

|  |
| --- |
| **EMPRESA** |
| **ÁREA DE SEGURIDAD** |
| **INFORME DE ANÁLISIS DINÁMICO**  **“<<name\_app>>–<<analysis\_version\_format\_01>>”**  <<analysis\_id>>  <<date\_format\_02>> |

Contenido

[I. Introducción 3](#_Toc86170925)

[II. Antecedentes 3](#_Toc86170926)

[III. Resumen Ejecutivo 3](#_Toc86170927)

[IV. Vulnerabilidades identificadas 3](#_Toc86170928)

[V. Plan de acción 4](#_Toc86170929)

[A. Objetivo general 4](#_Toc86170930)

[B. Metodología 4](#_Toc86170931)

[VI. Alcance de la evaluación 6](#_Toc86170932)

[VII. Estructura del Reporte 7](#_Toc86170933)

[VIII. Vulnerabilidades Asociadas al ambiente QA 7](#_Toc86170934)

[IX. Descripción de la criticidad 7](#_Toc86170935)

[X. Resumen técnico de hallazgos 9](#_Toc86170936)

[XI. Recomendaciones 9](#_Toc86170937)

[XII. Firmas y fechas de elaboración, revisión, recepción y aprobación 10](#_Toc86170938)

# Introducción

El equipo de seguridad informática de NUESRA EMPRESA por parte del equipo de pruebas de penetración, realiza el <<analysis\_version\_format\_02>> 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 <<request\_date\_format\_01>> con número de oficio <<REQUEST\_FOLIO>> por parte de <<responsible\_01>>, <<responsible\_charge\_01>>, para realizar el <<analysis\_version\_format\_02>> análisis de vulnerabilidades a los siguientes componentes:

* **<<app\_url>>**

El equipo de seguridad de NUESRA EMPRESA procedió a realizar el análisis dinámico.

# Resumen Ejecutivo

<<executive\_resume>>

# Vulnerabilidades identificadas

A continuación, se muestra una gráfica de las vulnerabilidades identificadas durante las pruebas de penetración realizadas a **<<name\_app>>.**

|  |  |
| --- | --- |
| **CRITICIDAD** | **VULNERABILIDADES IDENTIFICADAS** |
|  |
| CRÍTICA | 1.        Autenticación inapropiada |  |

***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 **<<name\_app>>,** 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

<<scope\_table>>

# Estructura del Reporte

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

<<vulnerabilities\_tables>>

# Vulnerabilidades Asociadas al ambiente QA

En esta sección se presentan las vulnerabilidades identificadas en el ambiente “QA”, sin embargo, no se detallan en este reporte debido a que son meramente propias de este ambiente y estas quedarán mitigadas al momento de liberar el aplicativo al ambiente productivo, Posterior a su liberación, es necesario que el área solicitante del presente análisis solicite la(s) validación(es) de la(s) siguiente(s) vulnerabilidad(es):

<<qa\_vulnerabilities\_list>>

# Malas Prácticas

En esta sección se presentan las malas prácticas identificadas en el aplicativo, sin embargo, El detalle de cada una de estas se encuentra en el documento Excel “Resumen de vulnerabilidades v2.xlsx”, Posterior a su liberación, es necesario que el área solicitante del presente análisis solicite la(s) validación(es) de la(s) siguiente(s) Mala(s) práctica(s):

<<bad\_practices\_list>>

# 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

* <<risk\_list>>

# Recomendaciones

* <<recomendation\_list>>

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

**Por parte del proveedor:**

|  |  |
| --- | --- |
| Fecha: | <<date\_format\_01>> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elabora** |  | **Revisa** |  | **Aprueba** |
| <<reporter\_01>>  Persona 1 |  | XXXXXXX  Persona 2 |  | XXXXXX  Persona 2 |

**Por parte de la secretaría:**

|  |  |
| --- | --- |
| Fecha: | <<date\_format\_01>> |

|  |  |  |
| --- | --- | --- |
| **Recibe** |  | **Vo. Bo.** |
| Lic. Jessica Magalli Torres Mejía  Persona 3 |  | Ing. Juan Víctor Reyna Villanueva  Persona 4 |