

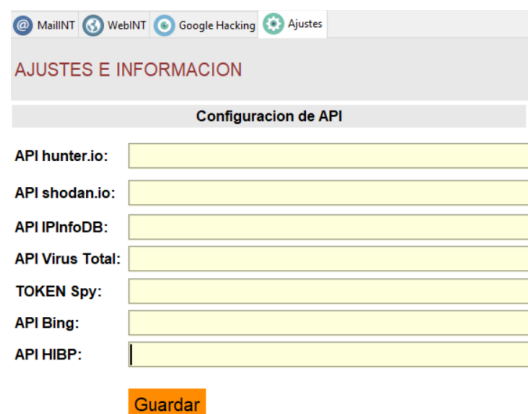
CEREBRO V1.0

MANUAL DE INSTALACIÓN Y USO DE LA HERRAMIENTA

INSTALACIÓN

Para instalar cerebro v1.0 se deben de seguir los pasos a continuación enumerados

- 1- Instalar Python 3.7.3
- 2- Instalar los requerimientos de la aplicación, estos están en el archivo de requirements.txt, para ello basta con abrir la terminal y posicionar en la carpeta donde esta el archivo y escribir **pip install -r requirements.txt**
- 3- Debe de registrarse en las paginas hunter.io, Shodan.io, Ipinfodb.com, virustotal.com, spyonweb.com, Outlook.com, haveibeenpwnd.com, todo esto para obtener acceso a las API de todos estos recursos.
- 4- En la terminal se ejecuta el comando Python **CEREBRO.py** para abrir la aplicación.
- 5- Ir a ajusta y escribir las respectivas API y hacer clic en guardar.



MailINT WebINT Google Hacking Ajustes

AJUSTES E INFORMACION

Configuracion de API

API hunter.io:

API shodan.io:

API IPInfoDB:

API Virus Total:

TOKEN Spy:

API Bing:

API HIBP:

Guardar

- 6- Cerrar la aplicación y abrirla nuevamente, y ya esta lista para que pueda buscar información de correos electrónicos, de sitios web o de cualquier otra índole con Google Hacking.

USABILIDAD

Buscar información de correo electrónico

Para la búsqueda de correos electrónicos se debe escribir la dirección de la cuenta de correo electrónico en el campo respectivo de la pestaña MailINT, hacer clic en Buscar, y esperar que la herramienta muestre los resultados.

CEREBRO v1.0 - AN OPEN SOURCE INTELLIGENCE TOOL

MailINT WebINT Google Hacking Ajustes

CORREO ELECTRONICO

garciaguirre@live.com

Buscar

INFORMACION

No hay resultados en Email Hunter

BRECHAS DE SEGURIDAD

Se han encontrado 11 coincidencias del correo garciaguirre@live.com en brechas de seguridad

- 1 - 000webhost
Titulo: 000webhost
Dominio: 000webhost.com
Fecha: 2015-03-01
- 2 - Adobe
Titulo: Adobe
Dominio: adobe.com
Fecha: 2013-10-04
- 3 - AntiPublic
Titulo: Anti Public Combo List
Dominio:
Fecha: 2016-12-16
- 4 - Canva
Titulo: Canva
Dominio: canva.com
Fecha: 2019-05-24
- 5 - Collection1
Titulo: Collection #1

PASTES

Se han encontrado 0 coincidencias del correo garciaguirre@live.com en Pastes

Buscar información de sitios web

Para la búsqueda de información de sitios web, ir a la pestaña WebINT y se debe escribir la dirección del dominio que se investiga, hacer clic en Buscar y esperar que la herramienta responda con la información, llenando las cajas de texto con la información obtenida, si desea realizar un reporte de la información, después de haberla encontrado, hacer clic en el botón de Reporte.

CEREBRO v1.0 - AN OPEN SOURCE INTELLIGENCE TOOL

MailINT WebINT Google Hacking Ajustes

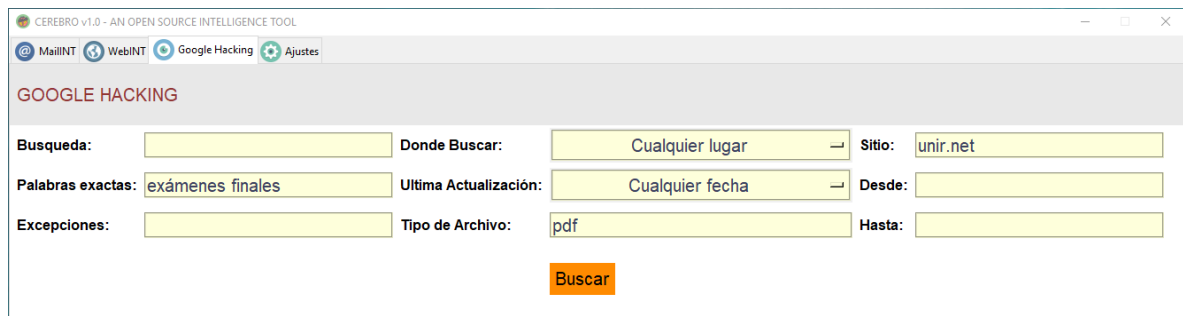
DOMINIO OBJETIVO: microsoft.com

Buscar Reporte

GENERALIDADES		LOCALIZACION		E-MAIL		RED INFO	
URL:	microsoft.com	País:	Singapore	Patron:		AS:	8075
IP:	104.215.148.63	Región:	Singapore	Disponible:		AS Name:	MICROSOFT MICROSOFT
Categoría:	computersandsoftware [information tech]	Ciudad:	Singapore	Webmail:		Hostname:	
Reputación:	safe	Código del país:	SG	Emails:		ISP:	Microsoft Corporation
Actualizado:	2019-08-21T16:26:06.158832	Código Postal:	179431			BGP route:	104.208.0.0/13
Organización:	Microsoft Azure	Latitud:	1.2931000000000097			WHOIS INFO	
		Longitud:	103.83579999999999			WHOIS: { "domain_name": { "MICROSOFT.COM",	
Puertos:	443 80	Zona Horaria:	+08:00			DNS INFO	
Antivirus usados:	71	SUBDOMINIOS		Pastes:		DNS Info: Información de Correos: id 58117 opcode QUERY	
Positivos:	0	mint.microsoft.com schemas.microsoft.com login.microsoft.com v10.events.data.microsoft.com aischool.microsoft.com watson.microsoft.com news.microsoft.com array612-prod.do.dsp.mp.m		Contiene: dox		SAME IP	
Fecha Escaneo:	2019-08-21 01:06:04			HOST INFO		Dominios: 1-advanced-windows-hosting.net 2-advancedwindowshosting.	
Enlace Escaneo:	https://www.virustotal.com/ur/1e9a70dc			S.O:	None		
Vulnerabilidades:	No hay vulnerabilidades			Headers:	{'Date': 'Wed, 21 Aug 2019 21:13:39 GMT', 'Server': 'Kestrel', 'Content-Len		

Búsqueda con Google hacking

Buscar información con Google Hacking es tan simple como elegir lo que se debe investigar, especificar si son palabras exactas, donde se quiere buscar, el tipo de archivo, definir rangos e incluso parámetros de tiempo cuando buscar la información.



The screenshot shows the CEREBRO v1.0 application window. At the top, there's a title bar and a menu bar with options: MailINT, WebINT, Google Hacking (selected), and Ajustes. Below the menu bar, the 'GOOGLE HACKING' section contains a search form with the following fields:

- Busqueda:** (empty text input)
- Donde Buscar:** (dropdown menu showing 'Cualquier lugar')
- Sitio:** (text input with 'unir.net')
- Palabras exactas:** (text input with 'exámenes finales')
- Última Actualización:** (dropdown menu showing 'Cualquier fecha')
- Desde:** (empty text input)
- Excepciones:** (empty text input)
- Tipo de Archivo:** (text input with 'pdf')
- Hasta:** (empty text input)

Below the form is an orange 'Buscar' button.



The screenshot shows the Google search results page for the query "exámenes finales" site:unir.net filetype:pdf. The search bar at the top contains the query. Below the search bar, there are tabs for 'Todo', 'Imágenes', 'Videos', 'Noticias', 'Maps', 'Más', 'Preferencias', and 'Herramientas'. The results section shows "Cerca de 92 resultados (0.43 segundos)".

The first result is a PDF document titled "EL BACHILLERATO RADIOFÓNICO: UNA REALIZACIÓN DE ... - ...". The snippet shows the URL <https://reunir.unir.net/.../6%20El%20Bachillerato%20Radiofónico.pdf?...> and mentions "por A Moreno García - 1973 - Mencionado por 1 - Artículos relacionados". The snippet also includes the date "1 jun. 2019" and the text "diferencia. 6. Exámenes finales.- Para que los estudios seguidos a través de las enseñanzas del Centro Nacional ~engan validez, los alumnos."

The second result is a PDF document titled "Universidad Internacional de La Rioja Facultad de ... - Re-Unir". The snippet shows the URL https://reunir.unir.net/.../2013_02_5_TFM_ESTUDIO_DEL_TRABAJO.pdf?... and mentions "por A Huguet-Parrilla - 2013 - Artículos relacionados". The snippet also includes the date "4 feb. 2013" and the text "En la medida de lo posible, los exámenes finales de trimestre están constituidos por problemas de cursos anteriores. A pesar de ello, una vez."