

TEAM CHALLENGE – INVESTIGACIÓN OSINT.



INFORME TÉCNICO

WWW.ECHAUREN.COM

REALIZADO POR: Alejandro, Ignacio, Leo y Víctor

THE BRIDGE DIGITAL
TALENT
ACCELERATOR

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Responsable del Análisis

- **Nombre del Analista:** Ignacio, Leo, Víctor, Alejandro
- **Cargo:** Analistas de Seguridad Informática
- **Pertenencia Organizacional:** Departamento de Seguridad de la Información, Empresa XYZ
- **Fecha del Análisis:** 22 de junio de 2024

Informe Técnico

1. Introducción

Este informe técnico detalla la identificación y gestión de datos sensibles encontrados en la plataforma de Echaurren y su entorno digital, así como proporciona una vista detallada de la configuración DNS y la información de registro WHOIS del dominio echaurren.com. El objetivo es mejorar la seguridad y el cumplimiento normativo de la plataforma.

2. Metodología de Identificación

2.1 Revisión de Enlaces y Contenidos

Se ha realizado una revisión exhaustiva de enlaces y contenidos disponibles en la plataforma, incluyendo políticas de privacidad, condiciones de uso y formularios de contacto.

2.2 Clasificación de Datos Sensibles

La información recolectada se ha categorizado en función de su naturaleza y potencial riesgo para la privacidad y seguridad de los usuarios.

3. Datos Sensibles Identificados

3.1 Información de Contacto y Geolocalización

- **Teléfonos y Correos Electrónicos:**

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

- Teléfono: 941354047
- Correo Electrónico: info@echaurren.com,
susana@echaurren.com, josefelix@echaurren.com,
iminfo@echaurren.com, protecciondatos@echaurren.com,
eventos@echaurren.com
- **Geolocalización:**
 - Enlace Google Maps: <http://goo.gl/maps/JGEvUsnybTH6c4q2842.4015463245932,-2.8498063672975777>

3.2 Información Personal

- **Nombre e Imagen:**
 - Fraancis Paniego Sanchez
 - francis@echaurren.com
 - c/ Jose Gracia n 19 ezcaray 26280 La Rioja España
- **Cuenta de Spotify:**
 - Enlace a cuenta de usuario:
<http://open.spotify.com/user/ulb82urhfgvsfmu8ts1n76mmd>

3.3 Información Financiera y de Transacciones

- **Detalles de Productos y Compras:**
 - Enlace a producto específico:
<https://echaurren.com/producto/experiencia-gastronomica-echaurren-tradicion/?add-to-cart=2909>

3.4 Cookies y Rastreo Web

- **Políticas de Cookies en Navegadores:**
 - Enlaces a políticas de cookies en varios navegadores como Firefox y Safari.

4. Medidas de Seguridad Recomendadas

4.1 Encriptación de Datos

- **Transmisión:** Utilizar HTTPS para todas las transmisiones de datos sensibles.

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

- **Almacenamiento:** Encriptar datos sensibles en reposo utilizando algoritmos robustos.

4.2 Control de Acceso

- **Autenticación y Autorización:** Implementar autenticación de múltiples factores (MFA) y políticas de autorización estrictas.
- **Registro y Monitoreo:** Mantener registros detallados de acceso y actividades relacionadas con datos sensibles.

4.3 Revisión y Actualización de Políticas

- **Políticas de Privacidad y Avisos Legales:** Revisar y actualizar regularmente para reflejar prácticas actuales y cumplimiento normativo.

5. Detalles de Configuración DNS y WHOIS

- **Consulta de Registro A:**
 - echaurren.com -> 82.98.178.143
- **Servidores de Nombres (Name Servers):**
 - ns.dinahosting.com → 82.98.128.132
 - ns2.dinahosting.com → 82.98.128.196
 - ns3.dinahosting.com → 72.29.96.10
 - ns4.dinahosting.com → 93.89.82.218
- **Intercambiador de Correo (MX):**
 - mail.echaurren.com → 82.98.160.13
- **Información WHOIS:**
 - Registrar: Dinahosting s.l.
 - Fecha de Creación: 28 de febrero de 2002
 - Fecha de Expiración: 28 de febrero de 2025
- **Conexiones de Red y Servicios Activos**
 - SSH (22/SSH)
 - FTP (21/FTP)
 - HTTP (80/HTTP, 443/HTTP)
 - SMTP (25/SMTP, 587/SMTP)
 - IMAP (143/IMAP, 993/IMAP)

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

- POP3 (995/POP3)
- MySQL (3306/MYSQL)

6. Conclusiones

La identificación y gestión adecuada de datos sensibles en la plataforma de Echaurren son esenciales para asegurar la privacidad de los usuarios y cumplir con las regulaciones vigentes. Las recomendaciones de seguridad propuestas buscan fortalecer la protección de datos en todas las áreas identificadas, asegurando que las prácticas de manejo de datos estén alineadas con las normativas de protección de datos.

Además, se han identificado **datos sensibles adicionales que requieren atención inmediata**, incluyendo:

- Información de contacto detallada de **José Félix Paniego y Francis Paniego Sánchez**, con direcciones de correo electrónico y **contraseñas encriptadas**.
- La necesidad de mejorar la protección de datos sensibles almacenados en la plataforma, como contraseñas encriptadas, para prevenir accesos no autorizados y posibles filtraciones.

Este informe integra tanto la identificación y gestión de datos sensibles en la plataforma de Echaurren como la información técnica relevante del dominio, proporcionando una visión completa para mejorar la seguridad y el cumplimiento normativo de la plataforma digital.

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Evidencias

Herramienta Photon:

La herramienta Photon en Kali Linux es una herramienta de escaneo web diseñada para realizar un escaneo exhaustivo de recursos web en busca de contenido y activos ocultos, como archivos, directorios, scripts, imágenes y más. Es especialmente útil para la recopilación de información y el análisis de superficie de ataque en aplicaciones web.

Con -d 0 se ejecuta el modo pasivo.

```
(root@kali)-[/home/kali/herramientas/Photon]
# python3 photon.py -u https://echaurren.com/ -o hotel_echaurren.com -d 0

Photon v1.3.2
[+] URLs retrieved from sitemap.xml: 17
[~] Level 1: 18 URLs
[!] Progress: 18/18
[~] Level 2: 43 URLs
[!] Progress: 24/43
```

```
(root@kali)-[/home/kali/herramientas/Photon]
# cd hotel_echaurren.com

(root@kali)-[/home/kali/herramientas/Photon/hotel_echaurren.com]
# ls
external.txt  files.txt  fuzzable.txt  internal.txt

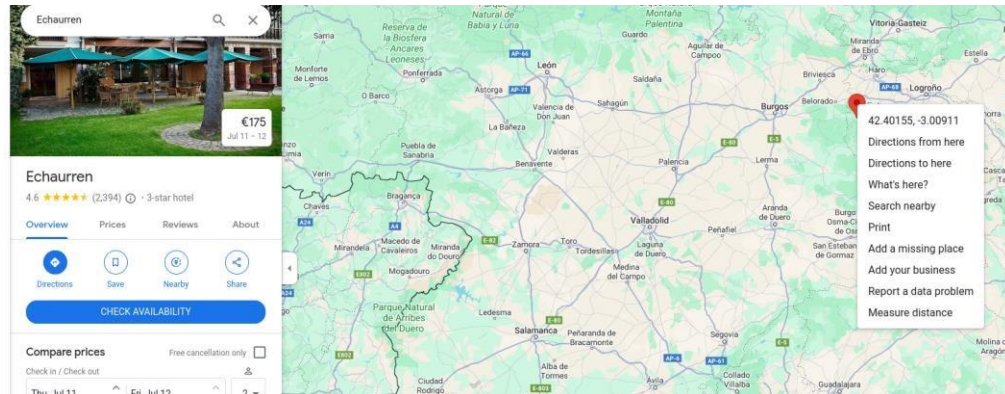
(root@kali)-[/home/kali/herramientas/Photon/hotel_echaurren.com]
# cat fuzzable.txt
https://echaurren.com/producto/experiencia-gastronomica-echaurren-tradicion/?add-to-cart=2909
https://echaurren.com/producto/experiencia-escapada-tradicion/?add-to-cart=2907
https://echaurren.com/producto/experiencia-gastronomica-el-portal-de-echaurren/?add-to-cart=2916
https://echaurren.com/producto/experiencia-escapada-el-portal-de-echaurren/?add-to-cart=2907
https://echaurren.com/producto/experiencia-gastronomica-echaurren-tradicion/?add-to-cart=6209
https://echaurren.com/producto/experiencia-gastronomica-el-portal-de-echaurren/?add-to-cart=2907
https://echaurren.com/producto/experiencia-escapada-el-portal-de-echaurren/?add-to-cart=2909
https://echaurren.com/producto/experiencia-dos-dias-gastronomicos/?add-to-cart=2917
https://echaurren.com/producto/experiencia-gastronomica-echaurren-tradicion/?add-to-cart=2914
https://echaurren.com/producto/experiencia-gastronomica-echaurren-tradicion/?add-to-cart=2907
https://echaurren.com/producto/experiencia-escapada-el-portal-de-echaurren/?add-to-cart=6209
https://echaurren.com/producto/experiencia-dos-dias-gastronomicos/?add-to-cart=2919
https://echaurren.com/producto/experiencia-escapada-tradicion/?add-to-cart=2919
https://echaurren.com/producto/experiencia-gastronomica-el-portal-de-echaurren/?add-to-cart=2917
https://echaurren.com/producto/experiencia-escapada-tradicion/?add-to-cart=2911
https://echaurren.com/producto/experiencia-escapada-el-portal-de-echaurren/?add-to-cart=2917
https://echaurren.com/producto/experiencia-gastronomica-el-portal-de-echaurren/?add-to-cart=2909
https://echaurren.com/producto/experiencia-escapada-tradicion/?add-to-cart=2916
https://echaurren.com/producto/experiencia-dos-dias-gastronomicos/?add-to-cart=2916
https://echaurren.com/producto/experiencia-dos-dias-gastronomicos/?add-to-cart=2907

(root@kali)-[/home/kali/herramientas/Photon/hotel_echaurren.com]
# cat files.txt
https://echaurren.com/wp-content/uploads/4.-SteakTartar_EchaurrenTraidicon.jpg
/pdfs/cartas/tradicion_menu_degustacion_frances.pdf
https://echaurren.com/wp-content/uploads/el_portal_menu_degustacion_frances-1.pdf
https://echaurren.com/wp-content/uploads/5.desayuno.jpg
https://echaurren.com/wp-content/uploads/5.ElPortaldeEchaurren.jpg
https://echaurren.com/wp-content/uploads/5.Helado_ElPortaldeEchaurren.jpg
https://echaurren.com/wp-content/uploads/5._H2M0641.jpg
/pdfs/cartas/el_cuartito_ingles_frances.pdf

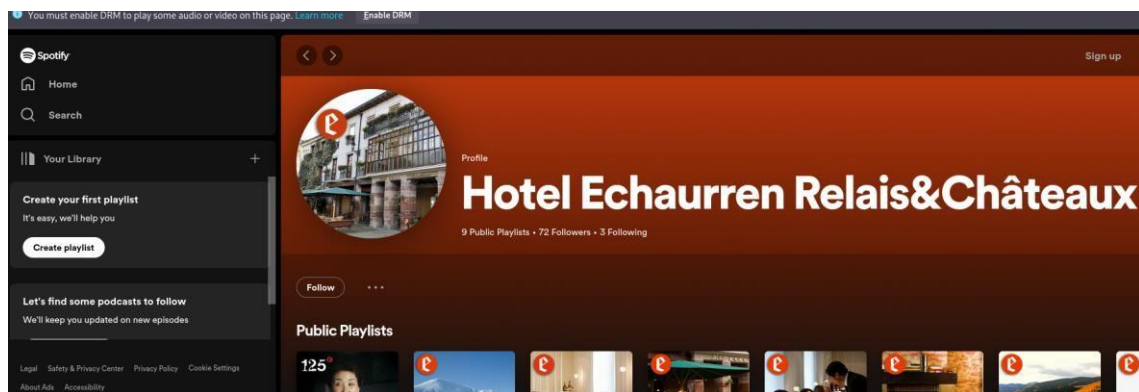
(root@kali)-[/home/kali/herramientas/Photon/hotel_echaurren.com]
# cat internal.txt
https://echaurren.com/experiencias//producto/experiencia-gastronomica-el-portal-de-echaurren/
https://echaurren.com/producto/experiencia-gastronomica-echaurren-tradicion/?add-to-cart=2909
https://echaurren.com/trabaja-con-nosotros/
https://echaurren.com/producto/experiencia-gastronomica-echaurren-tradicion/?add-to-cart=6209
https://echaurren.com/a-casa//contacto/
https://echaurren.com/politica-de-privacidad/tel:941354047
https://echaurren.com/en/work-with-us/
https://echaurren.com/en/en/contact/
https://echaurren.com/en/contact/tel:+34941354047
```


TEAM CHALLENGE – INVESTIGACIÓN OSINT.

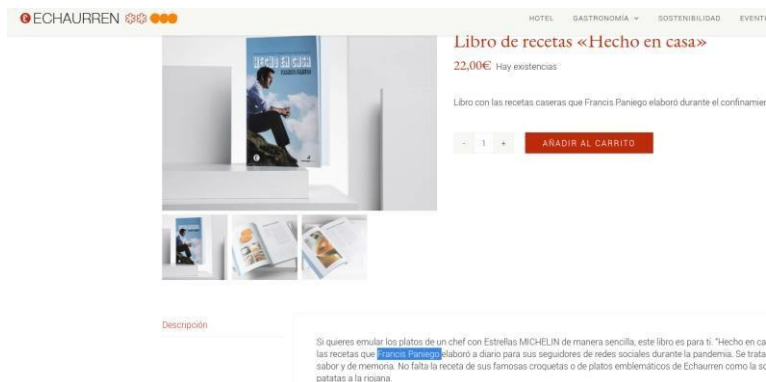
• Geolocalización



• Cuenta Spotify



• Información e imagen libro de Francis Paniego Sánchez



TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Herramienta Exiftool

ExifTool es una poderosa herramienta de línea de comandos que permite leer, escribir y editar metadatos de archivos. Es especialmente útil para trabajar con metadatos de archivos de imagen, audio, video y otros tipos de archivos. Aquí te explico cómo puedes utilizar ExifTool en Kali Linux:

The image shows three pages of a PDF menu titled 'EL PORTAL'. The first page is the cover, featuring a logo and text about the restaurant's cuisine. The second page is the 'MENU DÉGUSTATION 2024', listing various dishes and their ingredients. The third page is the 'MENU EN TABLE', listing dishes for a formal dinner. The menu is written in French and includes a signature at the bottom.

```
exiftool /home/kali/Desktop/el_portal_menu_degustacion_frances-1.pdf
ExifTool Version Number      : 12.76
File Name                    : el_portal_menu_degustacion_frances-1.pdf
Directory                    : /home/kali/Desktop
File Size                    : 137 kB
File Modification Date/Time  : 2024:06:20 06:41:05-04:00
File Access Date/Time       : 2024:06:20 06:41:06-04:00
File Inode Change Date/Time  : 2024:06:20 06:41:05-04:00
File Permissions             : -rw-rw-r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.7
Linearized                   : No
Page Count                   : 1
Language                     : es-ES
Tagged PDF                   : Yes
XMP Toolkit                   : 3.1-701
Producer                     : Microsoft® Word 2016
Creator                      : Francis Paniego Sanchez
Creator Tool                  : Microsoft® Word 2016
Create Date                  : 2024:05:03 16:25:38+02:00
Modify Date                   : 2024:05:03 16:25:38+02:00
Document ID                  : uuid:5CF52717-7807-40BE-8B77-9686EFD7F102
Instance ID                  : uuid:5CF52717-7807-40BE-8B77-9686EFD7F102
Author                       : Francis Paniego Sanchez
```


TEAM CHALLENGE – INVESTIGACIÓN OSINT.



```
(root@kali)-[/home/kali/herramientas/Photon/hotel_echaurren.com]
# exiftool /home/kali/Desktop/el_cuartito_ingles_frances.pdf
ExifTool Version Number      : 12.76
File Name                    : el_cuartito_ingles_frances.pdf
Directory                   : /home/kali/Desktop
File Size                    : 185 kB
File Modification Date/Time  : 2024:06:20 06:55:21-04:00
File Access Date/Time       : 2024:06:20 06:55:22-04:00
File Inode Change Date/Time  : 2024:06:20 06:55:21-04:00
File Permissions             : -rw-rw-r--
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
PDF Version                 : 1.7
Linearized                  : No
Page Count                  : 1
Language                    : es
Tagged PDF                  : Yes
XMP Toolkit                 : 3.1-701
Producer                   : Microsoft® Word 2016
Title                      : LA COCINA TRADICIONAL DE MI MADRE
Creator                    : HOTEL ECHAURREN
Creator Tool               : Microsoft® Word 2016
Create Date                : 2023:12:29 13:46:26+01:00
Modify Date                : 2023:12:29 13:46:26+01:00
Document ID                : uuid:D5FC5B42-C134-4607-8DA8-E53127B7B70D
Instance ID                : uuid:D5FC5B42-C134-4607-8DA8-E53127B7B70D
Author                     : HOTEL ECHAURREN
```

Herramienta Amass

Amass es una herramienta de código abierto utilizada para la recopilación de información de reconstrucción y enumeración de activos en el ámbito de la seguridad informática. Esta herramienta está diseñada para descubrir nombres de dominio, subdominios y direcciones IP asociadas con un dominio objetivo.

```
(root@kali)-[/home/kali/herramientas/Photon/hotel_echaurren.com]
# amass enum -passive -d echaurren.com
echaurren.com (FQDN) → mx_record → mail.echaurren.com (FQDN)
echaurren.com (FQDN) → a_record → 82.98.178.143 (IPAddress)
laarboledadelsur.echaurren.com (FQDN) → a_record → 82.98.178.143 (IPAddress)
82.98.128.0/18 (Netblock) → contains → 82.98.178.143 (IPAddress)
42612 (ASN) → managed_by → DINAHOSTING-AS, ES (RIROrganization)
42612 (ASN) → announces → 82.98.128.0/18 (Netblock)

The enumeration has finished
```

Subdominio nuevo

Laarboledadelsur

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Herramienta Spiderfoot

SpiderFoot es una herramienta de OSINT (Open Source Intelligence) diseñada para la recolección automatizada de datos y análisis de seguridad. Es utilizada para realizar investigaciones exhaustivas sobre personas, empresas, dominios, direcciones IP y otras entidades digitales.

OSINT1		FINISHED				
Summary		Correlations	Browse	Graph	Scan Settings	Log
						Search...
Browse / Country Name						
<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified		
<input type="checkbox"/>	United States	echaurren.com	sfp_countryname	2024-06-20 10:30:49		
<input type="checkbox"/>	United States	dinahosting.com	sfp_countryname	2024-06-20 10:38:54		
<input type="checkbox"/>	United States	synxis.com	sfp_countryname	2024-06-20 10:38:54		
<input type="checkbox"/>	United States	mcsv.net	sfp_countryname	2024-06-20 10:38:55		
				Search...		
Browse / Email Address						
<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified		
<input type="checkbox"/>	francis@echaurren.com	echaurren.com	sfp_emailformat	2024-06-20 10:32:56		
<input type="checkbox"/>	iminfo@echaurren.com	echaurren.com	sfp_skymem	2024-06-20 10:29:36		
<input type="checkbox"/>	iminfo@echaurren.com	echaurren.com	sfp_emailformat	2024-06-20 10:32:56		
<input type="checkbox"/>	info@echaurren.com	echaurren.com	sfp_skymem	2024-06-20 10:29:36		
<input type="checkbox"/>	josefelix@echaurren.com	echaurren.com	sfp_skymem	2024-06-20 10:29:36		

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Herramienta dehashed

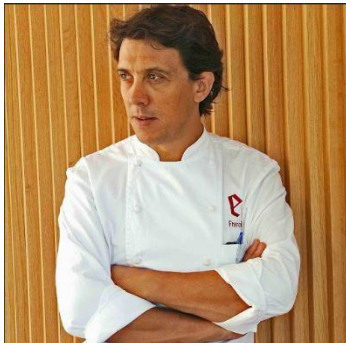
Dehashed es una plataforma que se utiliza principalmente para buscar y verificar contraseñas filtradas y otros datos comprometidos en bases de datos públicas y filtradas. Aquí te explico cómo puedes utilizar Dehashed:

<https://dehashed.com/>



Name	Chefe Paniego
Email	josefelix@echaurren.com
Username	10254484695235a0352cb88

Result #98857712	
Email	josefelix@echaurren.com
Hashed Password	\$2a\$08\$w0wrCgUBylkfahRy4l2/ Aen.WAlYyRJ6pSU2GbpDW3qv.G.WEYR:



Email	francis@echaurren.com
Password	2506fps

Result #118682508	
Name	FRANCIS PANIEGO SANCHEZ
Email	francis@echaurren.com
Address	C/PADRE JOSE GARCIA N 19, EZCARAY, 26280, LA RIOJA, SPA
I.P. Address	81.37.125.229

Email	francis@echaurren.com
Hashed Password	\$2a\$08\$w3JwQPsb.jD3HyodWZq5N..p[

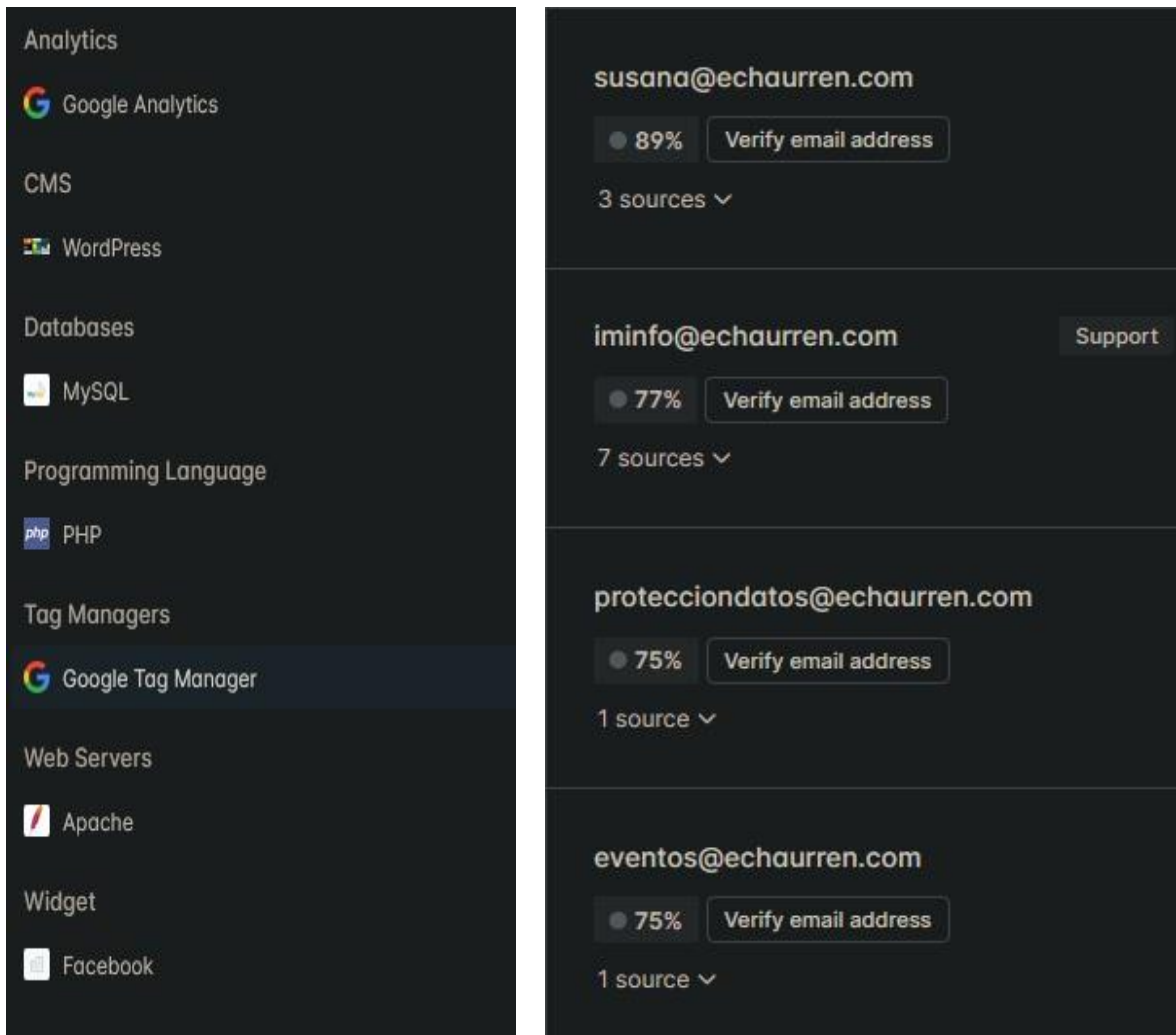
Email	info@echaurren.com
Password	628064

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Herramienta hunter.io

HUNTER.IO

Hunter.io es una herramienta de OSINT (Open Source Intelligence) especializada en la búsqueda y verificación de direcciones de correo electrónico. Es ampliamente utilizada por profesionales de ventas, marketing, recursos humanos y ciberseguridad para encontrar y verificar contactos en empresas específicas.



The image shows the Hunter.io web application interface. On the left is a dark sidebar with various tool categories and their logos. The main panel on the right displays search results for the domain 'echaurren.com', showing four email addresses with their verification status and source counts.

Category	Item
Analytics	Google Analytics
CMS	WordPress
Databases	MySQL
Programming Language	PHP
Tag Managers	Google Tag Manager
Web Servers	Apache
Widget	Facebook

Email Address	Verification Status	Action	Sources
susana@echaurren.com	89%	Verify email address	3 sources
iminfo@echaurren.com	77%	Verify email address	7 sources
protecciondatos@echaurren.com	75%	Verify email address	1 source
eventos@echaurren.com	75%	Verify email address	1 source

TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Herramienta ROBTEX

Robtex es una herramienta de OSINT (Open Source Intelligence) utilizada principalmente para recopilar y analizar información relacionada con dominios, direcciones IP y redes.

General	
FQDN	echaurren.com
Host Name	
Domain Name	echaurren.com
Registry	com
TLD	com
DNS	
IP numbers	82.98.160.13 82.194.88.38
Name servers	ns.dinahosting.com ns2.dinahosting.com ns3.dinahosting.com ns4.dinahosting.com
Mail servers	mail.echaurren.com

```
ns.dinahosting.com
a 82.98.128.132
  whois PROVIDER Local Registry Dinahosting S.L.
  route 82.98.128.0/18
    bgp AS42612
  descr SP_DINA
  location Spain
  ptr ns.dinahosting.com
```

```
ns2.dinahosting.com
a 82.98.128.196
  whois PROVIDER Local Registry Dinahosting S.L.
  route 82.98.128.0/18
    bgp AS42612
  descr SP_DINA
  location Spain
  ptr ns2.dinahosting.com
```

```
ns3.dinahosting.com
a 72.29.96.10
  whois Dinahosting S.L. (C02269407)
  route 72.29.96.0/19
    bgp AS30496
  descr colo4 customer network
  location Spain
  ptr ns3.dinahosting.com
```

```
ns4.dinahosting.com
a 93.89.82.218
  whois Dinahosting UK
  route 93.89.80.0/20
    bgp AS39326
  descr Goscomb Technologies Limited
  location United Kingdom
  ptr ns4.dinahosting.com
```

```
mx mail.echaurren.com
a 82.98.160.13
  whois Dinahosting Subred 2J3
  route 82.98.128.0/18
    bgp AS42612
  descr SP_DINA
  location Spain
  ptr hl74.dinaser.com
    a 82.98.131.90
    82.98.160.13
```


TEAM CHALLENGE – INVESTIGACIÓN OSINT.

Herramienta Censys

Censys es una plataforma de búsqueda y análisis de dispositivos conectados a Internet. Permite a los usuarios explorar y obtener información detallada sobre servidores, dispositivos IoT y otros equipos conectados a la red. La plataforma recopila datos a través de escaneos activos de IPs y puertos, y organiza esta información para ofrecer un panorama de la infraestructura global de Internet.

Hosts

Results: 1 Time: 0.33s

 **82.98.178.143** (hl1023.dinaser.com)

 Debian Linux 9.0  DINAHOSTING-AS (42612)  Madrid, Spain

[database](#) [remote-access](#) [email](#) [file-sharing](#)

 21/FTP

 22/SSH

 25/SMTP

 80/HTTP

 143/IMAP

 443/HTTP

 587/SMTP

 993/IMAP

 995/POP3

 3306/MYSQL

Firma empresa Echaurren:

Firma empresa contratada: