maker | La Redoute
www.laredoute.fr > ... > [Petit électroménager](#) > [Robot de cuisine](#) > [Blender](#) ▼
★★★★★ Note : 4,1 - 6 992 votes
Avec votre **blender** professionnel, créez facilement smoothies, milk shakes et glace pilée pour vos invités. Réalisez aussi facilement vos soupes de légumes, pâtes à crêpes ou cocktails à l'aide des différentes lames offertes avec votre **blender**. Grâce au couvercle anti-fuites, adieu les éclaboussures dans la cuisine !

Les résultats pointent seulement sur l'outil de cuisine.

Il est possible d'utiliser la fonction « - » avec d'autres fonctions pour limiter les résultats, par exemple : **-inurl:www*** qui supprime tous les résultats où l'URL commence par www.

- Il est possible de combiner plusieurs fonctions comme **site:lenomdusite - inurl:www***, ce qui donne : je veux tous les résultats de 'lenomdusite' mais pas ceux qui ont www et n'importe quoi derrière.

7. Exercice : Je veux faire une recherche de guide officiel d'office 365 sur le site de microsoft.com au format pdf. Si vous faites une recherche du style « guide office 365 ». Vous avez environ 8 280 000 résultats qui sortent. De plus, les résultats ne sont pas tous de la documentation provenant du site de Microsoft et sont souvent de simples pages html d'explications. Vous devez donc procéder étape par étape pour filtrer progressivement vos recherches.

Etape 1 :

Je veux afficher tous les sites de microsoft.com (**site:microsoft.com**)

Etape2 :

Je veux ensuite filtrer le sous domaine www. (**-inurl:www***)

Etape 3 :

J'ai des résultats dont l'URL (sous-domaine) correspond à curah et windows, qui ne m'intéressent pas, je veux donc les enlever **-inurl:curah* -inurl:windows***)

Etape 4 :

Je veux de la documentation au format PDF (**ext:pdf**)

Etape 5 :

Beaucoup de mes recherches pointent sur d'autres choses que « office 365 », ce qui n'est pas l'objet de ma recherche. Je veux donc des résultats pertinents sur office 365 (**intitle:office 365**)

Etape 6 :

Le résultat de ma recherche a déjà beaucoup diminué, mais j'ai encore des résultats qui ne m'intéressent pas, en rapport avec les termes de licences etc... Je veux trouver uniquement des guides (**intitle :guide**)

Maintenant, vous disposez d'une liste de liens de source officielle Microsoft, au format pdf, qui correspond à office 365. Vous remarquerez que vous passez de 8 280 000 résultats à 22.

Lien vers une liste de dorks exploitable :

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



Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category



Search

Search