Ceibal | Jóvenes a Programar

PROYECTO FINAL DE TESTING

Etapa 2: Testing

E-COMMERCE

OCTUBRE 2023

Equipo 2

Ezequiel Álvarez

Introducción

El propósito de este informe es proporcionar una visión detallada de la evaluación de ciertas pruebas individuales dentro del contexto del proyecto final de pruebas para Jóvenes a Programar. En particular, se enfoca en parte de las pruebas relacionadas con la evaluación de la página web de E-Commerce llamada "e.mercado," la cual se encuentra disponible en el siguiente enlace: https://japceibal.github.io/e-mercado-TESTING/

Este informe se centrará en la cobertura de los requisitos funcionales 04 y 05, así como los requisitos no funcionales relacionados con la seguridad de la aplicación web. Cada uno de estos requisitos se vincula la mayoría de veces con un caso de uso específico y con una serie de casos de prueba correspondientes.

Alcance

El alcance de este informe serán las pruebas que se realizaron en los requisitos funcionales:

RF04 - El sistema debe permitir a los usuarios registrados iniciar sesión proporcionando su dirección de correo electrónico y contraseña.

RF05 - El sistema debe validar las credenciales proporcionadas durante el inicio de sesión.

y los requisitos no funcionales:

RNF03 - Las contraseñas de los usuarios deben almacenarse de manera segura mediante algoritmos de hash y salting.

RNF04 - El sistema debe proteger contra ataques de fuerza bruta y ataques de suplantación de identidad.

RNF05 - Las comunicaciones entre el cliente y el servidor deben cifrarse mediante HTTPS.

Desarrollo

Requisitos funcionales:

RF04 - El sistema debe permitir a los usuarios registrados iniciar sesión proporcionando su dirección de correo electrónico y contraseña.

Link: https://trello.com/c/8dYD4ykj

Para probar este requisito se hicieron tres pruebas, una positiva en la que se comprobaría que el sistema permitiera iniciar sesión al usuario con email y contraseña válidos, otra negativa que fué para comprobar que el sistema no dejara iniciar sesión al usuario con email inválido y contraseña válida, y para finalizar, una negativa con el mismo propósito de esta última, la cual constaba de email válido y contraseña válida.

El resultado fué que el sistema demostró comportarse correctamente al pasar todas las pruebas.

RF05 - El sistema debe validar las credenciales proporcionadas durante el inicio de sesión.

Link: https://trello.com/c/wMGmomLn

Para probar este requisito se hicieron dos pruebas, una positiva en la que se comprobaría que el usuario pueda iniciar sesión con credenciales válidas, y la otra negativa que verificaría que el usuario no pueda iniciar sesión con credenciales inválidas

El resultado fué que el sistema demostró comportarse correctamente al pasar todas las pruebas.

Requisitos no funcionales:

RNF03 - Las contraseñas de los usuarios deben almacenarse de manera segura mediante algoritmos de hash y salting.

Link: https://trello.com/c/xVy5JZeS

Este requisito no funcional no se probó ya que no hay forma de acceder a la base de datos en el backend de la aplicación para probar dicho requisito.

RNF04 - El sistema debe proteger contra ataques de fuerza bruta y ataques de suplantación de identidad.

Link: https://trello.com/c/zgpppXVH

Para probar este requisito no funcional se hizo una prueba en la que se comprobaría que el sistema bloqueará el inicio de sesión tras 20 intentos seguidos y fallidos y/o mostrará un mensaje de advertencia que comunicaría que el inicio se bloqueó tras x números de intentos de inicio de sesión.

El resultado fué que el sistema no pasó la prueba.

RNF05 - Las comunicaciones entre el cliente y el servidor deben cifrarse mediante HTTPS..

Link: https://trello.com/c/4AUWr0eX

Para probar este requisito se hicieron dos pruebas, la primera, verificó que la conexión entre el cliente y el servidor se realiza de manera segura a través de HTTPS utilizando el comando curl. Y la segunda, verificó que la conexión entre el cliente y el servidor se realiza de manera segura a través de HTTPS utilizando el comando openssl s_client.

El resultado fué que el sistema demostró comportarse correctamente al pasar todas las pruebas.

Conclusión

El informe de evaluación de pruebas se centró en la evaluación de ciertos requisitos funcionales y no funcionales dentro del contexto del proyecto final de pruebas para "e.mercado". A lo largo de las tres partes del informe, se realizaron pruebas exhaustivas para evaluar la funcionalidad.

Con respecto a los requisitos funcionales, RF04 y RF05 relacionados con el inicio de sesión de usuarios. Las pruebas demostraron que el sistema permite a los usuarios autorizados iniciar sesión con credenciales válidas y bloquea el acceso a usuarios con credenciales inválidas. Esto indica que la funcionalidad de inicio de sesión se comporta como se espera.

Mencionando a los requisitos no funcionales RNF03 y RNF04. RNF03, que se refiere al almacenamiento seguro de contraseñas mediante hash y salting, no se pudo probar debido a la falta de acceso a la base de datos. Sin embargo, RNF04, que se relaciona con la protección contra ataques de fuerza bruta y suplantación de identidad, no se cumplió en la prueba realizada, lo que destaca la necesidad de implementar medidas adicionales de seguridad para abordar esta vulnerabilidad.

Con respecto al requisito no funcional RNF05, que exige que las comunicaciones entre el cliente y el servidor se cifren mediante HTTPS. Las pruebas demostraron que el sistema se comporta de manera adecuada al utilizar HTTPS para cifrar las comunicaciones entre el cliente y el servidor.

Para finalizar, el proyecto de pruebas para "e.mercado" ha tenido éxito en cumplir con algunos requisitos clave, como la funcionalidad del inicio de sesión y la implementación de HTTPS para la seguridad de las comunicaciones. Sin embargo, se identificó una debilidad en la protección contra ataques de fuerza bruta y suplantación de identidad (RNF04), lo que requiere una atención adicional para fortalecer la seguridad de la aplicación.

Ceibal | Jóvenes a Programar

PROYECTO FINAL DE TESTING

Etapa 3: Retesting

E-COMMERCE

NOVIEMBRE 2023

Equipo 2

Ezequiel Álvarez

Introducción

El propósito de este informe es proporcionar una visión detallada de la evaluación de ciertas pruebas individuales dentro del contexto del proyecto final de pruebas para Jóvenes a Programar. En particular, se enfoca en el retesting de la página web del E-Commerce llamado "e.mercado," la cual se encuentra disponible en el siguiente enlace: https://japceibal.github.io/proyecto-testing-retestingOF/

Este informe se centrará en la cobertura de las pruebas de regresión del RF04, así como las pruebas basadas en especificaciones de los RF05, RNF03, RNF04, RNF05. Cada uno de estos requisitos nombrados se vincula la mayoría de veces con un caso de uso específico y con una serie de casos de prueba correspondientes.

Alcance

En este informe se abordará el siguiente requisito funcional el cual está dentro de las pruebas de regresión:

RF04 - El sistema debe permitir a los usuarios registrados iniciar sesión proporcionando su dirección de correo electrónico y contraseña.

Además de los siguientes requisitos funcionales y no funcionales, los cuales forman parte de las pruebas en base a especificaciones:

RF05 - El sistema debe validar las credenciales proporcionadas durante el inicio de sesión.

RNF03 - Las contraseñas de los usuarios deben almacenarse de manera segura mediante algoritmos de hash y salting.

RNF04 - El sistema debe proteger contra ataques de fuerza bruta y ataques de suplantación de identidad.

RNF05 - Las comunicaciones entre el cliente y el servidor deben cifrarse mediante HTTPS.

Desarrollo y resultados clave

Pruebas de regresión

RF04 - El sistema debe permitir a los usuarios registrados iniciar sesión proporcionando su dirección de correo electrónico y contraseña

Tal y como la versión anterior, estas pruebas no cambiaron su resultado dado que el sistema demostró haberse comportado correctamente tras una prueba positiva en la que se comprobaría que el sistema permitiera iniciar sesión al usuario con email y contraseña válidos, otra negativa que fue para comprobar que el sistema no dejara iniciar sesión al usuario con email inválido y contraseña válida, y para finalizar, una negativa con el mismo propósito de esta última, la cual constaba de email válido y contraseña válida.

Pruebas en base a especificaciones

Requisitos funcionales

RF05 - El sistema debe validar las credenciales proporcionadas durante el inicio de sesión

Nuevamente el sistema se comporta según lo esperado, dado que pasó las dos pruebas, una positiva en la que se comprobaría que el usuario pueda iniciar sesión con credenciales válidas, y la otra negativa que verificaría que el usuario no pueda iniciar sesión con credenciales inválidas

Requisitos no funcionales

RNF03 - Las contraseñas de los usuarios deben almacenarse de manera segura mediante algoritmos de hash y salting

Este requisito no funcional no se probó ya que la base de datos proporcionada para ello es muy básica y simplificada, y no incluye características avanzadas de seguridad.

RNF04 - El sistema debe proteger contra ataques de fuerza bruta y ataques de suplantación de identidad

Para probar este requisito no funcional se hizo una prueba en la que se comprobaría que el sistema bloqueará el inicio de sesión tras 20 intentos seguidos y fallidos y/o mostrará un mensaje de advertencia que comunicaría que el inicio se bloqueó tras x números de intentos de inicio de sesión. El resultado, al igual que la versión anterior del sitio, fue que el sistema no pasó la prueba.

RNF05 - Las comunicaciones entre el cliente y el servidor deben cifrarse mediante HTTPS

Para probar este requisito se hicieron dos pruebas, la primera, verificó que la conexión entre el cliente y el servidor se realiza de manera segura a través de HTTPS utilizando el comando curl. Y la segunda, verificó que la conexión entre el cliente y el servidor se realiza de manera segura a través de HTTPS utilizando el comando openssl s_client. El resultado para esta nueva versión fué que el sistema demostró una vez más comportarse correctamente al pasar todas las pruebas.

Conclusiones

Con base en los resultados obtenidos durante el retesting de la página web "e.mercado" en el proyecto final de pruebas para Jóvenes a Programar, se pueden extraer las siguientes conclusiones:

Requisitos Funcionales (RF04 y RF05):

RF04, que se refiere al inicio de sesión de usuarios, ha demostrado consistencia en su comportamiento, manteniendo su funcionalidad para permitir a los usuarios registrados iniciar sesión de manera efectiva.
RF05, relacionado con la validación de credenciales durante el inicio de sesión, también ha mostrado un rendimiento adecuado al superar las pruebas positivas y negativas planificadas.
Requisitos No Funcionales (RNF03, RNF04, RNF05):

RNF03, que aborda el almacenamiento seguro de contraseñas mediante hash y salting, no pudo ser probado debido a limitaciones en la base de datos proporcionada.
RNF04, centrado en la protección contra ataques de fuerza bruta y suplantación de identidad, reveló una vulnerabilidad persistente, ya que el sistema no logró bloquear el inicio de sesión después de múltiples intentos fallidos. Esto sugiere la necesidad de mejoras en la seguridad contra este tipo de ataques.
RNF05, que exige la cifra de comunicaciones mediante HTTPS, ha demostrado ser efectivo, ya que superó las pruebas de conexión segura tanto con el comando curl como con openssl s_client.

Ceibal | Jóvenes a Programar

PROYECTO FINAL DE TESTING

Informe Ejecutivo

E-COMMERCE

NOVIEMBRE 2023

Grupo 254
Equipo 2

Ezequiel Álvarez

Resumen Ejecutivo

Este informe resume las conclusiones y resultados del proceso de testing llevado a cabo a lo largo del proyecto final de Testing. El objetivo principal del testing fue evaluar la calidad, funcionalidad, seguridad y rendimiento como aspectos generales del sistema web “e.Mercado”. A lo largo de las distintas fases del proyecto, el equipo de testing ha trabajado diligentemente para identificar y abordar cualquier problema que pudiera afectar la integridad y usabilidad del sistema.

Resultados Clave

Etapa 2

Autenticación de Usuario

Para comenzar a abordar con lo que autenticación de usuario se refiere, se hicieron 3 pruebas en base al RF04, que se refería al inicio de sesión con correo y contraseña del usuario y 2 pruebas en base al RF05, que se refería a validar las credenciales proporcionadas durante el inicio de sesión.
Con respecto al primer RF nombrado, se llevó a cabo una prueba positiva en la que se comprobaría que el sistema permitiera iniciar sesión al usuario con email y contraseña válidos, otra negativa que fué para comprobar que el sistema no dejara iniciar sesión al usuario con email inválido y contraseña válida, y para finalizar, una negativa con el mismo propósito de esta última, la cual constaba de email válido y contraseña válidas.
Con respecto al segundo RF, se hicieron 2 pruebas, una positiva en la que se comprobaría que el usuario pueda iniciar sesión con credenciales válidas, y la otra negativa que verificaría que el usuario no pueda iniciar sesión con credenciales inválidas.
Al finalizar todas estas pruebas se pudo observar que el sistema cumplía fielmente con la funcionalidad planteada en el ESRE, dado que ninguna prueba de los dos requisitos funcionales falló.

Seguridad

En el contexto de las pruebas de seguridad, se llevaron a cabo evaluaciones específicas para garantizar la integridad y robustez del sistema. Se abordaron tres requisitos no funcionales
En relación con el RNF03, Almacenamiento Seguro de Contraseñas, la prueba directa de este requisito se vio limitada por el hecho que se nos fué otorgada una base de datos demasiado simplificada del backend de la aplicación, impidiendo una evaluación precisa.
Para RNF04, Protección contra Ataques, se ejecutó una prueba que verificó la capacidad del sistema para bloquear el inicio de sesión después de 20 intentos fallidos consecutivos o mostrar un mensaje de advertencia. No obstante, el sistema no superó esta prueba, señalando posibles debilidades en la protección contra ataques de fuerza bruta y suplantación de identidad.
Por otro lado, RNF05, Cifrado de Comunicaciones, se sometió a dos pruebas. La primera confirmó la conexión segura entre el cliente y el servidor utilizando el comando curl, y la segunda lo hizo a través del comando openssl s_client.

Afortunadamente, el sistema demostró un comportamiento sólido al superar ambas pruebas, confirmando que las comunicaciones se realizan de manera segura mediante HTTPS.

Obtenemos como resultado de estas pruebas que mientras que el sistema cumplió exitosamente con el cifrado de comunicaciones (RNF05), se identificaron áreas de mejora en la protección contra ataques (RNF04), y la evaluación directa del almacenamiento seguro de contraseñas (RNF03) fue limitada dado la base de datos otorgada.

Etapa 3

Pruebas de regresión:

Para el RF04, que dicta que el sistema debe permitir a los usuarios registrados iniciar sesión proporcionando su dirección de correo electrónico y contraseña, las pruebas positivas y negativas anteriores se repitieron. Una prueba positiva validó que el sistema permitiera iniciar sesión con credenciales válidas, mientras que las pruebas negativas verificaron la correcta restricción de acceso en casos de email inválido y/o contraseña inválida. Los resultados persistieron, indicando que el sistema continuó comportándose conforme a lo esperado.

Retesting de Pruebas Basadas en Especificaciones:

Con respecto al RF05, que exige la validación de credenciales durante el inicio de sesión, las pruebas también se replicaron. Una prueba positiva confirmó que el usuario pudo iniciar sesión con credenciales válidas, y la prueba negativa corroboró que el sistema impidió el acceso con credenciales inválidas. Nuevamente, el sistema superó ambas pruebas, manteniendo su rendimiento efectivo.

En cuanto al RNF03, que establece que las contraseñas deben almacenarse de manera segura mediante algoritmos de hash y salting, no se pudo realizar una prueba directa debido a limitaciones en la base de datos proporcionada.

Para el RNF04, referente a la protección contra ataques, se repitió la prueba de bloqueo de inicio de sesión después de 20 intentos fallidos. Al igual que en la versión anterior, el sistema no superó esta prueba, señalando posibles vulnerabilidades en la protección contra ataques de fuerza bruta y suplantación de identidad.

En relación con el RNF05, que destaca la necesidad de cifrar las comunicaciones mediante HTTPS, las pruebas con curl y openssl s_client se reprodujeron. Afortunadamente, el sistema demostró una vez más su comportamiento sólido al pasar ambas pruebas, asegurando que las comunicaciones entre el cliente y el servidor se realicen de manera segura mediante HTTPS.

Las pruebas de regresión revelaron que, a pesar de ciertas áreas de mejora identificadas en los requisitos no funcionales, el sistema mantiene una consistencia en su rendimiento y continúa cumpliendo con parte de los estándares de seguridad establecidos.

Datos y métricas

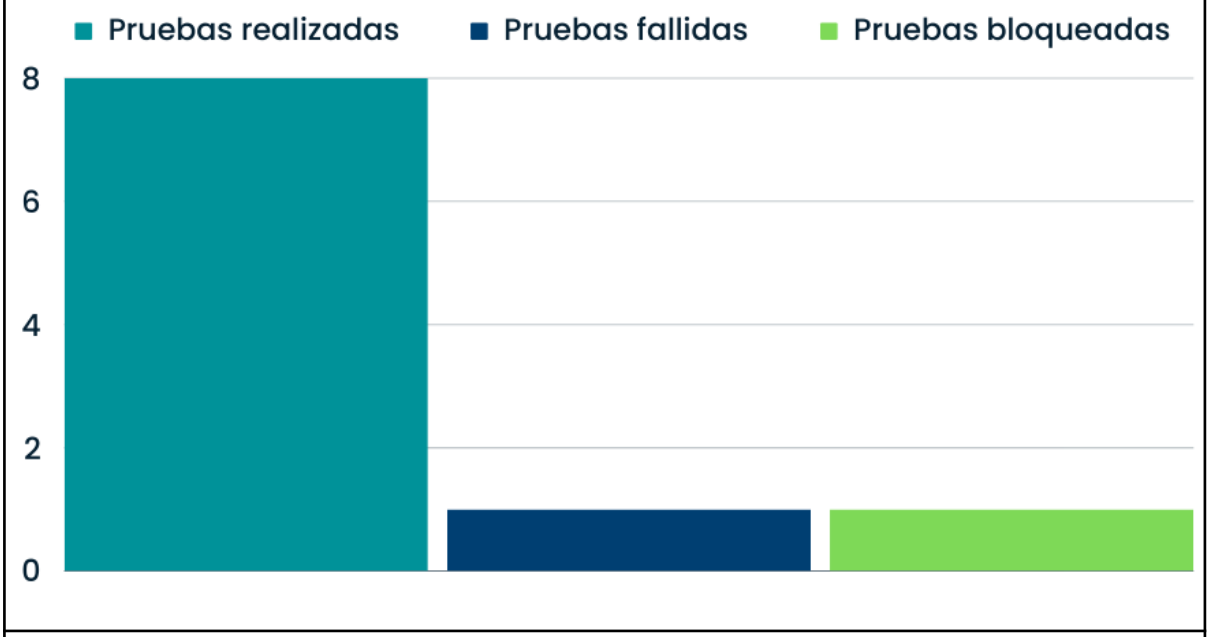

Gráfico 1: Estado de pruebas etapa 2

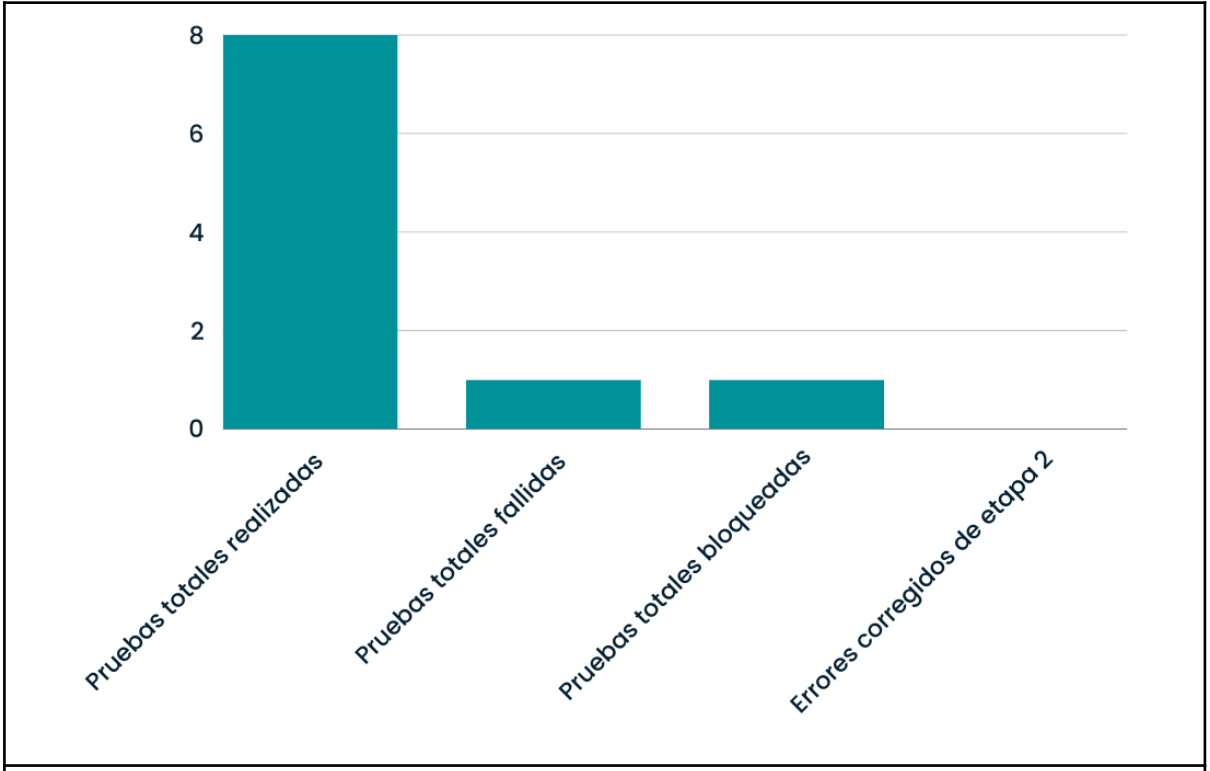

Gráfico 2: Estado de pruebas etapa 3 y errores corregidos etapa 2

Observaciones y Recomendaciones Finales

A la luz de los hallazgos surgidos en las etapas 2 y 3 del proyecto, se proponen las siguientes recomendaciones para elevar la calidad y seguridad del sistema:

- Refinamiento en Protección contra Ataques:

Se recomienda implementar medidas adicionales para fortalecer la protección contra ataques, especialmente en la detección y bloqueo de intentos de fuerza bruta y suplantación de identidad. Esto garantizará una capa adicional de seguridad y mitigará posibles riesgos de seguridad.

- Evaluación Detallada del Almacenamiento de Contraseñas:

Dada la limitación en la evaluación del almacenamiento seguro de contraseñas, se sugiere realizar pruebas más exhaustivas en un entorno que simule condiciones de producción realistas. Esto asegurará una comprensión completa de la seguridad en esta área crucial.

- Actualización de Entornos de Prueba:

Considerando la importancia de la evaluación de seguridad, se recomienda trabajar con bases de datos más representativas y completas en futuros procesos de testing. Esto permitirá una evaluación más precisa y exhaustiva de los aspectos de seguridad del sistema.

- Mantenimiento de Buenas Prácticas de Cifrado:

Dado el éxito en las pruebas de cifrado de comunicaciones, se aconseja mantener y actualizar regularmente las prácticas de cifrado para adaptarse a las últimas recomendaciones de seguridad. Esto asegurará una comunicación segura a medida que evolucionan las amenazas cibernéticas.

- Monitoreo Continuo de Rendimiento:

Se sugiere implementar un sistema de monitoreo continuo para evaluar y mitigar posibles vulnerabilidades de seguridad. Esto permitirá una respuesta proactiva a posibles amenazas y garantizará la integridad y la seguridad a lo largo del tiempo.

Conclusión

En conclusión, el proceso de testing del sistema "e.Mercado" ha arrojado resultados significativos tanto en términos de funcionalidad como de seguridad. Las pruebas de autenticación de usuario han validado con éxito la capacidad del sistema para gestionar el inicio de sesión con credenciales válidas, proporcionando una base sólida para la confianza en la experiencia del usuario.

Sin embargo, las pruebas de seguridad han identificado áreas de mejora, destacando la necesidad de una revisión más detallada en aspectos clave como el almacenamiento seguro de contraseñas y la protección contra ataques. La limitación en la base de datos otorgada ha impactado la evaluación de la seguridad, subrayando la importancia de entornos de prueba más representativos en futuras fases.

A pesar de estos desafíos, el sistema ha demostrado un rendimiento consistente en las pruebas de regresión, indicando una resistencia y estabilidad general. Las recomendaciones finales se centran en fortalecer la protección contra posibles vulnerabilidades de seguridad, mejorar la evaluación del almacenamiento de contraseñas y mantener prácticas de cifrado actualizadas.

.

En última instancia, la conclusión destaca la importancia de la seguridad continua y el monitoreo proactivo para adaptarse a las amenazas cambiantes. Al abordar las áreas de mejora identificadas, el sistema "e.Mercado" puede consolidar su posición como una plataforma web segura y eficiente, proporcionando a los usuarios y stakeholders la confianza necesaria en sus operaciones y transacciones.