Imagen que contiene texto, libro

Descripción generada automáticamente

|  |
| --- |
|  |
| **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN E INNOVACIÓN** |
| **DIRECCIÓN DE SEGURIDAD TECNOLÓGICA** |
| **INFORME DE ANÁLISIS DINÁMICO**  **“sembrandovidasvqa.sre.gob.mx– Octavo análisis”**  AD-21-066  08|2021 |
|  |

Contenido

[I. Introducción 3](#_Toc80324803)

[II. Antecedentes 3](#_Toc80324804)

[III. Resumen Ejecutivo 3](#_Toc80324805)

[IV. Vulnerabilidades identificadas 3](#_Toc80324806)

[V. Plan de acción 4](#_Toc80324807)

[A. Objetivo general 4](#_Toc80324808)

[B. Metodología 4](#_Toc80324809)

[VI. Alcance de la evaluación 6](#_Toc80324810)

[VII. Estructura del Reporte 7](#_Toc80324811)

[A. USO DEL MÉTODO GET CON INFORMACIÓN SENSIBLE 7](#_Toc80324812)

[B. AUTENTICACIÓN INAPROPIADA 10](#_Toc80324813)

[VIII. Descripción de la criticidad 13](#_Toc80324814)

[IX. Resumen técnico de hallazgos 14](#_Toc80324815)

[X. Recomendaciones 14](#_Toc80324816)

[XI. Firmas y fechas de elaboración, revisión, recepción y aprobación 15](#_Toc80324817)

# Introducción

El equipo de seguridad informática de TIC DEFENSE por parte del equipo de pruebas de penetración, realiza el octavo análisis dinámico, con el objetivo de identificar vulnerabilidades que afecten la integridad, confidencialidad y disponibilidad de los sistemas e información involucrados.

# Antecedentes

De acuerdo con la solicitud del día 13 de agosto de 2021 con número de oficio SRE/TIN/E-2701/2021 por parte de Homero Piedras Rodríguez, El Director de Área en la Dirección General de Tecnologías de Información e Innovación, para realizar el octavo análisis de vulnerabilidades a los siguientes componentes:

* **https://sembrandovidasvqa.sre.gob.mx/**

El equipo de seguridad de TIC DEFENSE procedió a realizar el análisis dinámico.

# Resumen Ejecutivo

Con el propósito de identificar las vulnerabilidades potenciales que pudieran comprometer la seguridad de la Información, se realizó el octavo análisis dinámico del aplicativo. Las vulnerabilidades identificadas podrían permitir a un usuario malintencionado descargar información de la aplicación sin iniciar sesión, obtener información en metadatos. Estos se clasifican con un riesgo **ALTO**, por lo que se considera que se deben realizar acciones inmediatas para mitigar las vulnerabilidades expuestas ya que estas podrían afectar directamente a la confidencialidad de los sistemas involucrados.

# Vulnerabilidades identificadas

A continuación, se muestra una gráfica de las vulnerabilidades identificadas durante las pruebas de penetración realizadas a **sembrandovidasvqa.sre.gob.mx.**

|  |  |
| --- | --- |
| **CRITICIDAD** | **VULNERABILIDADES IDENTIFICADAS** |
|  |
| CRÍTICA | 1.        Autenticación inapropiada |  |
| BAJA | 2. HOLA HOLA |  |
|  |  |  |
|  |  |  |
|  |  |  |

***Nota: La criticidad de las vulnerabilidades mencionadas en este documento, se cataloga de acuerdo con el escenario evaluado, por lo tanto, esta puede variar respecto al criterio de la secretaría (SRE) al igual que el nivel de prioridad para su remediación.***

# Plan de acción

## Objetivo general

Presentar los resultados de las pruebas realizadas a **sembrandovidasvqa.sre.gob.mx,** con la finalidad de identificar vulnerabilidades críticas dentro de los sistemas involucrados.

## Metodología

Las pruebas de seguridad están basadas en la metodología OWASP para evaluar la seguridad de un sistema, un aplicativo o red, validando y verificando metódicamente la efectividad de controles de seguridad de aplicaciones, realizándose una prueba de seguridad de aplicaciones web que se centra en evaluar la seguridad de la aplicación web, en el cual los procesos que se implican en un análisis activo son por cualquier debilidad, fallas técnicas o vulnerabilidades.

La prueba se divide en 2 fases:

* Modo pasivo:

En el modo pasivo, se intenta comprender la aplicación lógicamente, manipulando la aplicación para recopilar información comprendiendo la configuración implementada del servidor que aloja la aplicación web. Siendo en las plataformas de aplicación amplias y variadas, puede haber algunas claves o señales en errores de configuración que comprometen la aplicación, de la misma manera que una aplicación no segura puede comprometer el servidor. Por ejemplo, se puede usar un web proxy para observar todas las solicitudes y respuestas HTTP. Al final, se debe comprender todos los puntos de acceso de la aplicación (por ejemplo, encabezados HTTP, parámetros, recursos, archivos de configuración, complementos, cookies).

* Modo activo:

En esta fase, se comienza a probar utilizando la metodología descrita en la siguiente lista.

El conjunto de pruebas activas se ha dividido en subcategorías y controles:

* Recopilación de información
* Pruebas de configuración y gestión de implementación
* Pruebas de gestión de identidad
* Pruebas de autenticación
* Pruebas de autorización
* Pruebas de gestión de sesiones
* Prueba de validación de entrada
* Manejo de errores
* Criptografía
* Pruebas de lógica empresarial
* Pruebas del lado del cliente

Cualquier problema de seguridad que sea encontrado será presentado al equipo de desarrollo o infraestructura, junto con una evaluación de la criticidad, con una propuesta de mitigación o una solución técnica.

# Alcance de la evaluación

|  |  |
| --- | --- |
| **Dirección IP** | 172.18.217.32 |
| **URL** | [https://sembrandovidasvqa.sre.gob.mx](https://spcqa.sre.gob.mx) |
| **Descripción** | Sistema sembrandovidasvqa.sre.gob.mx |
| **Sistema Operativo** | Linux |

# Estructura del Reporte

A continuación, se presenta la estructura del documento para los hallazgos identificados

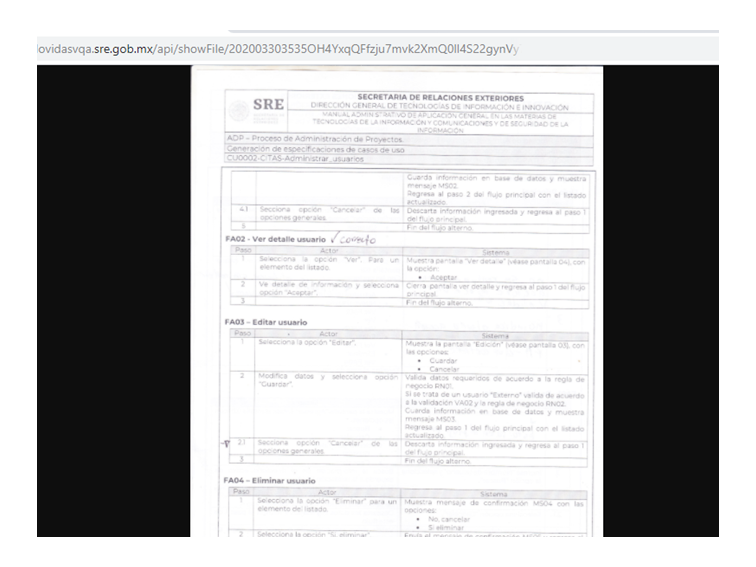
## USO DEL MÉTODO GET CON INFORMACIÓN SENSIBLE

| **CWE-598** | USO DEL MÉTODO GET CON INFORMACIÓN SENSIBLE | **7.4** |
| --- | --- | --- |
| VALORACIÓNCVSS FINAL:  AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N | | |
| NÚMERO DE OCURRENCIAS  1 | | |
| CLASIFICACIÓN  Confidencialidad | | |
| Dirección IP:  172.18.217.32 | Puerto TCP/UDP: 443 | |
| RIESGO | Un atacante podría interceptar y capturar la petición realizada al servidor por medio del método GET. La información que viaja en la URL puede ser utilizada para comprometer la confidencialidad de los datos de los usuarios. | |
| DESCRIPCIÓN | La aplicación realiza solicitudes de archivos a la API, pero no se esta validando que el usuario este autenticado en la API antes de procesar la solicitud, por lo que un usuario no autenticado puede descargar algunos archivos por medio del método GET. | |
| PROPUESTA DE REMEDIACIÓN | Se recomienda implementar mecanismos de autenticación en la API, o en su defectos procesarlos con peticiones POST en lugar de GET. | |
| REFERENCIAS EXTERNAS | https://cwe.mitre.org/data/definitions/598.html  https://owasp.org/www-community/vulnerabilities/Information\_exposure\_through\_query\_strings\_in\_url  https://portswigger.net/kb/issues/00400300\_password-submitted-using-get-method | |

La vulnerabilidad se presenta en la siguiente ruta:

* https://sembrandovidasvqa.sre.gob.mx/api/showFile

A continuación, se presenta la evidencia de la vulnerabilidad detectada.



En este imagen se muestra un documento que puede ser descargado y visualizado sin estar autenticado.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Estos archivos en el ambiente de QA simulan ser documentos personales. Por lo que es importante revisar que no se puedan descargar sin iniciar una sesión previamente.

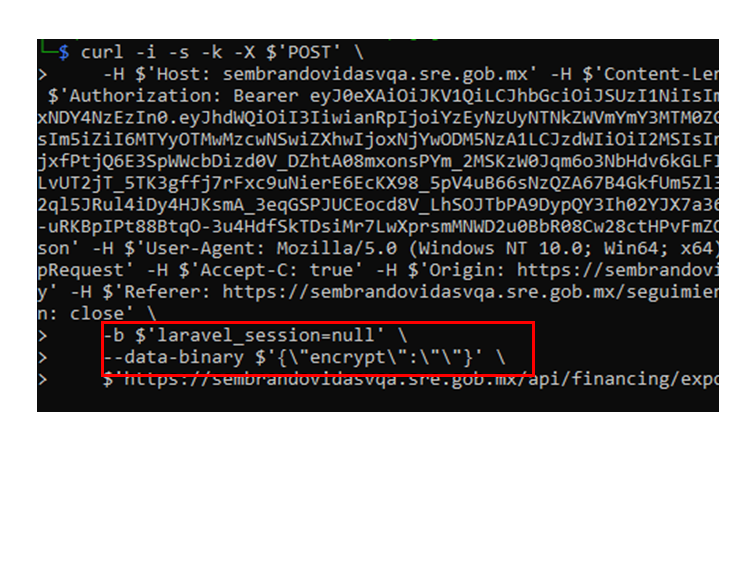
## AUTENTICACIÓN INAPROPIADA

| **CWE-287** | AUTENTICACIÓN INAPROPIADA | **3.1** |
| --- | --- | --- |
| VALORACIÓNCVSS FINAL:  AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | |
| NÚMERO DE OCURRENCIAS  1 | | |
| CLASIFICACIÓN  Confidencialidad | | |
| Dirección IP:  172.18.217.32 | Puerto TCP/UDP: 443 | |
| RIESGO | Un atacante puede descargar información de la aplicación sin iniciar sesión (sesión nula) aunque para eso tiene que conocer partes especificas de la solicitud. | |
| DESCRIPCIÓN | La aplicación no valida de manera apropiada que el usuario tenga iniciada sesión para procesar la solicitud aunque si cuenta con mecanismos auntenticación. | |
| PROPUESTA DE REMEDIACIÓN | Se recomienda corregir el proceso validación de esta solicitud y solicitudes similares. | |
| REFERENCIAS EXTERNAS | https://cwe.mitre.org/data/definitions/287.html  https://www.security-database.com/cwe.php?name=CWE-287 | |

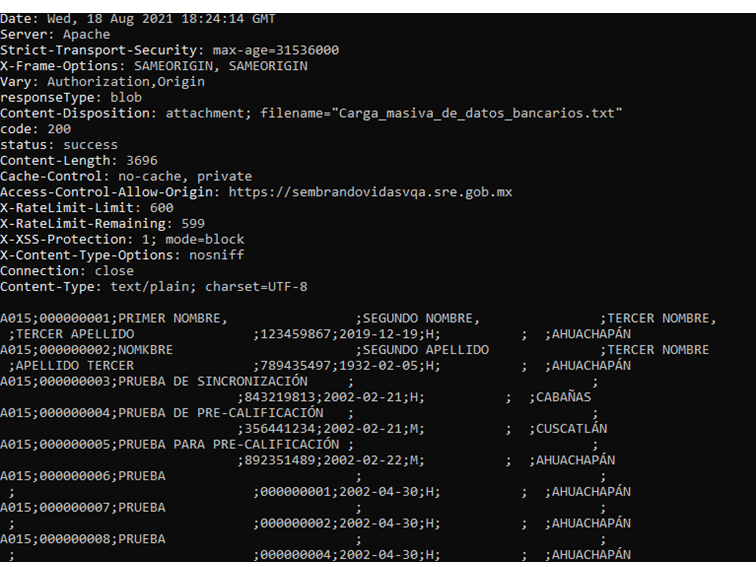
La vulnerabilidad se presenta en la siguiente ruta:

* https://sembrandovidasvqa.sre.gob.mx/api/financing/

A continuación, se presenta la evidencia de la vulnerabilidad detectada.



En la imagen se muestra como al poner la sessión de laravel en valores nulos y parte de los paramtros encriptados como vacios, es posible realizar la solicitud POST y descargar el archivo.



Se probó con un archivo de excel y un archivo de texto en ambos casos se pudo procesar la solicitud.

# Descripción de la criticidad

Para la evaluación de la criticidad, se emplea la siguiente categorización:

|  |  |
| --- | --- |
| **Colorimetría** | **Criticidad** |
|  | **CRÍTICA:** Estas vulnerabilidades son reportadas al momento de identificarlas en los equipos que, de acuerdo con el resultado de las pruebas de penetración, requieren de una acción inmediata, ya que pueden ser explotadas en el uso de la lógica de negocio del aplicativo, así también pueden ser explotadas fácilmente por un atacante poniendo en riesgo latente los activos de la institución. |
|  | **ALTA:** Equipos que, de acuerdo con el resultado de las pruebas de penetración, requieren de atención o una acción inmediata. Estas vulnerabilidades pueden ser explotadas fácilmente por un atacante poniendo en riesgo los activos de la empresa. |
|  | **MEDIA:** Estas vulnerabilidades son consecuencia de una configuración predeterminada o falta de aseguramiento en los activos. Su presencia no pone en riesgo inminente la integridad o confidencialidad de la información, sin embargo, es necesario mitigarlas. |
|  | **BAJA:** Equipos que tienen habilitados algunos puertos o servicios comunes de acuerdo al sistema operativo y que son necesarios, pero susceptibles de sufrir alguna vulnerabilidad. |
|  | **INFORMATIVA:** Notificaciones de sistema que no representan una vulnerabilidad, son de carácter informativo de algún puerto o servicio descubierto durante la aplicación de la prueba. |

# Resumen técnico de hallazgos

* Un atacante puede ingresar al sistema sin tener credenciales válidas para autenticarse en el aplicativo. Ya sea el nombre de usuario, la contraseña, o algún otro factor, no está siendo validado correctamente.
* Un atacante podría manipular el parámetro vulnerable para realizar una elevación de privilegios.
* Un atacante podría capturar credenciales en texto plano para autenticarse y manipular el sistema. Un atacante podría capturar credenciales en texto plano para autenticarse y manipular el sistema.
* Esta vulnerabilidad divulga información sensible a un atacante para completar un vector de ataque.
* Un atacante podría explotar las vulnerabilidades conocidas del componente utilizado en la aplicación.
* Al permitir el ingreso y almacenamiento de código, un atacante podría aprovechar la vulnerabilidad para obtener datos sensibles del cliente o servidor.
* La aplicación muestra en algunas ocasiones mensajes de error explícitos, lo cual puede favorecer a un atacante.

# Recomendaciones

* Se recomienda corregir el proceso validación de credenciales en el sistema.
* Se recomienda asignar privilegios mínimos para su operación a cada usuario, además de validar sus acciones y acceso a los recursos por medio de sus cookies de sesión.
* Se recomienda implementar mecanismos de verificación de integridad para asegurar que los datos no sean modificados durante el tránsito.
* Se recomienda utilizar cifrados robustos como AES256 para el envío de información, además de TLS.
* Se recomienda utilizar cifrados robustos (SHA-512, Argon2id, PBKDF2 o Bcrypt).
* Se recomienda deshabilitar cualquier código o herramienta de depuración.
* Instalar los parches de seguridad correspondientes o actualizar a la última versión del componente.
* Se recomienda implementar controles del lado del cliente que validen las entradas de los usuarios en todos los formularios.
* Se recomienda omitir todo tipo de caracteres especiales al almacenar la información en el servidor, además de verificar que dicha información corresponda exclusivamente al tipo de dato solicitado en los campos de los formularios, por ejemplo, si es un tipo de dato numérico, solo se deberán almacenar números.
* Asegúrese de que esta información no se muestre al usuario, reemplace el texto predeterminado que se muestra con un mensaje personalizado que no proporcione detalles innecesarios. Puede presentar al usuario un error genérico con un mensaje como "Error de aplicación" y un código de error para un seguimiento adicional.

# Firmas y fechas de elaboración, revisión, recepción y aprobación

**Por parte del proveedor:**

|  |  |
| --- | --- |
| Fecha: | 18/08/2021 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elabora** |  | **Revisa** |  | **Aprueba** |
| Osvaldo Hernández Morales  Operador de Controles Tecnológicos TIC Defense S.A. DE C.V. |  | Lázaro Santiago Cruz  Administrador del Centro de Operaciones de Seguridad (CiberSOC) TIC Defense S.A. DE C.V. |  | Reyes Abraham Orozco Macías  Líder del Proyecto  TIC Defense S.A. DE C.V. |

**Por parte de la secretaría:**

|  |  |
| --- | --- |
| Fecha: | 18/08/2021 |

|  |  |  |
| --- | --- | --- |
| **Recibe** |  | **Vo. Bo.** |
| Lic. Jessica Magalli Torres Mejía  Subdirectora de Seguridad Tecnológica  SRE |  | Ing. Juan Víctor Reyna Villanueva  Director de Seguridad Tecnológica  SRE |