// Instrucciones de Rellenado

Cualquier campo contenido entre corchetes en el siguiente formato: [X] deberá ser completado por el/los auditores correspondientes de acuerdo con los requisitos específicos de cada sección. Se sugiere omitir cualquier apartado precedido por "//" en el informe, ya que este contenido tiene carácter informativo y tiene el propósito de guiar al auditor o auditores en el proceso de llenado. Cabe mencionar que esta indicación podría no ser siempre aplicable, dado que algunos detalles se especifican directamente.

// Tarjeta de Presentación (1 Página)

En este segmento, es imprescindible adjuntar una tarjeta de presentación que represente al auditor o al equipo de auditoría. Esta tarjeta puede incluir elementos como el logotipo, imágenes u otros identificadores visuales. Los elementos requeridos son los siguientes:

- Logotipo distintivo.
- Nombre completo del auditor o denominación del equipo de auditoría (En caso de preferir el anonimato, se pueden utilizar seudónimos).
- Fecha completa (día, mes, año) en que se finalizó el llenado del informe.
- Versión del informe (En el caso de ser el primer informe para la aplicación en cuestión, la versión por defecto será 1.0).

Resumen

En esta sección, se detallan algunas de las vulnerabilidades identificadas en la aplicación. Se describe cómo estas vulnerabilidades podrían afectar a los activos y a la plataforma web en general. Es relevante destacar que este informe no pretende abarcar de manera exhaustiva todas las vulnerabilidades existentes o potenciales del aplicativo, sino que ofrece una selección representativa.

El informe concluye presentando un resumen cuantitativo de las vulnerabilidades encontradas, clasificadas según su grado de severidad. Ejemplo:

Crítico	Alto	Medio	Bajo	Informativo
2	1	3	10	12

Tabla de contenidos

"OWASP Risk Rating". Es de suma importancia que la descripción de la metodología sea comprensible y legible para que el cliente pueda tener una comprensión completa de su funcionamiento. Se exhorta a explicar con claridad cómo esta metodología seleccionada determina la gravedad de las vulnerabilidades mencionadas en el informe. Esto garantizará que el cliente comprenda de manera precisa los criterios utilizados en la evaluación de la severidad de las vulnerabilidades.

Reconocimiento

Observaciones - [X]

En X se debe insertar el título correspondiente a la vulnerabilidad que se explicará posteriormente en el informe.

[X1].[Z1]

El valor de X1 debe representar el número secuencial asignado a la vulnerabilidad en el informe. Si esta es la primera vulnerabilidad que se presenta en la tabla de contenidos, se utilizará "1". En caso de que Z1 sea superior a "9", se completará con "2", teniendo en cuenta un máximo de 9 (nueve) valores Z1 para cada valor X1. Z1 debe reflejar el número secuencial que sigue a X1. Si X1 es "1" y es la primera vulnerabilidad que se describe en la tabla de contenidos, Z1 también será "1". Si se trata de la segunda vulnerabilidad en el informe bajo X1 "1", Z1 cambiará a "2".

Nótese que este procedimiento se aplica para cada apartado individual de la tabla de contenidos.

Vulnerabilidades Informativas

En este segmento se detallarán las vulnerabilidades que se han identificado en la aplicación, las cuales tienen carácter informativo.

Conclusiones y recomendaciones finales

En esta sección se presentarán las conclusiones generales derivadas del análisis de vulnerabilidades. Asimismo, se ofrecerán recomendaciones finales destinadas a mejorar la seguridad del aplicativo.

Referencias

En esta parte se incluirán las fuentes y recursos consultados para llevar a cabo el análisis de vulnerabilidades y la elaboración del informe.

Reconocimiento

En esta sección, es necesario incluir toda la información recopilada sobre el sistema/aplicación, lo que podría incluir ejemplos como: Librerías y sus versiones, endpoints y sus respectivas llamadas, microservicios, etc. Además, puede agregar una lista de cada herramienta utilizada en esta fase y su propósito.

Observaciones

[Nombre del apartado]

Este segmento debe ser completado como un subtítulo, haciendo alusión a la sección de la aplicación a la cual se notificará acerca de la vulnerabilidad detectada en el formato posterior. Ejemplo de nombres de secciones:

LOGIN (Inicio de Sesión)

REGISTRO (Registro de Usuarios)

ADMIN PANEL (Panel de Administración)

HOME (Página de Inicio)

Se solicita la inclusión de la cantidad de plantillas correspondientes a la explicación de cada vulnerabilidad inherente a cada apartado, según sea necesario.

[X1].[Z1]

El valor de X1 debe representar el número secuencial asignado a la vulnerabilidad en el informe. Si esta es la primera vulnerabilidad que se presenta en la tabla de contenidos, se utilizará "1". En caso de que Z1 sea superior a "9", se completará con "2", teniendo en cuenta un máximo de 9 (nueve) valores Z1 para cada valor X1. Z1 debe reflejar el número secuencial que sigue a X1. Si X1 es "1" y es la primera vulnerabilidad que se describe en la tabla de contenidos, Z1 también será "1". Si se trata de la segunda vulnerabilidad en el informe bajo X1 "1", Z1 cambiará a "2".

Nótese que este procedimiento se aplica para cada apartado individual de la tabla de contenidos.

// Plantilla (Por favor, únicamente completar los campos)

// (Es posible que ciertos campos no puedan ser llenados por el auditor, como en el caso de información faltante o el descubrimiento reciente de una vulnerabilidad "0day", etc.)

Nombre: // Asigne un nombre identificativo para esta vulnerabilidad.

Descripción: // Proporcione una breve descripción acerca de la vulnerabilidad.

Detalle del negocio: // Se especifica el contexto del ataque. Por ejemplo, atacar un formulario de inicio de sesión en el contexto de un usuario que ya existe no es lo mismo que hacerlo en el contexto de un usuario recién registrado. También es diferente si el usuario tiene autenticación activada o si está bloqueado. Es fundamental detallar estos diferentes contextos.

Riesgo: // Defina tanto el impacto como el nivel de riesgo de la vulnerabilidad, utilizando una evaluación cualitativa y cuantitativa.

CVE: // Especificar el/los identificador/es CVE relacionado/s con esta vulnerabilidad. (Aclarar que este apartado es opcional, ya que es posible que la información no esté disponible para su inclusión).

CVSS: // Adjuntar el "Vector String" completo sobre la vulnerabilidad.

Tipo de vulnerabilidad: // Indique el tipo específico de vulnerabilidad, por ejemplo, XSS, CSRF, etc.

Categoría: // Mencione la categoría a la que pertenece la vulnerabilidad.

Ubicación de explotabilidad: // Especifique dónde ocurre esta vulnerabilidad, tomando en cuenta los alcances permitidos por el análisis.

Impacto real: // Explique el impacto observable por el auditor o el equipo de auditoría al explotar la vulnerabilidad. (Considere que en ocasiones no es viable debido a restricciones previamente mencionadas en la sección de Limitaciones y Descargo de Responsabilidad.)

Impacto mínimo: // Explique el impacto mínimo observable por el auditor o el equipo de auditoría al explotar la vulnerabilidad. (Considere que en ocasiones no es viable debido a restricciones previamente mencionadas en la sección de Limitaciones y Descargo de Responsabilidad.)

Impacto máximo: // Explique el impacto máximo observable por el auditor o el equipo de auditoría al explotar la vulnerabilidad que se puede alcanzar. (Considere que en ocasiones no es viable debido a restricciones previamente mencionadas en la sección de Limitaciones y Descargo de Responsabilidad.)

Pasos a seguir: // Detalle los pasos seguidos desde la fase de reconocimiento que condujeron a la identificación de un posible vector de vulnerabilidad, hasta lograr una explotación exitosa. Incluya las herramientas o metodologías empleadas.

Escenarios de riesgo: // Aporte diversos escenarios de riesgo potencial en los cuales esta vulnerabilidad podría ser aprovechada por un ciberdelincuente. Relacione estos escenarios

con el impacto en la continuidad del negocio para proporcionar una explicación sólida y con enfoque en la resolución a favor de los intereses comerciales.
Recomendaciones: // Proponga medidas de contramedida o defensa para abordar la vulnerabilidad en cuestión siempre en favor del negocio y su continuidad.

Vulnerabilidades Informativas

// (El valor X se completará con un número comenzando desde "1" en orden ascendente según corresponda al caso en cuestión.)

Nota N°[X]: // Proporcione aclaraciones adicionales sobre la aplicación (no necesariamente relacionadas con la seguridad) o explique una vulnerabilidad informativa que, si bien no posee un impacto concreto, podría ser escalable en términos de seguridad.

Conclusiones y recomendaciones finales

En esta sección, se abordan las conclusiones derivadas del análisis del aplicativo sometido a auditoría. Se aclara cualquier asunto pendiente o aspecto adicional que se considere relevante para una conclusión completa y precisa. Asimismo, se presentan recomendaciones, tanto relacionadas como no relacionadas directamente con la seguridad del aplicativo, con el fin de aportar valor y sugerir mejoras sustantivas.

Referencias

Cuando se haga referencia a otras entidades, sitios web, instituciones, aplicaciones u otros elementos, o cuando se realicen citas o menciones, se debe seguir el siguiente formato:

Nombre de la entidad o recurso citado [X].

(Dónde el valor X se completará con un número comenzando desde "1" en orden ascendente según corresponda al caso en cuestión.)

En última instancia, en esta sección se debe proporcionar el enlace URL completo y funcional correspondiente a la referencia mencionada en el siguiente formato:

Enlace Clickeable: [X] nombre vínculo/url/enlace.

// Ejemplo de categorías para utilizar

Controles de acceso: Relacionados con la autorización de usuarios y la evaluación de derechos.
Auditoría y registro: Relacionado con la auditoría de acciones o el registro de problemas. Autenticación: Relacionado con la identificación de usuarios. Configuración: Relacionado con las configuraciones de seguridad de servidores, dispositivos o software. Criptografía: Relacionado con la protección matemática de los datos. Exposición de datos: Exposición involuntaria de información sensible. Validación de datos: Relacionado con la confianza indebida en la estructura o los valores de los datos. Denegación de servicio: Relacionado con provocar fallos en el sistema. Notificación de errores: Relacionado con la notificación de condiciones de error de forma segura. Parcheado: Relacionado con mantener el software actualizado. Gestión de sesiones: Relacionado con la identificación de usuarios autenticados. Tiempo: Relacionado con las condiciones de tiempo, el bloqueo o el orden de las operaciones.

// ¿Qué es un CVE?

CVE significa "Common Vulnerabilities and Exposures" (Vulnerabilidades y Exposiciones Comunes). Es un sistema de identificación y seguimiento de vulnerabilidades de seguridad en software y hardware. Cada CVE asigna un número único a una vulnerabilidad específica, lo que ayuda a los investigadores, empresas y usuarios a hablar sobre problemas de seguridad de manera clara y precisa. Este sistema facilita la comunicación y la coordinación en la comunidad de seguridad cibernética para abordar y resolver problemas de manera efectiva.
Un CVE podría tener el siguiente formato: CVE-2023-12345.

"CVE" es la abreviatura de "Common Vulnerabilities and Exposures".

"2023" representa el año en el que se asignó el número CVE.

"12345" es el número identificador único de la vulnerabilidad dentro de ese año.

Puede encontrar CVE's en las siguientes páginas:

[1] https://cve.mitre.org

[2] https://nvd.nist.gov

[3] https://www.cvedetails.com