00/12/2021

Plan de pruebas de seguridad

Pruebas de seguridad sobre el portal UNIDAD NACIONAL DE PROTECCIÓN

El presente documento contiene el plan de pruebas de seguridad sobre las URL expuestas a internet de las aplicaciones remitidas por la UNIDAD NACIONAL DE PROTECCIÓN el objetivo de la prueba es identificar vulnerabilidades y dar las recomendaciones para mitigar el riesgo asociado a la explotación de las vulnerabilidades identificadas**.**

A continuación, se describen los puntos a ser tenidos en cuenta para llevar a cabo la actividad.

1. Alcance.
2. Requisitos.
3. Restricciones.
4. Contactos.
5. Metodología.
6. Entregable.
7. Ventana de actuación.

1. Alcance

El alcance de las pruebas de las pruebas está limitado a la URLs reportadas:

Portal – https://unp.gov.co
Ser web - https://ser.unp.gov.co/
Gedoc - https://bpm.unp.gov.co/
Correo – https://correo.unp.gov.co/owa
PQRS-WEB – https://pqrs.unp.gov.co

2. Requisitos

Para garantizar la correcta ejecución de las pruebas se debe cumplir con los siguientes requisitos:

- Las URLs descritas en el alcance deben estar activas.

- Para el análisis de las URLs que requieren credenciales y si así lo acepta la Entidad, deben ser entregados dos (2) usuarios de acceso uno privilegiado y otro sin privilegios. Se recomienda que estos usuarios deben ser creados solo para las pruebas a realizar y deben estar activos en el tiempo que se vayan a realizar las mismas, luego de esto deben ser eliminados.

3. Restricciones

- No se realizarán durante la ejecución de las pruebas ataques de Ingeniería social.
- No se realizarán durante las pruebas ataques de denegación de servicio.
- NO se realiza explotación de las vulnerabilidades encontradas.

4. Contactos

Nombre y apellido	Email	Teléfono
Franz Edwar Rojas Montañez	Franz.rojas@unp.gov.co	3185780351
Juan Manosalva	Juan.manosalva@unp.gov.co	3228494642
David Yacel Espinosa Vanegas	David.espinosa@unp.gov.co	300302371
Emil Mena	emena@mintic.gov.co	3016008406
Alexander Molina Sánchez	amsanchez@mintic.go.co	3204861055

5. Metodología

Las ejecuciones de las pruebas se realizan bajo las metodologías de pruebas de seguridad OSSTMM y OWASP, las actividades que se ejecutaran sobre los objetivos descritos en el alcance se describen a continuación:

Inicialmente se realiza una recolección y análisis de datos, con el fin de obtener la mayor información posible sobre el sistema a evaluar. De esta forma se podrá realizar un análisis más eficiente y productivo durante la siguiente fase, la cual consiste en la identificación de vulnerabilidades existentes.

- Identificación de servidores y análisis de puertos TCP/UDP
- Determinar servicios y versiones existentes en la máquina
- Análisis de las vulnerabilidades según servicio y versión
- Verificar los métodos HTTP (OPTIONS, TRACE…)
- Búsqueda de versiones antiguas y malas configuraciones
- Detección de fugas de información
- Búsqueda de información indexada por buscadores
- Búsqueda de información no indexada por buscadores

Con los datos obtenidos durante la primera fase, se procederá en un segundo tiempo a un análisis más exhaustivo en modalidad “Caja Negra” de los servidores donde se encuentras los

servicios web, con objeto de determinar posibles vulnerabilidades sobre el Sistema Operativo, sus aplicaciones y servicios (en caso de que aplique).

- Análisis SSL
- Analizar la versión de SSL
- Verificar la validación de los certificados digitales
- Verificar que no se pueda acceder a recursos por canales no seguros (SSL skip)
- Explotación de vulnerabilidades SQL
- Explotación de vulnerabilidades Xpath
- Explotación de vulnerabilidades LDAP
- Explotación de vulnerabilidades CSPP
- Explotación de vulnerabilidades XSS (Cross-Site Scripting)
- Modificación de parámetros
- Acceso a directorios/archivos no autorizados
- Análisis de servicios web
- Análisis de cookies y sesiones
- Determinar la información de la administración de la sesión
- Chequear si la misma información de sesión puede ser reutilizada en otra máquina / IP
- Determinar las limitaciones y cierres de la sesión

Para establecer las clasificaciones de impacto, se sigue como base la recomendación de la NVD, Base de Datos Nacional de Vulnerabilidades, en base a los resultados de los CVSS:

- La vulnerabilidad etiquetada de 'Crítica' tiene un CVSS base de puntuación entre 9.6 y 10.0.
- La vulnerabilidad etiquetada de 'Alta' tiene un CVSS base de puntuación entre 7.0 y 9.5.
- La vulnerabilidad etiquetada de 'Media' tiene un CVSS base de puntuación entre 4.0 y 6.9.
- La vulnerabilidad etiquetada de 'Baja' tiene un CVSS base de puntuación entre 0.1 y 3.9.
- La vulnerabilidad etiquetada de 'Información' tiene un CVSS base de puntuación de 0.0.

6. Entregable

Un solo informe que contiene, un resumen ejecutivo del resultado de las pruebas y un detallado técnico y recomendaciones de remediación de las vulnerabilidades encontradas.

Este informe será entregado a la Entidad cuatro (4) días hábiles después de terminada la prueba.

7. Ventana de actuación

Las pruebas se ejecutarán durante el periodo del 09 al 13 de diciembre de 2021, en una ventana de tiempo de las 07:00 hasta las 23:00 hora Colombia.

ITEM	URL	FECHA	HORA INICIO	HORA FIN
1	Portal – https://unp.gov.co	09/12/2021	07:00 am	11:00 pm
2	Correo – https://correo.unp.gov.co/owa	13/12/2021	07:00 am	11:00 pm
3	Gedoc - https://bpm.unp.gov.co/	Por Definir		
4	Ser web - https://ser.unp.gov.co/	Por definir		
5	PQRS-WEB – https://pqrs.unp.gov.co	Por definir		

Definiciones:

Vulnerabilidad: Un error, falla, debilidad, o la exposición de una aplicación, sistema, dispositivo o servicio que podría dar lugar a un incumplimiento de la confidencialidad, integridad o disponibilidad.

Amenaza: La frecuencia o probabilidad de que un hecho dañino se produzca.

Riesgo: Probable ocurrencia de que un atacante explote un fallo de seguridad en un activo determinado, en base a las amenazas existentes y al impacto potencial que representaría para el negocio de la compañía.

Activo: Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La empresa asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.

Confidencialidad: Garantía de que únicamente accederán a la información los elementos autorizados para ello, y que dichos elementos no van a convertir esa información en disponible para otras entidades.

Integridad: Garantía de que la información únicamente puede ser modificada por elementos autorizados asegurando métodos de proceso exactos y completos.

Disponibilidad: Garantía de que la información y los activos relacionados deben estar accesibles a elementos autorizados en tiempo, modo y lugar adecuado.

Si tienes alguna consulta técnica comunicarse con CSIRT Gobierno a través de los siguientes canales:

Csirtgob@mintic.gov.co

01 8000 910742 Opción 2.