

Desafío de Tripulaciones



Informe de Ciberseguridad

Equipo de Ciberseguridad:

- César de la Rosa Vila
- Rafael Otero
- Andreas Skrey
- Mario Creastao
- Ginner Baron
- Angel Carriel Velásquez
- Andrés García

ÍNDICE

1. Finalidad del documento	3
2. OSINT	4
2.1 Finalidad del informe:	4
2.2 Información del objetivo	4
2.2.1 Introducción:	4
2.2.2 Contacto y redes sociales.	4
2.3 Información administrativa	5
2.3.1 Datos fiscales.....	5
2.3.2 Datos comerciales.....	6
2.4 Información técnica	7
2.4.1 Direcciones IP:.....	10
2.4.2 Servidor:	11
2.5 Información corporativa	16
2.5.1 Equipo directivo	16
2.5.2 Personal de la empresa	16
2.6 Recomendaciones.....	16
3. Reglamento General de Protección de Datos (RGPD) y Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)	17
3.1 Introducción.....	17
3.2 Principios y Derechos del RGPD y LOPDGDD	17
3.3 Responsabilidades y Consideraciones Específicas	17
3.4 Privacidad desde el Diseño	18
3.5 Conclusión y Enfoque Centrado en el Sujeto de los Datos	19
4. SSDLC.....	20
4.1 Planificación del Concepto	20
4.2 Definición de Requisitos	20
4.3 Diseño Seguro.....	20
4.4 Desarrollo y Pruebas	21
4.5 Puesta en Marcha	21
4.6 Operaciones y Mantenimiento	21
4.7 Disposición	21
5. Dockerfile.....	23
6. Agentes maliciosos	27
6.1 definición	27
7. OWASP	28
7.1 Definición.....	28

7.2 Control de acceso vulnerado	28
7.3 Fallos criptográficos.....	29
7.4 Inyección	30
7.5 Diseño Inseguro	30
7.6 Configuración de Seguridad Incorrecta.....	32
7.7 Componentes Vulnerables y Desactualizados	32
7.8 Fallas de Identificación y Autenticación	33
7.9 Fallas en el Software y en la Integridad de los Datos	34
7.9 Fallas en el Registro y Monitoreo	35
7.10 Falsificación de Solicitudes del Lado del Servidor (SSRF).....	36
8. Phishing	38
8.1 Que es?.....	38
8.2 Prevención	38
9. Conclusión	40

1. Finalidad del documento

El propósito fundamental de este documento es establecer un marco integral de seguridad para el desarrollo y despliegue del proyecto, con el fin de asegurar la protección de la información y la funcionalidad de los sistemas involucrados. Se persigue alcanzar metas específicas, tales como entender el contexto funcional de la aplicación para identificar posibles vulnerabilidades, fortalecer los sistemas operativos y aplicativos necesarios, proponer una infraestructura escalable para el despliegue futuro y estudiar e implementar estrategias de backup.

Además, se busca aplicar la metodología del OWASP Top 10 para identificar y abordar posibles vulnerabilidades, analizar agentes maliciosos y vectores de ataque, evaluar la efectividad de los controles de seguridad propuestos durante la etapa de diseño y determinar el impacto técnico y de negocio de posibles vulnerabilidades.

El documento también destaca la importancia de ejecutar pruebas continuas con herramientas de código estático durante el desarrollo, con el objetivo de detectar malas prácticas y vulnerabilidades en cada entrega parcial. Al finalizar el desarrollo, se propone realizar una auditoría rápida con herramientas de pentesting para identificar problemas evidentes de seguridad sin entrar en detalles exhaustivos.

En conjunto, estas acciones tienen como finalidad garantizar un entorno seguro, minimizar riesgos y fortalecer la resiliencia del proyecto ante posibles amenazas cibernéticas.

2. OSINT

En una primera instancia realizamos un informe OSINT de la empresa a estudiar, SEVERAL ENERGY S.L. A continuación, expondremos la información hallada:

2.1 Finalidad del informe:

Estamos creando un documento sobre la empresa SEVERAL ENERGY S.L que se crea con el propósito de recopilar, analizar y presentar información relevante obtenida a través de fuentes de acceso público, como sitios web, redes sociales, bases de datos públicas y otras fuentes disponibles en línea.

2.2 Información del objetivo

2.2.1 Introducción:

En SEVERAL ENERGY S.L, ofrecen servicios de consultoría energética. Su objetivo es proporcionar soluciones personalizadas para optimizar el consumo de energía y reducir la huella ambiental de sus clientes.

Centran su atención en ofrecer soluciones a medida que permitan maximizar el ahorro en las facturas de luz y gas. Se comprometen a implementar medidas eficientes tanto en entornos domésticos como empresariales, con el objetivo de optimizar los recursos energéticos disponibles.

2.2.2 Contacto y redes sociales.

Utilizando la herramienta MR.Homles obtuvimos la siguiente información, la cual nos daba respuesta a las distintas redes sociales relacionadas con dicha empresa. Comprobamos las supuestas redes sociales obtenidas y no pudimos hacer matching con la empresa.

```

[N]CONNECTION-ERROR... TRYNG WITH NO PROXIES
[v]USERNAME severalenergy FOUND
[v]LINK: https://facebook.com/severalenergy
[I]TAGS:[Social,Chatting]

[+]TRYING ON: Disqus

[N]CONNECTION-ERROR... TRYNG WITH NO PROXIES
[!]USERNAME severalenergy NOT FOUND

[+]TRYING ON: Pinterest

[N]CONNECTION-ERROR... TRYNG WITH NO PROXIES
[v]USERNAME severalenergy FOUND
[v]LINK: https://pinterest.com/severalenergy
[I]TAGS:[Image,Social,Photo]

[+]TRYING ON: Passes

[N]CONNECTION-ERROR... TRYNG WITH NO PROXIES
[v]USERNAME severalenergy FOUND
[v]LINK: https://passes.com/severalenergy
[I]TAGS:[Image,Social,Photo]

```

LinkedIn: <https://www.linkedin.com/in/several-energy-787ab4263/>

InfoJobs: several energy → <https://www.infojobs.net/several-energy-sociedad-limitada./em-i98495456554548836986691023096225802243>

2.3 Información administrativa

2.3.1 Datos fiscales

Several Energy se estableció en España y se encarga de gestionar las operaciones y cuestiones comerciales relacionadas con la energía en el mercado español y, posiblemente, en otros mercados de habla hispana. Su función incluye actividades como la gestión de energía.

Ubicación:

[Dirección y teléfono de SEVERAL ENERGY SOCIEDAD LIMITADA.](#)

Domicilio social actual	CALLE JOSE LUIS PEREZ PUJADAS (ED FORUM), 14 Ver Mapa
Código Postal	18006
Municipio	GRANADA
Provincia	Granada

Información fiscal de la empresa:

Información de SEVERAL ENERGY SOCIEDAD LIMITADA.

Denominación	SEVERAL ENERGY SOCIEDAD LIMITADA.
CIF/NIF	B16870370
Número DUNS	4706... ?
Actividad Informa	Servicios prestados a las empresas ncop
CNAE	6399 - Otros servicios de información n.c.o.p.
SIC	7399 - Servicios comerciales SC
Objeto Social	Otros servicios de información. Otras actividades de apoyo a las empresas. Promoción inmobiliaria
Registro Mercantil	Registro Mercantil de Granada - 2 actos en BORME publicados
Actualización Ficha Empresa	16/10/2023
Última consulta empresa	08/01/2024
Consultas Empresa Total	71
Consultas Último Trimestre	11

2.3.2 Datos comerciales

Se puede observar que la empresa que estamos investigando se trata de una pequeña sociedad dado los datos encontrados.

Datos Comerciales de SEVERAL ENERGY SOCIEDAD LIMITADA.

[Estructura Corporativa](#)

Administrador Único [Disponible](#)

[Estructura Legal](#)

Forma Jurídica Sociedad limitada

Capital Social 3.000 €

Cotiza en Bolsa NO

[Último Acto BORME](#) 16/09/2021 Nombramientos

[Información Comercial](#)




Fecha Constitución 09/09/2021

Actividades Internacionales No constan

[Otra Información de Interés](#)

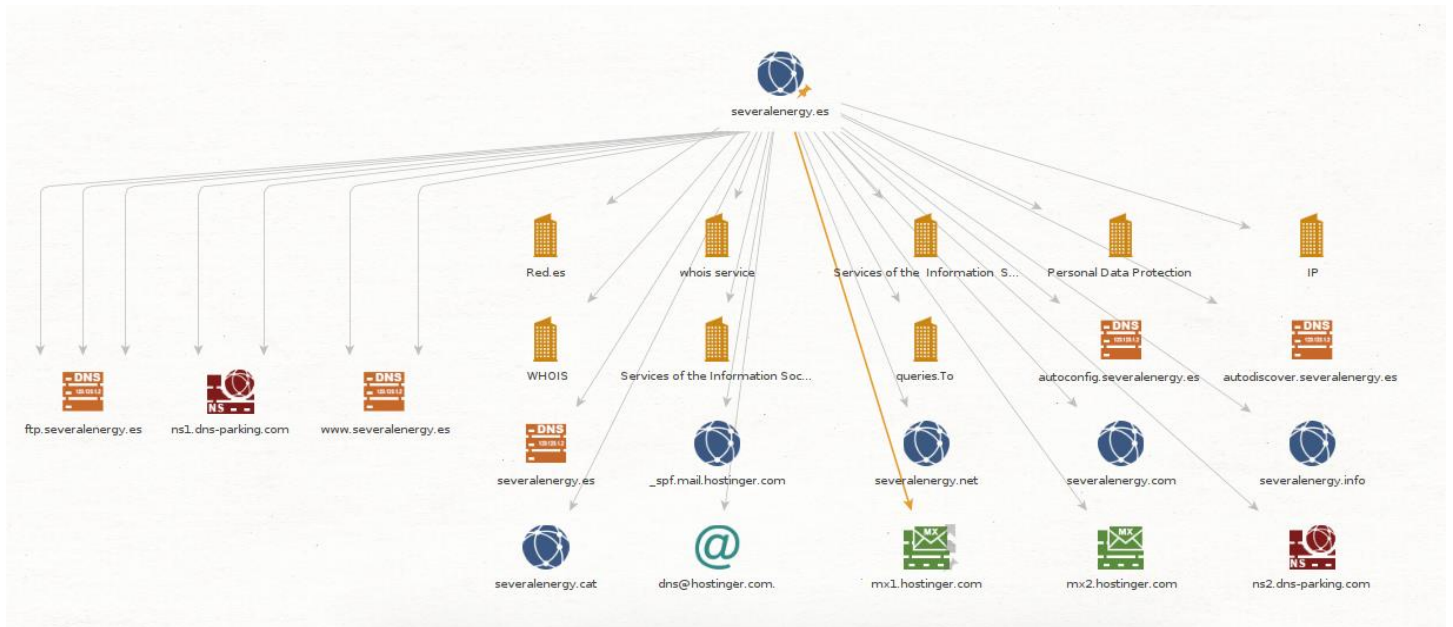
Fecha último dato 16/10/2023

En la siguiente imagen se muestran las posibles subvenciones a la empresa.

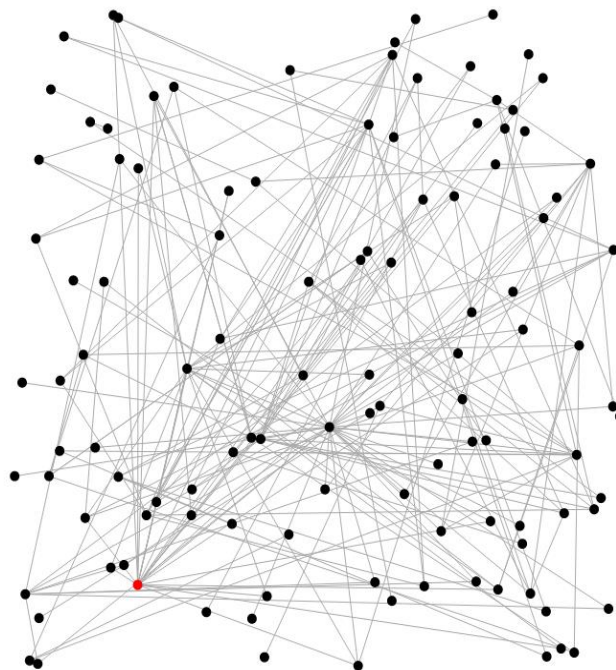
Posibles subvenciones para empresas similares a SEVERAL ENERGY SOCIEDAD LIMITADA.		
	Ayudas para programas de prevención de riesgos laborales.	Consultar
Categorías:	Formación, Prevención Riesgos Laborales, Asesorías, Auditorías y Consultorías Externas, Comercio	
Beneficiarios:	Asociaciones, Cooperativas y Sociedades Laborales no Agrarias, Entidades sin ánimo de lucro, Fundaciones, Organizaciones Empresariales y Sindicales	
Provincia:	Andalucía	
	Ayudas para la realización de actividades y proyectos de mejora en materia prevención...	Consultar
Categorías:	Prevención Riesgos Laborales, Asesorías, Auditorías y Consultorías Externas	
Beneficiarios:	Autónomos, Cooperativas y Sociedades Laborales no Agrarias, Microempresas (menos de 10 empleados), Pymes (menos de 250 empleados), Sociedades Civiles	
Provincia:	Andalucía	
	Subvenciones para la digitalización de las pymes.	Consultar
Categorías:	Equipamientos informáticos y Tecnología, Asesorías, Auditorías y Consultorías Externas	
Beneficiarios:	Autónomos, Cooperativas y Sociedades Laborales no Agrarias, Microempresas (menos de 10 empleados), Pymes (menos de 250 empleados), Sociedades Civiles	
Provincia:	Andalucía	

2.4 Información técnica

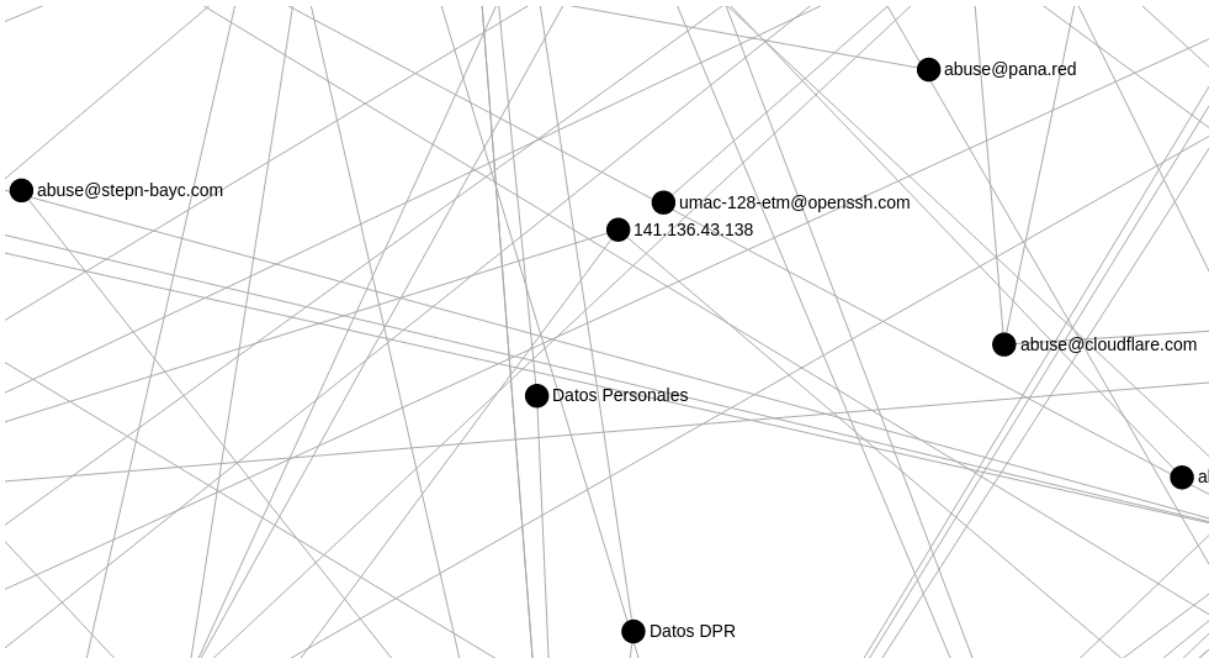
En este caso hemos utilizado Maltego para observar los diferentes sitios webs asociados a esta empresa, los diferentes DNS's y también podemos ver correos asociados a ella. Además de utilizar esta herramienta también probamos con otra la cual quizás es más intuitiva de usar.



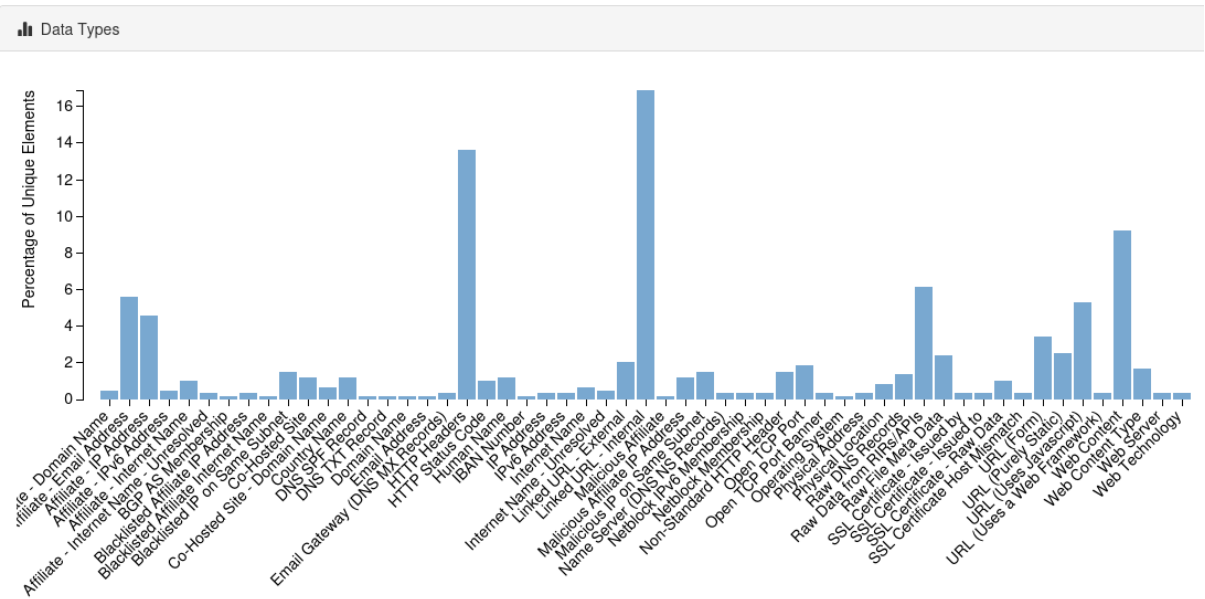
Utilizamos la herramienta SpiderFoot y pudimos obtener información similar a la anterior, se obtiene tanto un diagrama de barras como un diagrama en tres dimensiones; los cuales explicaremos a continuación:



En este último se observa la diferente información obtenida



Se pueden ver diferentes cuentas de emails e IP's asociados con la empresa. El diagrama de barras se ve de esta forma.



Las categorías que aparecen en la barra horizontal son las diferentes categorías obtenidas durante este proceso. Es de reseñar las diferentes IP's y emails asociados que se han hallado durante la búsqueda

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	3	8	2024-01-10 11:20:58
Affiliate - Email Address	33	64	2024-01-10 11:21:02
Affiliate - IP Address	27	29	2024-01-10 11:20:58
Affiliate - IPv6 Address	3	4	2024-01-10 10:31:42

Como resultado final se obtuvieron tres direcciones IP's relacionadas con la Sociedad.

Browse IP Address				
<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	141.136.43.154	severalenergy.es	sfp_dnsresolve	2024-01-10 10:09:49
<input type="checkbox"/>	141.136.43.154	www.severalenergy.es	sfp_dnsresolve	2024-01-10 11:04:45
<input type="checkbox"/>	153.92.2.19	autodiscover.severalenergy.es	sfp_dnsresolve	2024-01-10 11:05:25

2.4.1 Direcciones IP:

Con *dnsenum* confirmamos lo hallado con la anterior herramienta, obtuvimos las siguientes direcciones IPs.

```
dnsenum VERSION:1.2.6
severalenergy.es

Host's addresses:
severalenergy.es. 1784 IN A 141.136.43.154

Name Servers:
ns1.dns-parking.com. 14400 IN A 162.159.24.201
ns2.dns-parking.com. 14400 IN A 162.159.25.42

Mail (MX) Servers:
mx1.hostinger.com. 5 IN A 172.65.182.103
mx2.hostinger.com. 176 IN A 172.65.182.103

Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for severalenergy.es on ns1.dns-parking.com ...
AXFR record query failed: NOTIMP
Trying Zone Transfer for severalenergy.es on ns2.dns-parking.com ...
AXFR record query failed: NOTIMP
```

Con las IPs obtenidas utilizamos Shodan para realizar un análisis mayor ya que en esta página podemos observar los puertos que utilizan, donde se encuentra alojada la máquina y las tecnologías utilizadas para crear la página web.

141.136.43.154

Vista normal >_Datos sin procesar

Información general

Nombres de host	cpl90. hosting24.com hstgr.io
Dominios	HOSTING24.COM HSTGR.IO
País	Reino Unido
Ciudad	Manchester
Organización	Hostinger Internacional Limitada
ISP	Hostinger Internacional Limitada
ASN	AS47583

Tecnologías web

Alojamiento

Hostinger

Misceláneas

HTTP/3

Esta IP tiene los puertos 43 y 80 abiertos.

Open Ports

80 443

Al realizar el análisis no se han encontrado vulnerabilidades muy graves. Por ejemplo, en el puerto 443 al ser una conexión de manera predeterminada insegura la envía directamente al “*error 403 forbidden*”.

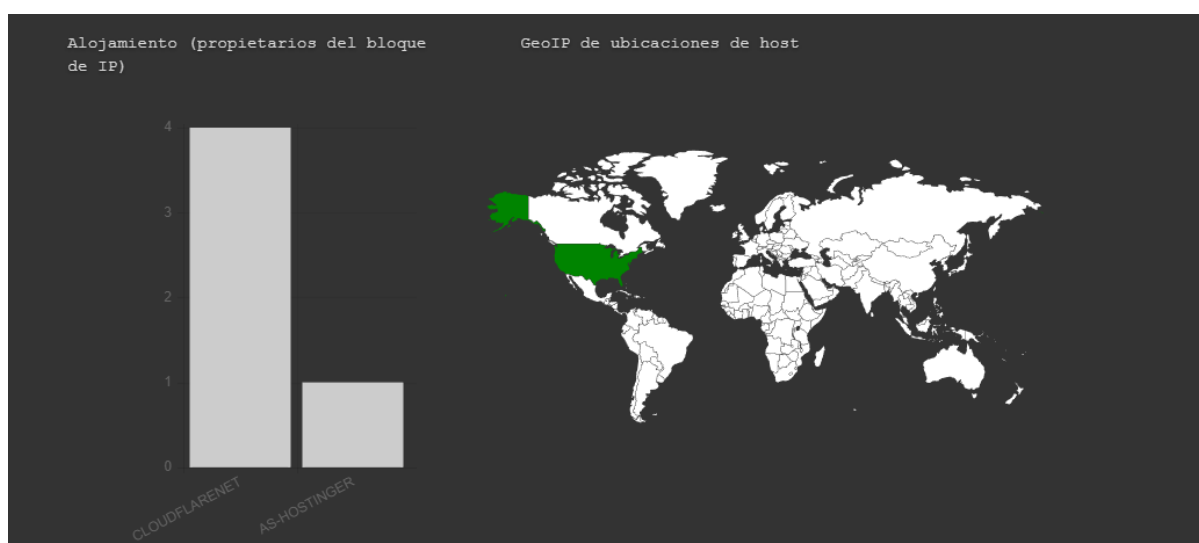
2.4.2 Servidor:

Los servidores que tiene Several Energy son los siguientes.

Name Servers:

ns1.dns-parking.com.	14400	IN	A	162.159.24.201
ns2.dns-parking.com.	14400	IN	A	162.159.25.42

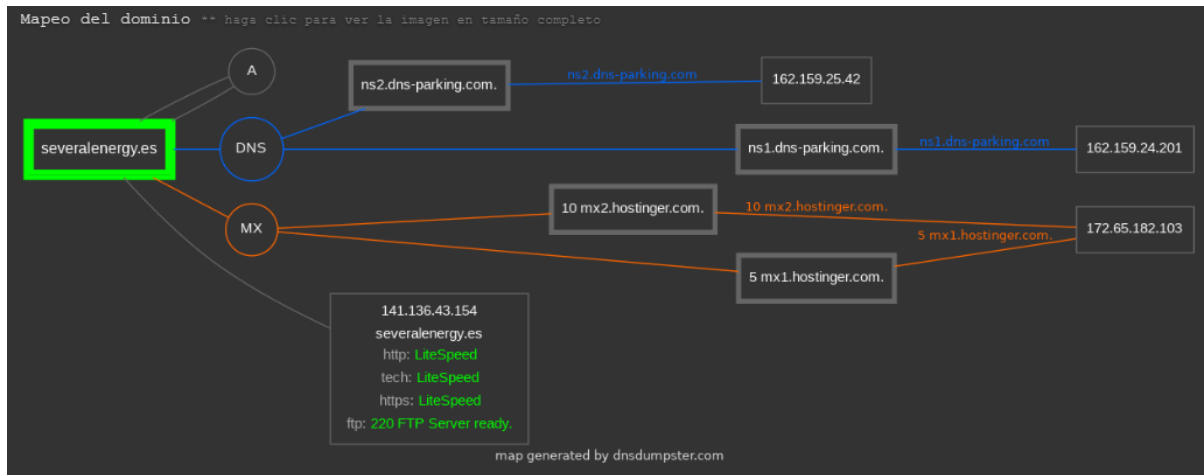
Con *DNS Dumpster* hemos conseguido ver dónde están localizados los servidores a nivel global, podemos observar que principalmente se encuentran en América, concretamente Estados Unidos.



Servidores DNS: Los servidores DNS sirven para convertir las solicitudes de nombres en direcciones IP, con lo que se controla a qué servidor se dirigirá un usuario final cuando escriba un nombre de dominio en su navegador web.

Servidores DNS		
ns2.dns-parking.com. 🌐 🔄 📡 📶 🟢	162.159.25.42 ns2.dns-parking.com	NUBEFLARENET desconocido
ns1.dns-parking.com. 🌐 🔄 📡 📶 🟢	162.159.24.201 ns1.dns-parking.com	NUBEFLARENET desconocido
Registros MX ** Aquí es donde va el correo electrónico del dominio...		
10mx2.hostinger.com. 🌐 🔄 📡 📶 🟢	172.65.182.103	CLOUDFLARENET Estados Unidos
5 mx1.hostinger.com. 🌐 🔄 📡 📶 🟢	172.65.182.103	CLOUDFLARENET Estados Unidos
Registros TXT ** Encuentre más hosts en las configuraciones del Marco de políticas del remitente (SPF)		
"v=spf1 incluye:_spf.mail.hostinger.com ~todos"		
Registros de host (A) ** Es posible que estos datos no estén actualizados ya que utiliza una base de datos estática (actualizada mensualmente)		
variasenergia.es 🌐 🔄 📡 📶 🟢 HTTP: LiteSpeed FTP: Servidor FTP 220 listo. TECNOLOGÍA HTTP: LiteSpeed	141.136.43.154 cpl90.hosting24.com	AS-HOSTINGER Reino Unido

El mapa del dominio permite utilizar varios dominios para una misma página web. Esto resulta muy útil cuando se utilizan sistemas de gestión de contenidos como WordPress ya que puedes estructurar múltiples dominios y subpáginas y conectarlos entre sí.



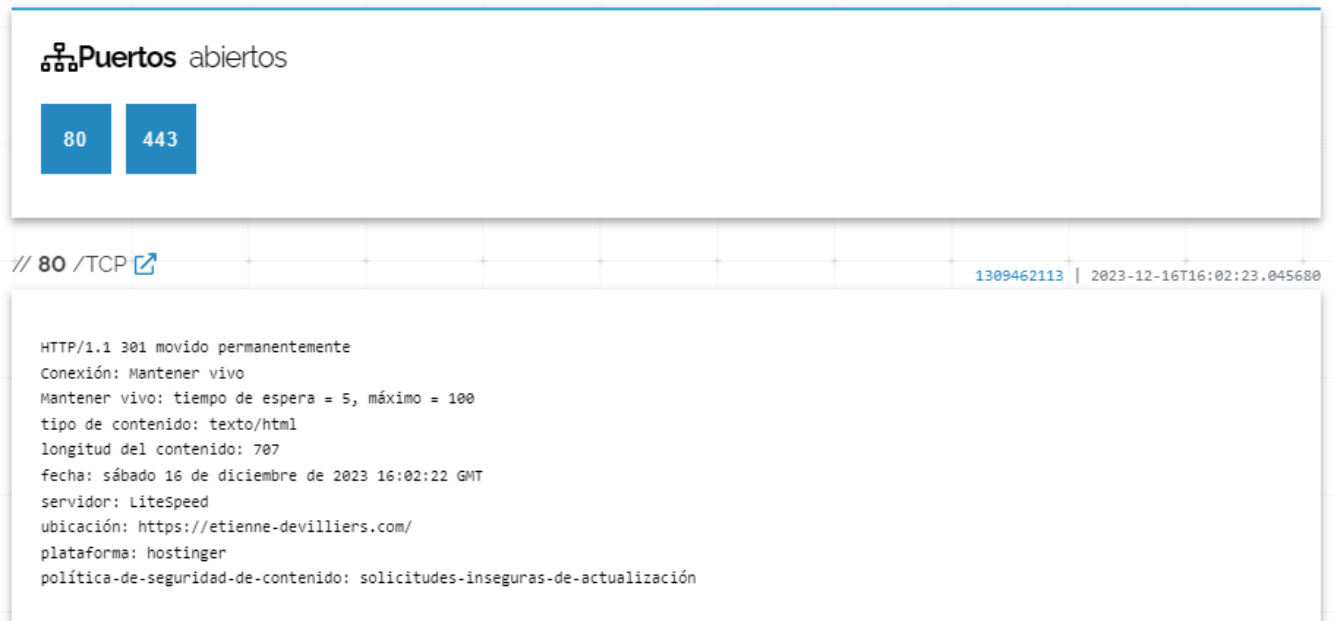
2.4.2.1 Máquina virtual:

Mediante MR.Homles hemos podido conseguir información sobre la máquina virtual de la empresa.

```
+ ]SEARCH INFORMATION FOR: severalenergy.es
v]IP: 141.136.43.154
v]NATION: United Kingdom
v]NATION-CODE: GB
v]REGION-CODE: ENG
v]REGION-NAME: England
v]CITY: Manchester
v]TIMEZONE: Europe/London
v]ISP: Hostinger International Limited
v]ORG: Hostinger International Limited
v]AS: AS47583 Hostinger International Limited
v]LAT: 53.4788
v]LONG: -2.2585
v]ZIP/POSTAL-CODE: M61
```

2.4.2.2 Servidor:

A continuación, buscaremos información de vulnerabilidades, información sobre los puertos que tiene abiertos e información más estricta sobre los servidores, por ejemplo saber dónde están alojadas las IP's, información sobre los certificados SSL y un largo etcétera.



Como ya hemos mencionado anteriormente dichos puertos se hallan abiertos, aunque los dos cuentan con requisitos de seguridad ante un posible ataque.

2.4.2.3 Tecnologías Utilizadas

Aquí podemos observar las tecnologías utilizadas para poder crear la web. Cada *widget* visto en la siguiente imagen ha sido utilizado para diferentes funcionalidades, como por ejemplo *Wordpress Plugins* el cual ha sido utilizado para obtener más herramientas funcionales, de esta manera tendrá más ventajas a la hora de crear la página web dado que le dará una funcionalidad extra.

Contact Form 7

[Contact Form 7 Usage Statistics](#) · [Download List of All Websites using Contact Form 7](#)

Specifically designed for wordpress blogs. Contact Form 7 can manage multiple contact forms, plus you can customize the form and the mail contents flexibly with simple markup.

Feedback Forms and Surveys

Lightspeed Cache

[Lightspeed Cache Usage Statistics](#) · [Download List of All Websites using Lightspeed Cache](#)

Wordpress performance cache.

WordPress Plugins

Google Font API

[Google Font API Usage Statistics](#) · [Download List of All Websites using Google Font API](#)

The Google Font API helps you add web fonts to any web page.

Fonts

Wordpress Plugins

[Wordpress Plugins Usage Statistics](#) · [Download List of All Websites using Wordpress Plugins](#)

Plugins are tools to extend the functionality of WordPress. The website uses various plugins from WordPress to provide additional functionality. Some of them may be listed here.

CrUX Dataset

[CrUX Dataset Usage Statistics](#) · [Download List of All Websites using CrUX Dataset](#)

CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.

CrUX Top 10m

[CrUX Top 10m Usage Statistics](#) · [Download List of All Websites using CrUX Top 10m](#)

Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 10 million.

2.5 Información corporativa

2.5.1 Equipo directivo

Ejecutivo de ventas: Julio Redondo Vicente

Ejecutivo de ventas: Inmaculada Serichol Lopez

Directora de proyectos: Yuleyxi Vallejo Tarira

Directora de proyecto: Natalia Juarez

Director de proyecto: Aitor Ortiz

Director comercial: Rafael Machin Torres

2.5.2 Personal de la empresa

Delegado de zona: Isael Cadenas Alvarez

Asesor Energetico: Oscar Gomez

Administrativo Energético: Miguel Angel Alava

Auxiliar administrativo: Celia Navarro Herrera

2.6 Recomendaciones

En rasgos generales no existen vulnerabilidades reseñables vistas, es cierto que al ser una microempresa la opción de búsqueda se reduce a poco y por tanto las posibles brechas de seguridad son menores.

Durante la realización del informe se percibió un fallo en la transferencia de zona lo cual es positivo ya que manifiesta una buena seguridad por parte de la empresa.

De manera general nuestras recomendaciones se centran en salvaguardar la integridad de la empresa contra posibles ciberamenazas, y por ende es crucial adoptar medidas como la capacitación contra phishing, el uso de comunicaciones seguras con VPN, máquinas virtuales actualizadas, contratación de expertos en ciberseguridad, mantenimiento constante de software y aplicando firewalls para proteger contra accesos no autorizados. Estas acciones fortalecen la seguridad de la empresa de manera integral.

3. Reglamento General de Protección de Datos (RGPD) y Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)

3.1 Introducción

El Reglamento General de Protección de Datos (RGPD), promulgado en 2018, constituye el marco legal que regula la protección de datos en todos los Estados miembros de la Unión Europea. En España, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) se erige como la normativa nacional que incorpora y adapta las directrices del RGPD. Este conjunto normativo tiene como objetivo salvaguardar la privacidad y los derechos digitales de los ciudadanos, estableciendo principios y directrices para el manejo ético de la información personal.

3.2 Principios y Derechos del RGPD y LOPDGDD

El RGPD y la LOPDGDD delinear principios fundamentales que las entidades deben observar al tratar datos personales. Estos principios incluyen la lealtad con el interesado, que garantiza que el tratamiento de datos sea transparente, legal y no fraudulento. Asimismo, se destaca la importancia de la transparencia, que exige que toda información relativa al tratamiento de datos sea fácilmente accesible y comprensible, utilizando un lenguaje claro y sencillo. La legitimación del tratamiento, la limitación de la finalidad, la minimización, el principio de exactitud y la integridad y confidencialidad son aspectos cruciales para asegurar el tratamiento ético de los datos personales. Estos datos comprenden cualquier información que permita identificar a una persona, como nombres, direcciones, teléfonos, datos sanitarios y financieros. El consentimiento informado, prestado de forma libre, revocable y con un lenguaje claro, es esencial para el tratamiento de datos.

3.3 Responsabilidades y Consideraciones Específicas

La integridad y confidencialidad de los datos son fundamentales, imponiendo medidas de seguridad adecuadas para protegerlos contra el tratamiento no autorizado, ilícito o cualquier pérdida, destrucción o daño accidental. La responsabilidad proactiva, reflejada en el término en inglés "accountability," implica que los responsables del tratamiento deben no solo cumplir con los principios mencionados, sino también ser

capaces de demostrar de manera efectiva su conformidad con estos requisitos normativos.

La LOPDGDD añade ciertas obligaciones específicas, como el registro de actividades de tratamiento de datos, que se aplica cuando se trata de datos sensibles o cuando la entidad tiene más de 250 empleados. También introduce el concepto de bloqueo de datos, un paso previo a la eliminación que impide el uso de los datos con cualquier fin, excepto para ponerlos a disposición judicial. Además, establece la necesidad de designar un Delegado de Protección de Datos (DPO) en ciertas organizaciones. El DPO tiene la responsabilidad de supervisar y monitorizar de forma independiente y confidencial el cumplimiento normativo en materia de protección de datos. A pesar de su función de monitoreo, la empresa sigue siendo la responsable final de cumplir con las leyes de protección de datos.

La designación de un DPO se aplica a organismos públicos, organizaciones que manejan datos especialmente sensibles (como datos de salud o afiliación política) y aquellas que tratan grandes volúmenes de datos personales de manera habitual, como aseguradoras, medios de comunicación o entidades bancarias.

3.4 Privacidad desde el Diseño

La privacidad desde el diseño se erige como un principio crucial para garantizar la protección integral de la información personal. Este enfoque implica adoptar una perspectiva orientada a la gestión del riesgo y a la responsabilidad proactiva para establecer estrategias que incorporen medidas de privacidad en cada fase del ciclo de vida de los datos. Los principios fundacionales de la privacidad desde el diseño incluyen la proactividad en lugar de la reactividad, el carácter preventivo en lugar del correctivo, la configuración predeterminada de la privacidad, la integración de la privacidad desde la fase de diseño, el enfoque en la funcionalidad total, el aseguramiento de la privacidad en todo el ciclo de vida y la transparencia en todas las prácticas relacionadas con el tratamiento de datos.

3.5 Conclusión y Enfoque Centrado en el Sujeto de los Datos

En conclusión, la implementación efectiva del RGPD y la LOPDGDD exige un compromiso integral con los principios y directrices establecidos. La transparencia, la integridad, la confidencialidad y la responsabilidad proactiva son esenciales para construir una cultura de privacidad robusta. La seguridad de la información, la designación de un DPO cuando sea necesario y la privacidad desde el diseño son pilares clave para construir una cultura de privacidad robusta. La seguridad de la información, la designación de un DPO cuando sea necesario y la privacidad desde el diseño son pilares clave para garantizar la conformidad con las leyes de protección de datos. Un enfoque centrado en el sujeto de los datos, que otorga a los usuarios un papel activo en la gestión y control de sus propios datos, refuerza aún más la protección de la privacidad en el entorno digital.

4. SSDLC

La implementación efectiva de prácticas y recursos en cada fase del SSDLC (Evaluación Integral del Ciclo de Vida del Desarrollo de Software y Seguridad) es esencial para garantizar que el diseño del proyecto siga las mejores prácticas de seguridad. A continuación, se presenta un desglose de cada fase con sus respectivas buenas prácticas y recursos clave.

4.1 Planificación del Concepto

En esta fase inicial, se recomienda realizar un análisis de riesgos, definir objetivos de seguridad y establecer un plan de seguridad. Los recursos clave incluyen análisis de riesgos, documentos de objetivos de seguridad y planes de seguridad. Además, se hace referencia a marcos reconocidos como el Marco de Ciberseguridad de NIST y la norma ISO/IEC 27001 para proporcionar orientación.

4.2 Definición de Requisitos

En esta etapa, es crucial identificar y documentar requisitos de seguridad, realizar evaluaciones de riesgos y incorporar requisitos de privacidad y cumplimiento normativo. Documentos de requisitos de seguridad, evaluaciones de riesgos y documentación de cumplimiento normativo son recursos fundamentales. Estándares como el Estándar de Verificación de Seguridad de Aplicaciones de OWASP y los Criterios Comunes refuerzan esta fase.

4.3 Diseño Seguro

La fase de diseño destaca la implementación de controles de seguridad, la aplicación de principios de seguridad y la utilización de la separación de privilegios. Documentos de diseño seguro, herramientas de modelado de amenazas y principios de seguridad aplicados al diseño son recursos clave. Referencias a recursos como la Hoja de Trucos de Arquitectura de Seguridad de Aplicaciones de OWASP y el Ciclo de Vida de Desarrollo Seguro de Microsoft enriquecen las prácticas de diseño seguro.

4.4 Desarrollo y Pruebas

Durante esta fase, se enfatizan prácticas como la incorporación de pruebas de seguridad en todas las etapas, el uso de análisis estático y dinámico de código, y la realización de pruebas de penetración. Herramientas esenciales como análisis estático y dinámico de código, marcos de pruebas de seguridad, y herramientas específicas como OWASP Testing Guide y OWASP ZAP son recursos valiosos para garantizar la detección temprana de vulnerabilidades.

4.5 Puesta en Marcha

Las buenas prácticas en esta etapa incluyen realizar pruebas finales antes del despliegue, configurar entornos de producción de manera segura e implementar la gestión de identidades y accesos. Documentos de pruebas finales, configuraciones seguras y la implementación de la gestión de identidades y accesos son recursos cruciales. Pautas como CIS Benchmarks y NIST SP 800-53 son referencias clave para asegurar un inicio seguro.

4.6 Operaciones y Mantenimiento

En esta fase, se recomienda establecer un proceso de monitorización continua de la seguridad, implementar parches y actualizaciones de seguridad regularmente, y realizar evaluaciones periódicas de riesgos. Herramientas de monitorización, procedimientos de actualización e informes de evaluaciones de riesgos son recursos esenciales. Referencias a herramientas como Security Onion y la National Vulnerability Database fortalecen la seguridad a lo largo del tiempo.

4.7 Disposición

Finalmente, en la fase de disposición, se destacan prácticas para planificar la disposición segura de datos y sistemas, eliminar datos de manera segura y cerrar cuentas y accesos. Planes de disposición, procedimientos de eliminación segura de datos y documentación de cierre de cuentas y accesos son recursos críticos. Referencias a pautas como el NIST SP 800-88 y la Hoja de Trucos de Desactivación de Aplicaciones de OWASP aseguran un enfoque seguro para la eliminación de datos y aplicaciones.

En resumen, el SSDLC es un marco integral que garantiza la integración de prácticas de seguridad en todas las fases del desarrollo de software. Comienza con la Planificación del Concepto, abordando el análisis de riesgos y estableciendo un plan de seguridad respaldado por estándares como el Marco de Ciberseguridad de NIST y la norma ISO/IEC 27001. A lo largo de las fases de Definición de Requisitos, Diseño Seguro, Desarrollo y Pruebas, Puesta en Marcha, Operaciones y Mantenimiento, y Disposición, se aplican buenas prácticas respaldadas por herramientas y estándares reconocidos para asegurar la seguridad continua en el ciclo de vida del software, desde la concepción hasta la eliminación segura de datos y sistemas.

5. Dockerfile

Para realizar la securización de la imagen emplearemos de base el sistema operativo “Alpine” el cual está de base más securizado que otros sistemas Linux.

Las primeras modificaciones y añadidos que le haremos a está, será asegurarnos de que la instalación salga de manera exitosa y que emplee repositorios con HTTPS para mayor seguridad.

```
FROM alpine
# Generación de fallos comunes para facilitar el debugeo del código con una tubería como prevención
SHELL ["/bin/sh", "-o", "pipefail", "-c"]
# Empleamos repositorios HTTPS para apk
RUN echo "https://alpine.global.ssl.fastly.net/alpine/v3.12.0/main" > /etc/apk/repositories \
    && echo "https://alpine.global.ssl.fastly.net/alpine/v3.12.0/community" >> /etc/apk/repositories
```

Crearemos las variables de entorno que utilizaremos más adelante para la creación del usuario, el home...

```
# Creamos un usuario por defecto
ENV APP_USER=app
# Creamos su directorio principal
ENV APP_DIR="/$APP_USER"
# Donde se almacenarán los datos
ENV DATA_DIR "$APP_DIR/data"
# Donde se almacenará la configuración
ENV CONF_DIR "$APP_DIR/conf"
```

Añadimos los certificados especificando que no se almacenen en caché, los cuales utilizaremos para el repositorio.

Además, realizaremos una actualización del sistema y la instalación de la herramienta necesaria para levantar el servidor, “npm”.

```
# Añadimos los certificados HTTPS que empleará para establecer las conexiones seguras
RUN apk add --no-cache ca-certificates
# Realizamos una actualización y añadimos el paquete npm
RUN apk update && apk upgrade
RUN apk add npm
```

Haremos la creación del usuario y eliminaremos cualquier registro de los “crontabs”.


```
# Creamos el usuario por defecto y su directorio
RUN adduser -s /bin/true -u 1000 -D -h $APP_DIR $APP_USER \
  && mkdir "$DATA_DIR" "$CONF_DIR" \
  && chown -R "$APP_USER" "$APP_DIR" "$CONF_DIR" \
  && chmod 700 "$APP_DIR" "$DATA_DIR" "$CONF_DIR"

# Si existen crontabs los eliminamos
RUN rm -fr /var/spool/cron \
  && rm -fr /etc/crontabs \
  && rm -fr /etc/periodic
```

Eliminamos comandos y permisos que pueden utilizarse para vulnerar la seguridad de nuestro sistema.

```
# Eliminamos varios comandos de admin
RUN find /sbin /usr/sbin \
  ! -type d -a ! -name apk -a ! -name ln \
  -delete

# Suprimimos los permisos de lectura-escritura excepto /tmp/
RUN find / -xdev -type d -perm +0002 -exec chmod o-w {} + \
  && find / -xdev -type f -perm +0002 -exec chmod o-w {} + \
  && chmod 777 /tmp/ \
  && chown $APP_USER:root /tmp/
```

Quitamos las cuentas por defecto que se crean y son innecesarias y retiramos la shell interactiva.

```
# Nos deshacemos todas las cuentas innecesarias menos app y root
RUN sed -i -r "^($APP_USER|root|nobody)/!d" /etc/group \
  && sed -i -r "^($APP_USER|root|nobody)/!d" /etc/passwd

# Quitamos la shell interactiva para todos
RUN sed -i -r 's#^(.):[^\:]*$#\1:/sbin/nologin#' /etc/passwd
```

Borramos archivos peligrosos y asignamos los permisos de los directorios del sistema a root.

```
# Borramos temp shadow, passwd, group
RUN find /bin /etc /lib /sbin /usr -xdev -type f -regex '.*-$' -exec rm -f {} +

# Nos aseguramos que los directorios del sistema son de root y no tiene permiso de escritura ninguno más
RUN find /bin /etc /lib /sbin /usr -xdev -type d \
  -exec chown root:root {} \; \
  -exec chmod 0755 {} \;
```

Borramos archivos suid, sgid y comandos que pueden ser peligrosos si un atacante decide penetrar en la máquina y buscar la elevación de privilegios para hacerse con el control total de ella.

```
# Eliminamos los archivos suid y sgid
RUN find /bin /etc /lib /sbin /usr -xdev -type f -a \( -perm +4000 -o -perm +2000 \) -delete

# Quitamos comandos que podrían ser peligrosos
RUN find /bin /etc /lib /sbin /usr -xdev \( \
  -iname hexdump -o \
  -iname chgrp -o \
  -iname ln -o \
  -iname od -o \
  -iname strings -o \
  -iname su -o \
  -iname sudo \
  \) -delete
```

Eliminamos scripts de inicio y configuraciones relacionadas con el kernel para evitar su explotación.

```
# Borramos los scripts de inicio
RUN rm -fr /etc/init.d /lib/rc /etc/conf.d /etc/inittab /etc/runlevels /etc/rc.conf /etc/logrotate.d

# Eliminamos configuraciones relacionadas con el kernel para aportar mayor seguridad
RUN rm -fr /etc/sysctl* /etc/modprobe.d /etc/modules /etc/mdev.conf /etc/acpi
```

Suprimimos la carpeta de root, el fstab y los posibles enlaces simbólicos que se hayan creado con el resto de modificaciones y añadidos con tal de no dejar ningún registro.

```
# Suprimimos el directorio de root
RUN rm -fr /root

# Quitamos fstab
RUN rm -f /etc/fstab

# Eliminamos enlaces simbólicos previos
RUN find /bin /etc /lib /sbin /usr -xdev -type l -exec test ! -e {} \; -delete
```

Por último, además de establecer por defecto el directorio del usuario nuevo, realizaremos la ejecución del script de post instalación.

```
# Damos permisos al scrip de post instalación
COPY post-install.sh $APP_DIR/
RUN chmod 500 $APP_DIR/post-install.sh

# Especificamos que el directorio por defecto sea /app
WORKDIR $APP_DIR
```

En el script empezamos especificando que acabe si ocurre algún error por motivos de seguridad.

```
#!/usr/bin/env sh

# Si algún comando falla, la instalación falla
set -e
set -o pipefail
```

Borramos el administrador de paquetes apk y cambiamos los permisos de los directorios.

```
# Eliminamos el administrador de paquetes apk
find / -type f -iname '*apk*' -xdev -delete
find / -type d -iname '*apk*' -print0 -xdev | xargs -0 rm -r --

# Indicamos permisos rx a todos los directorios, excepto a data
find "$APP_DIR" -type d -exec chmod 500 {} +
```

Ponemos que los archivos sean de lectura y ajustamos los permisos de los usuarios.

```
# Indicamos permiso r a los archivos
find "$APP_DIR" -type f -exec chmod 400 {} +
chmod -R u=rwx "$DATA_DIR/"

# Cambiamos los permisos para app
chown $APP_USER:$APP_USER -R $APP_DIR $DATA_DIR
```

Terminamos de modificar los permisos y por último, borramos este archivo.

```
# Eliminamos los permisos
find / \( -type f -o -type l \) -iname 'chown' -xdev -delete

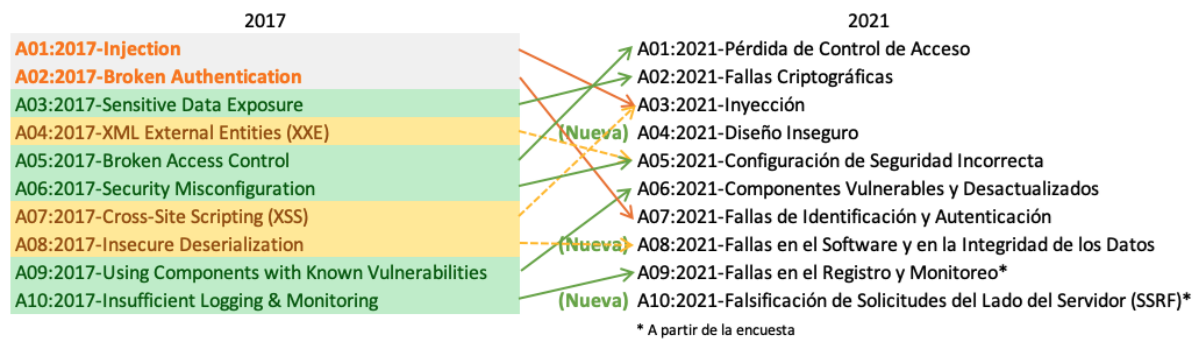
# Borramos este archivo
rm "$0"
```

6. Agentes maliciosos

6.1 definición

- Grupos o individuos con motivaciones políticas, sociales o ambientales que buscan interrumpir las operaciones de la empresa como una forma de protesta o para promover sus agendas.
- Hackers Individuos con habilidades técnicas avanzadas que pueden buscar vulnerabilidades en los sistemas de la empresa para acceder, manipular o robar información confidencial.
- Malware Software malicioso diseñado para dañar o infiltrarse en sistemas informáticos. Puede ser distribuido a través de correos electrónicos, sitios web comprometidos u otros medios.
- No son agentes maliciosos en sí mismos, las fallas técnicas y los desastres naturales pueden tener un impacto significativo en la infraestructura eléctrica. Sin embargo, los agentes maliciosos podrían intentar aprovecharse de situaciones de crisis.
- Cualquier trabajador no contento con la empresa

7. OWASP



7.1 Definición

El OWASP Top 10 es un informe que se actualiza con regularidad y en el que se exponen los problemas de seguridad de las aplicaciones web, centrándose en los 10 riesgos más importantes. El informe lo elabora un equipo de expertos en seguridad de todo el mundo. El OWASP hace referencia al Top 10 como un "documento de concienciación", y recomienda que todas las empresas incorporen el informe a sus procesos para minimizar o mitigar los riesgos de seguridad.

7.2 Control de acceso vulnerado.

Se refiere a la configuración con el fin de que los usuarios no puedan realizar acciones más allá de los permisos previstos.

La vulneración de estos puede provocar que se divulgue información no autorizada y/o modificación de datos.

Las formas más comunes son:

- Acceder a la API sin controles de acceso para POST, PUT y DELETE.
- Se vulnera el principio de mínimo privilegio, donde los permisos deberían concederse solo a usuarios o roles particulares.
- Permitir editar la cuenta de otra persona / usuario únicamente con su identificador único.
- Elevación de privilegios, realizar un escalado de privilegios o actuar como administrador pese a no contar con ese permiso.

¿Cómo prevenir?

- El control de acceso sólo es efectivo en código del lado del servidor de confianza o API sin servidor, donde el atacante no puede modificar la comprobación de control de acceso.
- Excepto para los recursos públicos, denegar por defecto.
- Limitar el acceso a la API y al controlador para minimizar el daño de las herramientas de ataque automatizadas.
- Implementar mecanismos de control de acceso.
- Los controles de acceso del modelo deben imponer la propiedad de los registros en lugar de aceptar que el usuario pueda crear, leer, actualizar o eliminar cualquier registro.
- Deshabilite el listado de directorios del servidor web y asegúrese de que los metadatos de archivos (por ejemplo, .git) y los archivos de copia de seguridad no están presentes en las raíces web.
- Registrar los fallos de control de acceso, alertando a los administradores.

7.3 Fallos criptográficos.

En un primer lugar hay que determinar las necesidades de protección de los datos que se van a almacenar,

Todo aquel dato que permitan identificar directa o indirectamente a las personas debe ser protegido adecuadamente según la RGPD.

Para toda esta información que debe ser protegida es necesario discernir que tipo de cifrado tiene implementado, si el certificado del servidor está correctamente validado, y si las contraseñas son encriptadas utilizando algoritmos seguros.

¿Cómo prevenir?

- Siempre cifrar los datos confidenciales en reposo.
- Asegurarse de que los algoritmos son sólidos
- Es recomendable cifrar todos los datos en tránsito con protocolos seguros TLS.
- Almacenar todas las contraseñas utilizando funciones hash fuertes.
- Evitar utilizar funciones criptográficas obsoletas como puede ser MD5 o SHA1.

7.4 Inyección

Una aplicación es vulnerable a un ataque por inyección cuando:

- Los datos proporcionados por el usuario no son validados, filtrados o “sanitizados” por la aplicación.
- Se utilizan datos dañinos dentro de los parámetros de búsqueda en consultas Object-Relational Mapping, para extraer registros adicionales sensibles.
- Se utilizan consultas dinámicas o llamadas no parametrizadas directamente en el intérprete.

¿Cómo prevenir?

- La revisión del código fuente es el mejor método para detectar si las aplicaciones son vulnerables a las inyecciones. Se recomienda encarecidamente realizar pruebas automatizadas de todos los parámetros, cabeceras, URL, cookies, JSON, SOAP y entradas de datos XML.
- Utilizar un API segura que evite el uso del intérprete SQL.
- Utilizar LIMIT y otros controles SQL dentro de las consultas para evitar la fuga masiva de registros en caso de inyección SQL.

7.5 Diseño Inseguro

El diseño inseguro es una categoría amplia que representa diferentes debilidades.

Un diseño seguro puede tener defectos de implementación que provoquen vulnerabilidades que puedan ser explotadas.

Nos encontramos 3 principales categorías:

1. Gestión de requerimientos y recursos

Es preciso recopilar los requerimientos para la aplicación con el negocio, incluidos los requisitos de protección relacionados con la confidencialidad, integridad, disponibilidad y autenticidad de todos los activos de datos y la lógica de negocio esperada.

Hay que analizar qué tan expuesta estará la aplicación y si se necesita separar funcionalidades (además del control de acceso).

Hay que recopilar los requerimientos técnicos, incluidos los funcionales de seguridad y los no funcionales. Establecer un presupuesto que cubra el diseño, construcción, prueba y operación.

2. Diseño seguro

El diseño seguro se trata de una metodología que evalúa constantemente las amenazas y garantiza que el código esté diseñado y probado de manera sólida para prevenir métodos de ataque conocidos. El modelado de amenazas debe estar integrado en sesiones de refinamiento (o actividades similares); buscar cambios en los flujos de datos y el control de acceso u otros controles de seguridad.

3. Ciclo de Desarrollo Seguro (S-SDLC)

El software seguro requiere un ciclo de desarrollo seguro, alguna forma de patrón de diseño seguro, metodologías de “pave road”, bibliotecas de componentes seguros, herramientas y modelado de amenazas.

¿Cómo prevenir?

- Limitar el consumo de recursos por usuario o servicio.
- Utilice el modelado de amenazas para flujos críticos de autenticación, control de acceso, lógica de negocio y todo clave.
- Establezca y use un ciclo de desarrollo seguro apoyado en Profesionales en Seguridad de -Aplicaciones para evaluar y diseñar la seguridad y controles relacionados con la privacidad.
- Escribir pruebas unitarias y de integración para validar que todos los flujos críticos son resistentes al modelo de amenazas. Recopilar casos de uso y casos de mal uso para cada capa de la aplicación.

7.6 Configuración de Seguridad Incorrecta

Una aplicación es vulnerable si:

- Se habilitan o instalan funciones innecesarias (por ejemplo, puertos, servicios, páginas, cuentas o privilegios innecesarios).
- Las cuentas predeterminadas y sus contraseñas siguen habilitadas y sin cambios.
- En los sistemas actualizados, las últimas funciones de seguridad están desactivadas o no están configuradas de forma segura.
- El servidor no envía cabeceras o directivas de seguridad, o no están configuradas con valores seguros.
- El software está obsoleto o es vulnerable
- La gestión de errores revela a los usuarios trazas de pila u otros mensajes de error demasiado informativos

¿Cómo prevenir?

- Una plataforma mínima sin características, componentes, documentación y muestras innecesarias. Eliminar o no instalar características y frameworks no utilizados.
- Un proceso automatizado para verificar la eficacia de las configuraciones y ajustes en todos los entornos.
- Un proceso de hardening repetible hace que sea rápido y fácil desplegar otro entorno que esté adecuadamente bloqueado.

7.7 Componentes Vulnerables y Desactualizados

Son vulnerables

- Si no conoce las versiones de todos los componentes que utiliza.
- Si el software es vulnerable, carece de soporte o no está actualizado.
- Si no analizas en búsqueda de vulnerabilidades de manera regular.

- Si no repara o actualiza la plataforma subyacente, frameworks y dependencias de manera oportuna y basada en el riesgo.
- Si los desarrolladores de software no testean la compatibilidad de las bibliotecas actualizadas, actualizadas o parcheadas.
- Si no asegura las configuraciones de los componentes

¿Cómo prevenir?

- Eliminar las dependencias que no son utilizadas, funcionalidades, componentes, archivos y documentación innecesarios.
- Realizar un inventario continuo de las versiones de los componentes en el cliente y en el servidor y sus dependencias. Supervisar continuamente fuentes como Common Vulnerability and Exposures (CVE) y National Vulnerability Database (NVD) para detectar vulnerabilidades en los componentes.
- Obtener componentes de fuentes oficiales a través de enlaces seguros.
- Supervisar las bibliotecas y los componentes que no sea mantenidos o no generen parches de seguridad para versiones anteriores.

7.8 Fallas de Identificación y Autenticación

Pueden encontrarse debilidades de autenticación si la aplicación:

- Permite ataques de fuerza bruta u otros ataques automatizados.
- Permite ataques automatizados como la reutilización de credenciales conocidas.
- Permite contraseñas por defecto, débiles o bien conocidas.
- Posee procesos débiles o no efectivos para las funcionalidades de olvido de contraseña o recuperación de credenciales.
- Almacena las contraseñas en texto claro, cifradas o utilizando funciones de hash débiles.
- No posee una autenticación multi-factor o la implementada es ineficaz.
- Reutiliza el identificador de sesión después de iniciar sesión.

¿Cómo prevenir?

- Implementar la autenticación multi-factor para evitar ataques automatizados.
- No incluir credenciales por defecto.
- Control de contraseñas débiles para comprobar que al menos no este en la lista de las 10000 peores.
- Limite o incremente el tiempo de espera entre intentos fallidos de inicio de sesión.
- Utilice un gestor de sesión en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio con alta entropía después de iniciar sesión.

7.9 Fallas en el Software y en la Integridad de los Datos

Los fallos de integridad del software y de los datos están relacionados con código e infraestructura no protegidos contra alteraciones.

- Un pipeline CI/CD inseguro puede conducir a accesos no autorizados, la inclusión de código malicioso o el compromiso del sistema en general. Además, es común en la actualidad que las aplicaciones implementen funcionalidades de actualización, a través de las cuales se descargan nuevas versiones de la misma sin las debidas verificaciones integridad que fueron realizadas previamente al instalar la aplicación.
- Los atacantes potencialmente pueden cargar sus propias actualizaciones para que sean distribuidas y ejecutadas en todas las instalaciones.

¿Cómo prevenir?

- Asegurarnos de que las bibliotecas y dependencias, tales como npm o maven son utilizadas desde repositorios confiables.
- Utilizar firmas digitales o mecanismos similares para verificar que el software o datos provienen efectivamente de la fuente esperada y no fueron alterados.
- Utilizar un proceso de revisión de cambios de código y configuraciones para minimizar las posibilidades de que código malicioso sea introducidos en su pipeline.

- El pipeline CI/CD posee adecuados controles de acceso, segregación y configuraciones.
- Los datos sin cifrar o firmar no son enviados a clientes no confiables.

7.9 Fallas en el Registro y Monitoreo

El registro y monitoreo pueden ser desafiantes para ser testeados, implicando entrevistas sobre si los ataques fueron detectados durante las pruebas de penetración.

No hay muchos datos de CVE/CVSS aun así, puede tener un gran impacto para la auditabilidad, visibilidad, alertas de incidentes y análisis forense.

Registros, detecciones, monitoreo y respuesta activas insuficientes pueden ocurrir en cualquier momento:

- Eventos auditables.
- Advertencias y errores generan registros poco claros, inadecuados y en algunos casos ni se generan.
- Registros en aplicaciones y API no son monitoreados para detectar actividades sospechosas.
- Los umbrales de alerta y procesos de escalamiento no están correctamente implementados o no son efectivos.
- Las pruebas de penetración y los escaneos utilizando herramientas de pruebas dinámicas de seguridad en aplicaciones (como ser OWASP ZAP) no generan alertas.
- Las aplicaciones no logran detectar, escalar, o alertar sobre ataques activos en tiempo real ni cercanos al tiempo real.

¿Cómo prevenir?

Los desarrolladores deberían implementar algunos o todos los siguientes controles, dependiendo del riesgo de la aplicación:

- Asegúrese de que las transacciones de alto valor poseen una traza de auditoria con controles de integridad para evitar la modificación o el borrado.

- Asegúrese de que los datos de registros son correctamente codificados para prevenir inyecciones o ataques.
- Asegúrese de que todos los errores de sesión y acceso se pueden registrar con suficiente contexto como para identificar cuentas sospechosas o maliciosas.
- Establezca o adopte un plan de respuesta y recuperación.

7.10 Falsificación de Solicitudes del Lado del Servidor (SSRF)

Las fallas de SSRF ocurren cuando una aplicación web está obteniendo un recurso remoto sin validar la URL proporcionada por el usuario. Permite que un atacante coaccione a la aplicación para que envíe una solicitud falsificada a un destino inesperado, incluso cuando está protegido por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL).

¿Cómo prevenir?

Los desarrolladores pueden prevenir SSRF implementando algunos o todos los siguientes controles de defensa en profundidad:

Desde la capa de red

Segmente la funcionalidad de acceso a recursos remotos en redes separadas para reducir el impacto de SSRF

Haga cumplir las políticas de firewall "denegar por defecto" o las reglas de control de acceso a la red para bloquear todo el tráfico de la intranet excepto el esencial.

Desde la capa de aplicación

Sanitizar y validar todos los datos de entrada proporcionados por el cliente.

Hacer cumplir el esquema de URL, el puerto y destino a través de una lista positiva de items permitidos.

Deshabilitar las redirecciones HTTP.

Tenga en cuenta la coherencia de la URL para evitar ataques como el enlace de DNS.

Medidas adicionales a considerar

No implementar otros servicios relevantes para la seguridad en los sistemas frontales.

Para frontends con grupos de usuarios dedicados y manejables, use el cifrado de red en sistemas independientes para considerar necesidades de protección muy altas.

8. Phishing

8.1 Que es?

Son correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados para manipular personas para que descarguen malware, compartan información confidencial (p. ej., números de la seguridad social y tarjetas de crédito, números de cuentas bancarias, credenciales inicio de sesión), o realicen otras acciones que los exponga a ellos mismos o a sus organizaciones al ciberdelito.

8.2 Prevención

Hemos creado una plantilla en forma de correo para que el equipo de Several Energy puede distribuir a todos sus empleados con el objetivo de prevenir posibles ataques de phishing en el futuro.

Asunto: Importante: Medidas de Prevención contra Phishing en Several Energy

Estimado equipo de Several Energy,

Esperamos que este mensaje les encuentre bien. La seguridad de la información es fundamental para garantizar el buen funcionamiento y la integridad de nuestros sistemas en Several Energy. En este sentido, nos dirigimos a ustedes para proporcionar pautas y consejos importantes para prevenir ataques de phishing, una amenaza creciente en el panorama de la ciberseguridad.

El phishing es un método utilizado por ciberdelincuentes para obtener información confidencial, como nombres de usuario, contraseñas y detalles financieros, simulando ser una entidad de confianza. Para fortalecer nuestras defensas contra este tipo de amenazas, les pedimos que tengan en cuenta las siguientes recomendaciones:

Desconfiar de correos electrónicos sospechosos:

Verifiquen la autenticidad de los correos electrónicos, especialmente aquellos que solicitan información confidencial.

Revisen cuidadosamente la dirección del remitente y busquen posibles errores o variaciones en el nombre de dominio.

No hagan clic en enlaces sin verificar:

Eviten hacer clic en enlaces de correos electrónicos no solicitados o que parezcan inusuales.

Siempre verifiquen la autenticidad de los enlaces pasando el cursor sobre ellos para revelar la URL completa antes de hacer clic.

Validación de sitios web:

Al ingresar información confidencial en un sitio web, asegúrense de que la conexión sea segura (comprobar que la URL comience con "https://").

Utilicen sitios web oficiales y eviten acceder a través de enlaces recibidos por correo electrónico.

Mantenimiento de contraseñas seguras:

Utilicen contraseñas robustas y eviten reutilizarlas en múltiples cuentas.

Cambien regularmente sus contraseñas y utilicen la autenticación de dos factores cuando sea posible.

Reporte de actividades sospechosas:

Si encuentran algún correo electrónico sospechoso o enlaces no seguros, repórtenlo inmediatamente a nuestro equipo de soporte de tecnología.

La seguridad cibernética es una responsabilidad compartida, y cada uno de ustedes juega un papel crucial en la protección de la información de la empresa. Manténganse alerta y sigan estas pautas para mitigar los riesgos asociados con el phishing.

Agradecemos su compromiso y colaboración en mantener un entorno digital seguro para todos.

Atentamente,

[Su Nombre]

[Su Cargo]

Several Energy

9. Conclusión

El informe generado concluye que la implementación de medidas integrales de seguridad es esencial para proteger la información y la funcionalidad de los sistemas involucrados en el desarrollo y despliegue de la herramienta.

Nos basamos en la metodología OWASP Top 10 para identificar y abordar vulnerabilidades, así como la importancia de realizar pruebas continuas durante el desarrollo para su monitorización.

Además de la protección de datos y el cumplimiento normativo, también presentamos un enfoque centrado en las personas para proteger su privacidad. La implementación exitosa del SSDLC es esencial para proteger los datos personales. Requiere una planificación cuidadosa y rigurosa desde el principio, con énfasis en identificar los riesgos, definir los objetivos de seguridad y referenciar marcos reconocidos.

En el análisis también destacamos riesgos específicos, proporcionando medidas preventivas detalladas, y aborda el phishing como una amenaza latente.

En general, es necesario destacar la importancia de una formación interna y planes de prevención contra las amenazas mas comunes en el día a día.