UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Actividad 17

Evaluación de Vulnerabilidades con CVSS v3.1

Integrantes:

Coronado Noriega Jesús Olaf	178991
De La Rosa Rodríguez Erik	177700
González Reyes Felipe de Jesús	181134
Mendoza Aguado Karina	179859
Serrano Zermeño Leonardo	177301
Pérez Ventura Juan Alejandro	180370

Materia:

CNO V: Seguridad Informática

Docente:

Servando López Contreras

San Luis Potosí, S.L.P.
15 de mayo de 2026

Índice

1. Introduccion

El presente documento desarrolla la evaluacion de una vulnerabilidad detectada en un sistema web interno mediante el modelo **CVSS v3.1** (*Common Vulnerability Scoring System*). A partir del escenario proporcionado, se identifican las metricas base, se construye la cadena vector, se calcula la puntuacion con la calculadora oficial de FIRST y se interpreta tecnicamente la severidad obtenida.

El proposito del analisis no es unicamente obtener un numero, sino justificar el riesgo en un contexto organizacional. Por ello, se explica por que la vulnerabilidad conserva relevancia aunque requiera privilegios elevados, que tipo de atacante podria explotarla y que implica que el impacto sea bajo en confidencialidad, integridad y disponibilidad.

2. Objetivos

2.1. Objetivo general

Aplicar el modelo CVSS v3.1 para evaluar la gravedad de una vulnerabilidad, interpretando correctamente sus metricas base y justificando la priorizacion del riesgo en un contexto organizacional.

2.2. Objetivos especificos

1. Identificar y comprender las metricas base de CVSS v3.1: AV, AC, PR, UI, S, C, I y A.
2. Construir correctamente una cadena vector CVSS a partir de un escenario tecnico.
3. Calcular la puntuacion base usando la calculadora oficial de FIRST.
4. Interpretar tecnicamente el resultado para priorizar acciones de mitigacion.

3. Escenario de evaluacion

Una organizacion detecta una vulnerabilidad en un sistema web interno con las siguientes caracteristicas:

Caracteristica	Descripcion del escenario
Vector de ataque	Puede explotarse a traves de la red.
Complejidad de ataque	La explotacion requiere baja complejidad.
Privilegios requeridos	Se necesitan privilegios elevados.
Interaccion del usuario	No requiere interaccion del usuario.
Alcance	No cambia el alcance.
Impacto en confidencialidad	Bajo.
Impacto en integridad	Bajo.
Impacto en disponibilidad	Bajo.

Tabla 1: Caracteristicas tecnicas de la vulnerabilidad evaluada.

4. Construccion del vector CVSS v3.1

La construccion del vector se realiza con base en las metricas base de CVSS v3.1. Cada valor se asigna directamente a partir de una caracteristica del escenario.

4.1. Asignacion de metricas base

Metrica	Valor	Justificacion tecnica
Attack Vector (AV)	Network (N)	La vulnerabilidad puede explotarse a traves de la red. Por ello, el vector de ataque corresponde a *Network*.
Attack Complexity (AC)	Low (L)	La explotacion requiere baja complejidad; no depende de condiciones especiales ni de estados poco probables del sistema.
Privileges Required (PR)	High (H)	El atacante necesita privilegios elevados para explotar la vulnerabilidad, por lo que la metrica se clasifica como *High*.
User Interaction (UI)	None (N)	No se requiere que otro usuario ejecute una accion, abra un archivo, acepte una solicitud o interactue con el sistema.

Metrica	Valor	Justificacion tecnica
Scope (S)	Unchanged (U)	El escenario indica que no cambia el alcance; el impacto permanece dentro del mismo componente o dominio de seguridad vulnerable.
Confidentiality (C)	Low (L)	El impacto en confidencialidad es bajo, lo que indica exposicion parcial o limitada de informacion.
Integrity (I)	Low (L)	El impacto en integridad es bajo, por lo que la alteracion de informacion o comportamiento es acotada.
Availability (A)	Low (L)	El impacto en disponibilidad es bajo, lo cual representa afectacion parcial del servicio, sin interrupcion total.

Tabla 2: Asignacion de metricas CVSS v3.1 con base en el escenario.

4.2. Cadena vector resultante

Con base en la asignacion anterior, el vector CVSS v3.1 correcto es:

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

Este vector representa una vulnerabilidad explotable por red, de baja complejidad, sin interaccion del usuario, con privilegios requeridos altos, sin cambio de alcance y con impactos bajos en confidencialidad, integridad y disponibilidad.

5. Calculo de la puntuacion

La puntuacion fue calculada en la calculadora oficial de CVSS v3.1 del sitio FIRST, disponible en:

https://www.first.org/cvss/calculator/3.1

El resultado obtenido para el vector evaluado fue el siguiente:

Elemento evaluado	Resultado
Cadena vector	`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L`
Puntuacion base	**4.7**
Severidad	**Media** / *Medium*
Rango de clasificacion	4.0–6.9

Tabla 3: Resultado del calculo CVSS v3.1.

Interpretacion inmediata del resultado: la puntuacion base de **4.7** ubica la vulnerabilidad en severidad **media**. No es un hallazgo critico, pero tampoco debe ignorarse, porque puede explotarse por red, requiere baja complejidad y no necesita interaccion del usuario.

6. Evidencia del uso de la calculadora oficial

La Figura 1 muestra la evidencia principal del uso de la calculadora oficial de FIRST. En la captura se observan las metricas base seleccionadas, el vector generado y la puntuacion **4.7 Medium**.

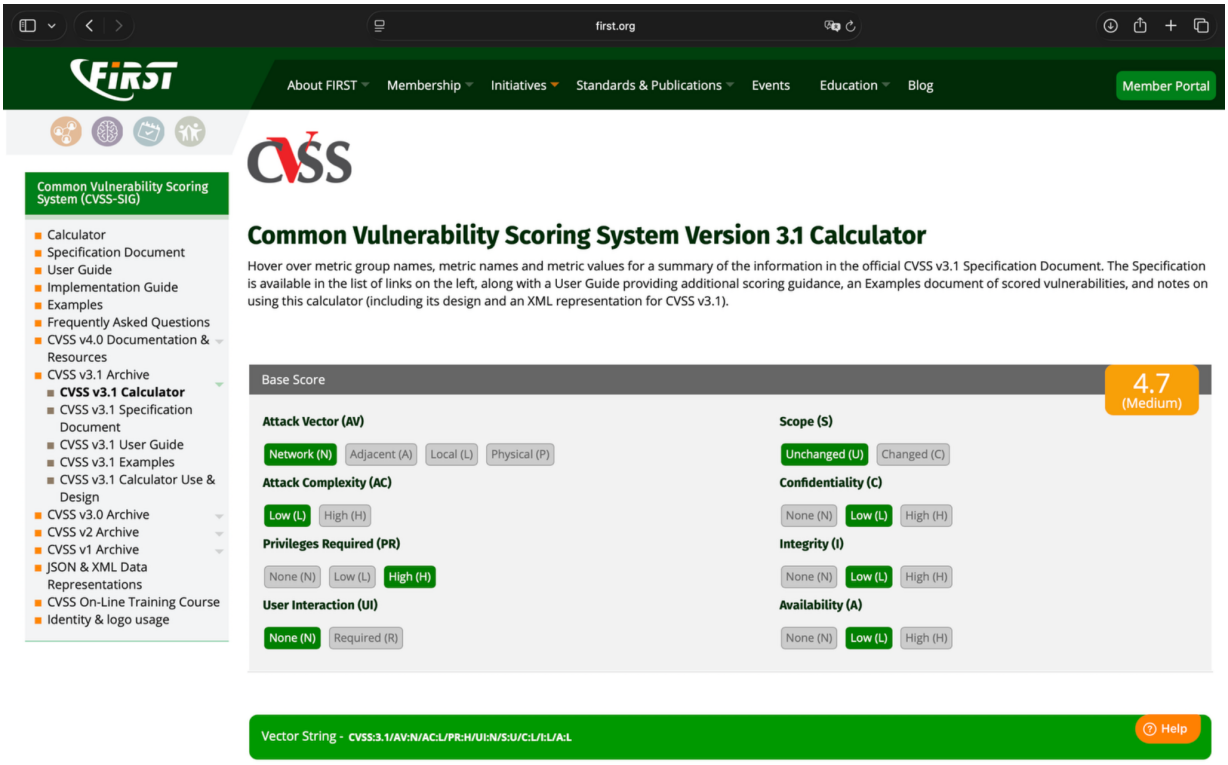

Figura 1: Captura de la calculadora oficial CVSS v3.1 con las metricas base seleccionadas y puntuacion 4.7 Medium.

La evidencia confirma que la cadena vector introducida en la herramienta fue:

`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L`

y que la puntuacion base calculada por FIRST corresponde a **4.7**, clasificada como **Medium**.

7. Interpretacion tecnica

7.1. Relevancia de la vulnerabilidad aunque requiere privilegios elevados

Aunque la vulnerabilidad requiere privilegios elevados, sigue siendo relevante porque ese requisito no elimina el riesgo; solamente reduce el numero de atacantes capaces de explotarla directamente. En un entorno real, un atacante puede obtener privilegios altos mediante robo de credenciales, reutilizacion de contraseñas, mala gestion de accesos, sesiones administrativas expuestas o escalamiento previo de privilegios. Una vez que el atacante cuenta con esos

permisos, la explotacion seria relativamente directa porque el vector es de red, la complejidad es baja y no se requiere interaccion de otro usuario.

Por lo tanto, esta vulnerabilidad no debe descartarse por tener *PR:H*. En seguridad organizacional, una falla que requiere privilegios elevados puede formar parte de una cadena de ataque mas amplia, especialmente cuando existen debilidades en control de accesos, administracion de cuentas o monitoreo de actividades privilegiadas.

7.2. Tipo de atacante que podria explotarla

El atacante mas probable seria un usuario interno con permisos elevados, un administrador malicioso, un exempleado cuya cuenta no fue revocada o un atacante externo que previamente comprometio una cuenta privilegiada. Tambien podria explotarla un adversario que combine esta vulnerabilidad con otros fallos, por ejemplo: acceso inicial mediante phishing, obtencion de credenciales administrativas y posterior abuso de la vulnerabilidad en el sistema web interno.

Esto significa que el riesgo no se limita a amenazas externas. Tambien debe analizarse desde la perspectiva de amenaza interna, abuso de privilegios y deficiencias en la gestion de identidades.

7.3. Significado de impacto bajo en confidencialidad, integridad y disponibilidad

Que el impacto sea bajo en confidencialidad, integridad y disponibilidad significa que la vulnerabilidad no permite comprometer completamente el sistema, extraer toda la informacion, modificar datos criticos de forma masiva ni dejar el servicio totalmente fuera de operacion. Sin embargo, si puede generar afectaciones parciales: exposicion limitada de datos, alteracion acotada de registros o degradacion menor del servicio.

En terminos de priorizacion, esto indica que la vulnerabilidad debe atenderse, pero no necesariamente con la misma urgencia que una vulnerabilidad alta o critica. Su tratamiento debe programarse dentro del proceso de remediacion, especialmente porque podria combinarse con otras debilidades del entorno.

8. Analisis de riesgo y priorizacion

La vulnerabilidad obtiene una puntuacion base de **4.7**, por lo que se clasifica como **Media**. Esta categoria refleja que el riesgo es real y debe gestionarse, pero que su severidad se encuentra limitada por dos factores principales: requiere privilegios elevados y los impactos tecnicos son bajos.

Aspecto	Analisis
Probabilidad de explotacion	Moderada. Requiere privilegios elevados, pero una vez obtenidos, la explotacion es sencilla por su baja complejidad.
Impacto tecnico	Bajo en confidencialidad, integridad y disponibilidad.
Exposicion	Relevante, ya que puede explotarse a traves de la red.
Prioridad de atencion	Media. Debe corregirse, pero puede priorizarse despues de hallazgos altos o criticos.
Riesgo organizacional	Puede aumentar si existen cuentas privilegiadas mal protegidas, ausencia de MFA, credenciales compartidas o monitoreo insuficiente.

Tabla 4: Analisis de priorizacion del riesgo.

9. Recomendaciones de mitigacion

Para reducir el riesgo asociado a esta vulnerabilidad, se proponen las siguientes acciones:

1. **Aplicar el principio de minimo privilegio:** limitar los permisos de cada usuario a lo estrictamente necesario.
2. **Auditar cuentas privilegiadas:** revisar cuentas administrativas activas, compartidas, obsoletas o sin justificacion operativa.
3. **Implementar autenticacion multifactor:** especialmente en cuentas con privilegios elevados o acceso a sistemas internos sensibles.
4. **Monitorear acciones administrativas:** registrar accesos, cambios de configuracion y operaciones criticas.
5. **Corregir la vulnerabilidad:** aplicar parche, ajuste de configuracion o control compensatorio segun corresponda.

6. **Validar la remediacion:** repetir pruebas despues de la correccion para confirmar que el vector ya no sea explotable bajo las mismas condiciones.

10. Conclusion

La vulnerabilidad evaluada mediante CVSS v3.1 obtuvo una puntuacion base de **4.7**, correspondiente a una severidad **Media**. El vector construido fue:

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

La puntuacion no es alta porque la explotacion requiere privilegios elevados y los impactos sobre confidencialidad, integridad y disponibilidad son bajos. Sin embargo, la vulnerabilidad sigue siendo relevante porque puede explotarse por red, requiere baja complejidad y no depende de la interaccion del usuario. En un ambiente organizacional, este tipo de hallazgo debe atenderse con prioridad media, acompañado de controles de acceso, monitoreo de cuentas privilegiadas y validacion posterior de la remediacion.

11. Anexos de evidencia complementaria

Las siguientes capturas complementan la evidencia del calculo. En ellas se observa que las metricas temporales y ambientales permanecen como *Not Defined*, por lo que la calificacion base de **4.7 Medium** no fue modificada por ajustes adicionales.

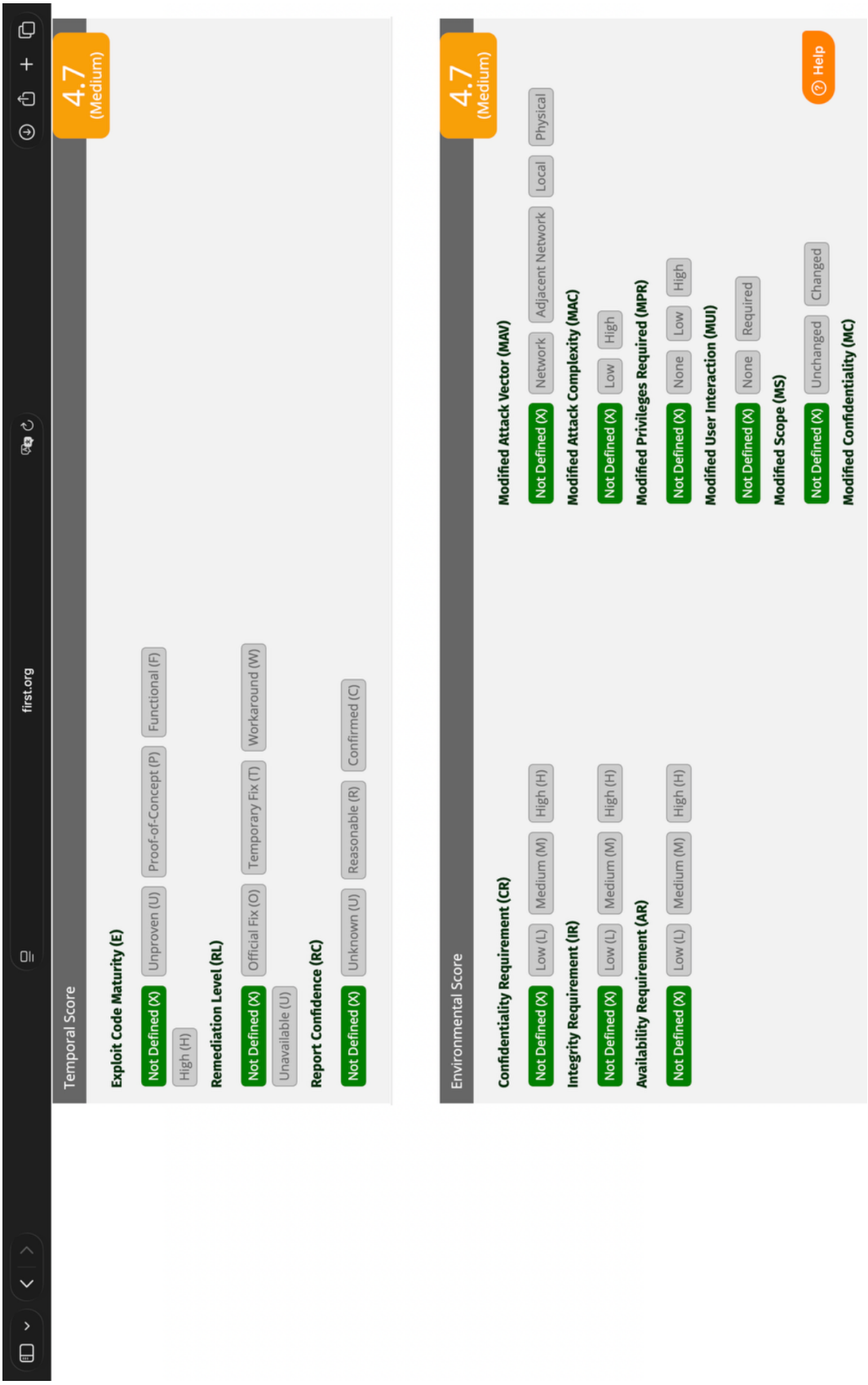

Figura 2: Captura complementaria de metricas temporales y ambientales en estado Not Defined.

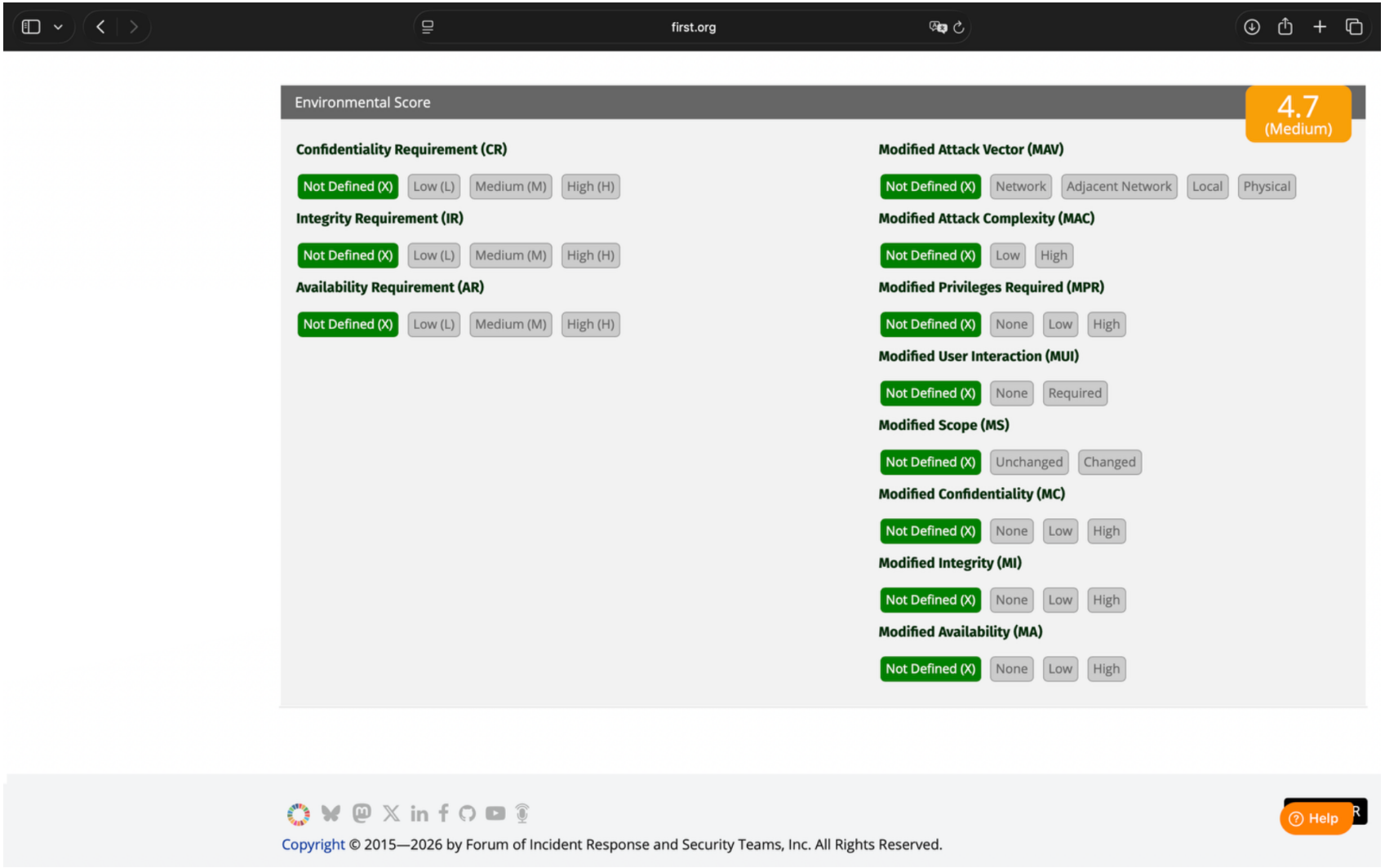

Figura 3: Captura complementaria de metricas ambientales en estado Not Defined y puntuacion conservada de 4.7 Medium.

Referencias

FIRST. (s. f.). *Common Vulnerability Scoring System Version 3.1 Calculator*. Recuperado de https://www.first.org/cvss/calculator/3.1

FIRST. (s. f.). *Common Vulnerability Scoring System v3.1: Specification Document*. Recuperado de https://www.first.org/cvss/v3.1/specification-document