

Informe de Supervisión # 1

CONTRATO No 1559 de 2024

Periodo del Informe: 20 de enero de 2025 al 19 de febrero de 2025

El supervisor del contrato hace constar que se ha realizado seguimiento a las actividades de la empresa **PASSWORD CONSULTING SERVICES S.A.S.**, quien ha concurrido en cada una de las citaciones y emitido un informe técnico para las actividades realizadas durante el periodo: **20 de enero de 2025 al 19 de febrero de 2025**

Periodo facturado: **20 de enero de 2025 al 19 de febrero de 2025**

Primer pago correspondiente al 50% del valor total del contrato, una vez se hayan realizado las pruebas de Ethical hacking de acuerdo con lo descrito en el anexo técnico, previa validación del informe de actividades y resultados por parte del supervisor del contrato.

Se da cumplimiento a lo establecido en el contrato, el contratista presenta un informe con:

- Metodología para las pruebas de Hacking Ético.
- Identificación de vulnerabilidades.
- Pruebas de hacking ético.
- Generación y socialización de resultados.
- Retest.
- Criterios de clasificación de vulnerabilidades.
- Tiempos de remediación
- Herramientas para explotación de vulnerabilidades
- Resultados de las pruebas de seguridad
- Explotación a la vulnerabilidad “Eternalblue” (Exitosa)
- Vulnerabilidad de firma SMB no requerida “SMB Signing not Required”
- Prueba de inyecciones SQL
- Prueba de inyecciones Cross-Site Scripting XSS (Parcialmente Exitosa)
- Verificación de seguridad de aplicaciones web.

Presentan pruebas de Ethical Hacking a los objetivos seleccionados por parte de la Entidad a nivel interno y externo en donde se incluya entre otras: enumeración de servicios, identificación de puertos y demás información de los activos. Mediante el uso de herramientas y estándares internacionalmente aceptadas, configuradas y programadas específicamente para validar o detectar vulnerabilidades técnicas en las plataformas de TRANSMILENIO acorde con la sección alcance del presente informe.

Presentan la metodología de análisis de vulnerabilidad utilizada en la infraestructura tecnológica de TRANSMILENIO, en pro de identificar todos los hallazgos existentes y posibles en la Entidad, y a su vez, proporcionar recomendaciones de seguridad que permitan mitigar en gran medida los hallazgos obtenidos a raíz de dicho procedimiento.

Nota: El presente informe se complementa con el informe de actividades presentado por el contratista donde se evidencia la prestación de servicios para la realización de un test de intrusión (ethical hacking), en cada una de las etapas que se surtieron los con los ajustes requeridos en cada una de las etapas.

Se verificó de igual manera el pago por concepto de parafiscales correspondiente al periodo del informe de actividades.

Cordialmente



JAVIER ALFONSO CASTAÑEDA PARRA
PROFESIONAL ESPECIALIZADO_06 TIC's