# INFORME DE VULNERABILIDADES PRESENTADO COMO PARTE DE LA SOLICITUD DE CERTIFICACION BAJO LA NORMATIVA CONTEMPLADA EN LA ORDENANZA ORD. N°2927/58

Santiago de Chile, de junio de 2023

**Sres. Departamento Jurídico de la Dirección del Trabajo.**

Su despacho Estimado:

Reciba un saludo cordial y respetuoso, en ocasión de hacer entrega a su despacho de la documentación requerida para optar por la certificación del Sistema para el registro y control de asistencia que lleva por nombre Técnico y comercial **XXXXXXXXX,** el cual es un sistema que no posee autorización previa y que es presentado por primera vez ante la DT.

La solicitud es realizada por **XXXXXXX**, Rut: **XXXXXXXX**, Email: **XXXXXXXXXX** (correo electrónico al cual debe ser respondida la solicitud), quien ocupa el cargo de **CEO de la empresa** XXXXXXX, Rut de la empresa: XXXXXXXXXX, con Domicilio en: XXXXXXXXXXXXXXXXXXXXXXXXXXXXX, comuna xxxxxx, Santiago, Región Metropolitana, Chile, Email: xxxxx@xxxx.

Por su parte la empresa **certificadora** que lleva por nombre **VELTEC INFORMÁTICA Y CÍA. LTDA, con RUT: 76.201.051-8** Domiciliada en: Paris #748 oficina 71 -E, Santiago, Chile, es la responsable del diseño formulario que fue creado con base en la normativa 2927/58 y cuyo diseño está orientado a determinar que los sistemas de asistencias cumplan a cabalidad con lo que ella establece.

Veltec como empresa certificadora también se encarga asesorar a la empresa que presenta la solicitud en el llenado de la información en el formulario antes mencionado, así como también de verificar la veracidad de la misma. El **representante legal de Veltec lleva por nombre Marcial Navarro Salinas, Rut: 9.982.336-4 y su Email de contacto es el siguiente:** [**mnavarro@veltec.cl.**](mailto:mnavarro@veltec.cl)

A continuación, presentamos la firma del solicitante a través de la cual manifiesta su autorización para presentar la solicitud de certificación del sistema **xxxxxxxxxxxxx** bajo la normativa que rige los sistemas de Registro y Control de asistencia.

# Marcial Navarro Salinas xxxxxxxxxx

**R. U. T.:** 9.982.336-4 **R. U. T.: xxxxxxxxx-8**

# CEO GERENTE GENERAL

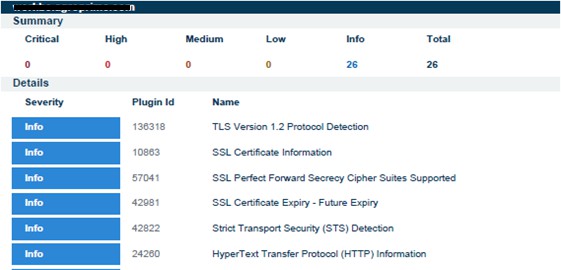
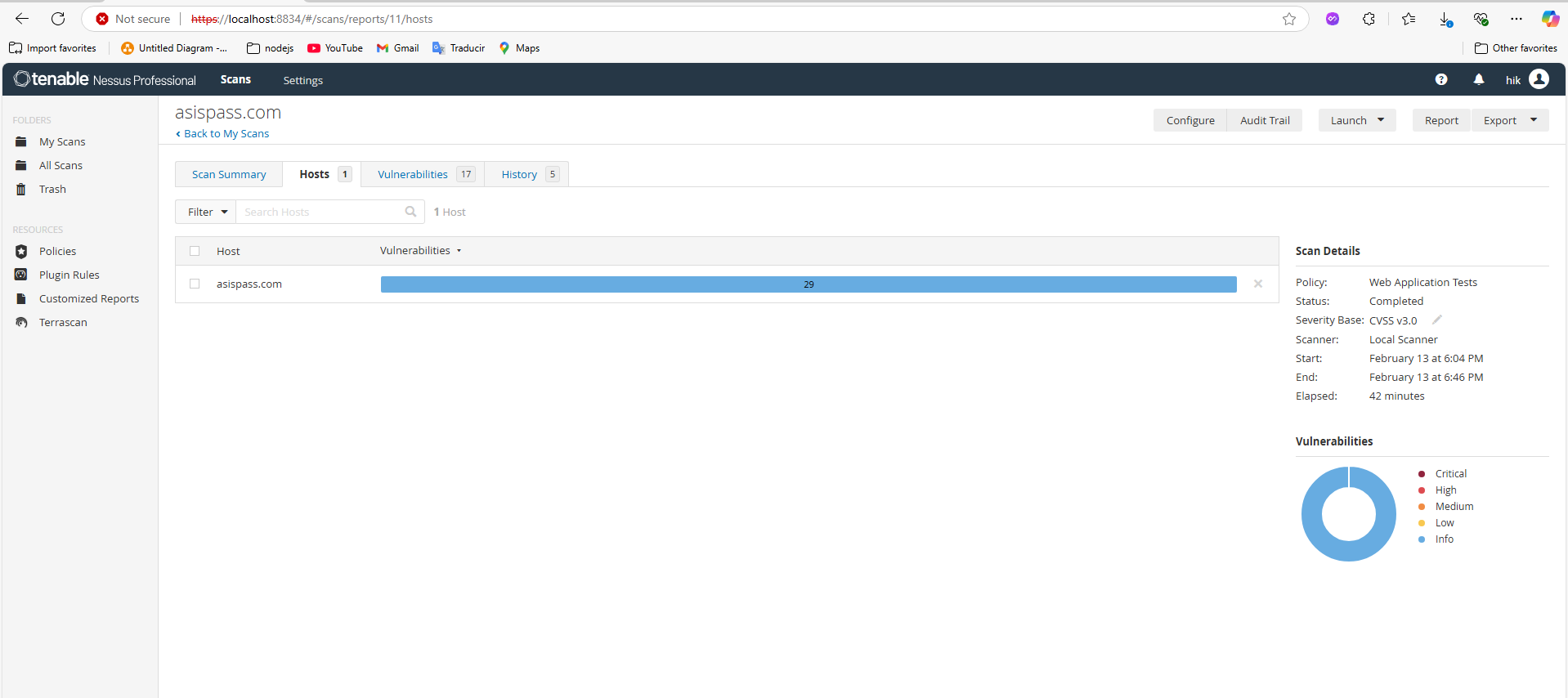
**VELTEC INFORMÁTICA Y CÍA. LTDA.** xxxxxxxxxxxxx

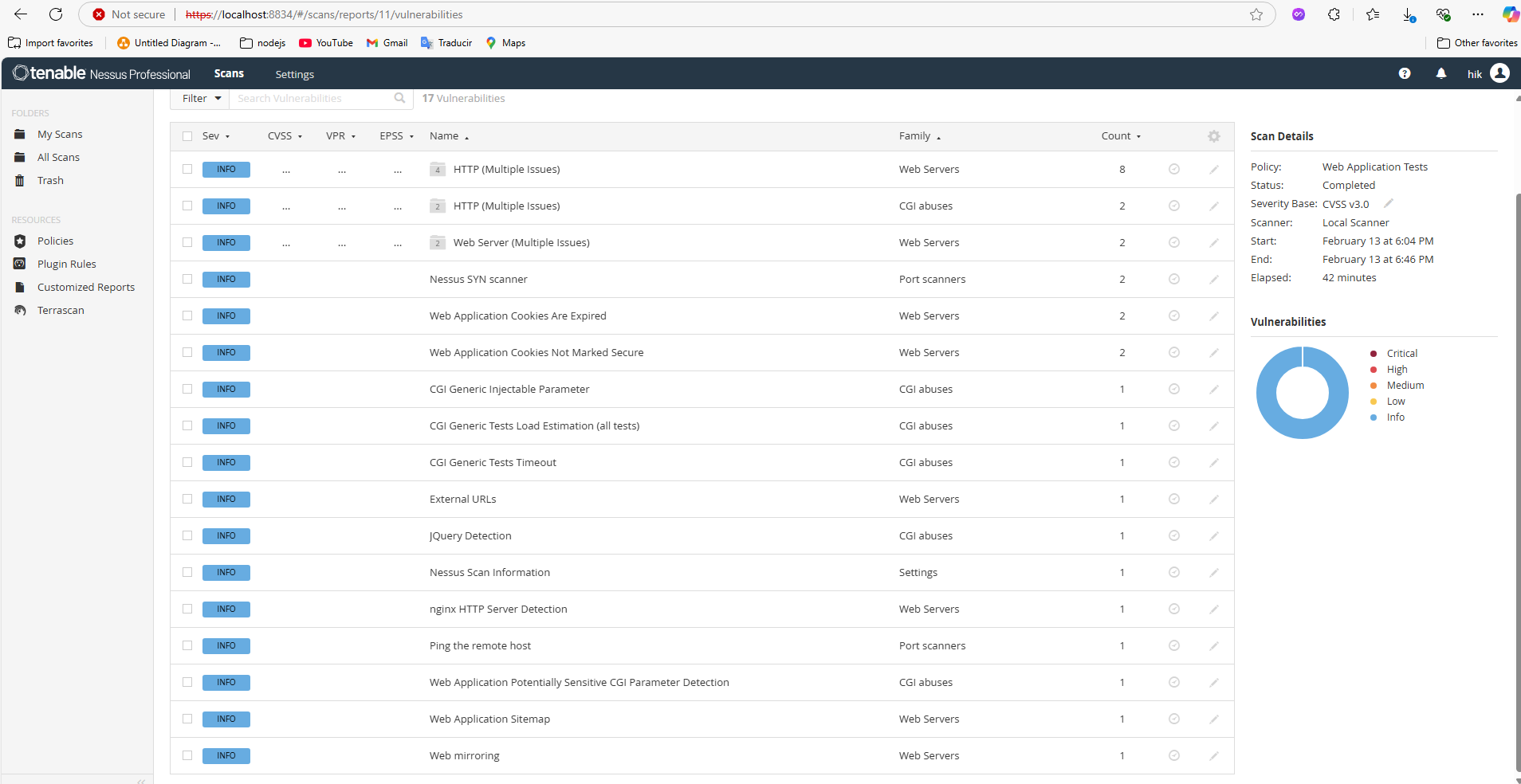
[mnavarro@veltec.cl](mailto:mnavarro@veltec.cl) xxxxxxx@xxxxxx

# RESULTADO DEL ANALISIS DE VULNERABILIDADES REALIZADO A SISTEMA AGROPRIME GESTIÓN DE PERSONAS

Se realizaron los escaneos al sistema ([asispass.com),](https://xxxxxx.cl/) a través de la herramienta Nessus (Tenable Nessus Professional 10.8.3) el día 13 de febrero del 2025, obteniendo como resultado 0 (cero) presencia de vulnerabilidades para los niveles críticas, altas, medias o bajas.

A continuación, se puede observar un segmento del resultado obtenido





# ÍNDICE DE CONTENIDOS

[INFORME DE VULNERABILIDADES PRESENTADO COMO PARTE DE LA SOLICITUD DE CERTIFICACION BAJO LA NORMATIVA CONTEMPLADA EN LA ORDENANZA ORD. N°2927/58 1](#_TOC_250003)

RESULTADO DEL ANALISIS DE VULNERABILIDADES REALIZADO A SISTEMA xxxxxxxxxxxxxxxxxxx 2

ÍNDICE 3

[INTRODUCCIÓN 4](#_TOC_250002)

[ANÁLISIS DE VULNERABILIDADES 5](#_TOC_250001)

[RESPONSABLES DEL INFORME 9](#_TOC_250000)

# INTRODUCCIÓN

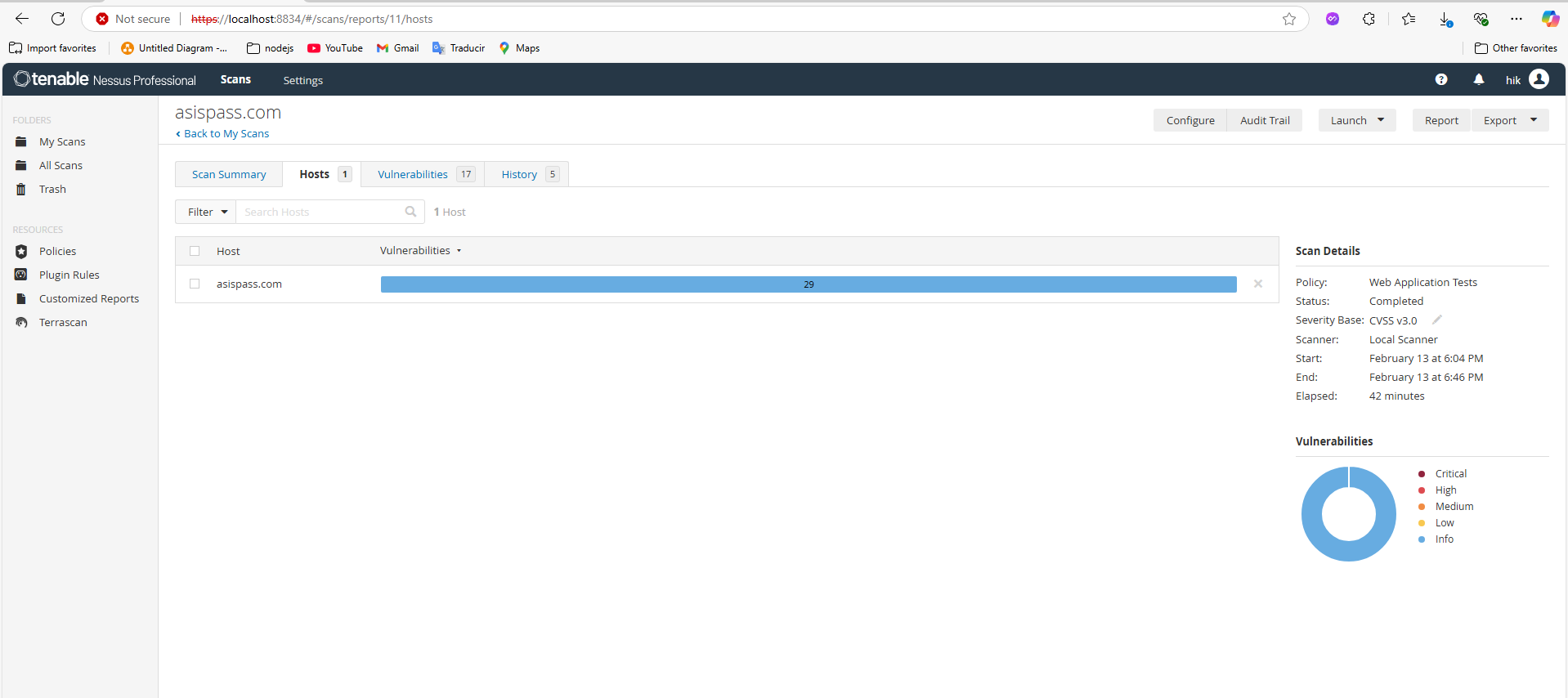
Se realizaron exploraciones de vulnerabilidad en la aplicación web seleccionada (Asispass.com), con riesgos clasificados en categorías según el nivel de amenaza y el grado de daño potencial que pueden representar. Este informe contiene los riesgos potenciales descubiertos de este análisis.

En las próximas secciones se notará como las pruebas que realizan cada uno de los plugins con los que trabaja el software de Nessus muestro de manera clara como no se presentan vulnerabilidad alguna indicándolo mediante una escala alguna.

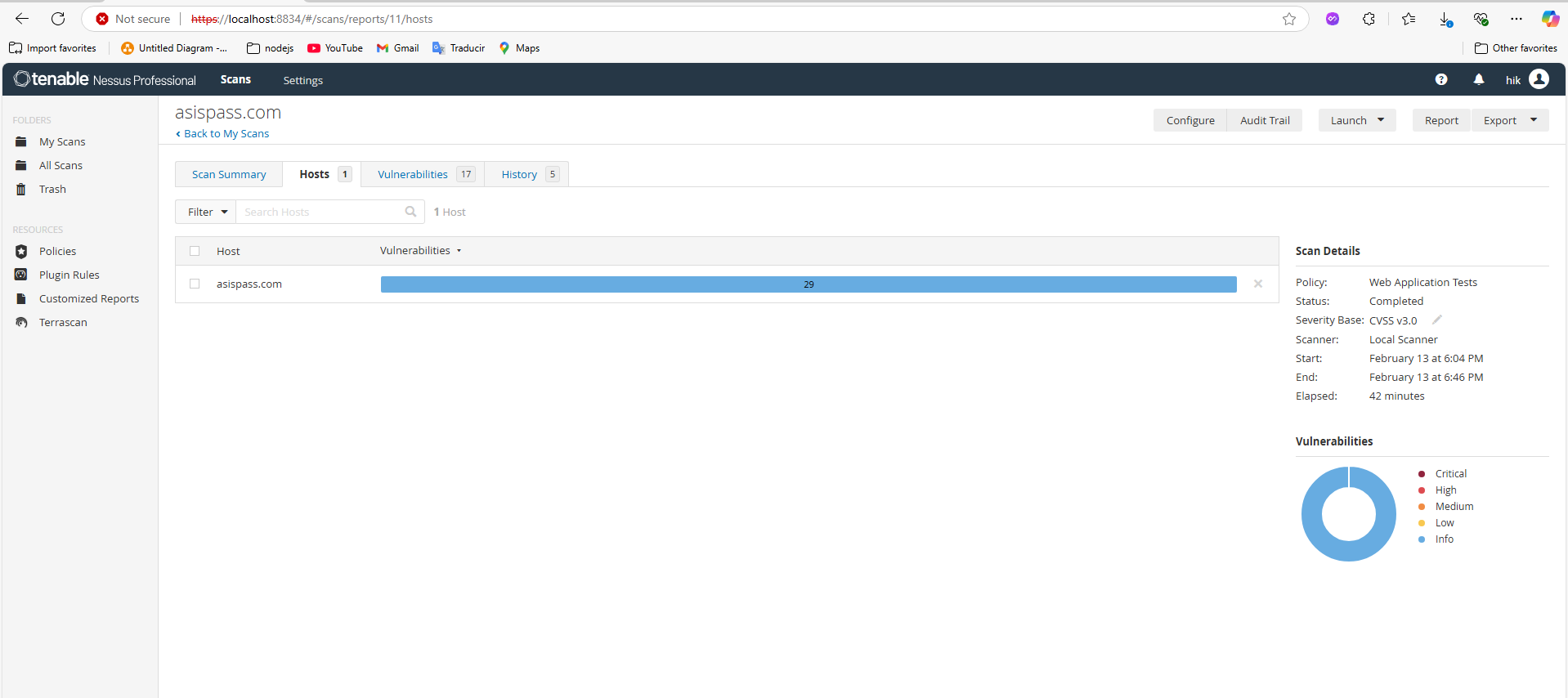
# ANÁLISIS DE VULNERABILIDADES

Se realizo el análisis de vulnerabilidad al sitio web de la solución de asistencia asispass, con el fin de encontrar puntos de vulnerabilidad que pudieran existir dentro del sistema. Del cual no encontraron vulnerabilidad alguno en las distintas categorías (Críticas, Altas, Medias o Bajas).

Por lo que continuación, presentamos imágenes del test realizado, sin embargo, junto con el informe se entregan los reportes que arroja la herramienta de testeo. Primero mostramos una imagen donde se muestra una vista completa de todo el reporte



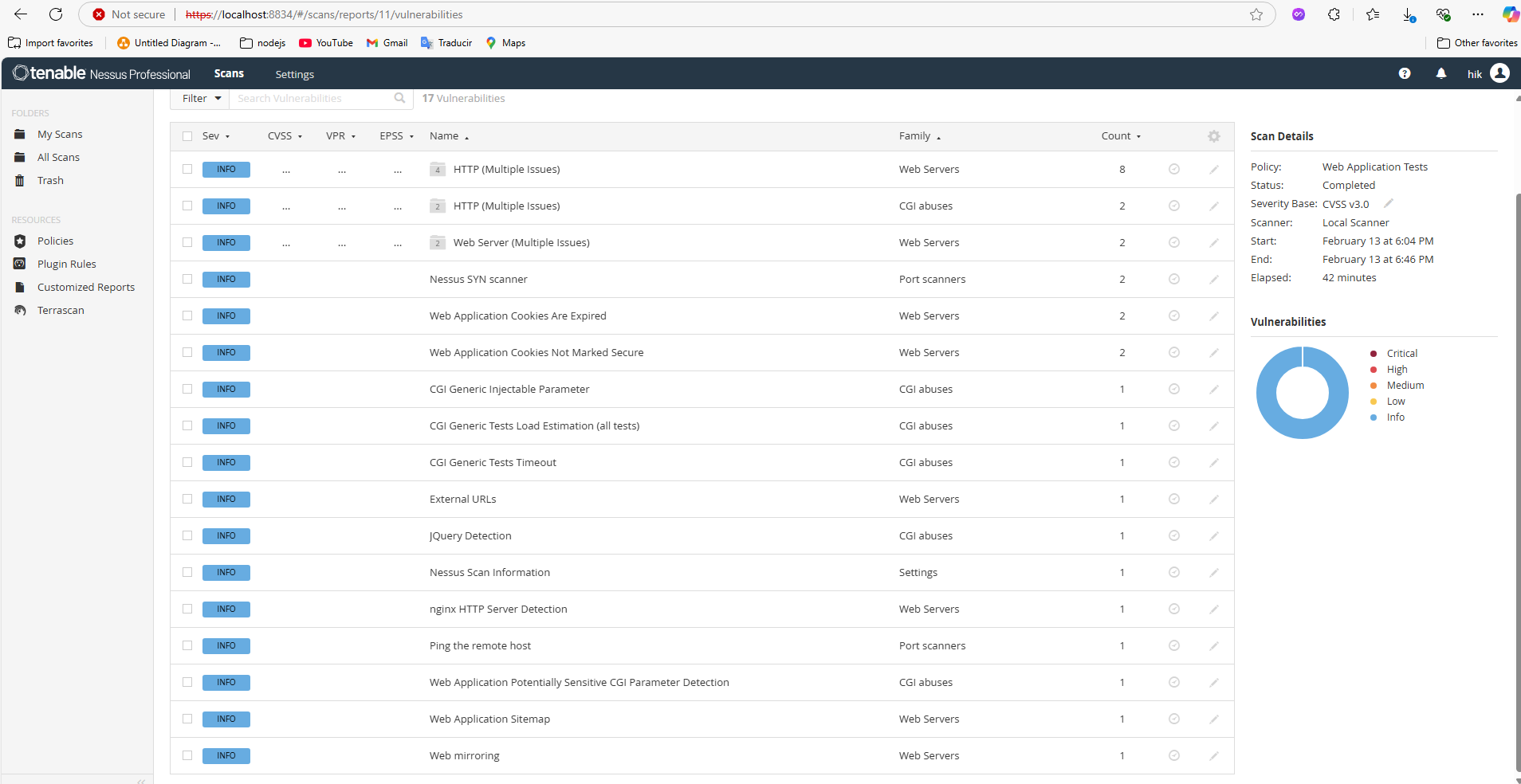
En la siguiente imagen mostrare como Nessus clasifica sus vulnerabilidades:



De manera simple indica lo siguiente:

* **Critical**: simplemente no hay opción ni espera, si existe una vulnerabilidad que este en este campo; hay que darle prioridad sobre todo.
* **High**: Altamente prioritarias y donde es una vulnerabilidad completamente delicada ya que pone en peligro la estabilidad del sistema.
* **Medium**: son vulnerabilidades que tienden a dar problema de funcionalidad y donde los usuarios del sistema están vulnerables en cuanto a bastante ataques.
* **Low**: son algunas vulnerabilidades donde son recomendaciones y en cierto modo no representan ningún peligro aun, pero se recomiendo tomarlas en cuenta.
* **Info**: son simplemente información o datos que indican que estamos en un buen estado pero que son consejos que da el sistema para lo mejora en futuros elementos. No son vulnerabilidades sino

A continuación, muestro como se ven las imágenes de cada uno de los elementos estudiados en nuestro sistema

En conclusión, luego de los análisis de vulnerabilidades practicados aplicación web Asispass.com que forma parte de la solución de asistencia AutomatismosLau LTDA, se pudo observar que no se encontraron vulnerabilidades de nivel críticas, altas, medias o bajas, y solo un grupo de sugerencias que serán evaluadas para futuros desarrollos.

# RESPONSABLES DEL INFORME

****

# Marcial Navarro Salinas xxxxxxxxxxxxx

**R. U. T.:** 9.982.336-4 **R. U. T.: xxxxxxxxx-8**

# CEO Director Ejecutivo Gerente General

# VELTEC INFORMÁTICA Y CÍA. LTDA. xxxxxxxxxxxxx

[mnavarro@veltec.cl](mailto:mnavarro@veltec.cl) [**xxxxxxxx@xxxxx.cl**](mailto:xxxxxxxx@xxxxx.cl)