|  |
| --- |
|  |
| **EJEMPLO** |
| **EJEMPLO** |

EJEMPLO

(Statement of Work – SOW)

**“<<Nombre\_del\_aplicativo\_portada>>”**

<<Fecha\_mes\_y\_año>>

**<<Folio>>**

Contenido

[A. Antecedentes 3](#_Toc78876204)

[B. Alcance de la presente Declaración de Trabajo (SOW) 3](#_Toc78876205)

[C. Actividades 3](#_Toc78876206)

[D. Agenda de trabajo 4](#_Toc78876207)

[E. Acuerdos 4](#_Toc78876208)

[F. Firmas de aceptación de la Declaración de Trabajo (SOW) 5](#_Toc78876209)

# Antecedentes

De acuerdo con la solicitud <<request\_folio>> realizada por el director de área, persona, con el fin de realizar el <<analysis\_version\_format\_02>> análisis de vulnerabilidades al sistema **<<Nombre\_del\_aplicativo\_En\_antecedentes>>**,se procederá a realizar el análisis dinámico.

# Alcance de la presente Declaración de Trabajo (SOW)

Este servicio tiene como alcance pruebas de seguridad en los siguientes activos tecnológicos de la CLIENTE:

|  |  |
| --- | --- |
| Nombre del aplicativo | <<Nombre\_del\_aplicativo\_Tabla>> |
| Nombre del servidor | <<Nombre\_del\_servidor>> |
| Dirección IP | <<Dirección\_IP>> |
| Tipo de Revisión | Análisis dinámico (pentest) |
| Fechas de Inicio | <<Fechas\_de\_inicio>> |
| Fecha Fin | <<Fecha\_Fin>> |
| Horario de pruebas | 9:00 a 18:00 hrs. |

# Actividades

Para cumplir con los objetivos mencionados en el numeral anterior, CLIENTE está de acuerdo en que “EMPRESA”, deberá llevar a cabo las siguientes actividades:

|  |  |  |  |
| --- | --- | --- | --- |
| Actividad | Técnica Empleada | Nivel de Riesgo | Riesgos Identificados |
| 1. Acceder a instancia del aplicativo por la URL | Consultas a la URL con directorios comunes o con herramienta que escanea todas las instancias del aplicativo. | Alto | Acceso a medios restringidos. |
| 1. Inyección de comandos o Código. | Introducción de comandos en los campos de texto. | Alto | Obtener información del servidor y el aplicativo. |
| 1. Subir archivo script. | Carga de archivos por un gestor de archivos en el aplicativo. | Alto | Obtener información del servidor y escalar privilegios de usuario. |
| 1. Escaneo de tráfico de solicitudes HTTP | Herramienta escaneo de tráfico por capa de presentación HTTP. | Medio | Obtener el token de sesión (cookie) y credenciales de acceso. |
| 1. Identificar vulnerabilidad por componente. | Escaneo mediante herramienta para identificar vulnerabilidades. | Bajo | Obtener información de las versiones y conocer si pueden explotarse por una vulnerabilidad registrada en el CVE NIST. |

# Agenda de trabajo

Por la intrínseca naturaleza de las pruebas de seguridad que serán ejecutadas, la siguiente tabla presenta el rango de fechas entre las cuales se llevará a cabo cada prueba. En todos los casos CLIENTE entiende y acepta que se lleven a cabo dichas pruebas, en el entendido que “EMPRESA” podrá realizarla cualquier día comprendido entre el rango indicado, sin previa notificación a CLIENTE, esto con el propósito de que la simulación se ejecute en las condiciones más cercanas a la operación normal de CLIENTE.

|  |  |  |
| --- | --- | --- |
| Actividad | Fecha Tentativa de Inicio | Fecha límite para la actividad |
| 1. Acceder a instancia del aplicativo por la URL | <<Fecha\_tentativa\_de\_inicio>> | <<Fecha\_límite\_para\_la\_actividad>> |
| 1. Inyección de comandos o Código. | <<Fecha\_tentativa\_de\_inicio>> | <<Fecha\_límite\_para\_la\_actividad>> |
| 1. Subir archivo script. | <<Fecha\_tentativa\_de\_inicio>> | <<Fecha\_límite\_para\_la\_actividad>> |
| 1. Escaneo de tráfico de solicitudes HTTP | <<Fecha\_tentativa\_de\_inicio>> | <<Fecha\_límite\_para\_la\_actividad>> |
| 1. Identificar vulnerabilidad por componente. | <<Fecha\_tentativa\_de\_inicio>> | <<Fecha\_límite\_para\_la\_actividad>> |

# Acuerdos

Con el propósito de no afectar a los sistemas de la CLIENTE durante la ejecución de las actividades descritas, La Secretaría y “EMPRESA” acuerdan:

|  |
| --- |
| Acuerdos |
| 1. Obtener una cuenta para acceder a través <<Concordancia\_2>> [<<URL\_Acuerdos\_tabla3>>](#_top) y realizar las pruebas en esas instancias. |
| 1. Obtener los privilegios para acceder <<Concordancia\_3>> [<<URL\_Acuerdos\_tabla3>>](#_top) y realizar las pruebas en esas instancias del portal. |
| 1. Liberación <<Concordancia\_2>> [<<URL\_Acuerdos\_tabla3>>](#_top) una vez hecha la remediación de las vulnerabilidades identificadas en el análisis dinámico (PenTest). |

# Firmas de aceptación de la Declaración de Trabajo (SOW)

|  |  |  |
| --- | --- | --- |
| **Área solicitante** | **Realiza** | **Área solicitada** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  <<Realiza\_Firmas\_de\_aceptación>> | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Tecnológica  CLIENTE |