

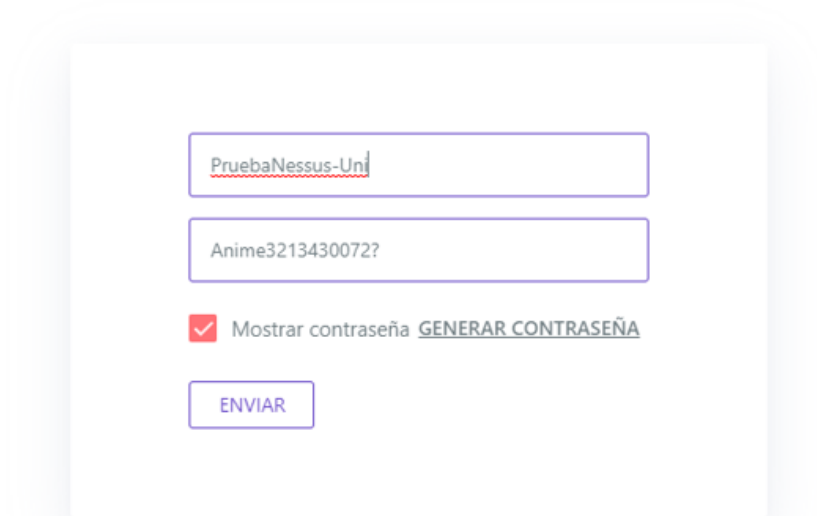
WORDPRESS

A. Descripción del proceso desarrollado para la instalación y el escaneo de un sitio web con WordPress

Primero se ingresa con el correo a 000webhost y luego se inicia un proyecto, en donde solicitan un nombre que en mi caso puso PruebaNessus-Uni y una contraseña

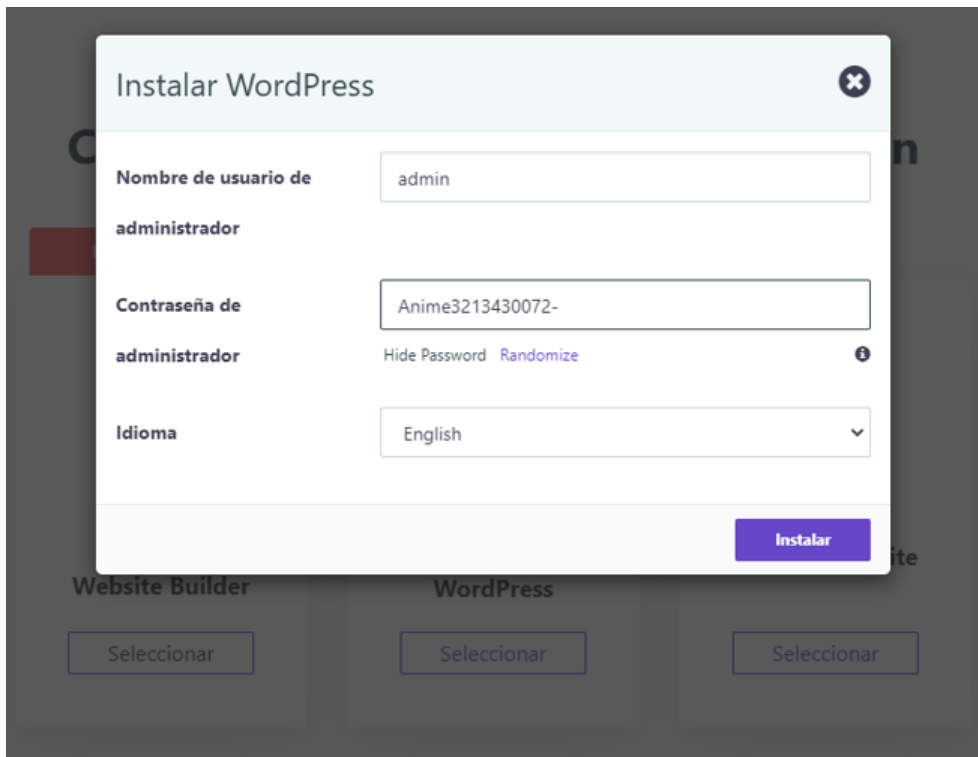
A great start is half the work

Name Your Project

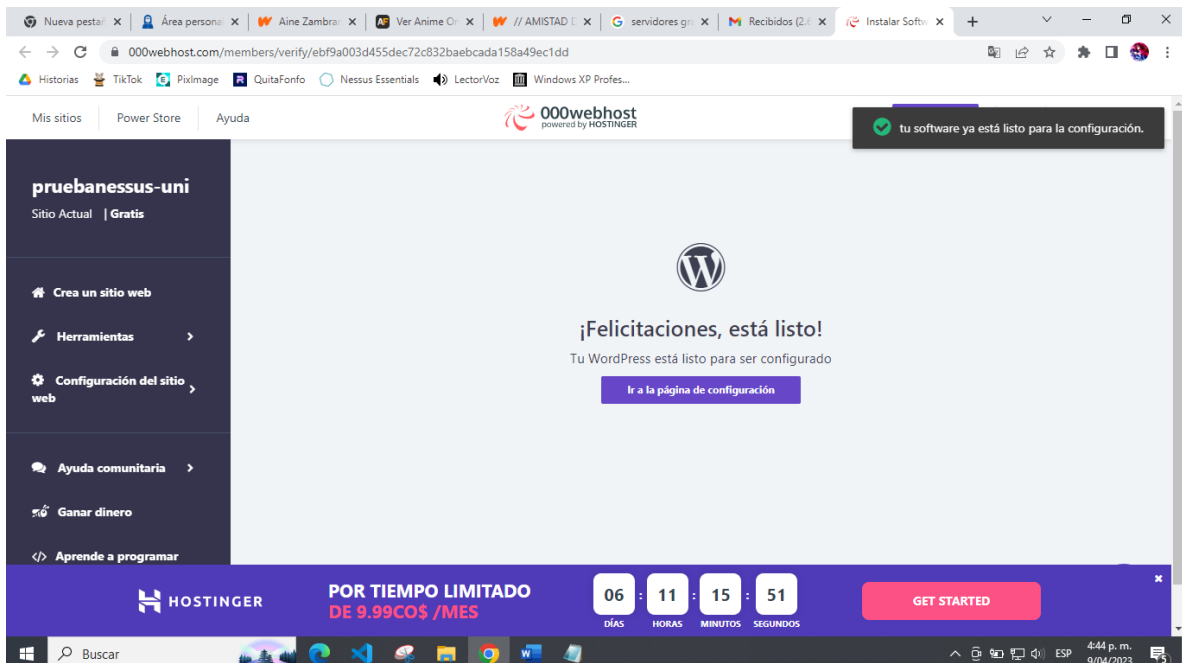


The screenshot shows a web form titled "Name Your Project" with a light blue background. It contains two text input fields. The first field is labeled "Project Name" and contains the text "PruebaNessus-Uni". The second field is labeled "Password" and contains the text "Anime3213430072?". Below the password field, there is a red checkmark icon followed by the text "Mostrar contraseña" and a link that says "GENERAR CONTRASEÑA". At the bottom of the form is a blue button labeled "ENVIAR".

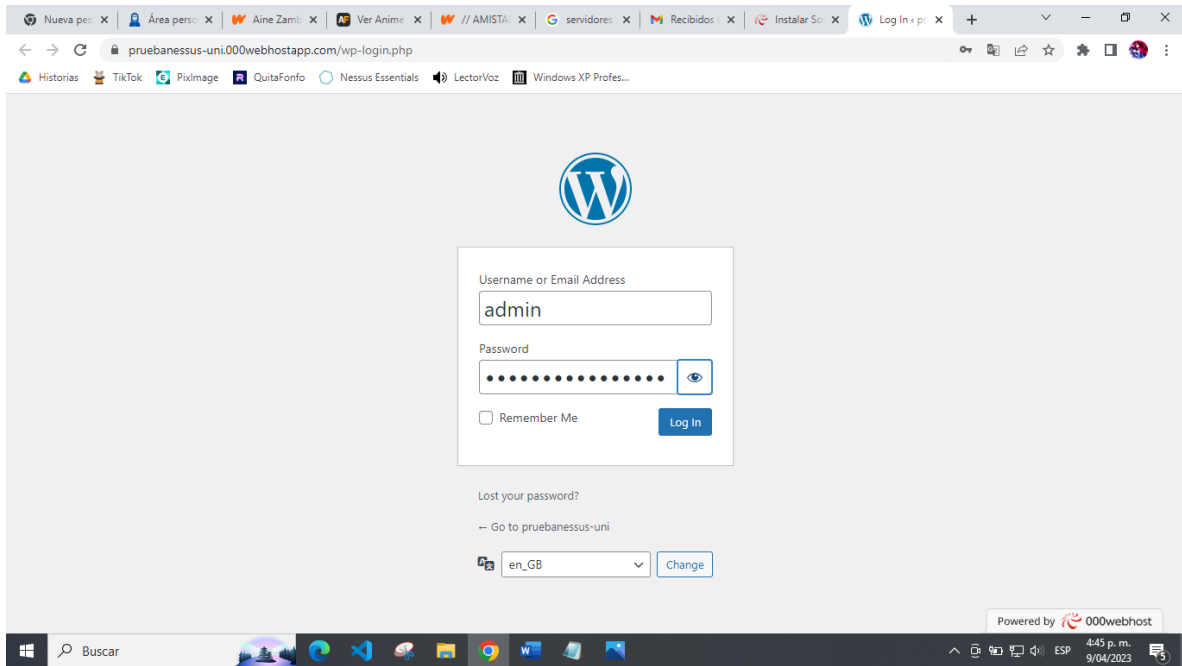
Luego se selecciona la opción e instalar el WordPress en el 000webhost



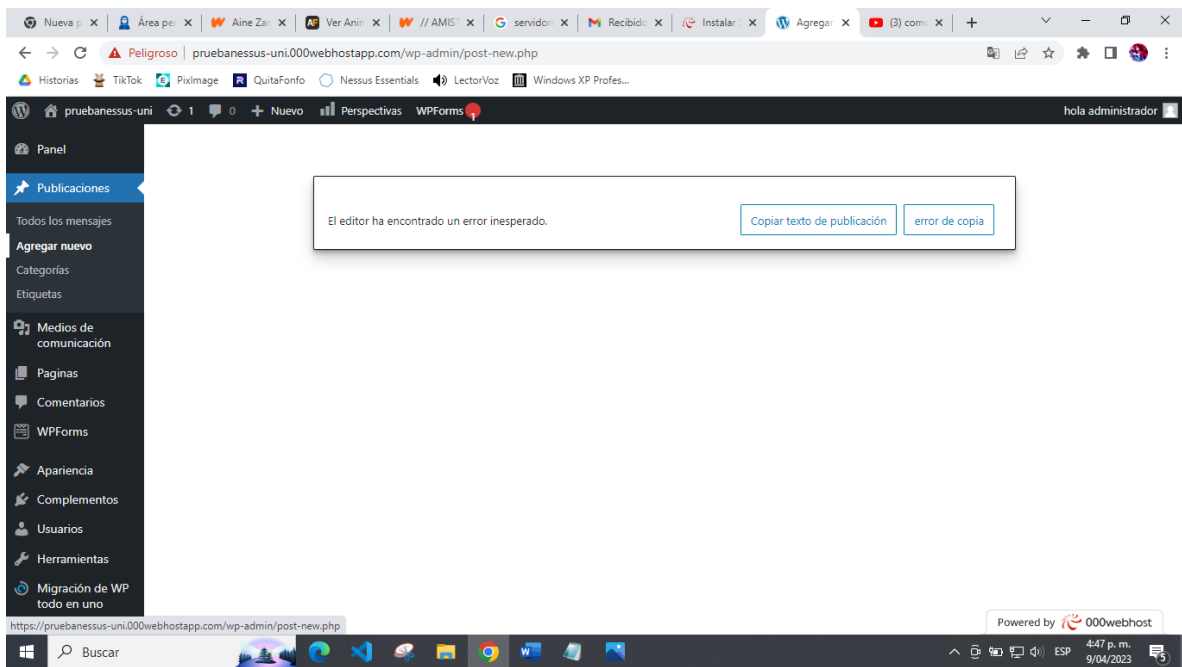
Esperamos unos pocos minutos para que se termine la descarga del WordPress y cuando este listo, damos clic a Ir a la página de configuración

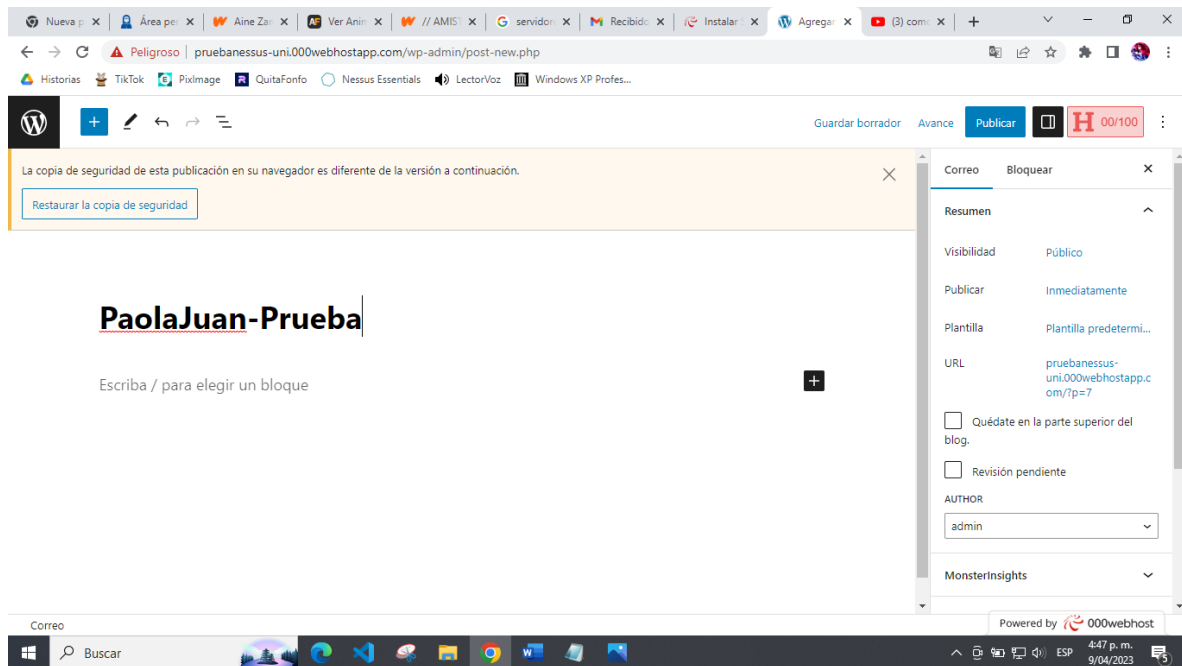


Para poder ingresar a las configuraciones y crear un sitio nos solicitan el usuario y la contraseña

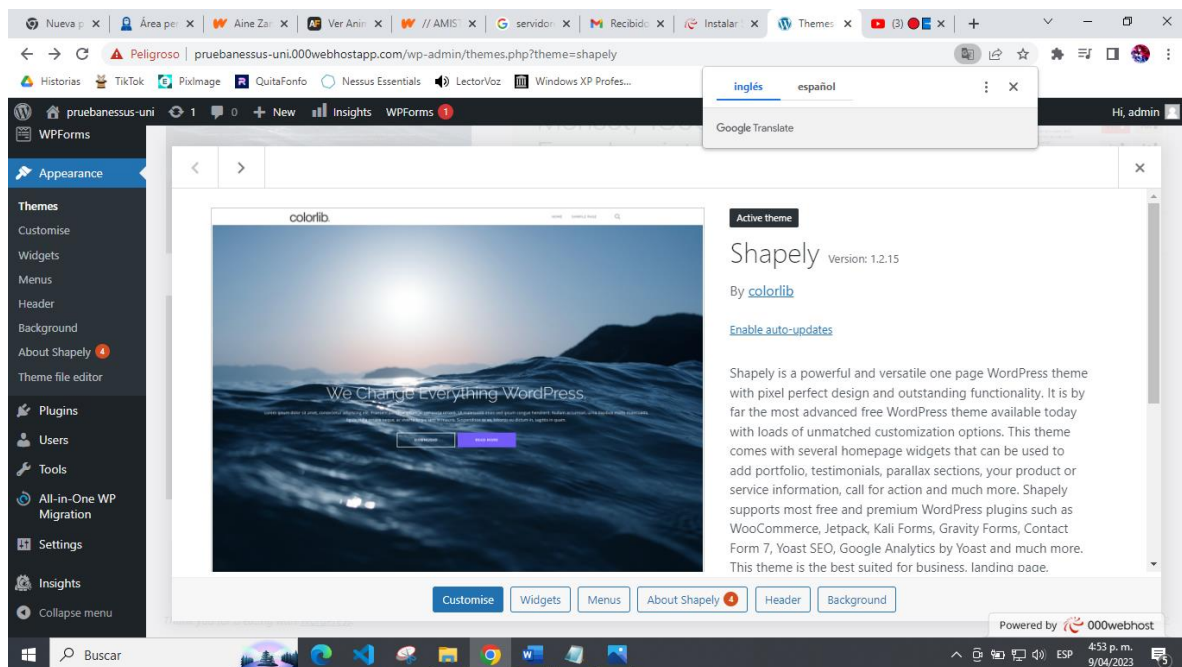


Luego creamos una publicación nueva con solo el título y damos clic al botón de **publicar**

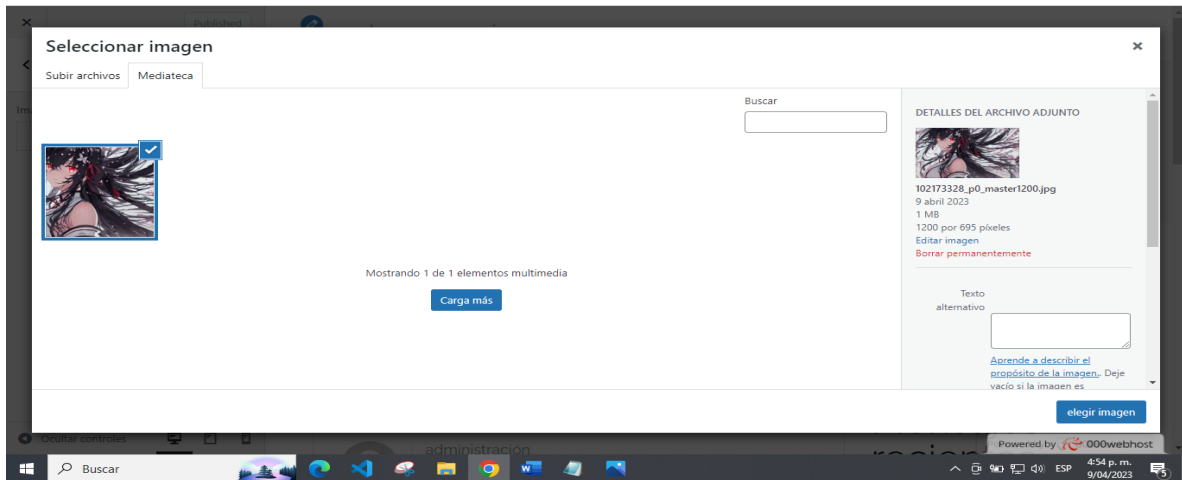
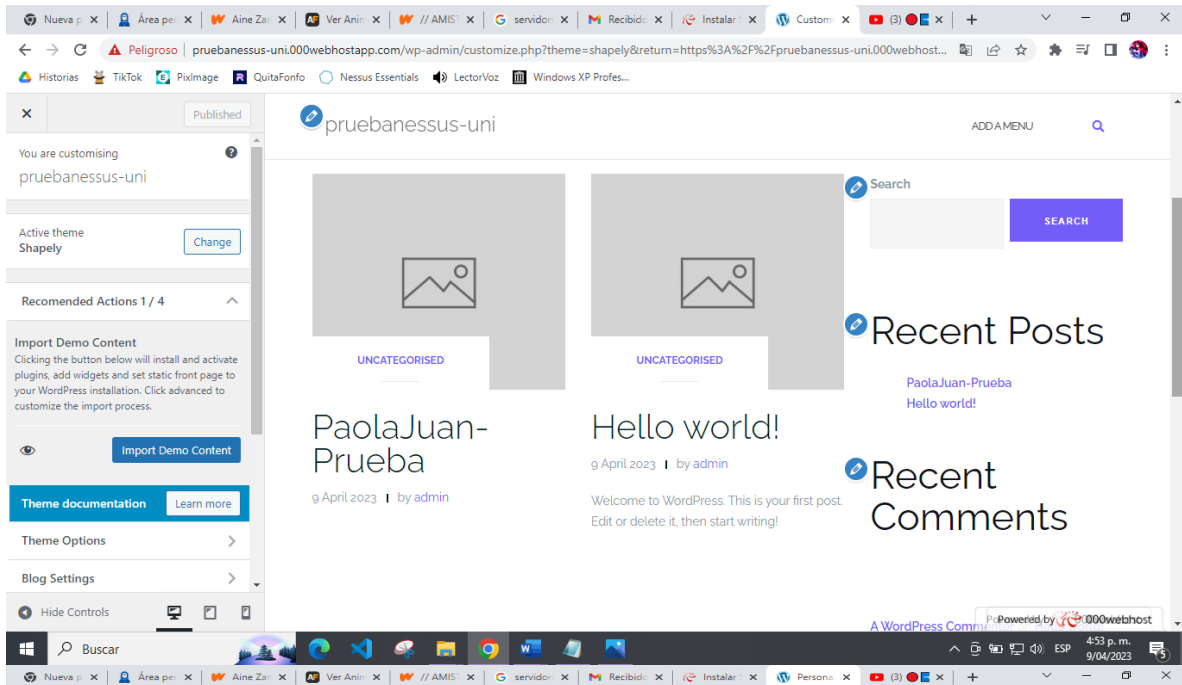


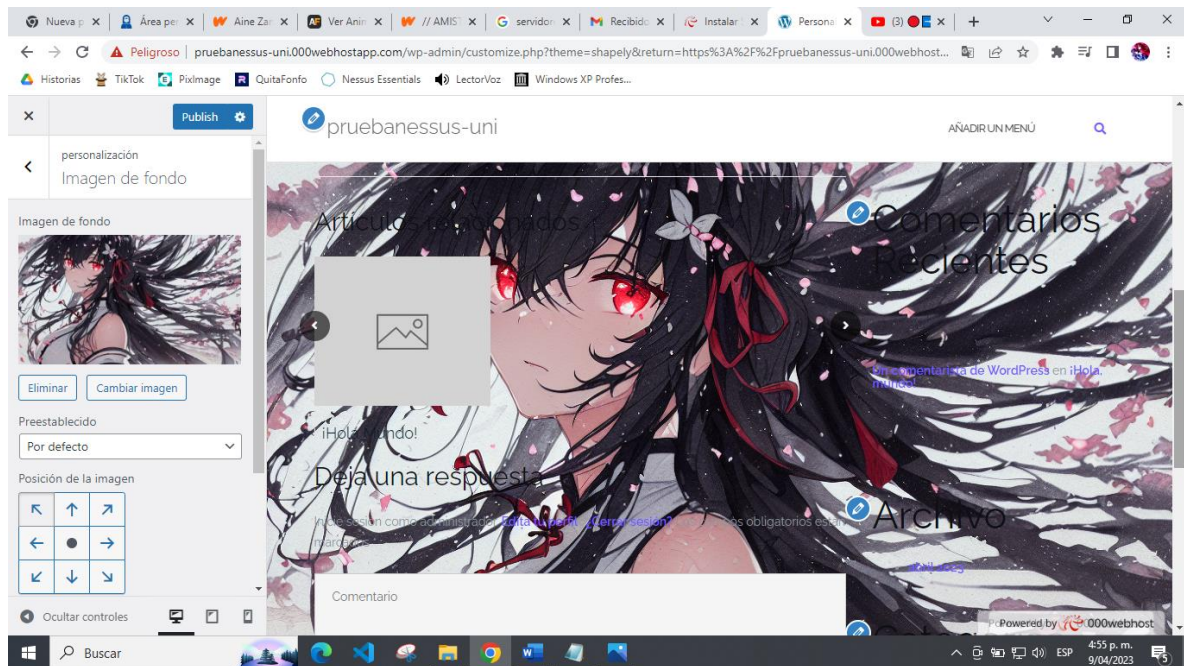


Luego se busca una apariencia del sitio web y se la activa al dar clic al botón **Customise**

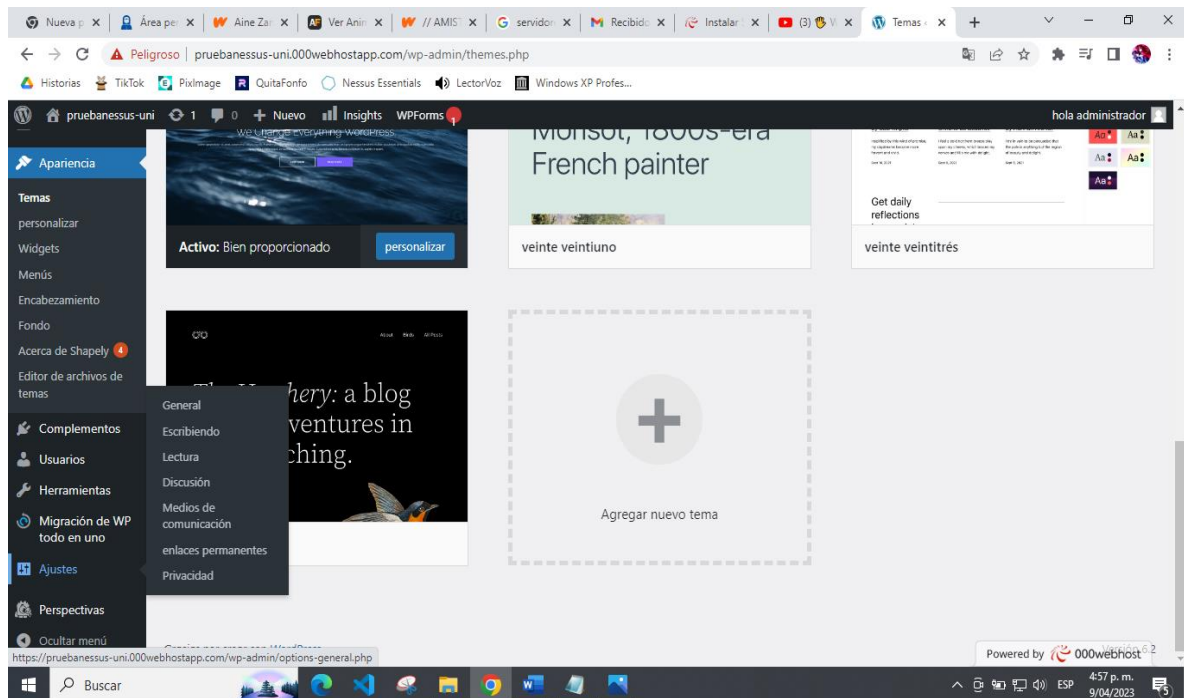


Como se puede observar se escoge la anterior publicación para editarla. Pero como solo vamos a comprobar las vulnerabilidades que nos da Nessus solo agrego una imagen para su decoración

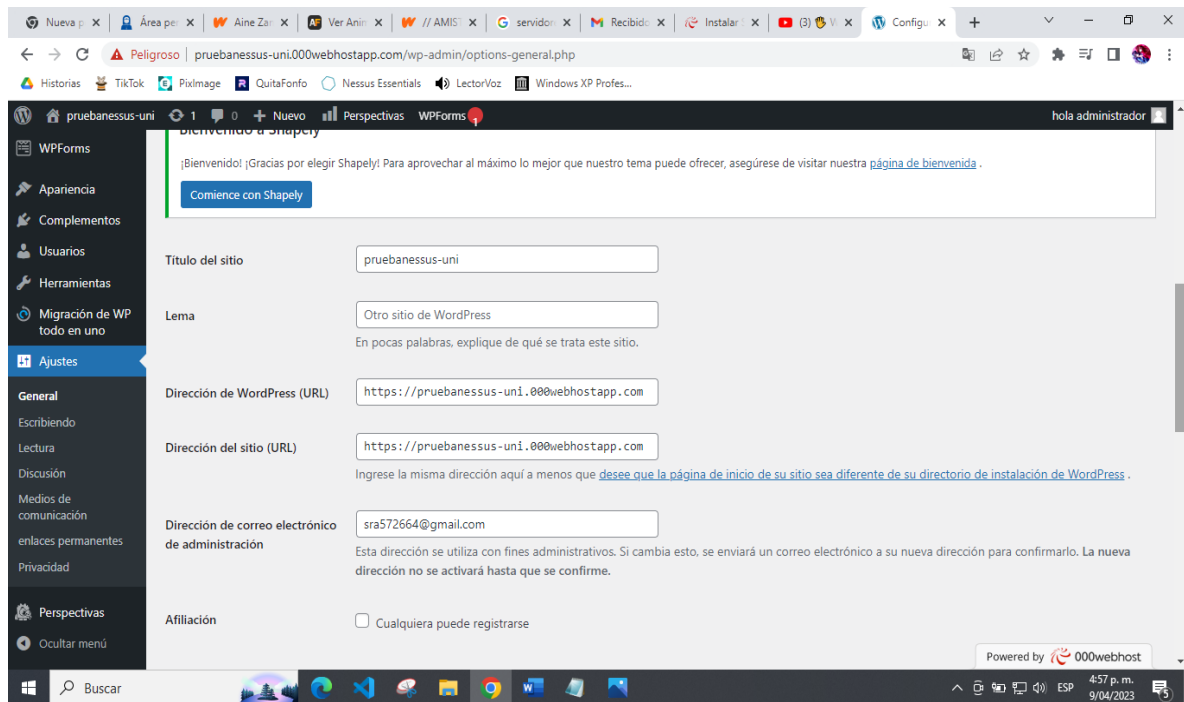




Para poder sacar el link de esta pagina creado con WordPress, nos ubicamos en las opciones laterales y damos clic a **Ajustes**, después a **General**



Copiamos la dirección url que aparece y luego nos dirigimos a Nessus



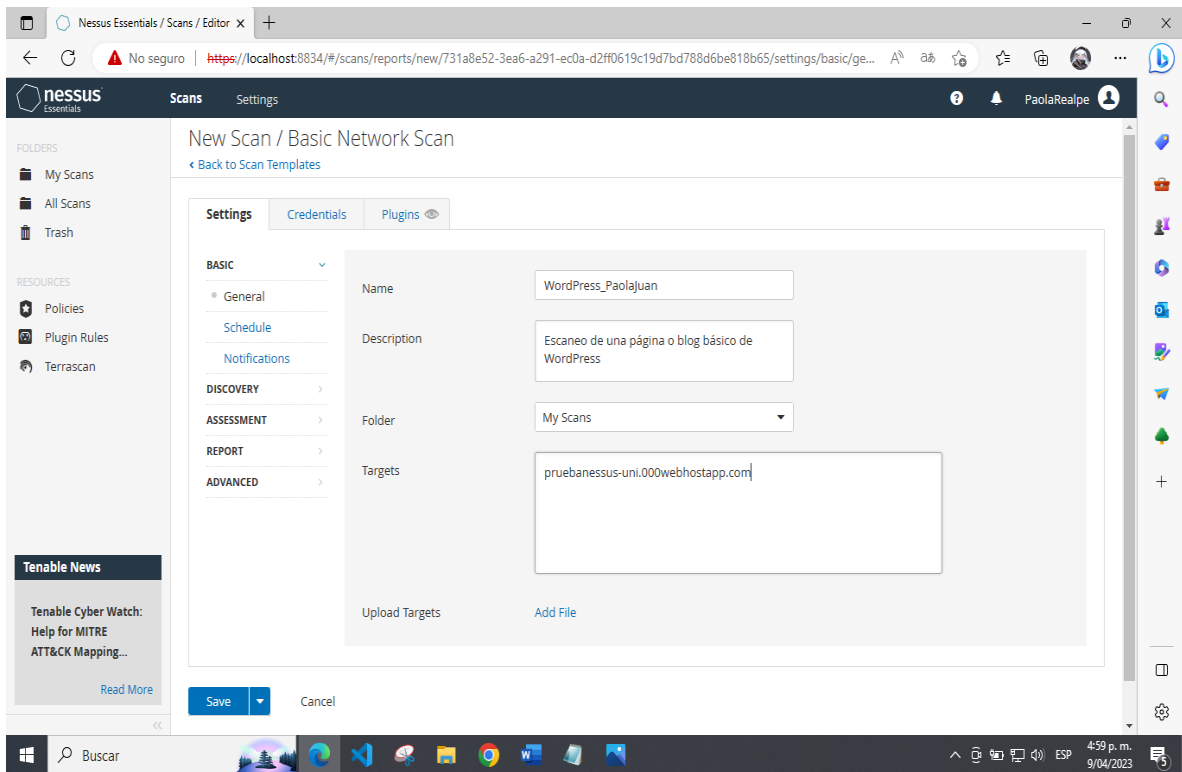
En Nessus se agrega un **new Scan**, para que analice una red o una página básica y encuentre sus vulnerabilidades

The top screenshot shows the 'My Scans' page in the Nessus Essentials web interface. The page has a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'My Scans' and includes a search bar and a table of scans.

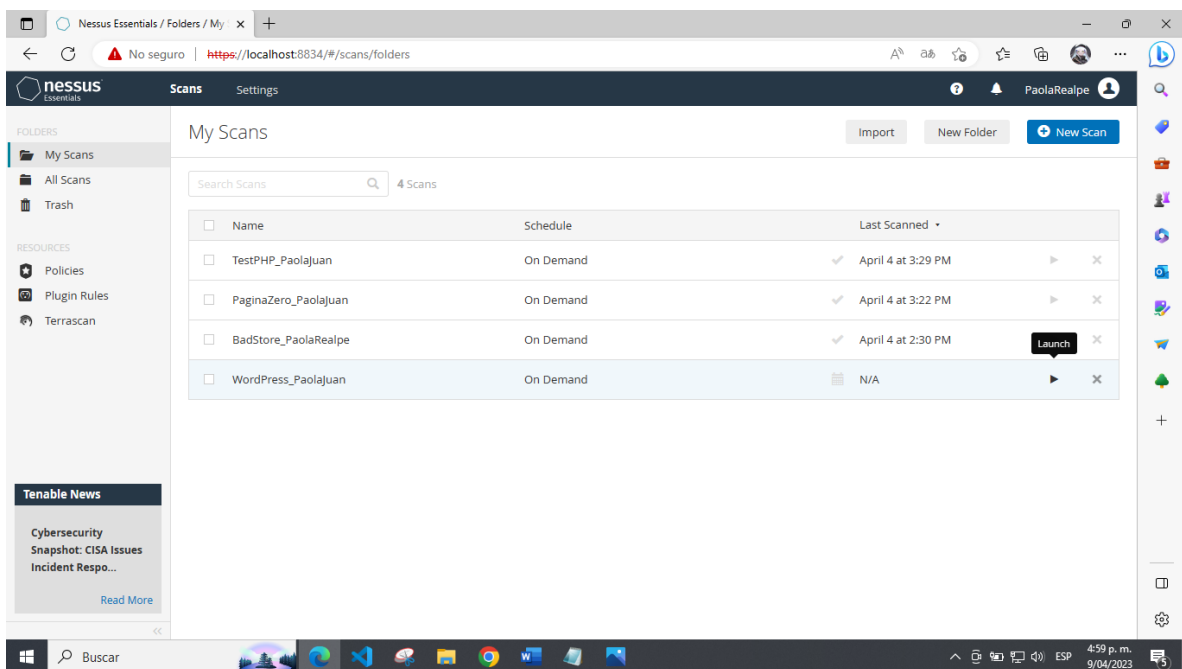
Name	Schedule	Last Scanned
TestPHP_PaolaJuan	On Demand	April 4 at 3:29 PM
PaginaZero_PaolaJuan	On Demand	April 4 at 3:22 PM
BadStore_PaolaRealpe	On Demand	April 4 at 2:30 PM

The bottom screenshot shows the 'Scan Templates' page. It features a 'Scanner' dropdown and a 'Search Library' bar. The page is divided into 'DISCOVERY' and 'VULNERABILITIES' sections. The 'DISCOVERY' section includes 'Host Discovery'. The 'VULNERABILITIES' section includes 'Basic Network Scan', 'Advanced Scan', 'Advanced Dynamic Scan', 'Malware Scan', 'Mobile Device Scan', 'Web Application Tests', 'Credentialed Patch Audit', and 'Intel AMT Security Bypass'.

Se agrega un nombre para el escaneo, una descripción y en el target el enlace copiado anteriormente para después guardar con el botón de **Save**

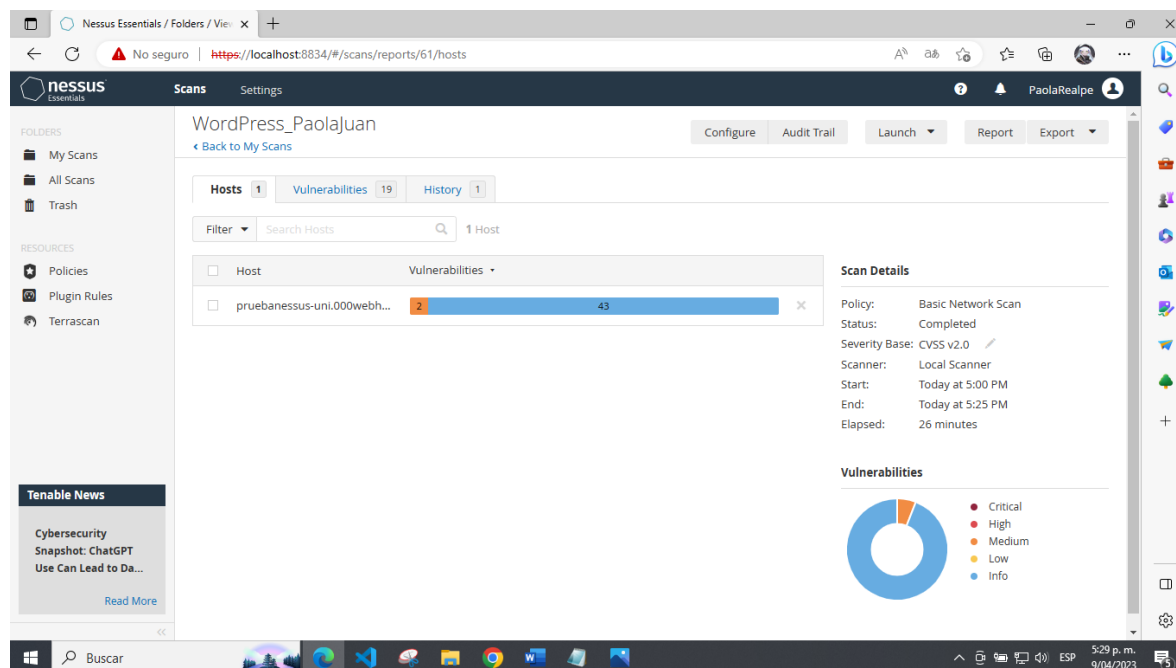


El siguiente paso es dar clic en el botón **Launch** para que comienza a analizar el sitio y encontrar las vulnerabilidades, se tiene en cuenta que este proceso se puede demorar varios minutos

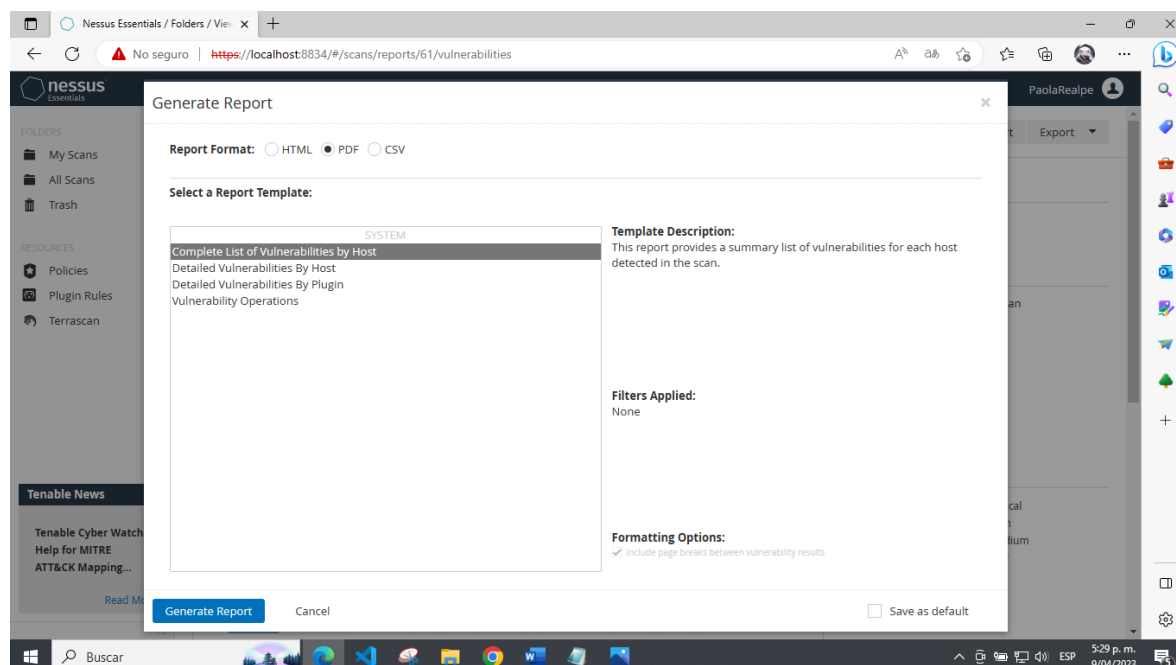


Al terminar el proceso damos sobre clic en **WordPress_PaolaJuan** y podemos observar las vulnerabilidades encontradas, que en este caso son 2 de nivel medio y 45 informativas.

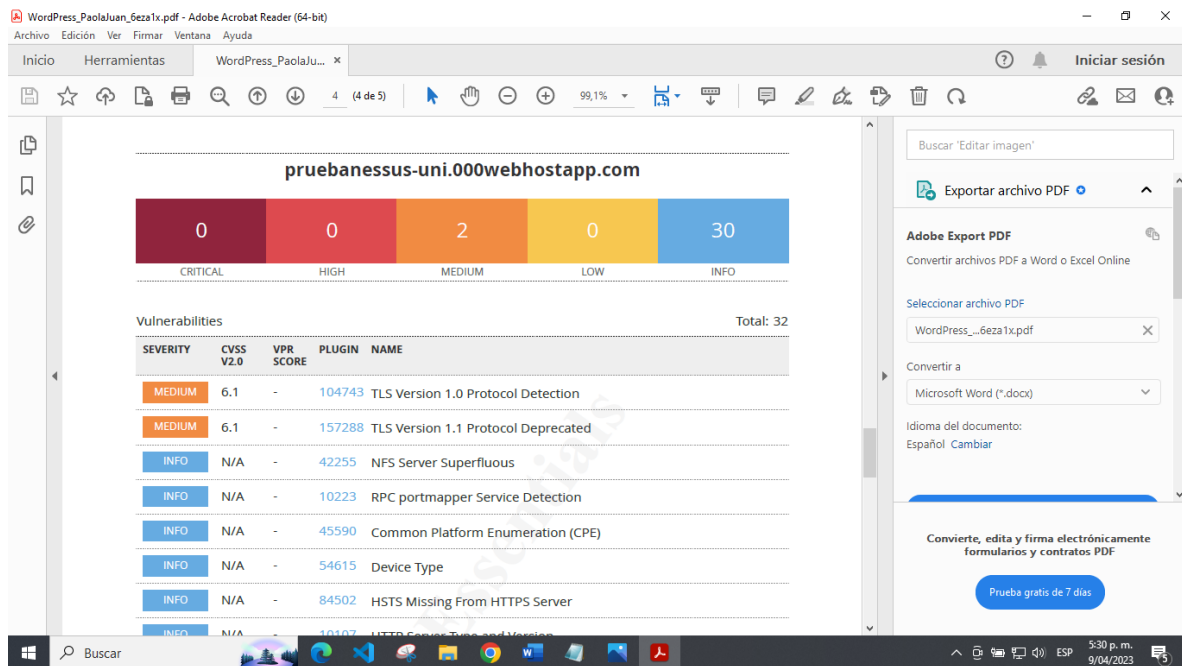
Para descargar el reporte nos vamos a la opción de **Report** de la parte superior y la seleccionamos



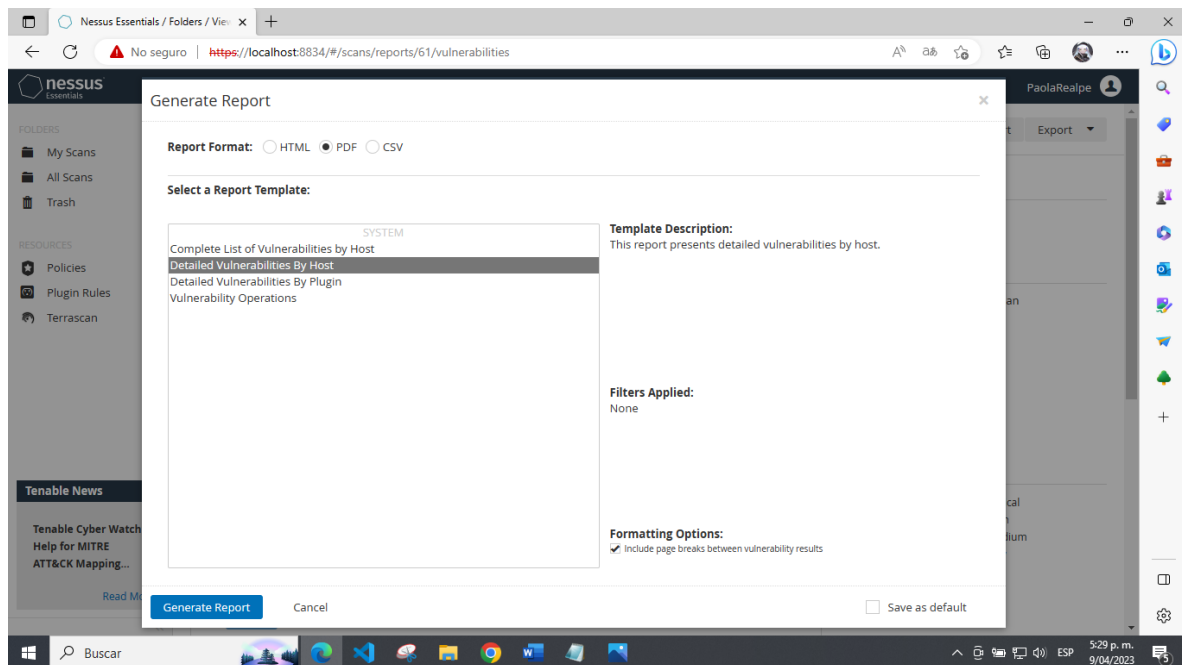
Generamos el reporte por pdf y seleccionamos la primera opción de **Complete List**

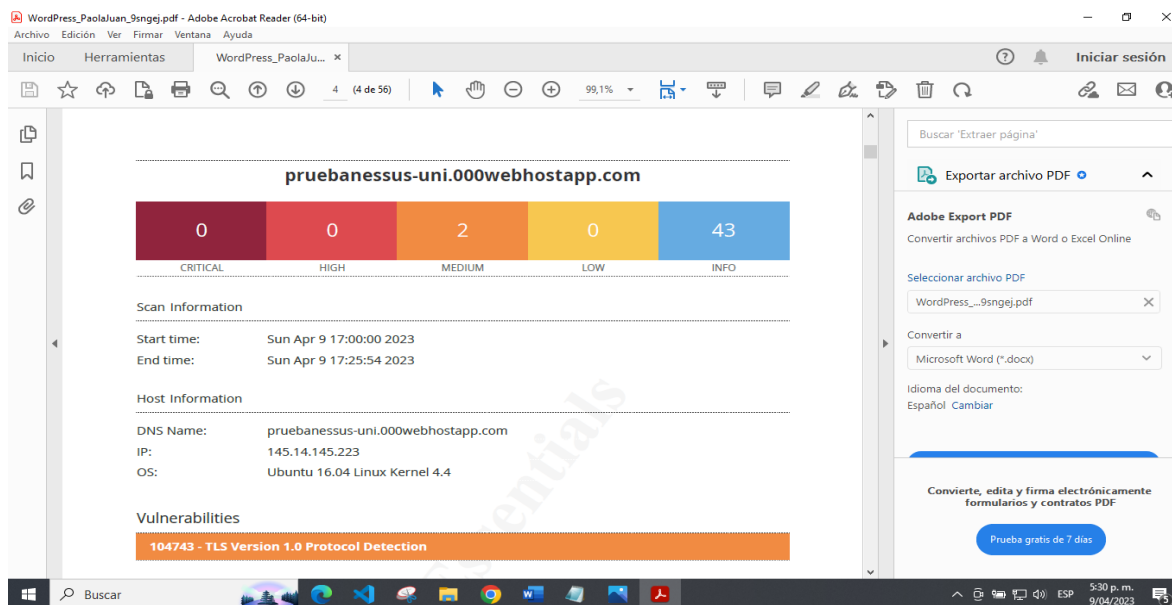


Como podemos observar en la siguiente imagen se generó el reporte



Hacemos el mismo procedimiento, pero esta vez para generar un reporte con mejor redacción y más detalles de cada vulnerabilidad, por lo que volvemos a dar clic en **Report** solo que esta vez seleccionamos la segunda opción de **Detailed Vulnerabilities**





WORDPRESS

Describe con sus propias palabras las vulnerabilidades encontradas en cada caso y describe con sus palabras teniendo en cuenta la documentación que sugiere nessus, como se debería solucionar o qué medidas se deben tomar para resolver la vulnerabilidad

MEDIUM - TLS Version 1.0 Protocol Detection (Detección de protocolo TLS versión 1.0)

Esta Vulnerabilidad de nivel medio que se encontró en WordPress donde se afirma que el servicio remoto actualmente está aceptando conexiones TLS 1.0, la cual posee grandes fallos criptográficos en su implementación, debido a que han salido nuevas versiones como el TLS 1.2 Y 1.3, por lo que se recomienda su uso. También se resalta que desde el 31 de marzo del 2020 estos puntos de conexión no están habilitados para la TLS 1.2 y versiones posteriores, por lo que se debe buscar una más actualizada para que se adapte a los servidores y navegadores web

SOLUCION NESSUS

La solución que aconseja Nessus es deshabilitar el TLS 1.0, excepto en terminales POS, debido a que se necesita una versión más reciente para establecer conexiones seguras entre un cliente y servidor, por lo que la versión que se debe utilizar es la de TLS 1.3 creada en el año 2018 que incluye la reducción de latencia de la conexión y una mayor eficiencia.

SOLUCION DE GRUPO

También se recomienda verificar la compatibilidad de TLS 1.2 o 1.3 de los navegadores y su interacción con los clientes, para que no se presenten posibles problemas, con ayuda de pruebas de seguridad para la verificación de una funcionalidad segura

MEDIUM - TLS Version 1.1 Protocol Deprecated (Protocolo TLS versión 1.1 en desuso)

El servicio carece de un soporte apto en cifrado para poder cumplir los requerimientos de seguridad necesarios, por lo que los cifrados donde se admiten antes del cálculo MAC y los modos de cifrado como GCM no se pueden usar con la versión de TLS que usa. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.

SOLUCION NESSUS

La solución que aconseja Nessus es deshabilitar el TLS 1.0, y actualizarla a una versión más reciente para que incluya los parches y las actualizaciones de seguridad

SOLUCION DE GRUPO

En base a la información recolectada se recomienda priorizar la seguridad por lo que se debe habilitar el TLS 1.2 o 1.3 en el servidor

INFO - Servidor NFS superfluo (Detección de servidor DNS)

El servidor NFS remoto no posee recursos compartidos disponibles para ser utilizado, en tal caso si se intenta acceder a un recurso, la respuesta del sistema fallara, por lo que la ejecución de un servicio no utilizado aumenta la superficie expuesta al host remoto, por lo que hay mas posibilidades de la presencia de vulnerabilidades que de paso a los ciberdelincuentes a atacar

SOLUCION NESSUS

La solución que aconseja Nessus es desactivar este servicio innecesario, que puede ser perjudicial para el sistema a largo plazo.

SOLUCION DE GRUPO

Se debe verificar la configuración con el servidor NFS para no exponer los recursos compartidos, como también la conectividad a la red y los servicios innecesarios que se están ejecutando en el servidor para desactivarlos, además de revisar los permisos de acceso para asegurar que los usuarios puedan acceder a los recursos y las personas no autorizadas no puedan hacerlo.

Puerto Hosts

2049 / TCP pruebanessus-uni.000webhostapp.com