

Sumario

BUSCADOR DE GOOGLE.....	2
GOOGLE DORKS.....	8
SHODAN.....	13
REFLEXIÓN ÉTICA.....	16

BUSCADOR DE GOOGLE

Voy a usar el buscador de google para recopilar informacion de la organizacion sony

-site:sony.com filetype:pdf “confidential” para indicar que el sitio web es sony.com y que me busque archivos con formato .pdf que lleven la palabra confidential para ver si encuentro documentos confidenciales, codigos documentos o archivos legales

Google site:sony.com filetype:pdf "confidential" X | | | |

Sony
https://www.sony.com › support › res › manuals PDF ⋮
Dismantling Information for Use by Professional Recyclers
Parts contain **confidential** information. Strictly follow the instruction whenever the components are repaired and/or replaced. 1-4 EXPLODED VIEW. AND PART LIST.
16 páginas

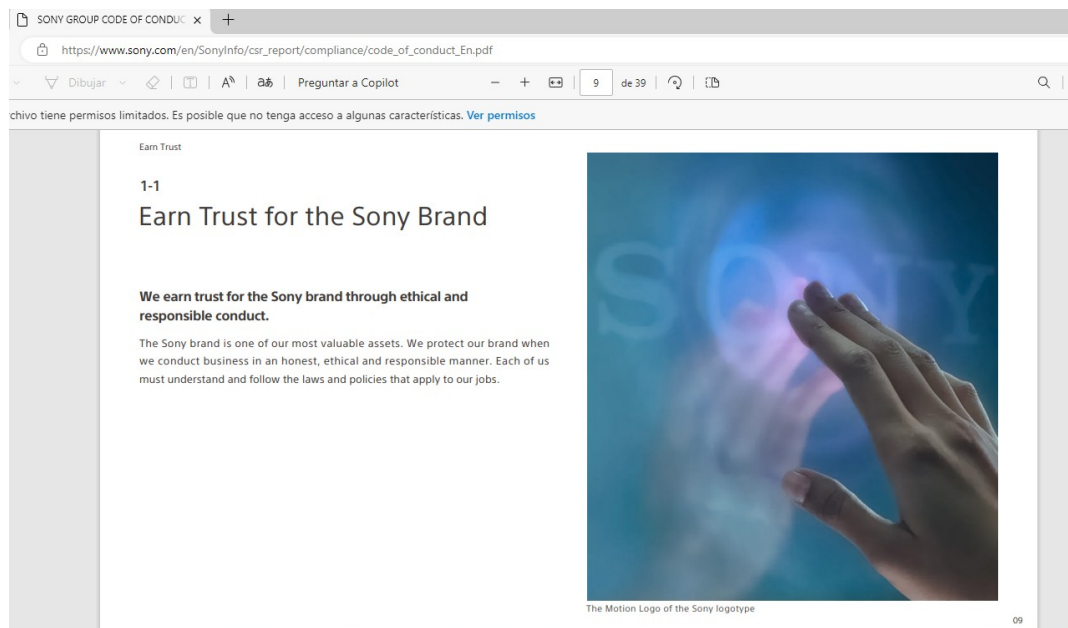
Sony
https://www.sony.com › support › res › manuals PDF ⋮
Compact Hi-Fi Stereo System
Confidential unpublished works. © 1992-1997 Dolby Laboratories. All rights reserved. ENERGY STAR® is a U.S. registered mark. As ENERGY STAR® Partner, Sony.

Sony
https://www.sony.com › csr_report › compliance PDF ⋮
SONY GROUP CODE OF CONDUCT
Our **confidential** and proprietary information, and such information entrusted to us from our suppliers, business partners or customers, is vital to our continued ...
39 páginas

Sony
https://www.sony.com › support › res › manuals PDF ⋮
confidential
Page 1. (**CONFIDENTIAL**. 2. 3. 4. B. DRAWING. SONY STANDARD. 1. H. H. A1. '09.4. K. —. 309,8. (12 1/4 inch). 619.5. (24 1/ ...

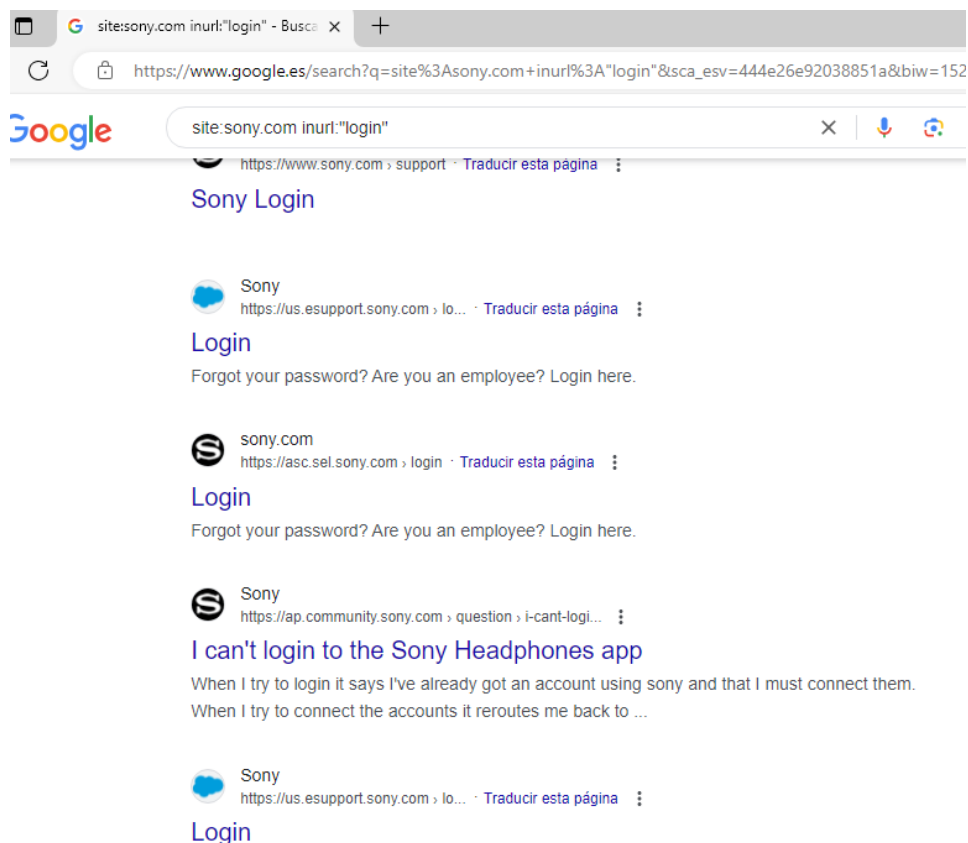
David Martínez 2ASIR

Por ejemplo encontré un pdf sobre el código de conducta de la empresa

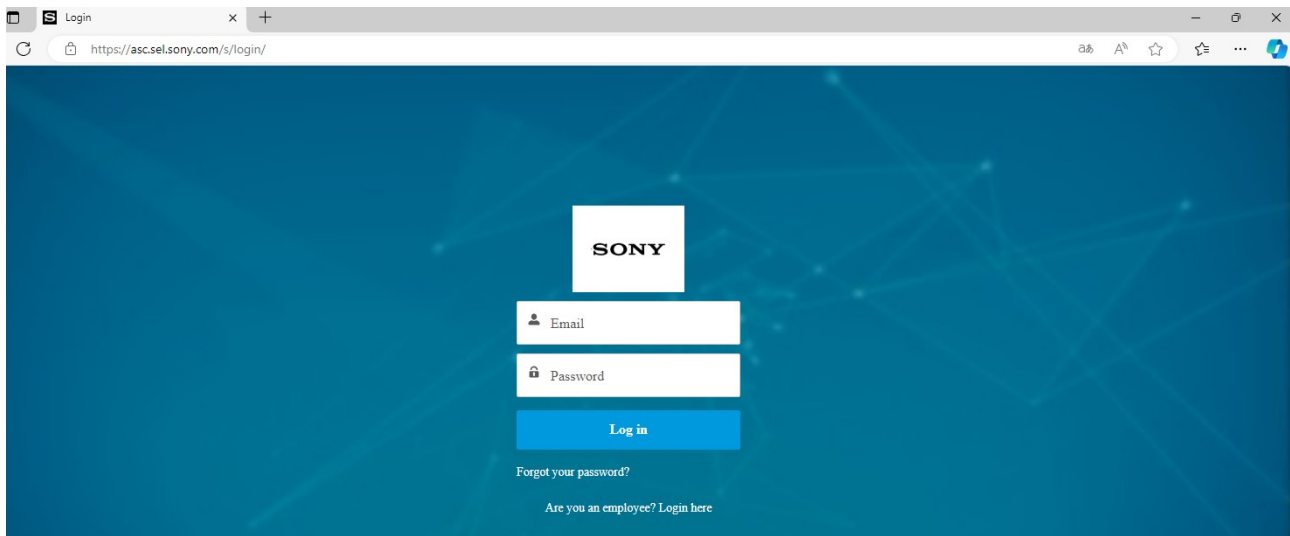


-site:sony.com inurl:login

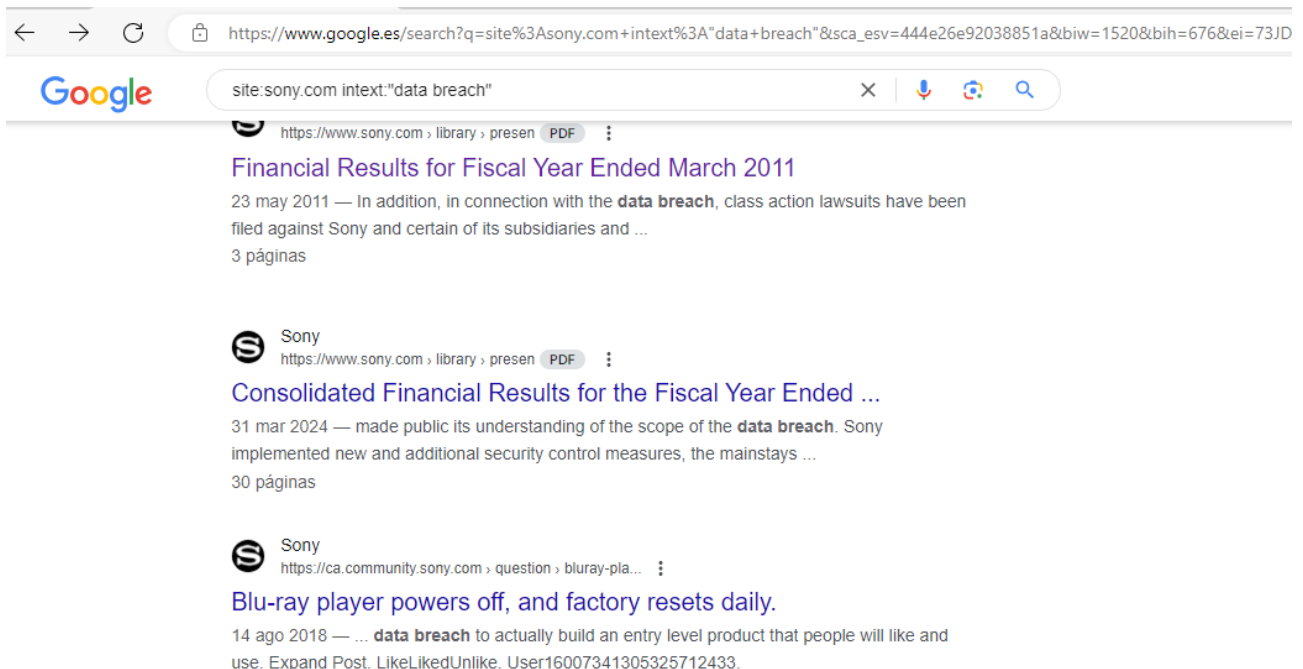
inurl busca paginas web cuya url contiene una palabra especifica, con esta busqueda encuentro paginas de inicio de sesión en sony.com

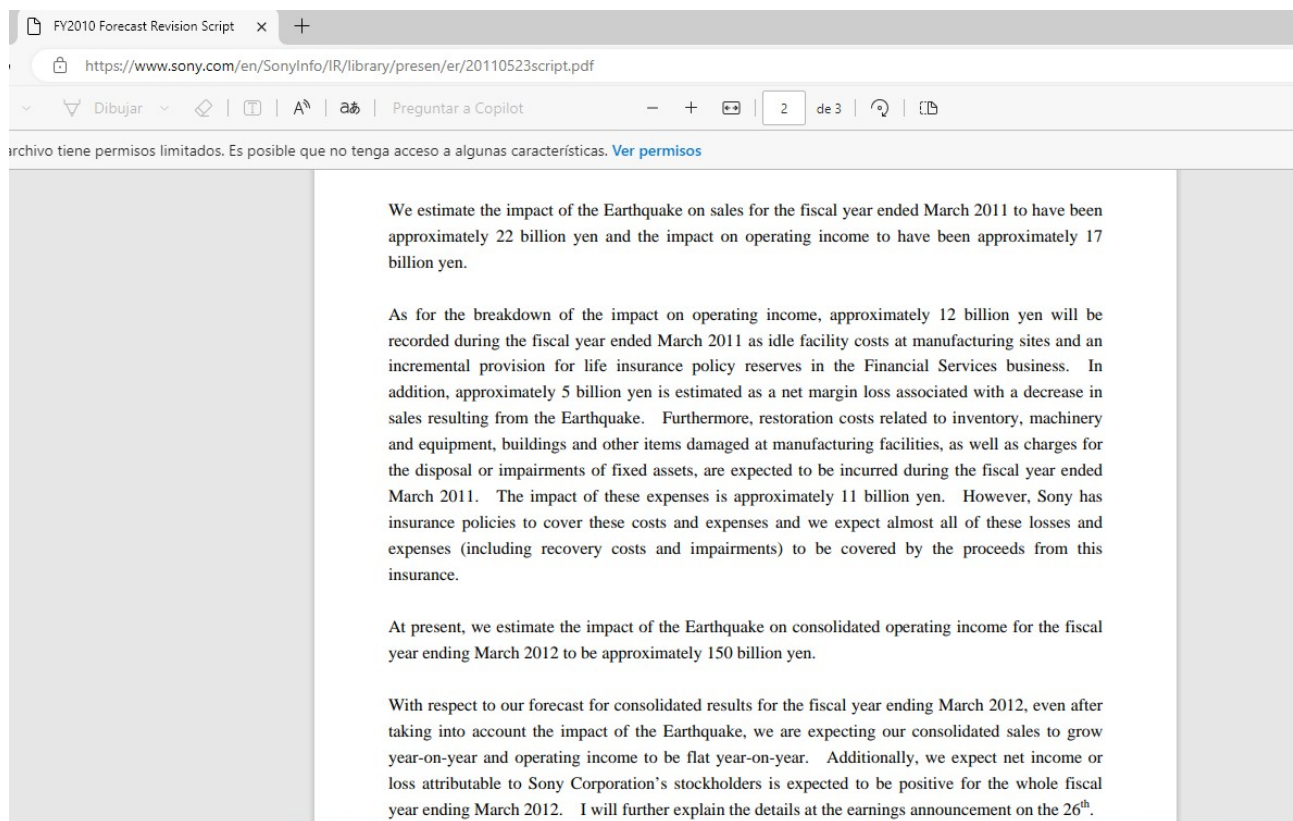


David Martínez 2ASIR



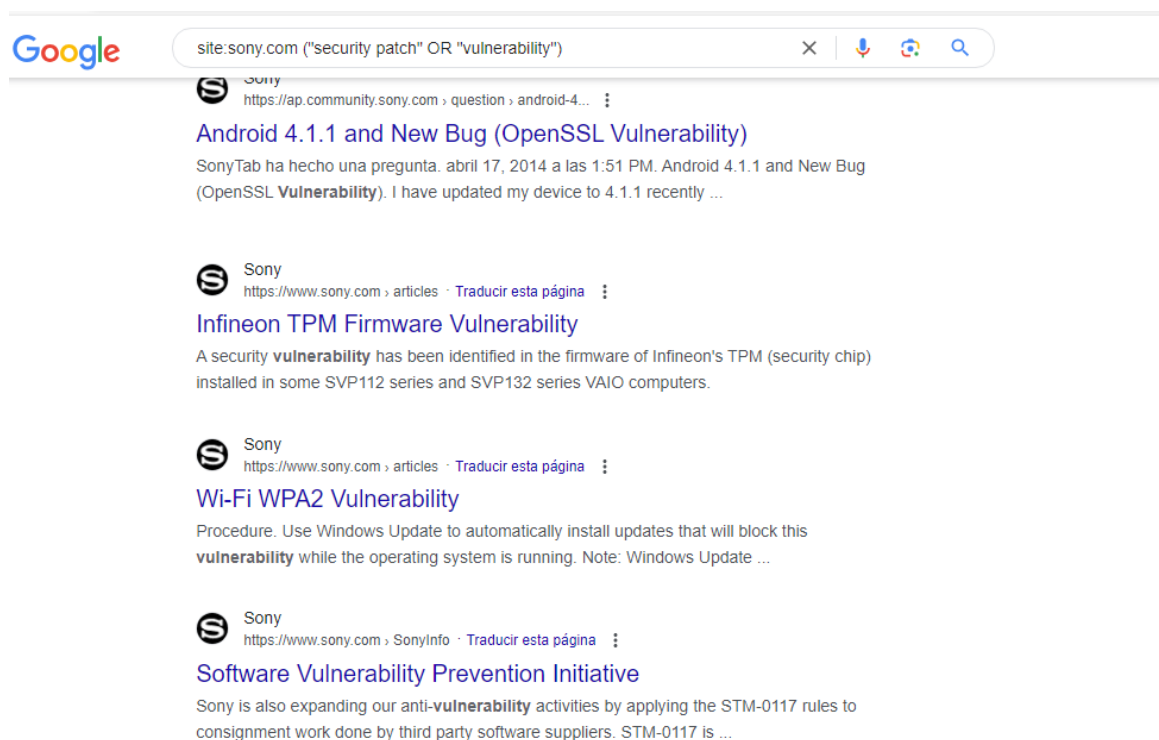
-site:sony.com intext:"data breach" Con intext buscas palabras específicas en el cuerpo de las páginas web, busco data breach para buscar informes relacionados con ciberataques y encontré documentos sobre datos financieros

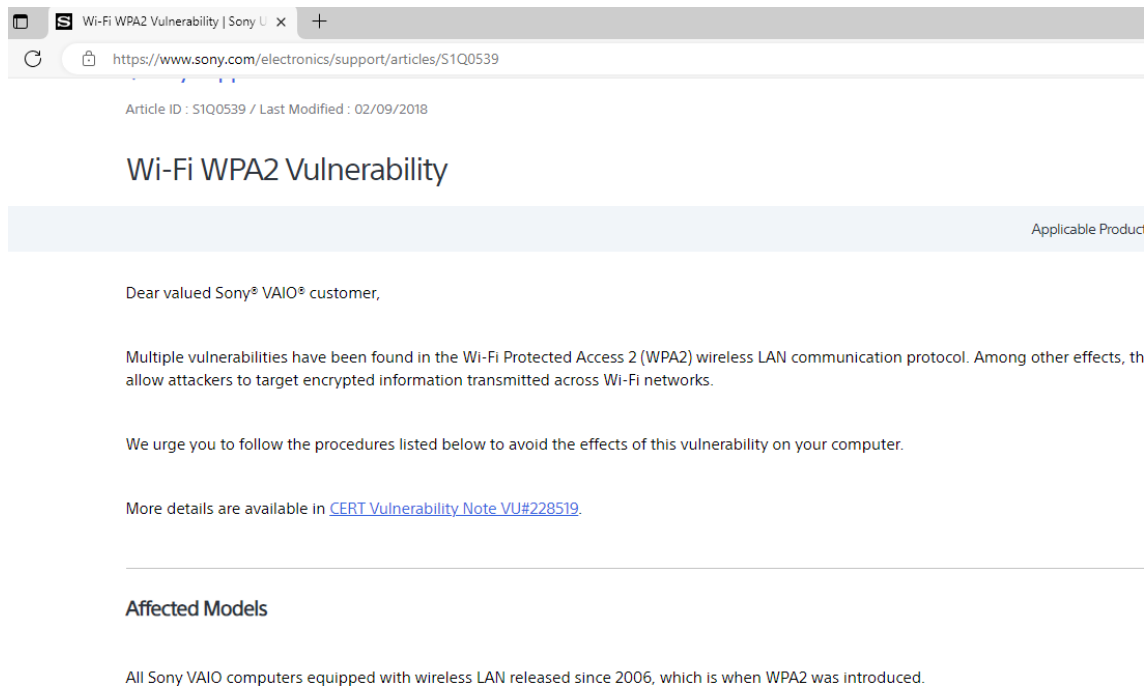




-site:sony.com (“security patch” or “vulnerability”)

Intento encuentre paginas relacionadas con parches de seguridad o vulnerabilidades y encuentro vulnerabilidades identificadas por sony

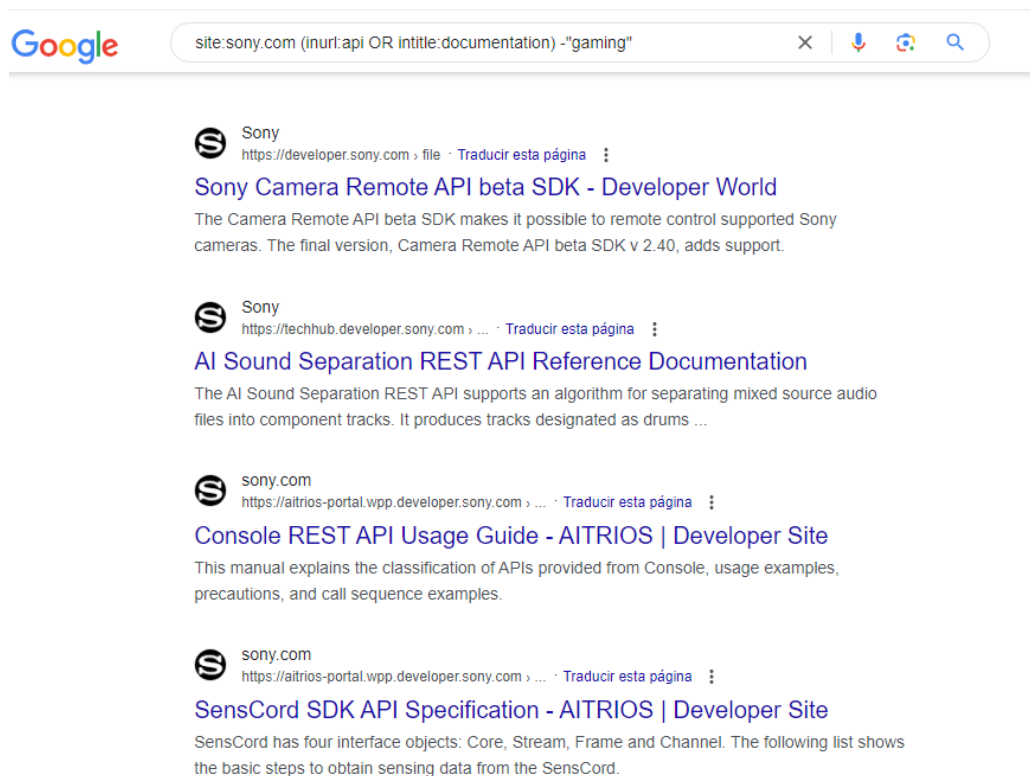




The screenshot shows a web browser window with the address bar displaying <https://www.sony.com/electronics/support/articles/S1Q0539>. The page title is "Wi-Fi WPA2 Vulnerability". Below the title, it says "Article ID : S1Q0539 / Last Modified : 02/09/2018". The main content area has a heading "Wi-Fi WPA2 Vulnerability" and a subheading "Applicable Product". The text reads: "Dear valued Sony® VAIO® customer," followed by "Multiple vulnerabilities have been found in the Wi-Fi Protected Access 2 (WPA2) wireless LAN communication protocol. Among other effects, they allow attackers to target encrypted information transmitted across Wi-Fi networks." It then states: "We urge you to follow the procedures listed below to avoid the effects of this vulnerability on your computer." and "More details are available in [CERT Vulnerability Note VU#228519](#)." Below this is a section titled "Affected Models" with the text: "All Sony VAIO computers equipped with wireless LAN released since 2006, which is when WPA2 was introduced."


-site:sony.com (inurl:api OR intitle:documentation) -"gaming"


Busco sitios relacionados con apis o documentacion tecnica que no tenga que ver con videojuegos y encuentre un api para una camara remota



The screenshot shows a Google search interface with the query "site:sony.com (inurl:api OR intitle:documentation) -"gaming"". The search results are as follows:

- Sony**
<https://developer.sony.com> › file › Traducir esta página
Sony Camera Remote API beta SDK - Developer World
The Camera Remote API beta SDK makes it possible to remote control supported Sony cameras. The final version, Camera Remote API beta SDK v 2.40, adds support.
- Sony**
<https://techhub.developer.sony.com> › ... › Traducir esta página
AI Sound Separation REST API Reference Documentation
The AI Sound Separation REST API supports an algorithm for separating mixed source audio files into component tracks. It produces tracks designated as drums ...
- sony.com**
<https://aitrios-portal.wpp.developer.sony.com> › ... › Traducir esta página
Console REST API Usage Guide - AITRIOS | Developer Site
This manual explains the classification of APIs provided from Console, usage examples, precautions, and call sequence examples.
- sony.com**
<https://aitrios-portal.wpp.developer.sony.com> › ... › Traducir esta página
SensCord SDK API Specification - AITRIOS | Developer Site
SensCord has four interface objects: Core, Stream, Frame and Channel. The following list shows the basic steps to obtain sensing data from the SensCord.

 Develop ▾

 English ▾

Log in


Download

GOOGLE DORKS

Vamos a entrar en la google exploit database para buscar dorks relevantes sobre información sensible, como contraseñas, archivos de configuración, o datos expuestos en servicios como Trello o GitHub.

-site:github.com intext:"unattend xmlns" AND "password" ext:xml

Este dork busca configuraciones sensibles en repositorios de GitHub relacionadas con archivos de configuración no atendida (unattended setup files). Los archivos XML con etiquetas como unattend xmlns se utilizan generalmente en procesos de instalación automatizada, como la configuración de sistemas Windows. La consulta se centra en localizar configuraciones que incluyan la palabra clave password, lo que sugiere que podrían contener credenciales almacenadas directamente en texto plano o referencias a contraseñas codificadas.

 EXPLOIT DATABASE

site:github.com intext:"unattend xmlns" AND "password" ext:xml

GHDB-ID:

7534

Author:

AFTAB ALAM

Published: 2021-11-01

Google Dork Description:

site:github.com intext:"unattend xmlns" AND "password" ext:xml

Google Search: site:github.com intext:"unattend xmlns" AND "password" ext:xml

←

→

Google Dork: site:github.com intext:"unattend xmlns" AND "password" ext:xml
Files Containing Juicy Info
Date: 29/10/2021
Exploit Author: Aftab Alam

Google

site:github.com intext:"unattend xmlns" AND "password" ext.xml

Todo Videos Imágenes Noticias Libros Web Finanzas Herramientas

GitHub
https://github.com › blob › main · Traducir esta página

unattend.xml

... <Password> <Value>P@ssword</Value> </Password> </AutoLogon> </component> ... <unattend xmlns="urn:schemas-microsoft-com:unattend"> <settings pass ...

GitHub
https://github.com › answer_files · Traducir esta página

autounattend.xml

17 jun 2024 — > <unattend xmlns="urn:schemas-microsoft-com:unattend"> <servicing ... <Password> <Value>UABhAHMAcWB3ADAACgBkACEAUABhAHMAcWB3AG8AcgBkAA ...

GitHub
https://github.com › blob › Autou... · Traducir esta página

unattended-setup-scripts/Autounattend.xml at master

> <unattend xmlns="urn:schemas-microsoft-com:unattend"> <settings pass ... <Password> <Value>Passw0rd</Value> <PlainText>true</PlainText> </Password> ...

GitHub
https://github.com › blob › master · Traducir esta página

unattend.xml - OpenNebula/addon-context-windows

16 ene 2024 — > <unattend xmlns="urn:schemas-microsoft-com:unattend"> <settings ... Password to be used only during initial provisioning. Must be ...

En los repositorios github encuentro ficheros unattend.xml que pueden contener contraseñas administrador, configuraciones de red, o claves de acceso a otros servicios

Go to file


- 3 Things to Know Before Deployi...
- Create a Zero-Touch USB Key for ...
- DIY Zero-Touch Provisioning Proc...
 - Apply-Image.ps1
 - Build-WinPE.ps1
 - Create-Win10-Media.ps1
 - README.md
 - unattend.xml**
- How to Add PowerShell Active Di...
- How to Migrate from McAfee M...
- No-Prompt Bootable ISO - Crow...
 - LICENSE
 - README.md

Code Blame 107 lines (107 loc) · 5.36 KB

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <!--Version 2.3-->
3 <unattend xmlns="urn:schemas-microsoft-com:unattend">
4   <settings pass="WindowsPE">
5     <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionS
6       <SetupUILanguage>
7         <UILanguage>en-US</UILanguage>
8       </SetupUILanguage>
9       <InputLocale>en-US</InputLocale>
10      <SystemLocale>en-US</SystemLocale>
11      <UILanguage>en-US</UILanguage>
12      <UserLocale>en-US</UserLocale>
13    </component>
14  </settings>
15  <settings pass="specialize">
16    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
17      <ComputerName>*</ComputerName>
18      <RegisteredOrganization>Cool Company, LLC.</RegisteredOrganization>
19      <RegisteredOwner>Cool Company, LLC.</RegisteredOwner>
20      <WindowsFeatures>
21        <ShowInternetExplorer>false</ShowInternetExplorer>
22      </WindowsFeatures>
23      <AutoLogon>
24        <Username>LocalAdmin</Username>
25        <Enabled>true</Enabled>
26        <LogonCount>10</LogonCount>
27        <Password>
28          <Value>P@ssword</Value>
29        </Password>
30      </AutoLogon>
31    </component>
32    <component name="Microsoft-Windows-Deployment" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
33      <RunSynchronous>
```



```
-site:github.com "BEGIN OPENSSSH PRIVATE KEY"
```

EXPLOIT
DATABASE

site:github.com "BEGIN OPENSSSH PRIVATE KEY"

GHDB-ID:

8451

Author:

KSTRAWNO

Published:


2024-08-23

Google Dork Description:

site:github.com "BEGIN OPENSSSH PRIVATE KEY"

Google Search:

site:github.com "BEGIN OPENSSSH PRIVATE KEY"



site:github.com "BEGIN OPENSSSH PRIVATE KEY"

Google

site.github.com "BEGIN OPENS SH PRIVATE KEY"

✕ | 🔍

Todo

Imágenes

Videos


Noticias

Web

Libros

Finanzas


Herramientas

 GitHub

<https://github.com> · [fleet](#) · [issues](#) · [Traducir esta página](#) · [⋮](#)

Support OpenSSH private key format for Git SSH ...


12 ene 2021 — PEM format keys must be explicitly requested by specifying the "-m PEM" flag. → cat id_rsa -----BEGIN OPENS SH PRIVATE KEY----- ...

 GitHub

<https://github.com> · [issues](#) · [Traducir esta página](#) · [⋮](#)

OpenSSH keys not accepted · Issue #6312 · rundeck ...


24 jul 2020 — -----BEGIN OPENS SH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAAAAlwAAAAAdzc2gtcn...

 GitHub

<https://github.com> · [valohai](#) · [ope...](#) · [Traducir esta página](#) · [⋮](#)

valohai/openssh-key: Tools to deal with OpenSSH2 ...

These key files are the default format generated by ssh-keygen since OpenSSH 7.8 (2018-08-24) and can be recognized from their -----BEGIN OPENS SH PRIVATE KEY----- ...

 GitHub

<https://gist.github.com> · [perja12](#) · [Traducir esta página](#) · [⋮](#)

Convert SSH private key to classic format

If you generate a key pair with ssh-keygen you can, depending on version, get a private key with the header -----BEGIN OPENS SH PRIVATE KEY-----

David Martínez 2ASIR

Un usuario filtra su clave ssh

Support OpenSSH private key format for Git SSH authentication #221

Closed janeczku opened this issue on Jan 12, 2021 · 8 comments

janeczku commented on Jan 12, 2021 · edited

Since OpenSSH 7.8, the `ssh-keygen` command creates keys in the OpenSSH private key format instead of the PEM format. PEM format keys must be explicitly requested by specifying the `-m PEM` flag.

```
→ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b381bnIzeC1rZXktajEAAAAACmFiczIiNi1jdHIAAAAGYmlyeXB0AAAAGAAAAB++y/vlu6 (....)
```

That means a lot of users are probably already using private keys in the OpenSSH format. Adding a GitRepo in fleet using this key format result in the following error:

```
data does not contain a valid RSA or ECDSA private key
```

Git Repo: repo-with-ssh-auth Git Updating

Workspace: fleet-default Age: 21 min Overview YAML 1

data does not contain a valid RSA or ECDSA private key

0	0	0	0	0
Ready	Transitioning	Warning	Error	Unknown

[Resources](#) [Conditions](#)

Assignees

- StrongMc
- bmdesper
- nickgerac

Labels

- kind/enhancement

Projects

None yet

Milestone

v2.5.8

Development

No branches or pull requests

-intext:"aws_access_key_id" | intext:"aws_secret_access_key" filetype:json | filetype:yaml

Este dork está diseñado para encontrar claves de acceso a AWS (Amazon Web Services) que se hayan expuesto inadvertidamente en archivos JSON o YAML públicos. Estas claves incluyen el `aws_access_key_id` y el `aws_secret_access_key`, que son esenciales para acceder a los recursos de AWS. Si alguien obtiene estas claves, puede acceder a recursos en la nube de AWS, lo que podría resultar en la exfiltración de datos sensibles o el abuso de recursos.

EXPLOIT DATABASE

intext:"aws_access_key_id" | intext:"aws_secret_access_key" filetype:json | filetype:yaml

GHDB-ID: 8446	Author: JOEL INDRA	Google Dork Description: intext:"aws_access_key_id" intext:"aws_secret_access_key" filetype:json filetype:yaml
Published: 2024-07-04		Google Search: intext:"aws_access_key_id" intext:"aws_secret_access_key" filetype:json filetype:yaml

Dork For : Finding exposed cloud service credentials

Regards,

Google

intext:"aws_access_key_id" | intext:"aws_secret_access_key" filetype:json | filetype:yaml

Todo Productos Imágenes Videos Noticias Libros Web Más Herramientas

GitHub
https://github.com › examples › 2... · Traducir esta página

20-secret-aws-credentials.yaml

... AWS_ACCESS_KEY_ID: ... AWS_SECRET_ACCESS_KEY: ... # optionally specify the region
#AWS_REGION: ... # optionally specify the token #AWS_SESSION_TOKEN ...

GitHub
https://github.com › workflows · Traducir esta página

main-workflow.yaml

... AWS_ACCESS_KEY_ID }} aws-secret-access-key: \${ secrets.AWS_SECRET_ACCESS_KEY ...
AWS_ACCESS_KEY_ID=" >> \$GITHUB_ENV echo "AWS_SECRET_ACCESS_KEY ...

Patrocinado

<> Code Issues Pull requests Discussions Actions Projects Security Insights

Files

main

Go to file

github/workflows

main-workflow.yaml

chart

config

gradle

src

.gitignore

.gitmodules

AWSCloudFormationTemplate.json

Dockerfile

Dockerfile.agent

README.md

agent-scrape-config-https.yml

agent-scrape-config.yml

build.gradle

ct.yaml

docker-compose.yaml

env.properties

env_agent.properties

gradle.properties

asserts-aws-cloudwatch-exporter / .github / workflows / main-workflow.yaml

arramos84 change workflow name to test credentials ✓

Code Blame 183 lines (153 loc) · 4.86 KB

```
1 name: Build and Publish Aws-Exporter
2
3 on:
4   pull_request:
5     branches:
6       - main
7   push:
8     branches:
9       - main
10    tags:
11      - 'v*'
12
13 env:
14   REGISTRY: asserts
15
16 jobs:
17   lint:
18     name: Lint Helm Chart
19     runs-on: ubuntu-20.04
20     steps:
21       - name: Checkout
22         uses: actions/checkout@v3
23         with:
24           fetch-depth: 0
25
26       - name: Set up Helm
27         uses: azure/setup-helm@v3
28         with:
29           version: v3.10.0
30
```

David Martínez 2ASIR

SHODAN

Vamos a realizar 3 búsquedas avanzadas en Shodan, usando filtros como port:, country:, o org:, para identificar dispositivos o servicios expuestos en internet.

-port:21 country:"US"

Este dork busca servidores que tienen el puerto 21 (usado por FTP) abierto en dispositivos ubicados en los Estados Unidos. Los resultados muestran servidores FTP, algunos de los cuales pueden permitir accesos no seguros o estar mal configurados, lo que puede poner en riesgo la seguridad de los datos almacenados.

The screenshot shows the Shodan search interface. At the top, the search bar contains 'port:21 country:US'. Below the search bar, the total number of results is 2,138,165. The left sidebar lists top cities and organizations. The main content area shows three search results. The first result is for IP 169.244.51.227, which is a ProfFTPD Server (Debian) with a login error. The second result is for IP 34.8.82.31, which is a Google LLC server with no data returned. The third result is for IP 172.80.72.124, which is a BT-PANEL server with an SSL certificate.

TOP CITIES	Count
Kansas City	373,647
Los Angeles	229,074
Phoenix	146,261
Provo	136,731
Atlanta	129,538

TOP ORGANIZATIONS	Count
Google LLC	460,382
Unified Layer	128,472
Incapsula Inc	110,678
PEG TECH INC	67,292
GoDaddy.com, LLC	60,844

TOP PRODUCTS	Count
Pure-FTPd	793,750
Microsoft ftpd	68,034
ProFTPD	35,181
Multicraft ftpd	15,270

169.244.51.227
www.abbott-memorial.lib.me.us
Abbott Memorial Library (Dexter)
United States, Dexter

220 ProfFTPD Server (Debian) [::ffff:169.244.51.227]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
214-CMD XCMD CDDP XCUP SHUT* QUIT PORT PASV
214-EPRT EPSV ALLO RNFR RNTD DELE HDTN RND
214-XRND HND ...

34.8.82.31
31.82.8.34.bc.googleusercontent.com
Google LLC
United States, Kansas City

No data returned

172.80.72.124
eSited Solutions
United States, Los Angeles

startls self-signed

SSL Certificate
Issued By:
I-Common Name:
172.80.56.50
I-Organization:
BT-PANEL
Issued To:
I-Common Name:
172.80.56.50
I-Organization:
BT-PANEL
Supported SSL Versions:
TLSv1.2

220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 3 of 50 allowed.
220-Local time is now 04:56. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minute...

IP:169.244.51.227

PAIS: Estados Unidos

Ciudad: Dexter

The screenshot shows the Shodan search interface. At the top, the search bar contains 'port:21 country:US'. Below the search bar, the total number of results is 2,138,165. The left sidebar lists top cities and organizations. The main content area shows three search results. The first result is for IP 169.244.51.227, which is a ProfFTPD Server (Debian) with a login error. The second result is for IP 34.8.82.31, which is a Google LLC server with no data returned. The third result is for IP 172.80.72.124, which is a BT-PANEL server with an SSL certificate.

TOP CITIES	Count
Kansas City	373,647
Los Angeles	229,074
Phoenix	146,261
Provo	136,731
Atlanta	129,538

TOP ORGANIZATIONS	Count
Google LLC	460,382
Unified Layer	128,472
Incapsula Inc	110,678
PEG TECH INC	67,292
GoDaddy.com, LLC	60,844

TOP PRODUCTS	Count
Pure-FTPd	793,750
Microsoft ftpd	68,034
ProFTPD	35,181
Multicraft ftpd	15,270

169.244.51.227
www.abbott-library.com
www.abbott-memorial.lib.me.us
Abbott Memorial Library (Dexter)
United States, Dexter

220 ProfFTPD Server (Debian) [::ffff:169.244.51.227]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
214-CMD XCMD CDDP XCUP SHUT* QUIT PORT PASV
214-EPRT EPSV ALLO RNFR RNTD DELE HDTN RND
214-XRND HND ...

34.8.82.31
31.82.8.34.bc.googleusercontent.com
Google LLC
United States, Kansas City

No data returned

172.80.72.124
eSited Solutions
United States, Los Angeles

startls self-signed

SSL Certificate
Issued By:
I-Common Name:
172.80.56.50
I-Organization:
BT-PANEL
Issued To:
I-Common Name:
172.80.56.50
I-Organization:
BT-PANEL
Supported SSL Versions:
TLSv1.2

220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 3 of 50 allowed.
220-Local time is now 04:56. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minute...

David Martínez 2ASIR

-port:8080 "webcam" country:"US"

Este dork busca cámaras web o cámaras IP expuestas en el puerto 8080, que a menudo se utiliza como un puerto alternativo para la administración web de cámaras y otros dispositivos. La búsqueda está limitada a los Estados Unidos, lo que ayuda a localizar dispositivos vulnerables en esa región.

SHODAN

Explore

Downloads

Pricing

port:8080 "webcam" country:"US"

TOTAL RESULTS

54

TOP CITIES

Atlanta

3

Phoenix

3

Ashburn

2

Cedar Knolls

2

Fremont

2

More...

TOP ORGANIZATIONS

Charter Communications Inc

7

Linode

6

Charter Communications

5

Comcast Cable Communications, Inc.

5

CenturyLink Communications, LLC

4

More...

TOP PRODUCTS

View Report

Browse Images

View on Map

Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

webcamXP 5

98.5.185.34

syn-098-005-185-034.res.spectrum.com

Charter Communications Inc

United States, Lockport

id

HTTP/1.1 200 OK

Connection: close

Content-Type: text/html; charset=utf-8

Content-Length: 7433

Cache-control: no-cache, must revalidate

Date: Sun, 24 Nov 2024 20:50:58 GMT

Expires: Sun, 24 Nov 2024 20:50:58 GMT

Pragma: no-cache

Server: webcamXP 5

IP:98.5.185.34
PAIS:Estados Unidos
Ciudad:Lockport

98.5.185.34

Regular View

Raw Data

© OpenMapTiles Satellite | © MapTiler | © OpenStreetMap

// TAGS

id

// LAST SEEN

General Information

Hostnames

syn-098-005-185-034.res.spectrum.com

Domains

SPECTRUM.COM

Country

United States

City

Lockport

Organization

Charter Communications Inc

ISP

Charter Communications Inc

ASN

AS11351

Open Ports

8080 9000

// 8080 / TCP

-738548669 | 2024-11-24T21

webcamXP 5

webcamXP 5

HTTP/1.1 200 OK

Connection: close

Content-Type: text/html; charset=utf-8

Content-Length: 7433

Cache-control: no-cache, must revalidate

Date: Sun, 24 Nov 2024 20:50:58 GMT

Expires: Sun, 24 Nov 2024 20:50:58 GMT

Pragma: no-cache

Server: webcamXP 5

Web Technologies

JavaScript Frameworks

MooTools

David Martínez 2ASIR

-org:"Cisco" port:443

Este dork busca dispositivos de **Cisco** expuestos en el puerto 443, que generalmente se utiliza para conexiones seguras HTTPS. Este tipo de búsqueda puede revelar dispositivos de red como routers, switches o firewalls de Cisco que pueden estar mal configurados o con vulnerabilidades de seguridad.

SHODAN

Explore

Downloads

Pricing

org:"Cisco" port:443

TOTAL RESULTS

45,827

TOP COUNTRIES

United States

25,690

United Kingdom

3,065

Japan

3,053

Netherlands

2,474

Australia

2,341

More...

TOP ORGANIZATIONS

Cisco Webex LLC

35,298

Cisco OpenDNS LLC

7,237

CISCO SYSTEMS, INC.

1,995

Cisco Spark

355

Cisco Systems, Inc.

170

More...

TOP PRODUCTS

View Report

View on Map

Advanced Search

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

173.39.227.221

gnta@mc222.webex.com
webex.com
www.webex.com
Cisco Webex LLC
United States, Dallas

SSL Certificate

Issued By:
HydantID Server CA 01
Issued To:
Common Name:
*.webex.com
Organization:
Cisco Systems Inc.
Supported SSL Versions:
TLSv1.2

HTTP/1.1 400 Not Acceptable
Content-Length: 0

Cisco Integrated Management Controller

173.39.89.132
CISCO SYSTEMS, INC.
India, Bengaluru
self-signed

SSL Certificate

Issued By:
Common Name:
C-series CIMC
Issued To:
Common Name:
C-series CIMC
Organization:
Cisco Self Signed
Supported SSL Versions:
TLSv1.2

HTTP/1.1 200 OK
Server: webserver
Date: Sun, 24 Nov 2024 20:18:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Cache-control: max-age=0, no-cache, no-store
PreventCache: nocache
Pragma: no-cache
Content-Encoding: gzip
Strict-Tr...

Activar Windows
Ve a Configuración para z

IP:173.39.89.132
Pais:India
Ciudad:Bengaluru

173.39.89.132

Regular View

Raw Data

Tags

self-signed

LAST SEEN: 2024-11-

General Information

Country

India

City

Bengaluru

Organization

CISCO SYSTEMS, INC.

ISP

CISCO SYSTEMS, INC.

ASN

AS109

Open Ports

80 443

80 / TCP

202302959 | 2024-11-24T07:11:22.678

HTTP/1.1 302
Server: webserver
Date: Sun, 24 Nov 2024 06:12:55 GMT
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Location: https://173.39.89.132:443/login.html
Set-Cookie: sessioncookie=/path/; expires=Wed, 23 Mar 2005 07:12:00 GMT;
Cache-control: max-age=0, no-cache, no-store
PreventCache: nocache
Pragma: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'none'; child-src 'self' *; script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self' *; font-src 'self' data:; img-src 'self' data:; style-src 'self' 'unsafe-inline'; frame-src 'self';
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive

Cisco Integrated Management Controller

```
HTTP/1.1 200 OK
Server: webserver
Date: Sun, 24 Nov 2024 20:18:29 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Cache-control: max-age=0,no-cache,no-store
PreventCache: nocache
Pragma: no-cache
Content-Encoding: gzip
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'none'; child-src 'self' *; script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self' *; font-src 'self' data; img-src 'self' data; style-src 'self' 'unsafe-inline'; frame-src 'self';
X-Robots-Tag: noindex, nofollow, nosnippet, noarchive
```

SSL Certificate

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    b1:7c:f3:96:79:5e:31:6e
  Signature Algorithm: sha512WithRSAEncryption
  Issuer: C=US, ST=California, L=San Jose, CN=C-series CIMC, O=Cisco Self Signed, OU=PID:UCSC-C220-M45 SERIAL:FCH22097A0B
  Validity
    Not Before: Mar 21 17:57:07 2018 GMT
    Not After : Mar 20 17:57:07 2023 GMT
  Subject: C=US, ST=California, L=San Jose, CN=C-series CIMC, O=Cisco Self Signed, OU=PID:UCSC-C220-M45 SERIAL:FCH22097A0B
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
```

REFLEXIÓN ÉTICA

Google Hacking, implica el uso de operadores avanzados en el motor de búsqueda de Google para encontrar información sensible expuesta públicamente en sitios web. A través de búsquedas específicas, los hackers pueden descubrir contraseñas, configuraciones de servidores, documentos privados, y otros datos confidenciales que no deberían estar accesibles. Mientras que Google Hacking puede ayudar a los profesionales de la ciberseguridad a identificar riesgos de exposición de datos, su uso en sistemas ajenos sin permiso es ilegal y poco ético. Si un hacker accede a datos sensibles sin autorización, no solo viola leyes sobre protección de datos y privacidad, sino que también pone en peligro la integridad de los sistemas afectados. Por otro lado, **Shodan** es un motor de búsqueda que permite explorar dispositivos conectados a Internet, desde servidores hasta cámaras de seguridad y sistemas industriales. Aunque esta herramienta puede ser útil para los expertos en seguridad al identificar dispositivos expuestos o mal configurados, también puede ser utilizada por ciberdelincuentes para encontrar objetivos vulnerables. Los atacantes pueden aprovecharse de dispositivos expuestos sin contraseñas o con configuraciones débiles, lo que puede resultar en el robo de información, sabotaje de sistemas e incluso en ataques a infraestructuras críticas. En este contexto, los hackers éticos tienen una responsabilidad crucial. Su trabajo es identificar y corregir vulnerabilidades de manera legal y respetuosa. Deben obtener permiso explícito de las organizaciones antes de realizar cualquier tipo de auditoría de seguridad y seguir principios éticos que prioricen la protección de los usuarios y sistemas.