

Recopilación Pasiva de Información Aplicación de Google Hacking y Shodan en Ciberseguridad

Índice

Introducción.....	2
Contexto y Relevancia de la Recopilación Pasiva de Información.....	2
Objetivos del Trabajo.....	3
Estructura del Documento.....	3
Fundamentos Teóricos.....	4
Google Hacking y sus Técnicas Principales.....	4
Shodan: El Motor de Búsqueda para Dispositivos Conectados.....	5
Aspectos Éticos en la Recopilación Pasiva de Información.....	5
Metodología.....	6
Parte 1: Uso de Google Hacking.....	6
Google Gruyere.....	6
Descripción de las Búsquedas Avanzadas.....	6
Ejemplos de Comandos.....	8
Parte 2: Exploración de Shodan.....	9
Búsquedas Avanzadas con Filtros.....	10
Procedimientos de Documentación.....	11
Uso de filtros en Shodan.....	14
Búsquedas con el filtro Port.....	15
Búsquedas con el filtro Country.....	15
Búsquedas con el filtro org.....	15
Resultados.....	17
Resultados de las Búsquedas con Google Hacking.....	17
Resultados de las Búsquedas con Shodan.....	19
Resultados del parámetro port.....	19
Resultados de las Búsquedas con Country.....	24
Resultados de las Búsquedas con org.....	25
Reflexión Ética.....	29
Implicaciones Éticas del Uso de Google Hacking y Shodan.....	29
Referencias.....	30

• Introducción

○ Contexto y Relevancia de la Recopilación Pasiva de Información

- La **recopilación pasiva de información**, o **enumeración pasiva de información**, es una técnica utilizada en ciberseguridad para obtener datos sobre sistemas, redes y activos digitales sin interactuar directamente con ellos ni generar alertas. A diferencia de las técnicas activas, la recopilación pasiva se enfoca en observar y analizar información disponible, evitando riesgos innecesarios para los sistemas.
- Esta técnica es esencial para la **detección temprana de amenazas**, ya que permite identificar actividades maliciosas sin intervenir en los sistemas. También facilita la **evaluación de la postura de seguridad** de una organización al identificar vulnerabilidades sin intentar explotarlas, lo que reduce el riesgo de comprometer la infraestructura.
- El **OSINT** o **Inteligencia de Fuentes Abiertas**, es un término utilizado para describir la recopilación de información de fuentes públicas disponibles en Internet. OSINT incluye datos de redes sociales, sitios web, foros, bases de datos públicas y otros recursos accesibles al público sin necesidad de acceso especial o permisos.

- Entre las técnicas más comunes se encuentran el **monitoreo de tráfico de red**, el **análisis de registros y eventos** y el **escaneo pasivo de vulnerabilidades**. Estas permiten detectar patrones anómalos, actividades sospechosas o posibles debilidades en los sistemas sin interferir con ellos. Además, herramientas como **Google Hacking** y **Shodan** se utilizan para recopilar información pública sobre dispositivos y servicios expuestos en la red.
- En este trabajo, la recopilación pasiva de información mediante **Google Hacking** y **Shodan** demostrará cómo estas herramientas permiten identificar dispositivos y datos expuestos, proporcionando un enfoque eficaz para la **planificación de estrategias de seguridad** y la **investigación forense**.

○ **Objetivos del Trabajo**

- El objetivo de este trabajo es aplicar técnicas de recopilación pasiva de información, centrándonos en el uso de herramientas como **Google Hacking** y **Shodan**, y reflexionar sobre sus implicaciones éticas. Se explorarán dos enfoques en la recopilación pasiva: el estricto, que evita interacciones directas con el objetivo, y el más flexible, que permite interacciones mínimas según el contexto de la prueba de penetración y las reglas de compromiso establecidas con el cliente.
- Se busca destacar cómo la recopilación pasiva, a través de herramientas como Google Hacking y Shodan, puede ser un punto de partida para descubrimientos significativos en ciberseguridad, facilitando la identificación de dispositivos y datos expuestos, y mejorando el éxito de las evaluaciones de seguridad. Además, se abordarán las consideraciones éticas relacionadas con la recopilación de información, enfatizando la importancia de respetar la privacidad y las políticas de uso de los recursos públicos, así como la necesidad de actuar de manera responsable y transparente en todas las fases del proceso de evaluación.

•

○ **Estructura del Documento**

- **Resumen:** Esta sección proporciona brevemente los objetivos del estudio, las herramientas utilizadas, los principales resultados obtenidos y una reflexión sobre las implicaciones éticas asociadas con el uso de estas técnicas.
- **Introducción:** Aquí se contextualiza la recopilación pasiva de información, destacando su relevancia en el campo de la ciberseguridad. Se define la importancia de las técnicas de Google Hacking y Shodan, así como los objetivos específicos que se pretenden alcanzar con este trabajo.
- **Fundamentos Teóricos:** Esta sección se divide en tres partes. Se explica qué es Google Hacking y sus principales técnicas, se describe Shodan y su funcionamiento, y se introducen las implicaciones éticas del uso de estas herramientas.
- **Metodología:** Se detalla el proceso seguido para implementar las búsquedas avanzadas en Google y Shodan. Se describen los pasos realizados y las estrategias de búsqueda empleadas, así como la documentación de los resultados.

- **Resultados:** En esta parte se presentan los resultados obtenidos de las búsquedas realizadas con Google Hacking y Shodan, mostrando ejemplos de los comandos utilizados y los dispositivos o servicios expuestos encontrados.
- **Reflexión Ética:** Se aborda la importancia de considerar las implicaciones éticas del uso de Google Hacking y Shodan, así como las responsabilidades que debe asumir un hacker ético durante la recopilación de información.
- **Referencias:** Finalmente, se incluye una lista completa de todas las fuentes consultadas para la elaboración del trabajo, siguiendo un formato de citación adecuado.

• Fundamentos Teóricos

○ Google Hacking y sus Técnicas Principales

- **Google Dorks o Dorking**, también conocido como **Google Hacking** es una técnica que consiste en aplicar la búsqueda avanzada de Google para conseguir encontrar en Internet información concreta a base de ir filtrando los resultados con operadores conocidos como Dorks, que son símbolos que especifican una condición. Por ejemplo, si ponemos en nuestro texto de búsqueda las dobles comillas ("texto"), buscará información que coincida exactamente con el texto. Es decir, si buscamos "OSI", nos devolverá el contenido que concuerde exactamente con ese término. A lo largo de este artículo te enseñaremos cómo te puede ser útil.
- **Operadores de Google**
- Los operadores de búsqueda de Google son herramientas poderosas que permiten refinar y personalizar las consultas, facilitando la obtención de información específica. A continuación, se presenta una tabla con algunos de los operadores más útiles en **Google Hacking**.

Operador	Descripción	Ejemplo
Cache	Busca la versión almacenada en caché de una página. Por ejemplo:	cache:https://www.google.com/
filetype	Esto buscará archivos PDF que contengan la frase "guía de seguridad informática".:	filetype:pdf "guía de seguridad informática"
site	Esto buscará el término "ciberseguridad" solo en el sitio web de Wikipedia.	site:wikipedia.org ciberseguridad
intitle	Esto buscará páginas con la frase "vulnerabilidad de software" en el título.	intitle:"vulnerabilidad de software"
inurl	Esto buscará páginas que contengan "login" en la URL	inurl:login
intext	Esto buscará páginas que contengan la frase "análisis de riesgo" en el texto del contenido.	intext:"análisis de riesgo"
related	Esto buscará sitios web relacionados con "bbc.com".	related:bbc.com
source	Esto buscará artículos de Google Noticias provenientes de "nytimes.com" y que	source:nytimes.com "nueva tecnología"

	contengan "nueva tecnología".	
before	Esto buscará información sobre "seguridad informática" publicada antes de 2021.	"seguridad informática" before:2021
after	Esto buscará información sobre "tendencias de ciberseguridad" publicada después de 2023.	"tendencias de ciberseguridad" after:2023
" " (comillas)	Busca una frase exacta.	"ciberseguridad en 2023"
OR	Busca uno de varios términos.	ciberseguridad OR protección de datos
- (signo menos)	Excluye un término.	antivirus -Norton

Shodan: El Motor de Búsqueda para Dispositivos Conectados

Shodan es un motor de búsqueda, una página que sirve para encontrar cosas en Internet. Es un buscador de sistemas y servicios conectados a internet, lo que busca son máquinas conectadas a la red.

Shodan funciona escaneando continuamente la red para identificar y categorizar dispositivos conectados a Internet. Utiliza una tecnología avanzada que explora el paisaje digital y obtiene información detallada sobre cada dispositivo, incluyendo su dirección IP, ubicación geográfica y, en algunos casos, los puertos abiertos y servicios disponibles.

En este aspecto, **utilizar Shodan es completamente legal**, ya que se limita a mostrar información que ya está en Internet. En cambio, **lo que no es legal es acceder a los servidores que se muestran** en los resultados, ya que puedes estar cometiendo delitos de ciberdelincuencia.

Shodan te va a permitir encontrar cualquier tipo de dispositivo conectado a Internet, desde webcams, televisores inteligentes y dispositivos del hogar hasta semáforos, turbinas eólicas, y cualquier otro tipo de infraestructura que use la red para enviar los datos. No es un buscador de servidores vulnerables, sino que encuentras todos los dispositivos, y puede que algunos sean vulnerables.

Ejemplo

Podrías buscar dispositivos que están ejecutando una versión específica de un software conocido por tener vulnerabilidades. Por ejemplo, si quieres encontrar dispositivos que están ejecutando una versión vulnerable de Apache Struts, puedes usar:

Apache Struts 2.3.15

Este comando buscará en la base de datos de Shodan todos los dispositivos que estén ejecutando esa versión específica de Apache Struts, la cual es conocida por tener vulnerabilidades de seguridad. Al realizar esta búsqueda, podrás identificar fácilmente aquellos sistemas que podrían ser susceptibles a ataques, permitiendo una evaluación más efectiva de la postura de seguridad.

Aspectos Éticos en la Recopilación Pasiva de Información

La recopilación de datos es esencial para el crecimiento y desarrollo de muchas empresas y organizaciones. Sin embargo, también es importante tener en cuenta que los datos recopilados

pertenecen a individuos. Recopilar y utilizar estos datos de manera irresponsable o poco ética puede tener consecuencias negativas, tanto para los usuarios como para la reputación de la organización.

Los principios éticos de la recopilación de datos

Al recopilar y utilizar datos de manera ética, se deben considerar principios fundamentales, como:

- **Consentimiento informado:** Obtener el consentimiento de los usuarios antes de recopilar cualquier tipo de datos personales. Los usuarios deben estar completamente informados sobre cómo se utilizarán sus datos.
- **Transparencia:** Las organizaciones deben ser claras en sus prácticas de recopilación de datos y proporcionar información comprensible sobre cómo se recopilan, almacenan y utilizan.
- **Responsabilidad y rendición de cuentas:** Las organizaciones deben asumir la responsabilidad de sus prácticas de recopilación de datos y asegurarse de cumplir con todas las leyes y regulaciones aplicables.

Privacidad y anonimización de datos

La privacidad de los usuarios es una preocupación clave en la recopilación de datos. Es fundamental proteger la información personal y garantizar que no se revele de manera inapropiada o sin el consentimiento del usuario. La anonimización de datos es una forma efectiva de proteger la privacidad, pero es crucial entender que no es infalible y que existen riesgos de reidentificación.

Cumplir con las leyes y regulaciones

Es esencial cumplir con todas las leyes y regulaciones aplicables en cuanto a la recopilación, almacenamiento y uso de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea. Esto no solo protege a los usuarios, sino que también ayuda a las organizaciones a evitar consecuencias legales y daños a su reputación.

Metodología

Parte 1: Uso de Google Hacking

Google Gruyere

Para el uso de Google Hacking usaremos la siguiente página web llamada **Google Gruyere** se creó este sitio vulnerable a propósito por Google para fines educativos, como enseñar técnicas de hacking web, incluidas búsquedas avanzadas.

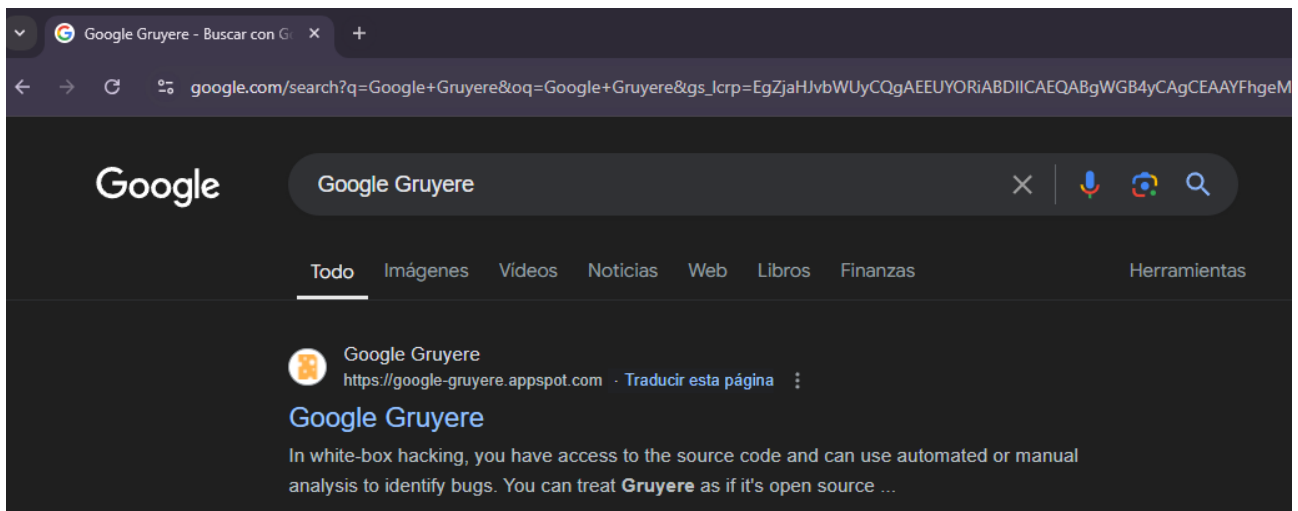
El sitio web tiene registro incluido, pero el registro es de forma ficticia y simula ciertos aspectos de una página web.

Para realizar esta tarea solo tenemos que escribir los parámetros en la barra de búsqueda que nos ayudaran a sacar cierta información del sitio Web Google Gruyere como veremos a continuación.

Descripción de las Búsquedas Avanzadas

Antes de empezar con la búsqueda avanzada necesitamos entrar en la página web de Google Gruyere con los siguientes pasos:

Paso 1: En la barra de búsqueda de nuestro navegador escribimos Google Gruyere y nos dirigimos al primero enlace: <https://google-gruyere.appspot.com/>.



Paso 2: Veremos una página web con el título “Web Application Exploit and Defenses”, dentro de la página en la parte de abajo veremos la palabra “CONTINUE” le damos clic en ella:

WARNING: Accessing or attacking a computer system without authorization is illegal in Google service. You should use what you learn from the codelab to make your own app

Continue >>

© Google 2017 [Terms of Service](#)
The code portions of this codelab are licensed under the Creative Commons Attribution-No Derivative Works 4.0 International license <<https://creativecommons.org/licenses/by/3.0/us>>.

Paso 3: Veremos un texto donde te dirá que para entrar en la página web tienes que darle en <https://google-gruyere.appspot.com/start> le damos clic en él.



Web Application Exploits and Defenses (Part 1)

A Codelab by Bruce Leban, Mugdha Bendre, and Parisa Tabriz

Setup

To access Gruyere, go to <https://google-gruyere.appspot.com/start>. AppEngine will start a new instance of Gruyere for you at <https://google-gruyere.appspot.com/123/> (where 123 is your unique id). Each instance of Gruyere is "sandboxed" from anyone else using Gruyere. You'll need to use your unique id instead of 123 in all the examples. If you want to share your in successful attack), just share the full URL with them including your unique id.

The Gruyere source code is available online so that you can use it for white-box hacking. You can browse the source code at the files from <https://google-gruyere.appspot.com/gruyere-code.zip>. If you want to debug it or actually try fixing the bugs, you can clone the Gruyere locally in order to do the lab.

Paso 4: Te aparecerá esta página con tu id único y un mensaje de advertencia avisando de que no es seguro y que no pongas datos personales. Le tienes que dar clic en “Agree & Start”.

Start Gruyere

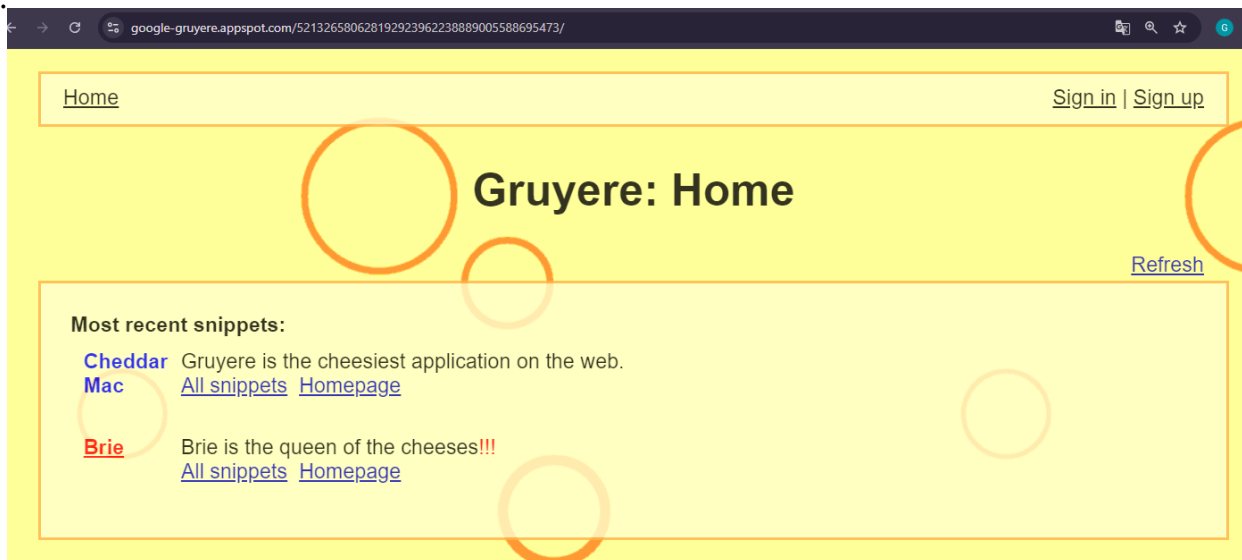
Your Gruyere instance id is 521326580628192923962238889005588695473.

**WARNING: Gruyere is not secure.
Do not upload any personal or private data.**

By using Gruyere you agree to the [terms of service](#).

Agree & Start

Paso 5: Ya finalmente nos encontraremos en la página principal



Parámetros avanzados de Google

Parámetro site y filetype:

Estos parámetros nos ayudan a buscar los archivos expuestos en el dominio de Google Gruyere. El parámetro **site**: nos ayuda a buscar en una web en concreto y el parámetro **filetype**: encontrara archivos específicos, como documentos PDF o logs

Parámetro intext:

Si queremos buscar una palabra clave o información sensible como “password” o “username” podemos usar el parámetro **intext**:

Parametros inurl y intitle

Para intentar encontrar paneles de administración o páginas ocultas relacionadas con la gestión del sitio, puedes usar **inurl**: o **intitle**:

Ejemplos de Comandos

site:google-gruyere.appspot.com filetype:txt

Con la anterior búsqueda veremos archivos de texto expuestos en el dominio de Google Gruyere.

site:google-gruyere.appspot.com intext:password

Este comando buscará cualquier mención de la palabra "password" dentro de las páginas del dominio Google Gruyere.

site:google-gruyere.appspot.com inurl:admin

Esto intentará encontrar URLs en el dominio que contengan la palabra "admin".

Parte 2: Exploración de Shodan

Explica cómo realizaste las búsquedas avanzadas en Shodan, utilizando filtros como *port:* o *org:*. Indica si creaste una cuenta en Shodan y cómo documentaste los resultados.

Búsquedas Avanzadas con Filtros

Para la exploración en Shodan, se pueden usar una variedad de filtros avanzados que nos permiten delimitar los resultados, como puertos abiertos, organizaciones, o la localización geográfica de algún dispositivo. A continuación podremos ver una tabla que presentar algunos de los filtros más relevantes utilizados, con una breve descripción y ejemplos de su aplicación.

Nombre del Filtro	Descripción	Ejemplo
Port:	Busca dispositivos que tengan un puerto específico abierto. Esto es útil para encontrar servicios que utilicen un puerto particular, como FTP (21), HTTP (80), etc.	port:22 (Buscar dispositivos con el puerto SSH abierto)
org:	Filtra los resultados por la organización a la que pertenecen los dispositivos o servidores expuestos.	org:"Google" (Buscar dispositivos pertenecientes a Google)
country:	Filtra los dispositivos por país, según la IP geolocalizada.	country:"ES" (Buscar dispositivos en España)
hostname:	Filtra los resultados por el nombre del host del dispositivo, útil para encontrar dominios específicos.	hostname:"example.com" (Buscar dispositivos con el dominio example.com)
os:	Filtra dispositivos por el sistema operativo que están ejecutando. Esto puede ser útil para identificar dispositivos que usen versiones específicas de software.	os:"Windows 10" (Buscar dispositivos que usen Windows 10)
city:	Filtra los dispositivos por ciudad. Similar a country: , pero con un enfoque más local.	city:"Madrid" (Buscar dispositivos en Madrid)
isp:	Filtra por proveedor de servicios de Internet (ISP), útil para identificar qué dispositivos están bajo la red de un proveedor en particular.	isp:"Movistar" (Buscar dispositivos que usen Movistar como ISP)
before:	Busca dispositivos que fueron detectados antes de una fecha específica, en formato Año-Mes-Día.	before:2023-01-01 (Buscar dispositivos detectados antes del 1 de enero de 2023)
after:	Busca dispositivos que fueron detectados después de una fecha específica.	after:2023-01-01 (Buscar dispositivos detectados después del 1 de enero de 2023)
product:	Filtra los dispositivos que	product:"Apache" (Buscar

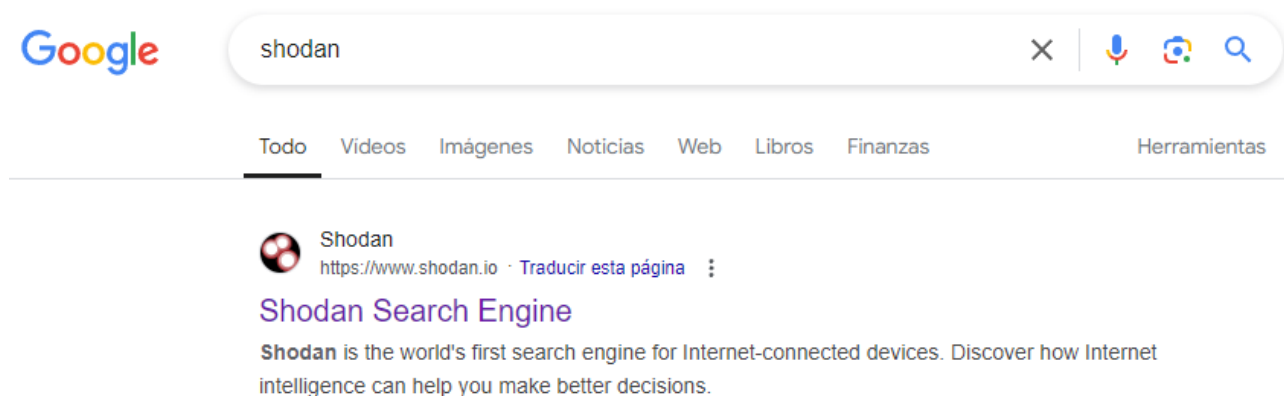
	utilizan un software o producto específico. Esto es útil para identificar servicios como Apache o Nginx.	dispositivos que utilicen Apache)
net:	Filtra los dispositivos dentro de un rango específico de direcciones IP.	net:"192.168.1.0/24" (Buscar dispositivos en la red 192.168.1.x)
title:	Busca dispositivos según el título HTML de la página web.	title:"Login" (Buscar dispositivos con "Login" en el título HTML)
has_screenshot:	Busca dispositivos que tengan capturas de pantalla en los resultados de Shodan. Es útil para visualizar cámaras o interfaces gráficas expuestas.	has_screenshot:true (Buscar dispositivos con capturas de pantalla)
ssl:	Filtra dispositivos que utilizan certificados SSL (Secure Sockets Layer) específicos, útil para buscar información sobre certificados expuestos.	ssl:"Let's Encrypt" (Buscar dispositivos con certificados emitidos por Let's Encrypt)

Procedimientos de Documentación

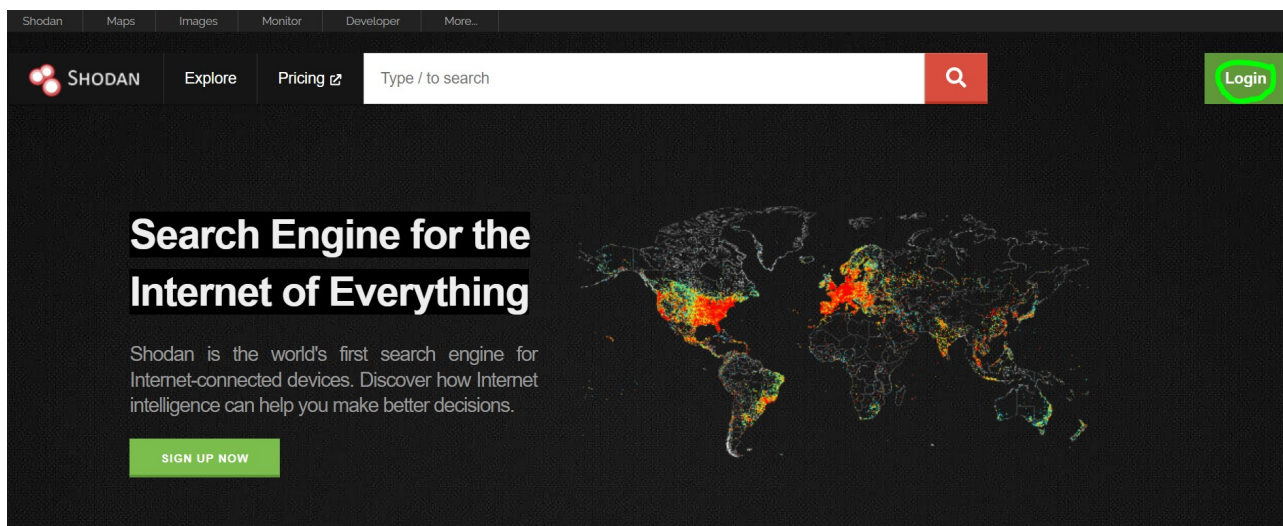
Introducción a Shodan

Ahora procederemos a realizar una pequeña guía para acceder a la herramienta de Shodan y nos detendremos en algunos aspectos interesantes de dicha herramienta.

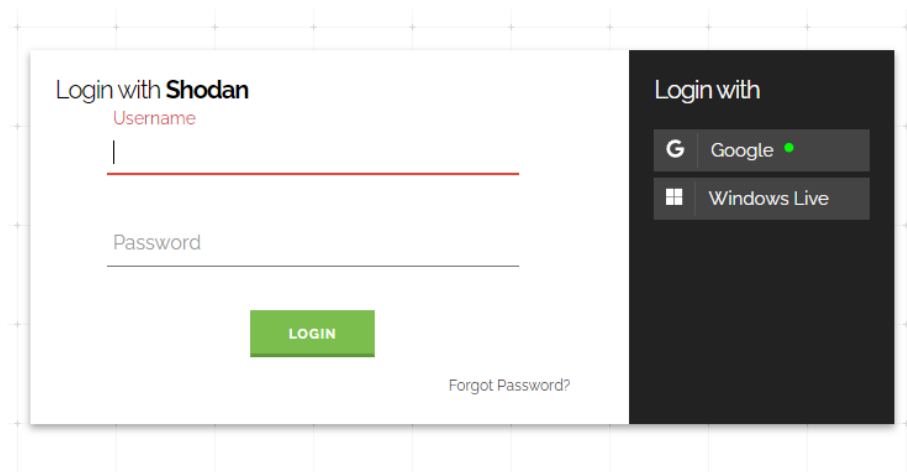
Para comenzar iremos a nuestro buscador de preferencia y escribiremos la palabra Shodan. Luego tendremos que hacer clic en <https://www.shodan.io/>.



Ahora dentro del home de Shodan en la parte superior izquierda veremos un enlace llamado **Login** le daremos clic en él.



Esto nos llevara a su página de registro. Puedes crearte una cuenta o acceder desde la cuenta de correo de Gmail o desde Windows Live con correos de Hotmail o Outlook. En mi caso lo haré a través de la cuenta de Gmail. Las cuentas de estudiante por lo general no permiten el acceso a Shonda



Ahora ya entramos en la página principal de Shodan donde podremos ver una serie de guías que nos pueden ayudar al uso de dicha herramienta de forma un poco más avanzada. Nuestra cuenta al ser gratuita tendrá una serie de limitaciones. Podemos ver una serie de paneles donde tendremos ayudas.



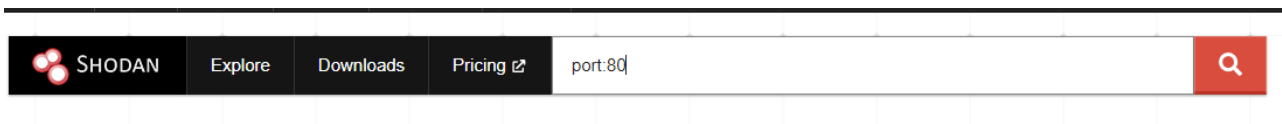
En otra parte de la página tendremos **Hoja de truco sobre filtros** donde nos pondrá ejemplos de algunos de sus filtros al pinchar en alguno de los ejemplos nos llevara a una página con los filtros aplicados.

Hoja de trucos sobre filtros

Actualmente, Shodan rastrea casi 1500 puertos en Internet. A continuación, se muestran algunos de los filtros de búsqueda más utilizados para comenzar.

Nombre del filtro	Descripción	Ejemplo
ciudad	Nombre de la ciudad	Dispositivos en San Diego
país	Código de país de 2 letras	Puertos abiertos en Estados Unidos
http.titulo	Título del sitio web	Sitios web "hackeados"
neto	Rango de red o IP en notación CIDR	Servicios en el rango de 8.8.0.0 a 8.8.255.255
org	Nombre de la organización propietaria del espacio IP	Dispositivos en Google

Para poder aplicar los filtros tendremos que hacerlo desde el buscador de la página. Por ejemplo si queremos realizar búsquedas de puertos 8081 (TCP/UDP) abiertos en equipos escribiremos **port:8181** y le daremos al icono de la lupa.



Nos saldrá una página con una serie de nombres e Ips. Pero comenzaremos por la parte de la izquierda donde podemos ver **Top Country** al darle a **More** podremos ver los países donde más puertos 8081 abiertos tienen en la base de datos de Shodan, También nos arrojará la cantidad de equipos en total que tienen en esta caso 144.268.521:

TOTAL RESULTS

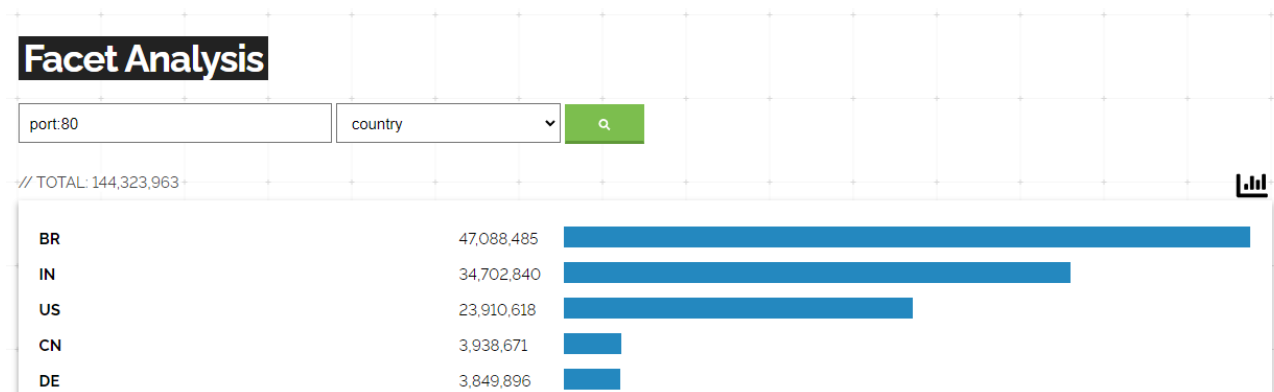
144,268,521

TOP COUNTRIES



Brazil	47,088,456
India	34,650,158
United States	23,909,529
China	3,938,603
Germany	3,849,736
More...	

Aquí podemos ver los países donde más puertos 8081 abiertos tienen en la base de datos de Shodan: Si le damos clic alguno de ellos se añadirá al filtro la búsqueda de ese país.

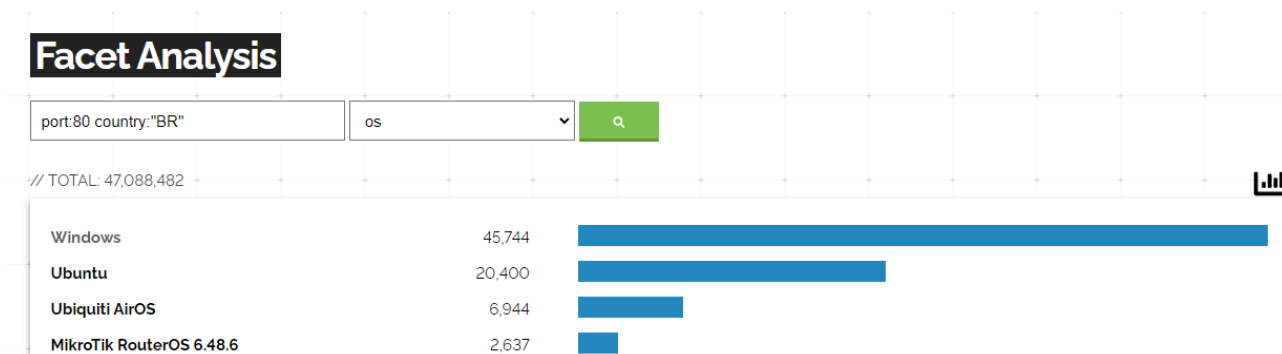


Otro aspecto interesante que podremos encontrar son los sistemas operativos que más tienen los equipos con puerto 8181 abiertos

TOP OPERATING SYSTEMS

Windows	45,745
Ubuntu	20,400
Ubiquiti AirOS	6,944
MikroTik RouterOS 6.48.6	2,637
MikroTik RouterOS 6.49.10	1,382
More...	

Al igual que con los países si le damos clic algunos se aplicaran al filtro, añadiendo en la búsqueda por ejemplo los SO Windows.



Uso de filtros en Shodan

En estos ejemplos usaremos tres filtros:

- **Port:** Nos ayuda a buscar por puertos abiertos. Ejemplo: port:554 (RTSP) Protocolo de Transmisión en Tiempo Real, que suelen usar las cámaras IP.
- **Country:** Nos ayuda a buscar por país. Ejemplo: country:"ES" busca por España.
- **Org:** Permite buscar dispositivos por la organización a la que pertenecen. Ejemplo: org:"Universidad de Madrid" busca dispositivos asociados con la Universidad de Madrid en España.

Búsquedas con el filtro Port

Cómo hemos visto anteriormente para que los filtros de Shodan se apliquen tenemos que escribirlos en su barra de búsqueda.

En este caso vamos a usar el filtro **port** que nos dice los puertos abiertos. Miraremos los equipos con el **puerto 22** abiertos que es el puerto SSH o Secure Shell que es el nombre del protocolo cuya función es el acceso remoto a un servidor.

Al escribir port:22 podremos ver una serie de resultados a nuestra búsqueda, nosotros nos centraremos en la primera.

En primera estancia los resultados obtenidos son:

IP y Hostname que es la 137.110.137.59, que esta asociada con el dominio gertle.ucsd.edu, que podría corresponder a la Universidad de California, San Diego en Estados Unidos.

También nos muestra que el dispositivo está ejecutando un servidor SSH-2.0-OpenSSH-8.2p1 en una máquina con el sistema operativo Ubuntu 4.0.11 que es una de las primeras versiones de Ubuntu en 2004 .

Podemos ver el tipo de clave o key type que es una **ssh-rsa**. RSA proviene de las iniciales de sus tres creadores, Rivest, Shamir y Adleman, allá por 1997. El objetivo de RSA es crear una llave generada por el algoritmo RSA. Esta llave en realidad está compuesta por dos partes, una parte pública y otra parte privada. Cuando te conectas a un servidor, éste envía un desafío cifrado con la clave pública. Solo la clave privada puede descifrarlo, lo que verifica la identidad del cliente. Una vez autenticado, se establece una sesión segura utilizando un algoritmo de cifrado simétrico (como AES), pero la autenticación inicial se basa en RSA.

137.110.137.59

gertle.ucsd.edu
University of California, San
Diego
 United States, San
Diego

SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQgQDQLZrmb2SPbWHLv1SYtfYkcDzFGmhTyHHsmINCfgnPzar1
oo/b6ceeu7WjV5WEcG4pUgdMzBgHXS2ZOM6C1J3EsFJjv2IoaghuvPDgj441AVnFTCrNFyctfpQQ
AIJcU05+JXxAKQb9uN3SqK/zgaZhDgpmqq2nYQ4MGaE2TuGb1EvJyiS1RmJ2uaavf2Kcynw7jwaT
y6...

Para obtener una información más completa le daremos clic en la IP: 137.110.137.59 nos mostrará la siguiente página con este enlace: <https://www.shodan.io/host/137.110.137.59> esta información la veremos con más detalle en el apartado: [Resultados de las Búsquedas con Shodan](#).

Búsquedas con el filtro Country

Este filtro es útil para detectar equipo o servidores de diferentes países, dentro de Shodan se podría decir que es un filtro de geolocalización, como lo pueden ser **city**, **postal**, **geo** y **región**.

Para ver más información sobre los resultados del filtro Country lo veremos con más detalle en el apartado: [Resultados de las Búsquedas con Country](#).

Búsquedas con el filtro org

Este filtro nos ayuda a buscar dispositivos de una organización específica, en este caso buscaremos del excelentísimo Ayuntamiento de Cartagena. De todos los resultados el primero es el de Agencia de colocación – Ayuntamiento de Cartagena con la ip: 77.230.242.33 que es una entidad pública que

tiene como objetivo facilitar la inserción laboral de los ciudadanos y promover el empleo. Como dato curioso el servidor no se encuentra en Madrid.

Aquí veremos la parte de Issued To o Emitido/a a

Common Name o nombre común: *cartagena.es nos dice que el certificado SSL es válido para cualquier subdominio de cartagena.es


Organization : AYUNTAMIENTO DE CARTAGENA es el nombre de la organización a la que se emitió el certificado.

Agencia de Colocación - Ayuntamiento de Cartagena

77.230.242.33

static-33-242-230-77.ipcom.
comunitel.net

AYUNTAMIENTO DE
CARTAGENA

 Spain, Madrid



SSL Certificate

Issued By:

| Common Name:
ACCVCA-120

| Organization:
ACCV

Issued To:

| Common Name:
*.cartagena.es

| Organization:
AYUNTAMIENTO DE
CARTAGENA

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2,
TLSv1.3

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 22 Oct 2024 23:45:12 GMT

Content-Type: text/html

Content-Length: 27526

Connection: keep-alive

Cache-Control: private

Set-Cookie: ASPSESSIONIDQSTDBTTR=OPLBAFODJEENBEMAOEFHBCG; path=/
X-Powered-By: ASP.NET

X-Frame-Options: SAMEORIGIN

En el apartado de resultados veremos con más detalle dos partes que no vimos en los dos anteriores filtros **port** y **country**, que son **Web Technologies** y **Vulnerabilities** del <https://www.shodan.io/host/77.230.242.33>. Todo esto lo veremos con más detalle como siempre en: [Resultados de las Búsquedas con org](#).

Resultados

Resultados de las Búsquedas con Google Hacking

Al ejecutar `site:google-gruyere.appspot.com filetype:txt` esta línea de comando, se podrían encontrar varios archivos de texto expuestos que contenían información sobre usuarios registrados y configuraciones del sitio. En un escenario real, este tipo de archivos podría incluir contraseñas o datos confidenciales.

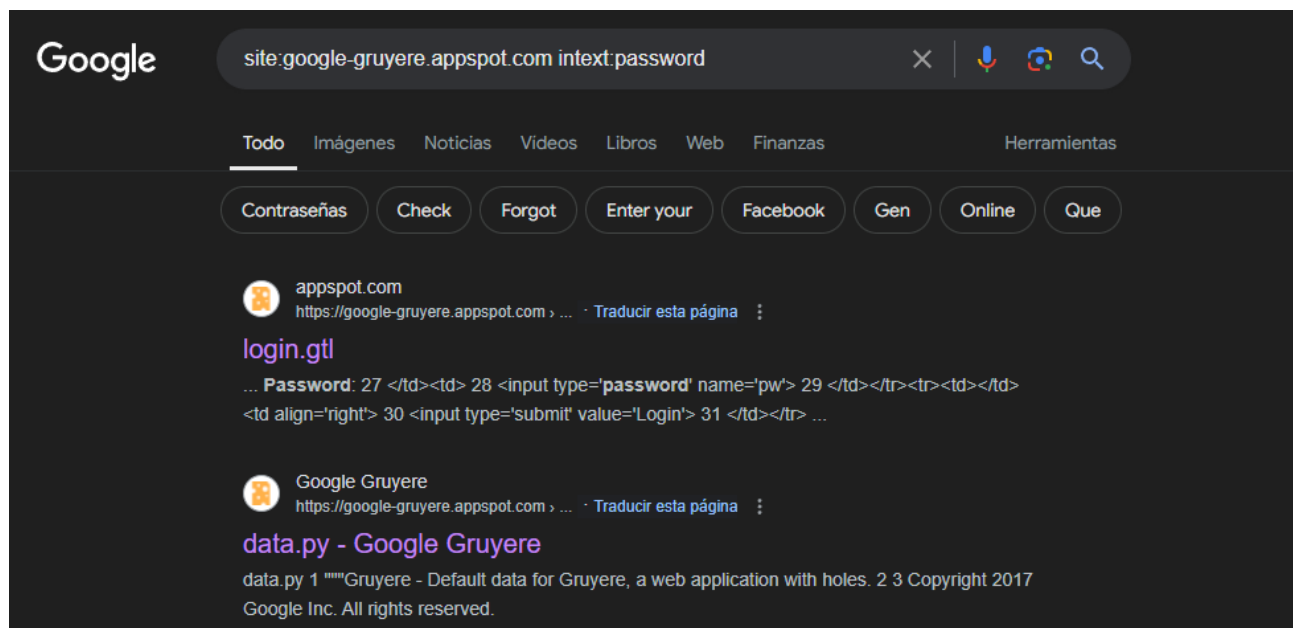
En nuestro caso concreto en Google Gruyere podremos visualizar la siguiente información en `https://google-gruyere.appspot.com/code/secret.txt`:

```
secret.txt
1 Cookie!
```

`site:google-gruyere.appspot.com intext:password`

Esta búsqueda reveló varias páginas donde la palabra "password" estaba presente, lo que sugiere la exposición de credenciales o instrucciones sobre contraseñas.

En este caso en primera estancia nos muestra una serie de páginas. Nosotros nos centremos en la de **Login.gtl** y **Data.py**



Login.gtl

Al entrar dentro veremos las siguientes líneas en html:

```

21 <table><tr><td>
22     User name:
23 </td><td>
24     <input type='text' name='uid'>
25 </td></tr><tr><td>
26     Password:
27 </td><td>
28     <input type='password' name='pw'>
29 </td></tr><tr><td></td><td align='right'
30     <input type='submit' value='Login'>
31 </td></tr></table>

```

En documento html las Línea 24: <input type='text' name='uid'> - Nos dice el nombre de usuario.
 Línea 28: <input type='password' name='pw'> -Nos muestra la contraseña del usuario.

***gtl.py** es el lenguaje de plantilla Gruyere.

Data.py

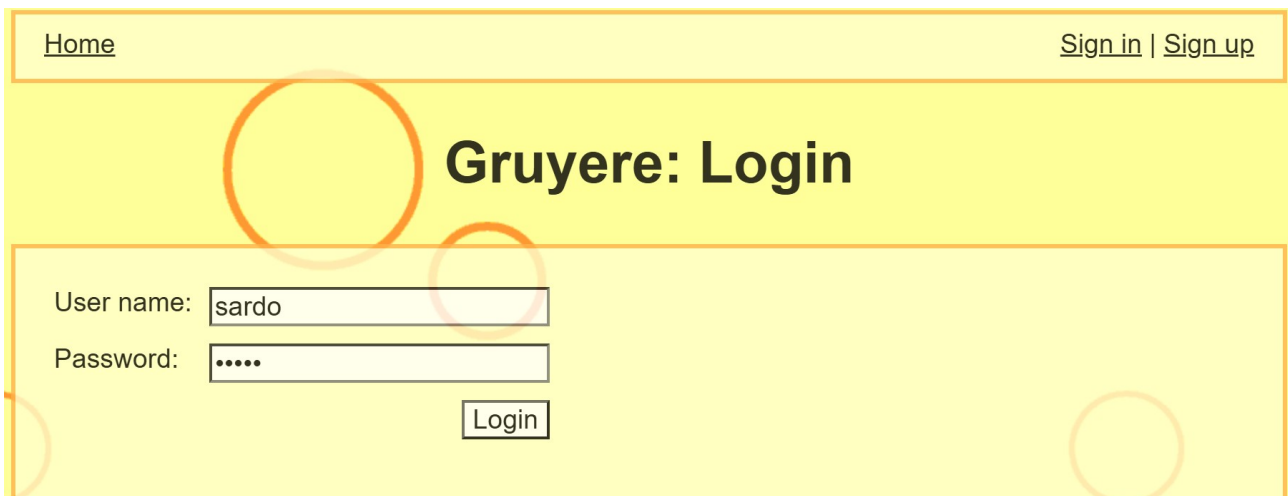
Aquí mostraremos más concretamente la parte donde nos muestra el usuario sardo y su contraseña odras.

```

    ],
  },
  'sardo': {
    'name': 'Miss Sardo',
    'pw': 'odras',
    'is_author': True,
    'is_admin': False,
    'private_snippet': 'I hate my brother Romano.',
    'web_site': 'https://www.google.com/search?q="pecorino+sardo"',
    'color': 'red',
    'snippets': [],
  },

```

Si iniciamos sesión con la siguiente información podremos entrar en su cuenta.



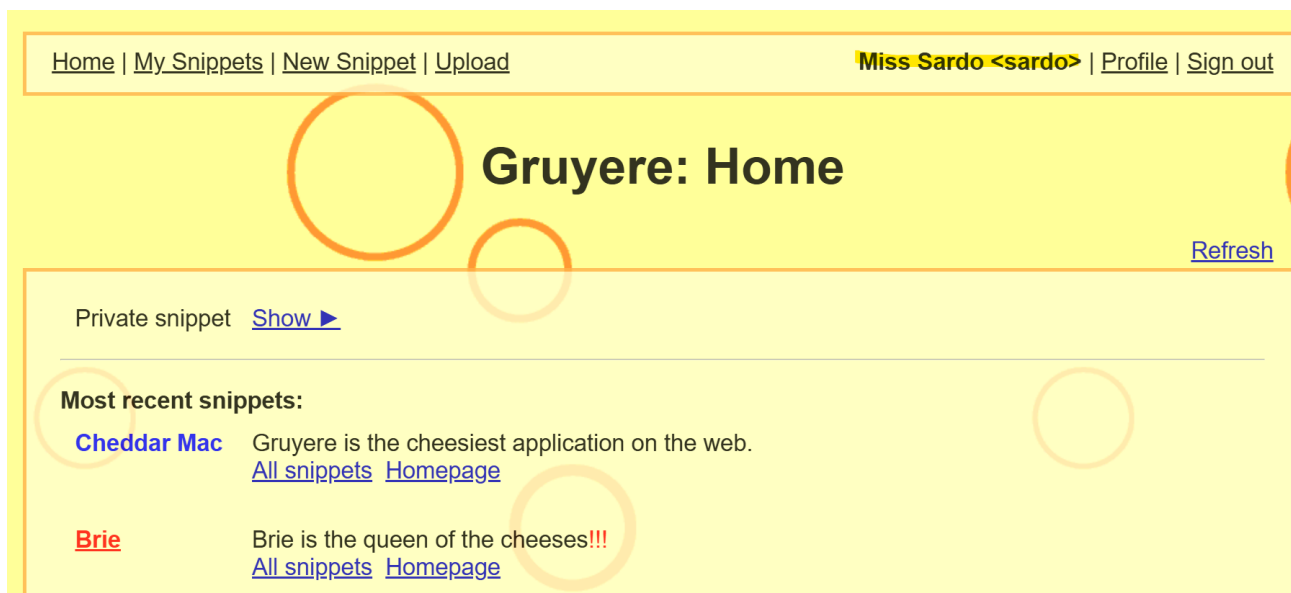
Home Sign in | Sign up

Gruyere: Login

User name:

Password:

Aquí podemos ver su sesión iniciada.



***data.py** almacena los datos predeterminados en la base de datos. Hay una cuenta de administrador y dos usuarios predeterminados.

Resultados de las Búsquedas con Shodan

Presenta los resultados de tus búsquedas en Shodan, indicando los dispositivos o servicios expuestos que encuentres (IP, ubicación geográfica, etc.), siempre dentro del marco ético y legal. Análisis y Discusión

Resultados del parámetro port

Ahora nos detendremos en más de talle de la información que nos brinda los tres apartados de <https://www.shodan.io/host/137.110.137.59>. En estos resultado haremos más detalle a la parte de los algoritmos de puerto SSH.

General Information

Podemos ver que el **Hostname** del equipo es `gentle.ucsd.edu` esto quiere decir que pertenece a Universidad de California, San Diego.

Domains: Se identifica el dominio principal al que pertenece el host, en este caso **ucsd.edu**. Los dominios permiten organizar los recursos de internet en jerarquías y se usan para localizar equipos, servicios, y sitios web dentro de una red específica. Este dominio de nivel superior `.edu` está reservado para instituciones educativas, principalmente en los Estados Unidos.

Country/City: El servidor está ubicado en los Estados Unidos, específicamente en la ciudad de San Diego.

Organization/ISP: Tanto la organización como el proveedor de servicios de Internet (ISP) son la Universidad de California, San Diego.

ASN: El número AS (Sistema Autónomo) es AS7377, un identificador asociado al bloque de IPs que maneja esta organización.


Operating System: El sistema operativo detectado en el servidor es Linux.

**El ASN (Número de Sistema Autónomo) es un identificador único que se asigna a cada sistema autónomo en internet. Un sistema autónomo es una red o conjunto de redes que está bajo el control administrativo de una organización o entidad única y que tiene políticas de enrutamiento comunes.*

137.110.137.59 ☐ Regular View ☒ Raw Data

General Information	
Hostnames	gentle.ucsd.edu
Domains	UCSD.EDU
Country	United States
City	San Diego
Organization	University of California, San Diego
ISP	University of California, San Diego
ASN	AS7377
Operating System	Linux

El apartado de **Open Ports**, nos dice que el puerto **22 SSH**. Este puerto se utiliza para el acceso remoto seguro mediante el protocolo Secure Shell (SSH). Sin embargo, si está mal configurado o protegido por contraseñas débiles, puede ser vulnerable a ataques de fuerza bruta. y puerto **TCP 2000 usa el Protocolo de Control de Transmisión**. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión, necesita un proceso de negociación inicial entre las partes para establecer y asegurar una comunicación antes de que se transmita cualquier dato.

 **Open Ports**

22

2000

En la parte derecha lo correspondiente al **sub-apartado “Open Ports”** en Shodan, específicamente al puerto 22/TCP. Podemos ver:

Versión del servicio: OpenSSH 8.2p1.

- **Sistema operativo:** Ubuntu 4ubuntu0.11.
- **Clave pública:** (SSH-RSA) utilizada para autenticar las conexiones SSH

- **Fingerprint:** un hash que sirve para identificar la clave pública de manera única.

// 22 / TCP

1852888852 | 2024-10-21T23:35:10.982758

OpenSSH 8.2p1 Ubuntu 4ubuntu0.11

SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQgQDQLZrmb2SPbWHLv1SYtfYkcDzFGmhTyHHsmINCfgnPzar1
oo/b6ceeu7WjV5WEcG4pUgdMzBgHXS2ZOM6C1J3EsFJjv2IoaghuvPDgj44lAVnFTCrNFyctfpQQ
AIJcU05+JXxAKqb9uN3SqK/zgaZhDgpmqq2nYQ4MGaE2TuGb1EvJyiSlRmJ2uaavf2Kcynw7jwaT
y6ZjSueiifhJHj3kryx7pjFTlo/RWbc762cXJ3tiKSpRNfo4CBk6fcIXbs+sc2f1mJmReqPIlbuJ
br607oHd4A89r+gj+526I/J7qyIr0fz05E/NvqvoCbv9+ZE7HWn9qmuAVdTYSCPPLJeJJf1sxCNd
GRBlFIIn5TB6vvdoo8oDHdyS6+k4r9EmiLVt8ErSmx5GS7R6A4VaT7r1pL3+GWeoFNgrmk01uYZLV
vo8UlaHLnxcnFVhvBBYvCU1eS2U6B3yyFFCvosHQAMOHCVOST9y71520q84eco3feSfaZti3AGPm
hWjwFVSfk20=

Fingerprint: da:b1:d7:76:ea:82:f1:6f:98:ac:c0:a4:bb:7e:73:bf

En la siguiente imagen podemos ver una lista de algoritmos de intercambio de claves (Kex) utilizados en protocolos criptográficos para comunicaciones seguras en SSH. Estos algoritmos permiten a dos partes negociar y establecer una clave de cifrado compartida, que luego se usa para cifrar las comunicaciones entre ellas. Algunos de los algoritmos vistos son:

- **curve25519-sha256:** Ofrece alta seguridad y es eficiente en términos de computación.
- **ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521:** Utilizan criptografía de curva elíptica, que proporciona una seguridad fuerte con tamaños de clave más pequeños.
- **diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256:** Basados en el intercambio de claves de Diffie-Hellman, estos algoritmos permiten a dos partes establecer una clave compartida de manera segura incluso en presencia de un observador.
- **kex-strict-s-v00@openssh.com:** Un algoritmo específico de OpenSSH que proporciona un nivel adicional de seguridad

Kex Algorithms:

```
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256
kex-strict-s-v00@openssh.com
```

En la siguiente imagen veremos **algoritmos de clave del host del servidor**, Se utilizan para autenticar la identidad del servidor al cliente. Podemos ver los siguientes algoritmos:

*Una función criptográfica hash- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente

- **rsa-sha2-512:** Este algoritmo crea un hash de 512 bits.
- **rsa-sha2-256:** Este algoritmo crea un hash de 256 bits.
- **Ssh-rsa:** Este algoritmo no usa hash específico. Se considera menos seguro que los esquemas con SHA-2.
- **ecdsa-sha2-nistp256:** Es un algoritmo de firma digital basado en ECDSA (Elliptic Curve Digital Signature Algorithm), que es más eficiente que RSA en términos de tamaño de clave y procesamiento. Usa la curva elíptica NIST P-256, que proporciona un alto nivel de seguridad con una clave más pequeña.
- **Ssh-ed25519:** Es una implementación del algoritmo de firmas EdDSA (Edwards-curve Digital Signature Algorithm), que utiliza la curva Ed25519. Este es uno de los algoritmos más rápidos y seguros disponibles hoy en día para SSH, diseñado para proporcionar alta seguridad con un tamaño de clave pequeño y baja carga de procesamiento.

Server Host Key Algorithms:

```
rsa-sha2-512
rsa-sha2-256
ssh-rsa
ecdsa-sha2-nistp256
ssh-ed25519
```

Ahora podemos ver algoritmos de cifrado que se utilizan para proteger la comunicación entre el cliente y el servidor..

chacha20-poly1305@openssh.com: Cifrado rápido y eficiente que combina ChaCha20 (encriptación) y Poly1305 (autenticación).

aes128-ctr, aes192-ctr, aes256-ctr: Versiones de AES (128, 192, 256 bits) en modo CTR, usado para encriptación de flujo. AES-256 es el más seguro.

aes128-gcm@openssh.com, aes256-gcm@openssh.com: AES con autenticación integrada (modo GCM), ofreciendo encriptación y verificación de datos, con claves de 128 y 256 bits.

Encryption Algorithms:

```
chacha20-poly1305@openssh.com
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
```

Ahora veremos algoritmos MAC (Message Authentication Code) o (Código de autenticación del mensaje). Estos algoritmos son utilizados para garantizar la autenticación y la integridad de los mensajes en una sesión SSH, algunos con mayores niveles de seguridad gracias al modo "etm".

- **umac-64-etm@openssh.com, umac-128-etm@openssh.com:** Versiones de UMAC (64 y 128 bits), que proporcionan autenticación rápida con la opción "etm" (Encrypt-Then-MAC) para mayor seguridad.
- **hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com:** Versiones de HMAC (256, 512 bits y SHA-1), utilizadas para autenticación de mensajes con la opción "etm" para mayor seguridad.
- **umac-64@openssh.com, umac-128@openssh.com:** UMAC normal sin "etm", sigue siendo rápido pero con menos protección.
- **hmac-sha2-256, hmac-sha2-512, hmac-sha1:** Algoritmos HMAC utilizados para verificar la integridad y autenticidad de los datos.

MAC Algorithms:

```
umac-64-etm@openssh.com
umac-128-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
hmac-sha1-etm@openssh.com
umac-64@openssh.com
umac-128@openssh.com
hmac-sha2-256
hmac-sha2-512
hmac-sha1
```

Por último veremos los algoritmos de compresión en SSH, son utilizados para mejorar la eficiencia de las transmisiones de datos.

none: No se aplica ningún algoritmo de compresión. Esta opción es útil cuando la compresión no es necesaria o cuando se prioriza la velocidad sobre la reducción de datos.

zlib@openssh.com: Utiliza el algoritmo de compresión zlib, que es conocido por ser eficiente y rápido. Este algoritmo comprime los datos antes de transmitirlos, lo que puede reducir significativamente el tamaño de los datos enviados a través de la conexión SSH, mejorando el rendimiento de la red.

Compression Algorithms:

```
none
zlib@openssh.com
```

Volver a [Uso de filtros en Shodan](#).

Resultados de las Búsquedas con Country

En esta apartado nos centraremos en detalles más específicos con la parte de la localización.

Como podemos ver en la parte de la izquierda de la búsqueda de **country"ES"** que corresponder a la búsqueda en España. Shodan tiene en su base de datos 5.525.343 de millones de resultados.

De los cuales Madrid con 2.006.647 millones y Barcelona con 212.959 son las ciudades con más resultados.

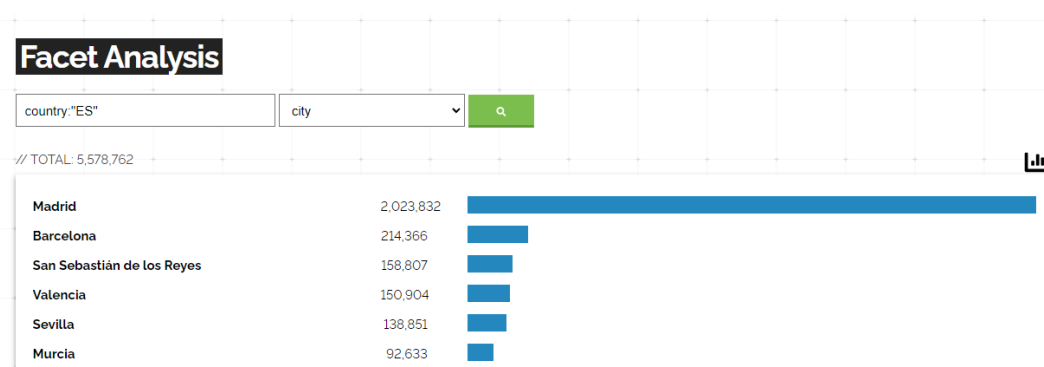
TOTAL RESULTS

5,526,343

TOP CITIES

Madrid	2,006,647
Barcelona	212,959
San Sebastián de los Reyes	157,284
Valencia	149,312
Sevilla	137,831
More...	

Si le damos clic en **More** podemos ver todas las ciudades de España donde nos dan resultados. Ordenados de mayor a menor.



Volver a [Uso de filtros en Shodan](#).

Resultados de las Búsquedas con org

En estos últimos resultados obtenidos con el filtro **org** en Shodan, nos centraremos en dos aspectos clave: **la tecnología web** utilizada y **las vulnerabilidades** detectadas. Es importante destacar que se han identificado puertos abiertos, como el puerto 443 y el puerto 80.

Puerto 443: Este puerto es utilizado para **HTTPS**, lo que garantiza la **transmisión segura de datos cifrados** entre el servidor y el cliente. El uso de este puerto es crucial para proteger la información sensible durante la comunicación.

Puerto 80: Este puerto se utiliza para **HTTP**, que es la **transmisión de datos sin cifrar**. Si un dispositivo o servidor tiene este puerto abierto y no implementa un protocolo seguro como HTTPS, los datos pueden ser **fácilmente interceptados** por atacantes. Es fundamental migrar hacia HTTPS para asegurar la confidencialidad y la integridad de los datos.

Open Ports

80

443

Ahora vemos que usan un servicio **nginx** que es un famoso software de servidor web de código abierto. En su versión inicial, funcionaba en servidores web HTTP. En la imagen nos muestra en el código de error 301 que el recurso ha sido movido de forma permanente a la nueva URL <https://77.230.242.33/>

// 80 / TCP 

-2100514759 | 2024-10-18T01:05:26.761503

nginx

301 Moved Permanently

```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Fri, 18 Oct 2024 01:05:26 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://77.230.242.33/
X-Frame-Options: SAMEORIGIN
```

Mostraré una pequeña parte del **certificado SSL**, que está firmado con un algoritmo fuerte (SHA-256 con RSA de 2048 bits) y es válido desde junio de 2024 hasta junio de 2025.

SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

36:11:1b:e2:7a:25:38:97:1f:22:24:e7:20:cc:ef:c9

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=ACCVCA-120, OU=PKIACCV, O=ACCV, C=ES

Validity

Not Before: Jun 13 07:40:00 2024 GMT

Not After : Jun 13 07:39:00 2025 GMT

Subject: organizationIdentifier=VATES-P3001600J, C=ES, ST=MURCIA, L=CARTAGENA, O=AYUNTAMIENTO DE CARTAGENA, CN=*.cartagena.es/businessCategory=Government Entity/jurisdictionC=ES/serialNumber=P3001600J

Subject Public Key Info:

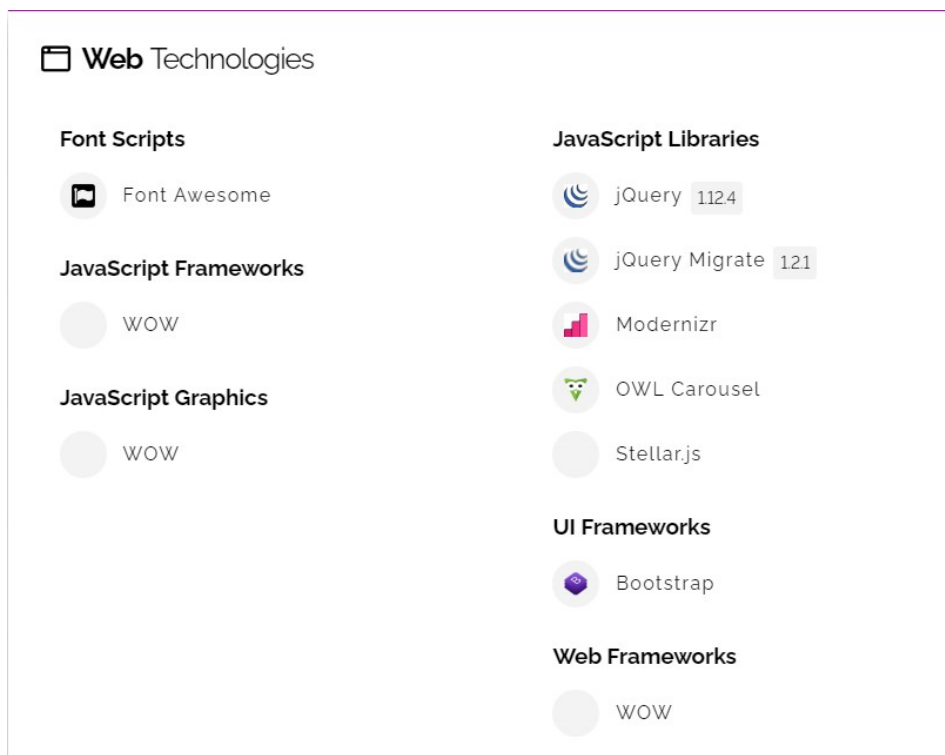
Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

En el apartado de **tecnología web** podemos ver una variedad de mejoras para su funcionalidad y diseño. Las más destacadas son:

- **Font Awesome:** Un conjunto de iconos escalables usados en diseño web.
- **JavaScript Libraries:** Incluyen jQuery, jQuery Migrate para simplificar el manejo del DOM y eventos, Modernizr para detección de características en navegadores, y OWL Carousel y Stellar.js para efectos de animación y carruseles.
- **Framework de UI:** Utiliza **Bootstrap**, que facilita la creación de interfaces responsive.



En el apartado de vulnerabilidades podemos ver cuatro **CVE Common Vulnerabilities and Exposures** (Vulnerabilidades y Exposiciones Comunes). Que es un sistema de clasificación que

asigna un identificador único a cada vulnerabilidad. Esto nos ayuda a facilitar intercambio de información sobre las vulnerabilidades entre diferentes organizaciones y herramientas. Todas estas vulnerabilidades se puede encontrar en **National Vulnerability Database** o La Base de Datos Nacional de Vulnerabilid en <https://nvd.nist.gov/vuln/search> en **Vulnerabilities -CVE**

En este caso podemos ver el **CVE-2020-11023** que nos quiere decir que se hizo el registro en el año 2020 y su ID es 11023. En la descripción del NVD nos dice “En versiones de jQuery mayores o iguales a la 1.0.3 y anteriores a la 3.5.0, el paso de HTML que contiene elementos <option> de fuentes no confiables, incluso después de desinfectarlos, a uno de los métodos de manipulación del DOM de jQuery (es decir, .html(), .append() y otros) puede ejecutar código no confiable. Este problema está parchado en jQuery 3.5.0.”

Otra CVE del mismo año que la anterior. La CVE CVE-2020-11022. En este caso esta afecta a versiones JQuery desde 1.2 hasta el 3.4.0.

Las diferencias de **CVE-2020-11023** es una vulnerabilidad específica relacionada con los elementos <option>, mientras que **CVE-2020-11022** se refiere a una vulnerabilidad más general en el manejo de HTML no confiable en jQuery.

Vulnerabilities

All ports ▼

Latest ▼

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2020

CVE-2020-11023

4.3 In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

CVE-2020-11022

4.3 In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Otra vulnerabilidad del año 2019 es la CVE-2019-11358 que nos dice que “jQuery antes de la versión 3.4.0, como se usa en Drupal, Backdrop CMS y otros productos, maneja mal jQuery.extend(true, {}, ...) debido a la contaminación de Object.prototype. Si un objeto de origen sin sanear contenía una propiedad __proto__ enumerable, podría extender el Object.prototype nativo.” Esto podría permitir a un atacante ejecutar código no confiable o realizar ataques de **cross-site scripting (XSS)**.

***cross-site scripting (XSS):** Se trata de un tipo de ataque que aprovecha fallas de seguridad en sitios web y que permite a los atacantes implantar scripts maliciosos en un sitio web legítimo (también víctima del atacante) para ejecutar un script en el navegador de un usuario desprevenido

que visita dicho sitio y afectarlo, ya sea robando credenciales, redirigiendo al usuario a otro sitio malicioso, o para realizar defacement en un sitio web.

2019

CVE-2019-11358

4.3 jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, [], ...)` because of `Object.prototype` pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native `Object.prototype`.

La ultima vulnerabilidad se registro en 2015 y es **CVE-2015-9251** y nos dice que “jQuery antes de la versión 3.0.0 es vulnerable a los ataques de secuencias de comandos entre sitios (XSS) cuando se realiza una solicitud Ajax entre dominios sin la opción `dataType`, lo que hace que se ejecuten respuestas de texto/javascript.” Esto permite ataques de ataques de secuencias de comandos entre sitios (XSS) o Cross-Site Scripting.

2015

CVE-2015-9251

4.3 jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the `dataType` option, causing text/javascript responses to be executed.

Volver a [Uso de filtros en Shodan](#).

Reflexión Ética

Implicaciones Éticas del Uso de Google Hacking y Shodan

Tras realizar este proyecto utilizando **Google Hacking** y **Shodan**, he reflexionado sobre los riesgos que conlleva su uso malintencionado y, en particular, la facilidad con la que herramientas como Shodan pueden comprometer la privacidad de muchos hogares. Por ejemplo, la exposición de cámaras IP que vigilan bebés podría ser considerada una forma de recopilación pasiva de información, **lo que plantea serios cuestionamientos éticos**.

Es importante subrayar que el acceso a puertos abiertos sin el consentimiento de la persona afectada constituye un delito según la **Ley Orgánica 10/1995, del Código Penal, en su Artículo 197 bis**. Este artículo establece que *"El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos [...] será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses"*.

Shodan es una herramienta que proporciona mucha información sobre la seguridad de los equipos y puede utilizarse para ayudar a empresas y personas a protegerse de los **cracker (a menudo mal llamados hackers)**. Sin embargo, la responsabilidad legal sobre el uso de dicha información recae

en el usuario que maneja la herramienta. **Google Hacking**, por otro lado, puede revelar datos valiosos de sitios web que, si no están bien protegidos, pueden convertirse en grandes vulnerabilidades. **Pero, al igual que no puedes llevarte un coche abierto aunque tenga las llaves puestas**, el hecho de que un sistema o servicio no esté bien protegido no significa que su acceso sea legítimo. Cualquier acceso o daño a dichos servicios estará sujeto a las leyes vigentes.

Por ello, es crucial recalcar **la importancia de los permisos y del uso adecuado de la información recopilada**, sobre todo para realizar auditorías que ayuden a mejorar la seguridad de los datos, uno de los recursos más valiosos en el mundo actual. La pregunta que surge es: ¿Nos motiva más el deseo de hacer el bien o de hacer el mal? Esta dualidad es donde entra en juego **la ética del hacker**. En una auditoría, un hacker puede tener acceso a información sensible que podría dañar a una empresa o ser utilizada para extorsionar, pero **es fundamental que la integridad personal prevalezca al manejar esa información**.

En última instancia, la semilla de la ética reside en la educación y los valores que se enseñan desde el principio de nuestras vidas. También es crucial **la concienciación sobre la ciberseguridad**, tanto en el ámbito empresarial como en el personal. Las leyes juegan un papel importante en protegernos de aquellos que desean cometer delitos cibernéticos utilizando herramientas como Shodan y Google Hacking. Asimismo, **las denuncias y el registro de estos ataques son esenciales para combatir este tipo de amenazas**.

Referencias

Lista completa de todas las fuentes que hayas utilizado para elaborar tu trabajo. Utiliza un formato de citación adecuado (APA, IEEE, etc.) y asegúrate de incluir toda la documentación relacionada con Google Hacking, Shodan y cualquier material teórico o práctico que hayas consultado.

<https://www.silikn.com/2023/10/el-papel-esencial-que-desempena-en-la.html> (artículo sobre el papel esencial de la recopilación pasiva en la ciberseguridad).

<https://frikisdelhacking.com/seguridad-informatica/hacking-etico/recopilacion-pasiva-de-informacion/> (Un enfoque estratégico sobre la recopilación pasiva de información, también conocida como OSINT (Inteligencia de Fuentes Abiertas)).

<https://www.incibe.es/ciudadania/blog/google-dorks-te-ayuda-encontrar-informacion-sobre-ti-en-la-red> (Descripción sobre el termino Google Hacking).

<https://developers.google.com/search/docs/monitor-debug/search-operators?hl=es> (Operadores de Google).

<https://www.xataka.com/basics/shodan-que-se-puede-usar-este-buscador-dispositivos-conectados-a-internet> (Descripción de Shodan).

<https://data-universe.org/la-importancia-de-la-etica-en-la-recopilacion-de-datos-guia-completa/> (Ética en la Recopilación de Datos: Guía Completa de Práctica Responsable y Confiable).

<https://www.imperva.com/learn/application-security/google-dorking-hacking/> (Ejemplos de Google Hacking y como consejos de como evitarlos)

<https://google-gruyere.appspot.com/> (Página web vulnerable creada por Google).

<https://www.shodan.io/search/filters> (filtros de Shodan).

<https://certisec.org/what-is-shodan-full-guide-to-shodan-and-its-capabilities/> (Guía de Shodan).

<https://www.stationx.net/how-to-use-shodan/> (Guía de Shodan con Kali Linux).

<https://www.redeszone.net/noticias/seguridad/navegadores-web-alternativos/> (Guía de Shodan para CMD de Windows).

https://es.wikipedia.org/wiki/Secure_Shell (Información sobre el protocolo SSH).

<https://www.studocu.com/ec/document/instituto-superior-tecnologico-vida-nueva/software/uso-de-rsa-en-ssh-servidores/54833552> (Información sobre tipo de clave SSH-RSA).

https://en.wikipedia.org/wiki/Ubuntu_version_history (Versiones Ubuntu).

https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo (Información sobre ASN).

<https://protecciondatos-lopd.com/empresas/algoritmo-diffie-hellman/> (¿Qué es el algoritmo Diffie-Hellman?).

<https://www.eduardocollado.com/2020/08/28/algoritmos-de-cifrado-en-ssh/> (Algoritmos de cifrado en SSH).

<https://latam.kaspersky.com/blog/que-es-un-hash-y-como-functiona/2806/> (¿Qué Es Un Hash Y Cómo Funciona?).

<https://es.wikipedia.org/wiki/UMAC> (En criptografía, un código de autenticación de mensajes basado en hashing universal o UMAC)

<https://es.wikipedia.org/wiki/HMAC> (criptografía, un HMAC (a veces expandido como código de autenticación de mensajes en clave-hash o código de autenticación de mensaje basado en hash).

<https://www.hostinger.es/tutoriales/que-es-nginx> (¿Qué es NGINX y cómo funciona?).

<https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/> (ataque de XSS o Cross-Site Scripting).

<https://nvd.nist.gov/vuln/search> (Buscador de vulnerabilidades del National Vulnerability Database).

<https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444> (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal).

https://www.youtube.com/watch?v=jhqESj5aE_I&ab_channel=TokerSploit (COMO USAR SHODAN | APRENDE HACKING ETICO DE FORMA SEGURA Y LEGAL)