



Burp Suite for Pentester

Web Scanner & Crawler



WWW.HACKINGARTICLES.IN

Contenido

El rastreador del eructo.....	3
¿Qué es el rastreador?.....	3
Personalización del rastreador.....	9
Configuración de URL fuera de alcance	9
Escaneo de vulnerabilidades a través de Burpsuite	14
Auditoría con la configuración predeterminada	15
Definición de configuraciones de auditoría.....	20
Rastreo y escaneo con un escenario avanzado.....	26
Eliminar las tareas definidas.....	27

El rastreador del eructo

¿Qué es el rastreador?

El término rastreador web o araña web es el más común y se utiliza varias veces al probar una aplicación web. Entonces, ¿qué es este rastreador?

Llevando su nombre, podemos representar que un rastreador examina una región específica lenta y profundamente y luego despliega la salida con un formato definido.

Entonces, ¿el Burp's Crawler es lo mismo?

Según Port Swigger, "la fase de rastreo implica navegar por la aplicación, seguir enlaces, enviar formularios e iniciar sesión para catalogar el contenido de la aplicación y las rutas de navegación dentro de ella".

En palabras más simples, podemos decir que el rastreador burp se mueve programáticamente dentro de toda la aplicación web, sigue las URL de redireccionamiento, inicia sesión dentro de los portales de inicio de sesión y luego los agrega todos en una estructura similar a un árbol en la vista Mapa del sitio en Target. pestaña.

Sin embargo, este rastreador funciona de manera similar a las herramientas "Dirb" o "DirBuster": los escáneres de contenido web, que fuerzan al servidor web a volcar las URL visitadas, no visitadas y ocultas de la aplicación web.

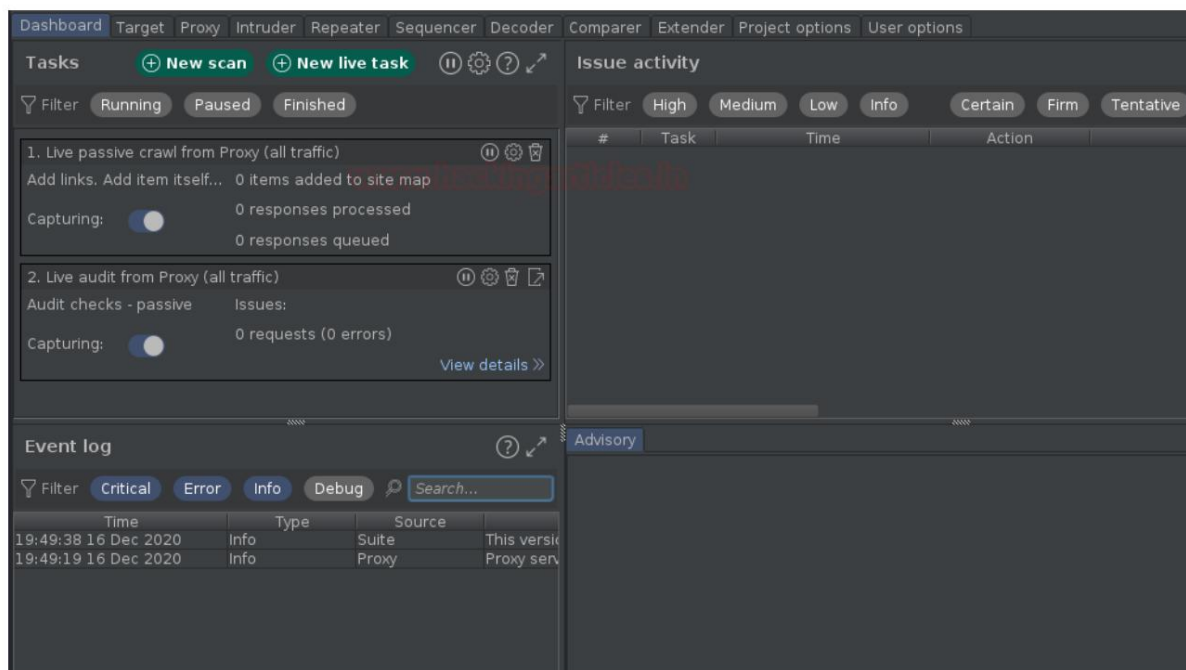
Anteriormente, en las versiones anteriores de burp suite decía "1.7", este rastreador se denominó "Spider". Entonces, ¿por qué sucede esto? ¿Qué nuevas características tiene el rastreador de eructos que hicieron que la araña desapareciera?

¡¡Vamos a desenterrarlo!!

¡Rastrea con configuraciones predeterminadas!

Si está familiarizado con la función de araña, es posible que sepa que la araña muestra una pestaña específica dentro del panel de burpsuite. Pero con las mejoras, el rastreador de eructos viene predefinido dentro de la sección del tablero. Sin embargo, nos ayuda así a monitorizar y controlar las actividades automatizadas del eructo en un único lugar.

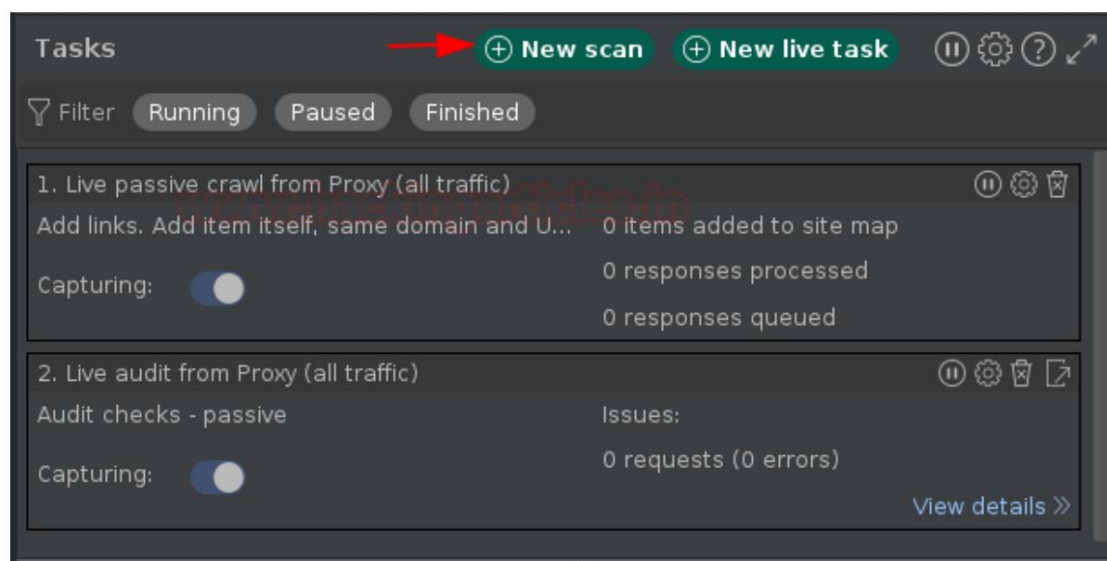
Entonces, para iniciar con el rastreador, activemos nuestra suite de eructos y redirijamos a la sección Panel de control allí.



Tan pronto como lleguemos al panel del tablero, podremos ver la cantidad de subsecciones especificadas. Explorémoslos en detalle:

1. **Tareas:** la sección "Tareas" incluye el resumen de todos los rastreos y análisis en ejecución, ya sea son definidos por el usuario o automatizados. Aquí podemos pausar y reanudar las tareas individuales, o todas las tareas juntas, e incluso podemos ver las versiones detalladas de un rastreo o auditoría específicos.
2. **Registro de eventos:** la función de registro de eventos genera todos los eventos que sigue la suite Burp, como si el proxy se iniciara, se generará el evento o una sección específica no funciona correctamente, luego se generará un registro de eventos con el .
3. **Actividad del problema:** esta sección elimina las vulnerabilidades comunes dentro de la aplicación que el paquete de eructos analiza y, además, podemos segregarlas todas aplicando los filtros definidos según su gravedad y destructividad.
4. **Aviso:** esta es una de las secciones más importantes del panel de control del eructo, ya que demuestra la vulnerabilidad seleccionada en forma ampliada, definiendo la carga útil con una Solicitud y respuesta, mencionando la causa de su existencia, definiendo los pasos de mitigación y eliminando la referencia y las puntuaciones CVSS para nuestra revisión.

Por lo tanto, para explorar la aplicación web debemos presionar el botón "Nuevo escaneo" ubicado en la parte superior de la sección Tareas .



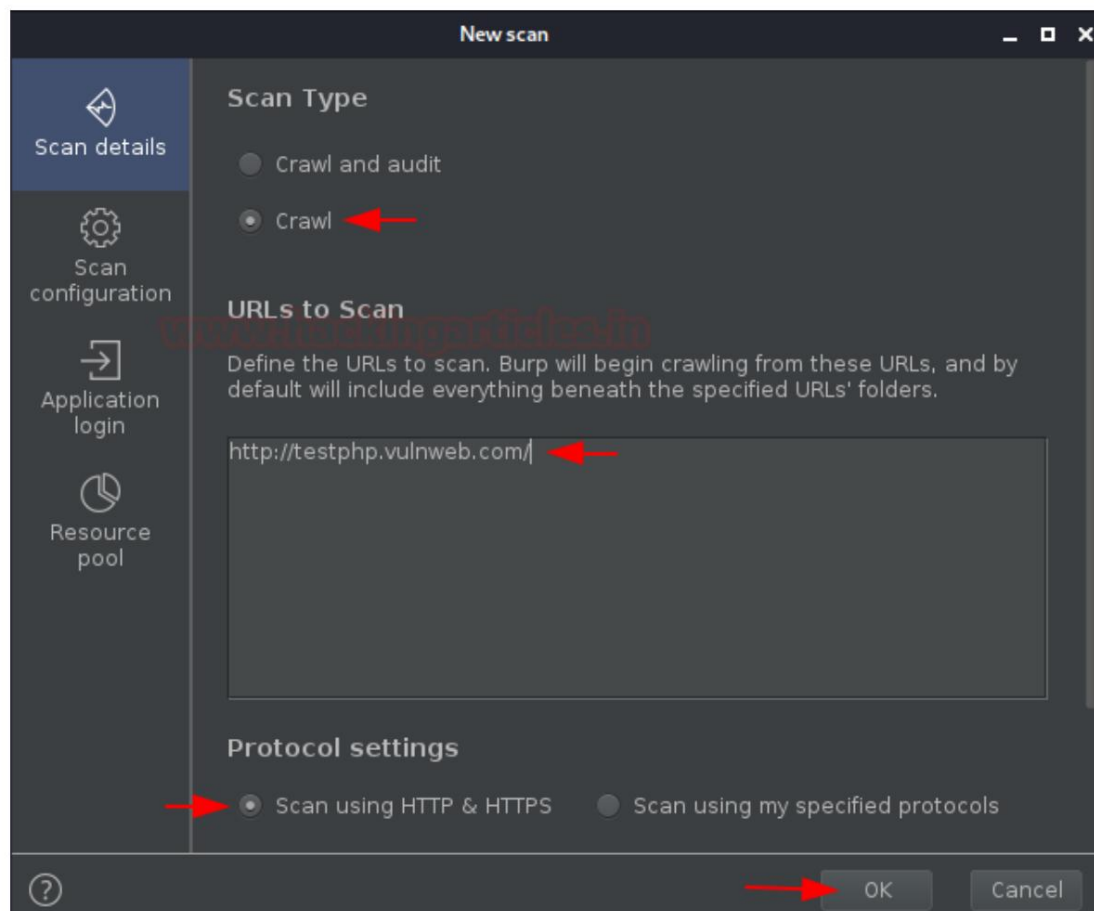
Tan pronto como lo hagamos, seremos redirigidos a una nueva ventana emergente que indica "Nuevo escaneo".

Allí seremos recibidos con dos opciones:

- Rastreo y auditoría
- Gatear

Sin embargo, para esta sección, solo haremos "Rastrear" . Y el otro, lo discutiremos más adelante en este artículo.

A medida que avanzamos con las configuraciones predeterminadas, simplemente escribiremos la URL de prueba , es decir, "http://testphp.vulnweb.com/" y presionaremos el botón "Aceptar" .



Mientras lo hacemos, la ventana desaparecerá y en el tablero alinearemos nuestra nueva tarea como "Rastrear test.vulnweb.com", y en el registro de eventos, podemos ver que obtuvimos el evento "Rastrear". comenzó".

The screenshot shows the Burp Suite interface. At the top, there are buttons for '+ New scan' and '+ New live task'. Below these are filter buttons for 'Running', 'Paused', and 'Finished'. The 'Tasks' section lists three tasks:

1. Live passive crawl from Proxy (all traffic) [Status: Stopped]
 - Add links. Add item itself, sam... 0 items added to site map
 - Capturing: ☐ 0 responses processed, 0 responses queued
2. Live audit from Proxy (all traffic)
 - Audit checks - passive Issues:
 - Capturing: ☐ 0 requests (0 errors)
 - [View details >>](#)
3. Crawl of testphp.vulnweb.com [Status: Running]
 - Default configuration 280 requests (4 errors)
 - 47 locations crawled
 - Unauthenticated crawl. Estim...
 - [View details >>](#)

Below the tasks is the 'Event log' section, indicated by a red arrow. It has filter buttons for 'Critical', 'Error', 'Info', and 'Debug', and a search bar. The event log table shows the following entries:

Time	Type	Source	Message
20:15:02 16 Dec 2020	Info	Task 3	Crawl started.
20:07:51 16 Dec 2020	Info	Suite	This version of Burp Suite wa

En unos minutos, la tarea de rastreo finalizará y recibiremos la notificación allí. ¿Pero dónde está el resultado?

Como se definió anteriormente, el rastreador descarga el resultado en un formato similar a un árbol en la vista Mapa del sitio en la pestaña Destino, vayamos allí.

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Project options

User options

xssValidator

Site map

Scope

Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://testphp.vulnweb.com

/

AJAX

index.php

Mod_Rewrite_Shop

artists.php

artist=1

artist=2

artist=3

cart.php

categories.php

disclaimer.php

guestbook.php

hpp

index.php

listproducts.php

login.php

product.php

search.php

secured

signup.php

Contents

Host	Method	URL	Params	Status	Length
http://testphp.vulnweb.com	GET	/		200	5175
http://testphp.vulnweb.com	GET	/AJAX/index.php		200	4453
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/		200	1191
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/BuyPr...		200	316
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/BuyPr...		200	291
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/BuyPr...		200	308
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/Detail...		200	529
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/Detail...		200	535
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/Detail...		200	495
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/RateP...		200	316
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/RateP...		200	291
http://testphp.vulnweb.com	GET	/Mod_Rewrite_Shop/RateP...		200	308
http://testphp.vulnweb.com	GET	/artists.php		200	5545
http://testphp.vulnweb.com	GET	/artists.php?artist=1	✓	200	6468
http://testphp.vulnweb.com	GET	/artists.php?artist=2	✓	200	6410
http://testphp.vulnweb.com	GET	/artists.php?artist=3	✓	200	6410
http://testphp.vulnweb.com	GET	/cart.php		200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	GET	/categories.php		200	6332

¡¡Excelente!! Tenemos lo que deseamos. En el panel derecho tenemos casi todas las URL de la página web, además de eso, muestra los métodos HTTP y una sección de parámetros que define qué URL requiere un valor de parámetros dentro de ella.

Existen varias vulnerabilidades importantes debido a los campos de entrada no desinfectados, por lo que con estos datos volcados podemos simplemente segregar las URL que contienen los valores de entrada que, por lo tanto, se pueden probar más a fondo. Y para ello simplemente haga doble clic en el campo “Parámetros” .

Contents					
Host	Method	URL	Params	Status	Length
http://testphp.vulnweb.com	GET	/artists.php?artist=1	✓	200	6468
http://testphp.vulnweb.com	GET	/artists.php?artist=2	✓	200	6410
http://testphp.vulnweb.com	GET	/artists.php?artist=3	✓	200	6410
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/cart.php	✓	200	5120
http://testphp.vulnweb.com	POST	/guestbook.php	✓	200	5627
http://testphp.vulnweb.com	GET	/hpp/?pp=12	✓	200	599
http://testphp.vulnweb.com	GET	/hpp/params.php?aaaa%2...	✓	200	214
http://testphp.vulnweb.com	GET	/hpp/params.php?p=valid...	✓	200	221
http://testphp.vulnweb.com	GET	/listproducts.php?artist=1	✓	200	8211
http://testphp.vulnweb.com	GET	/listproducts.php?artist=2	✓	200	5410
http://testphp.vulnweb.com	GET	/listproducts.php?artist=3	✓	200	4916
http://testphp.vulnweb.com	GET	/listproducts.php?cat=1	✓	200	8097
http://testphp.vulnweb.com	GET	/listproducts.php?cat=2	✓	200	5528
http://testphp.vulnweb.com	GET	/listproducts.php?cat=3	✓	200	4916
http://testphp.vulnweb.com	GET	/listproducts.php?cat=4	✓	200	4916
http://testphp.vulnweb.com	GET	/product.php?pic=1	✓	200	6645
http://testphp.vulnweb.com	GET	/product.php?pic=2	✓	200	6585
http://testphp.vulnweb.com	GET	/product.php?pic=3	✓	200	6618
http://testphp.vulnweb.com	GET	/product.php?pic=4	✓	200	6670

Sin embargo, si queremos consultar las páginas o un directorio específico, simplemente podemos navegar por el lado izquierdo y seleccionar la opción que deseemos allí.

IGNITE Technologies

Página 8 de 28

The screenshot displays a web browser's developer tools interface. On the left, a file explorer shows the directory structure of `http://testphp.vulnweb.com`. The `guestbook.php` file is highlighted with a red arrow. On the right, the 'Contents' tab shows a table of network requests. The first request is a POST to `/guestbook.php` with a status of 200. Below this, the 'Request' tab is selected, showing the raw request data. The request is a POST to `/guestbook.php` with a status of 200. The raw request data is visible, showing the URL and various headers.

Host	Method	URL	Params	Status
http://testphp.vulnweb.com	POST	/guestbook.php	✓	200
http://testphp.vulnweb.com	GET	/guestbook.php		200

Request Response

Raw Params Headers Hex

```

1 POST /guestbook.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Referer: http://testphp.vulnweb.com/guestbook.php
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 50
12
13 name=anonymous+user&text=604111&submit=add+message

```

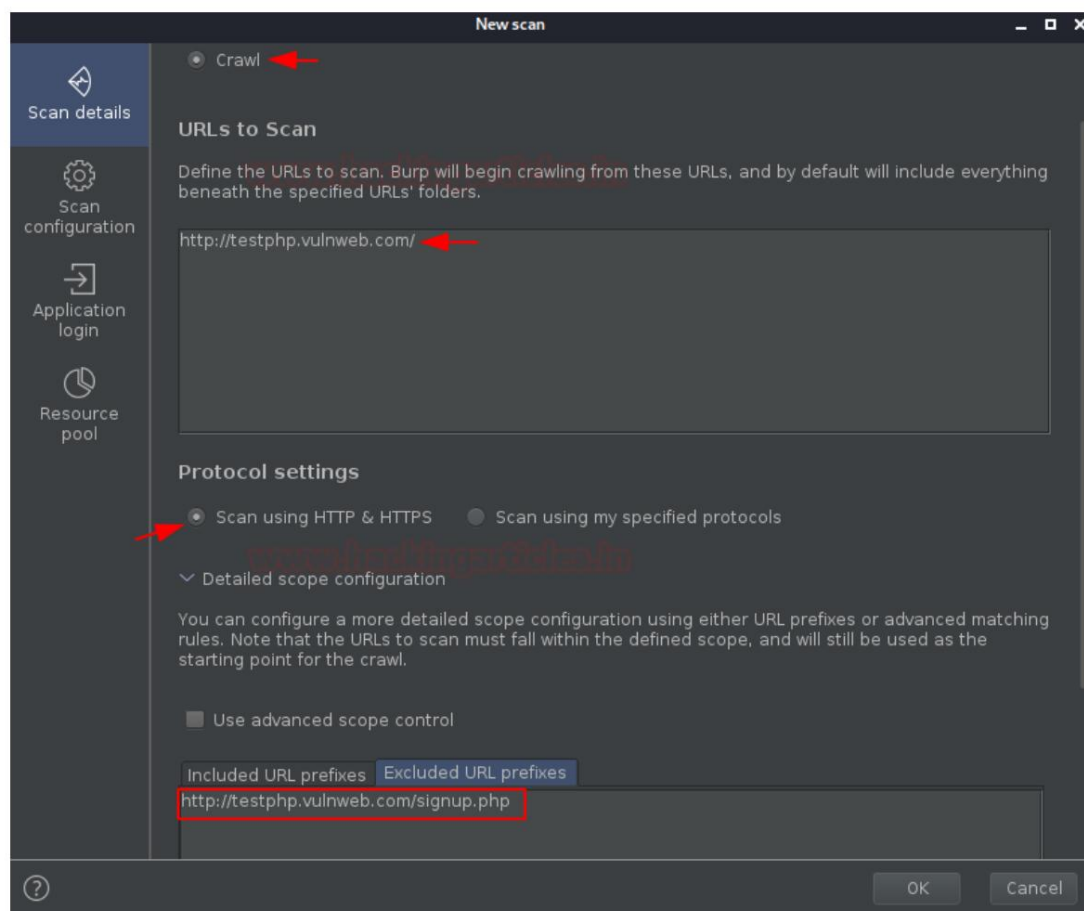
Personalizando el rastreador

¿ Qué pasa si algunas páginas web específicas están fuera de alcance? ¿ O el sitio web necesita algunas credenciales específicas para navegar por páginas web restringidas?

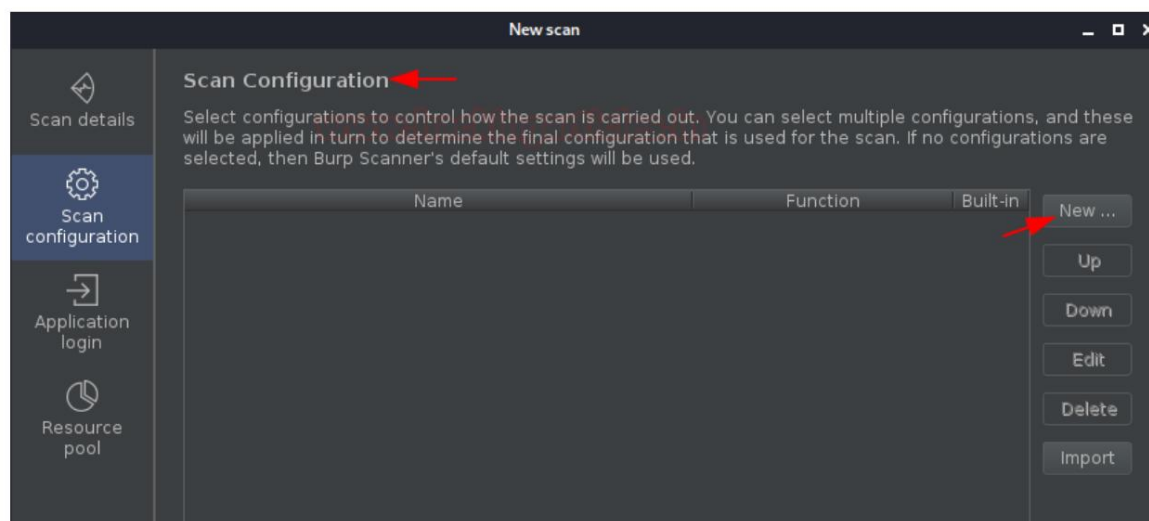
Por lo tanto, en tales casos, necesitamos configurar nuestro rastreador para que funcione como queremos. Entonces, para hacer esto, volvamos al tablero y seleccionemos la opción "Nuevo escaneo" nuevamente. Pero por esta vez no presionaremos "Aceptar" después de configurar la URL.

Configuración de URL fuera de alcance

A continuación, en la configuración del protocolo, hay una opción para la Configuración de alcance detallada, donde simplemente navegaremos hasta los "Prefijos de URL excluidos" e ingresaremos la URL fuera de alcance, es decir, `http://testphp.vulnweb.com/signup. PHP`

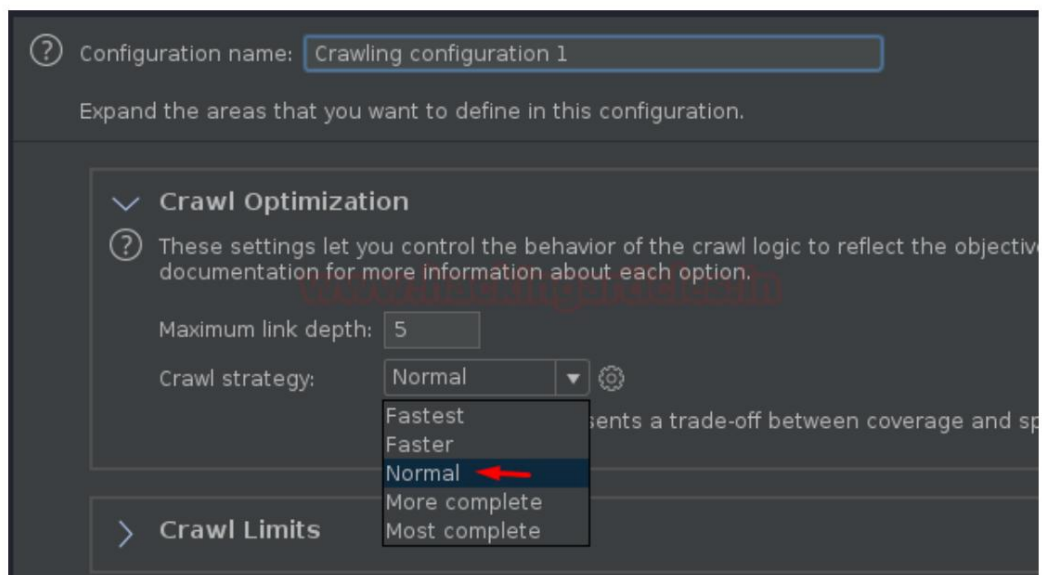


Para una mayor personalización, pasaremos a la opción Configuración de escaneo . Y allí presionaremos el botón "Nuevo" para configurar un nuevo rastreador.

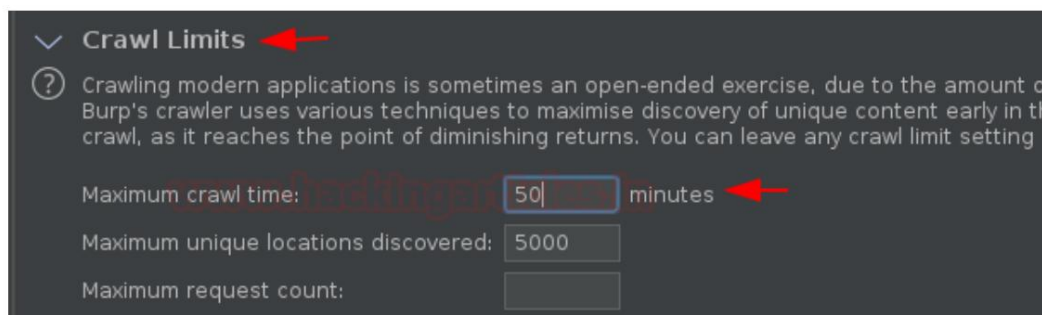


Nada más hacerlo se nos abrirá otra ventana con las opciones de configuración. Mantengamos el nombre de configuración como predeterminado, sin embargo, puedes cambiarlo si así lo deseas.

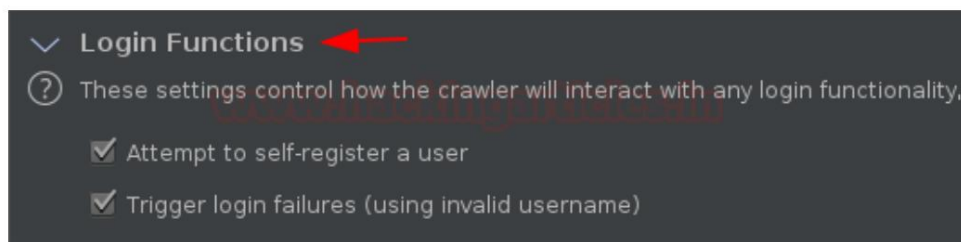
Además, la opción de optimización de rastreo se segrega dentro del "Más rápido al más profundo", por lo que la cambiaremos según nuestros requisitos.



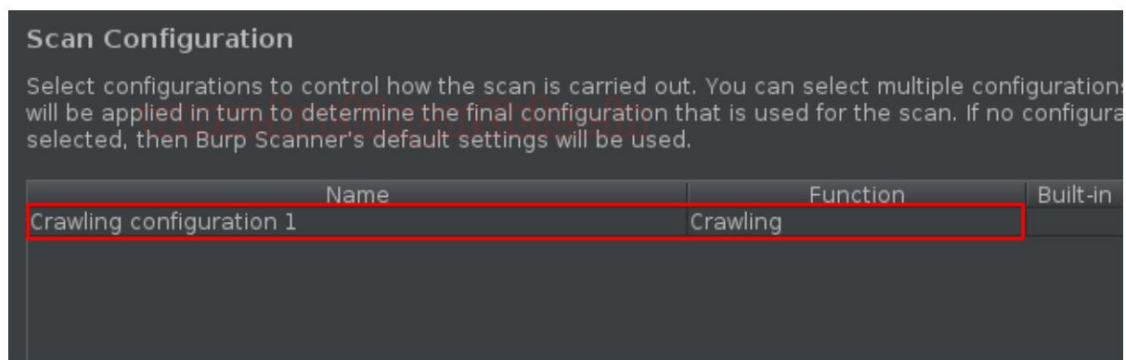
El límite de rastreo se considera un factor importante ya que determina el tiempo necesario y la profundidad para rastrear una aplicación. De este modo, estableceremos el límite máximo de rastreo en 50 minutos y el máximo de ubicaciones únicas descubiertas en 5000.



Algunas aplicaciones incluyen portales de registro de usuario o de inicio de sesión, por lo que verificar ambas opciones guiará al rastreador del eructo a registrarse automáticamente con algunos valores aleatorios si se encuentra con un portal de registro e incluso usar credenciales incorrectas en los portales de inicio de sesión para determinar el comportamiento del sitio web.

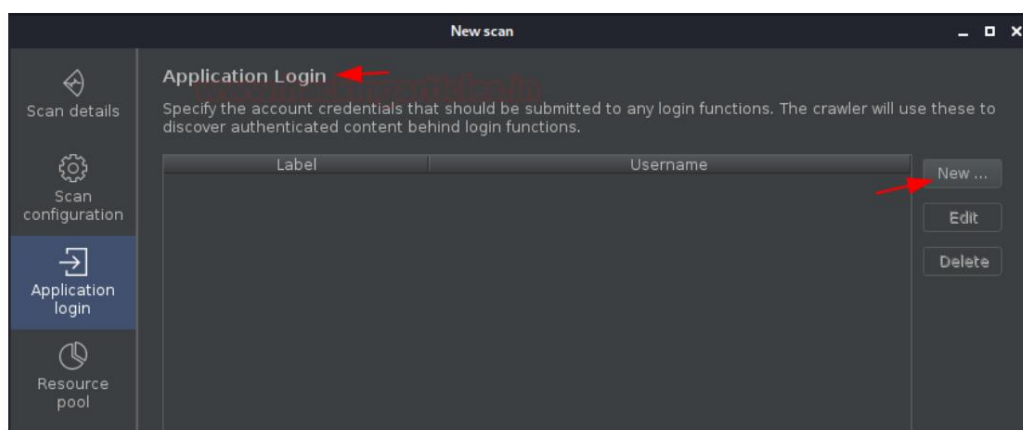


Ahora, con todas estas configuraciones, tan pronto como presionamos el botón "Guardar", nuestro rastreador aparece en el panel de Nuevo escaneo.

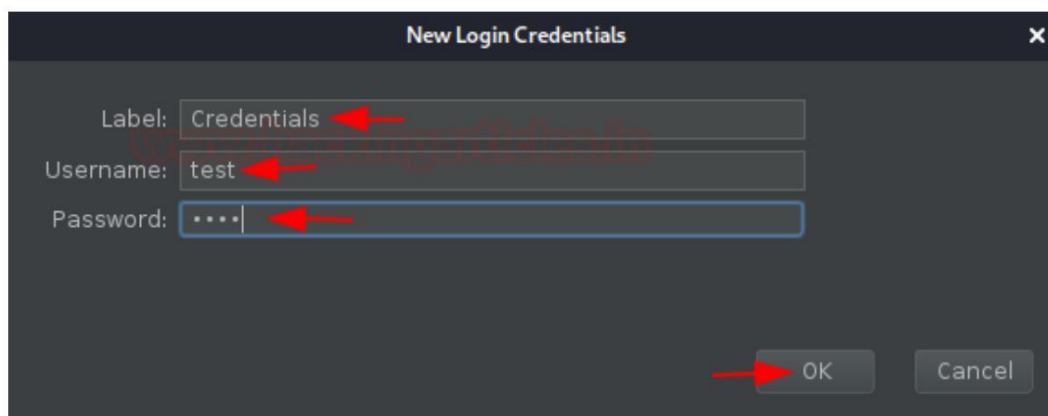


¿Qué pasa si el rastreador encuentra páginas restringidas? ¿O un portal de administración? Por lo tanto, para tales situaciones, proporcionemos algunas credenciales predeterminadas para que el rastreador pueda usarlas.

Navegue a la sección "Inicio de sesión de la aplicación" y haga clic en "Nuevo".



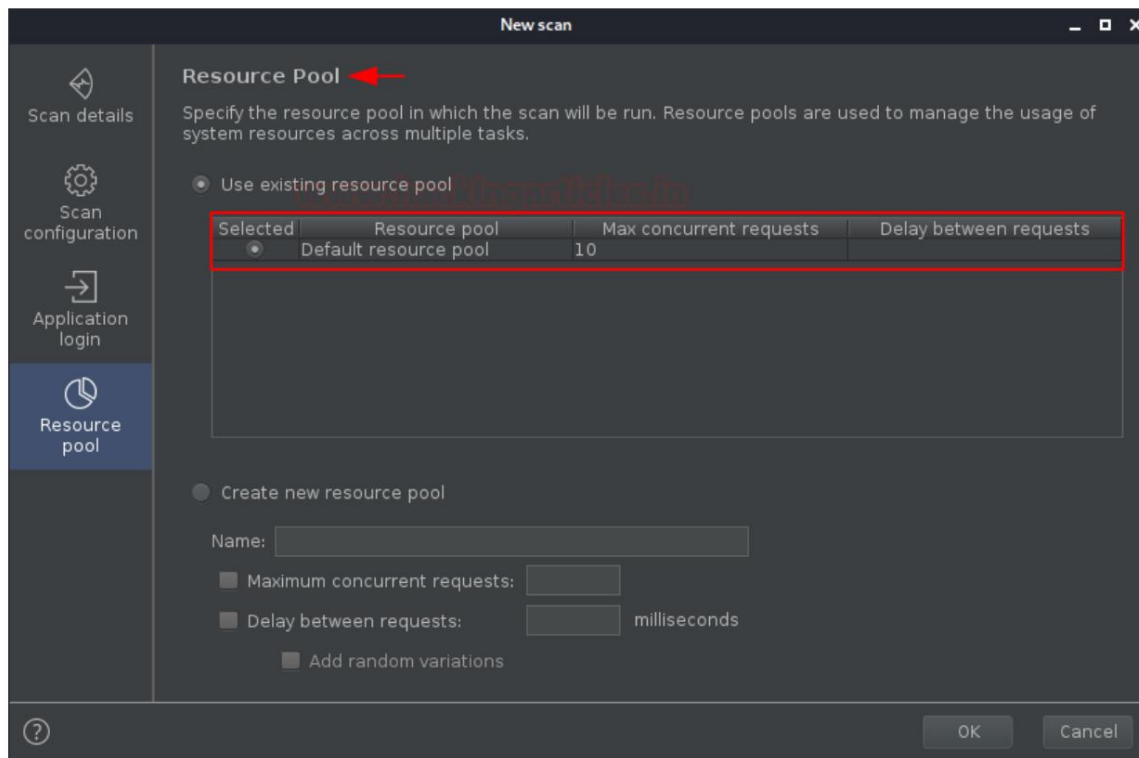
En el cuadro emergente, ingrese las credenciales deseadas y presione el botón "Aceptar".



Junto con todas estas cosas, tenemos una opción más dentro del "Nuevo panel de análisis", es decir, "Grupo de recursos".

Un grupo de recursos es una sección definida para las solicitudes simultáneas o, en términos más simples, podemos decir cuántas solicitudes enviará el rastreador a la aplicación de una sola vez y cuál sería el intervalo de tiempo entre las dos solicitudes.

Por lo tanto, si está probando una aplicación frágil que podría sufrir una cantidad excesiva de solicitudes, puede configurarla en consecuencia, pero como estamos probando la aplicación de demostración, la configuraremos de forma predeterminada.



New scan

Resource Pool ←

Specify the resource pool in which the scan will be run. Resource pools are used to manage the usage of system resources across multiple tasks.

☒ Use existing resource pool

Selected	Resource pool	Max concurrent requests	Delay between requests
<input checked="" type="radio"/>	Default resource pool	10	

☐ Create new resource pool

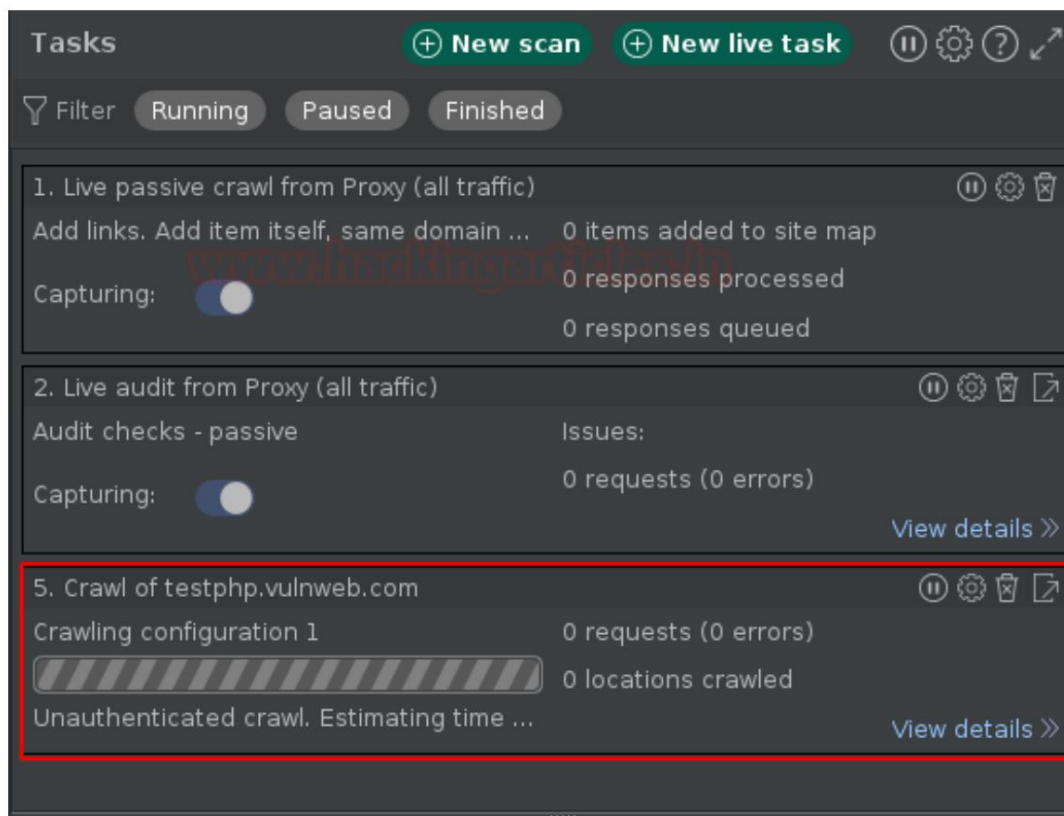
Name:

☐ Maximum concurrent requests:

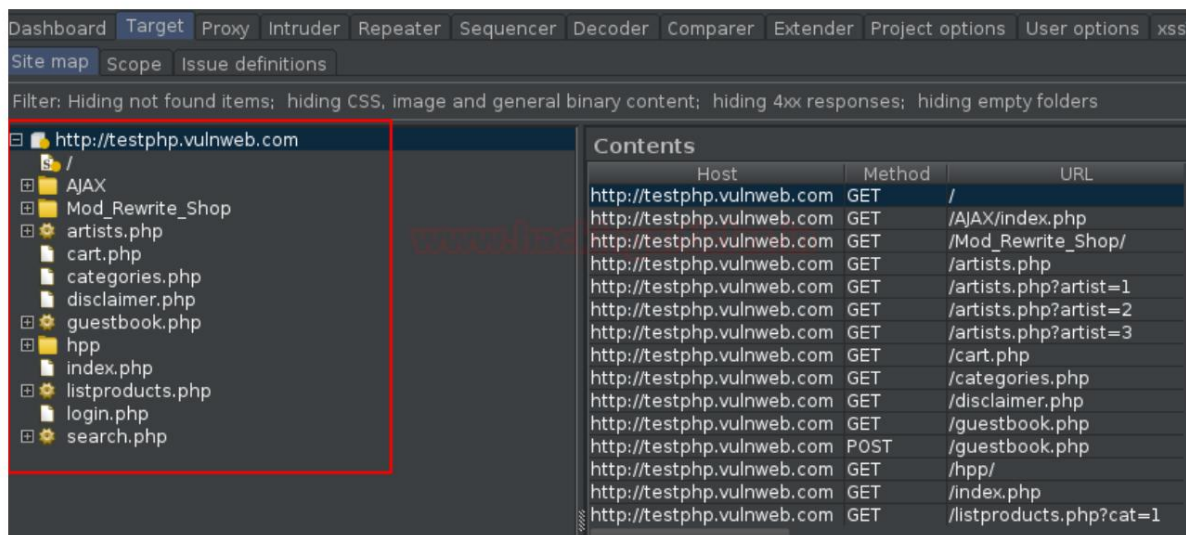
☐ Delay between requests: milliseconds

☐ Add random variations

Ahora, cuando presionemos el botón "Aceptar", se iniciará nuestro rastreador, que podrá ser monitoreado en el tablero.



¡¡Ahora esperemos a que termine!! A medida que navegamos a la pestaña Destino, apareceremos en la lista de resultados y allí podremos notar que no se menciona la página de registro, lo que indica que nuestra configuración funcionó correctamente.



Escaneo de vulnerabilidades en Burpsuite

En lugar de ser una herramienta inicial, el Burp Suite también actúa como un escáner de vulnerabilidades. De este modo, escanea las aplicaciones con el nombre de "Auditoría". Hay varios escáneres de vulnerabilidades en la web y el burp suite es uno de ellos, ya que está diseñado para ser utilizado por los evaluadores de seguridad y para encajar estrechamente con

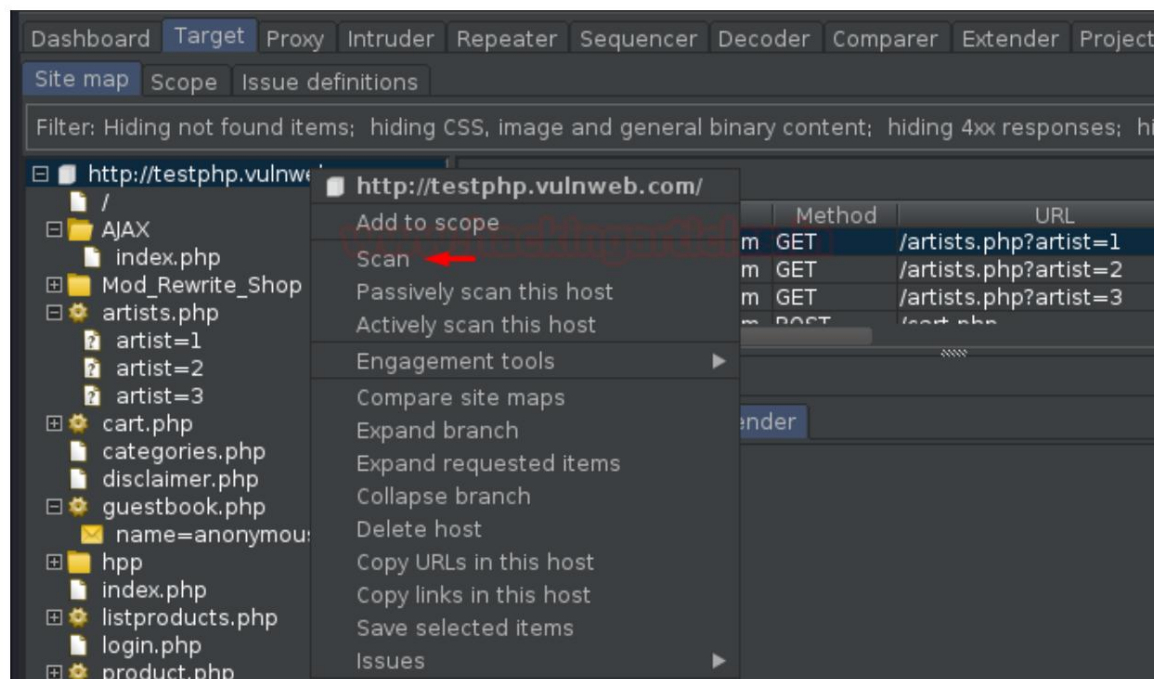
las técnicas y metodologías existentes para la realización de pruebas de penetración manuales y semiautomáticas de aplicaciones web.

Así que analicemos la aplicación vulnerable "testphp.vulnweb" y veamos qué vulnerabilidades importantes contiene.

Auditoría con la configuración predeterminada

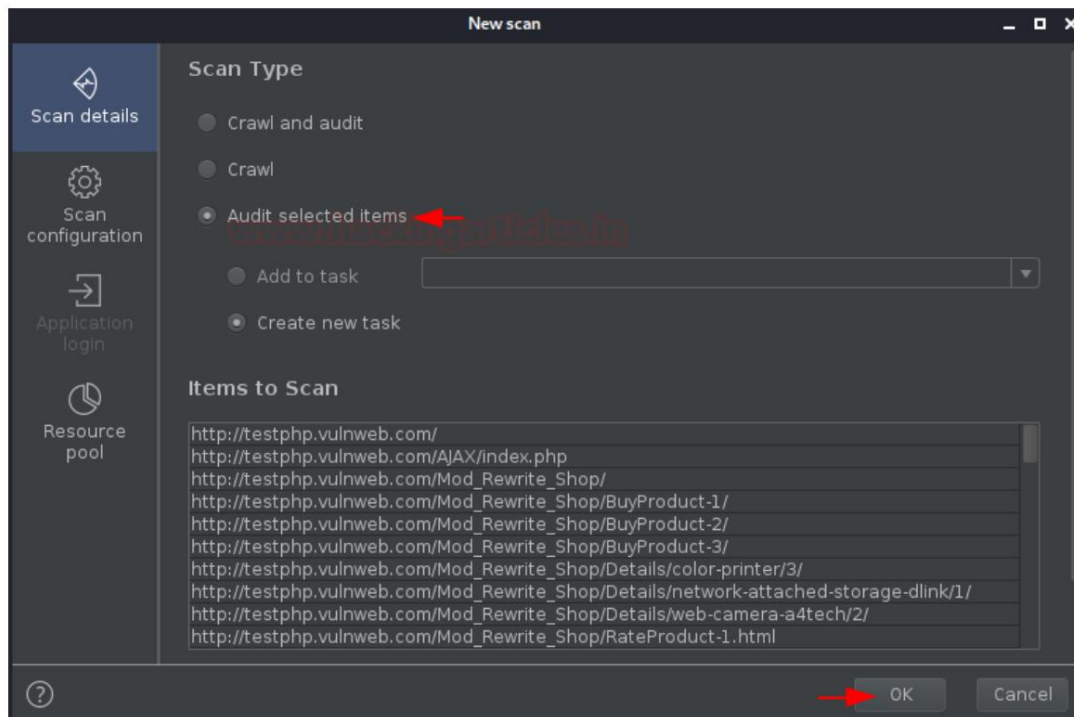
Como ya hemos rastreado la aplicación, sería más sencillo auditarla; sin embargo, para iniciar un escáner, todo lo que necesitamos es una URL, ya sea que la obtengamos al aceptar la solicitud o a través de la pestaña de destino.

En la captura de pantalla, puede percibir que hemos enviado la URL base haciendo clic derecho y optando por "Escanear".



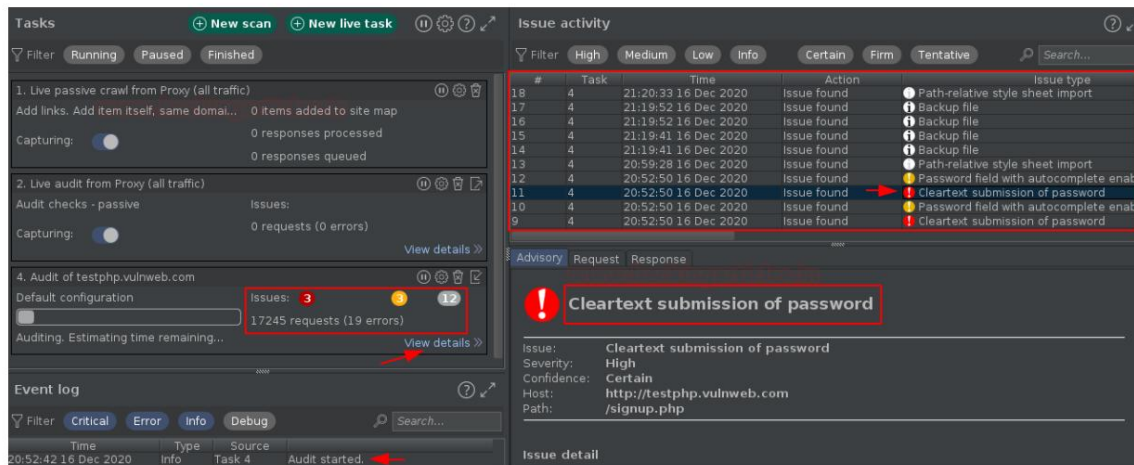
Tan pronto como lo hagamos, seremos redirigidos nuevamente al Panel de control del nuevo escaneo. ¡¡Pero espera!! Esta vez tenemos una opción más, es decir, "Auditar elementos seleccionados", tan pronto como la seleccionemos obtendremos todas las URL dentro del cuadro Elemento a escanear (esto sucede porque hemos optado por la solicitud base).

Como estamos tratando con la auditoría predeterminada, simplemente presionaremos el botón "Aceptar" allí.



Y ahora supongo que sabes a dónde tenemos que ir. ¡¡Sí!! La pestaña Panel de control.

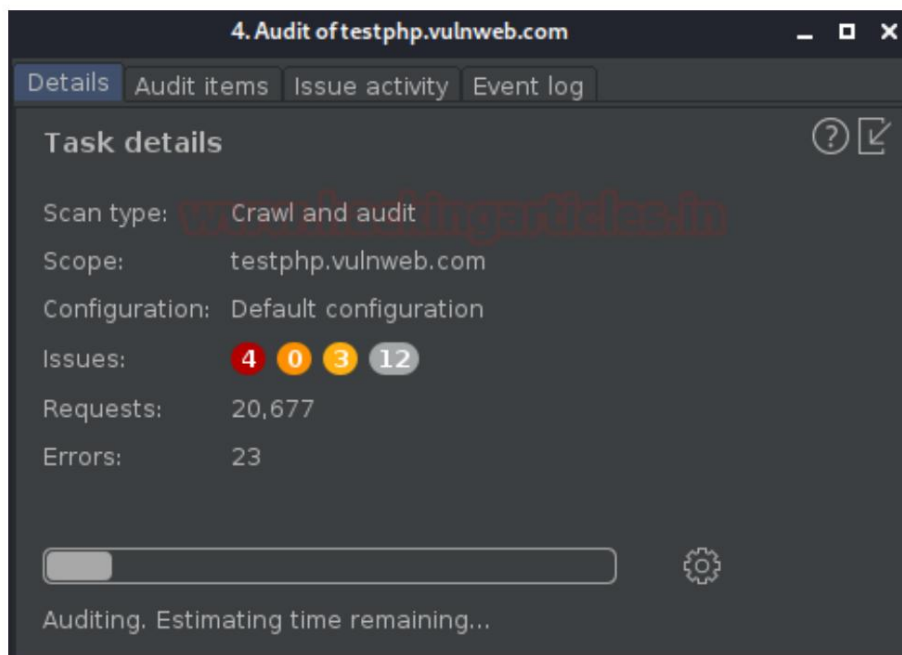
Esta vez no solo se cambia la sección Tareas y el registro de eventos, sino que también podemos ver las variaciones en la actividad de problemas y las secciones de asesoramiento.



En la imagen de arriba, podemos ver que en unos pocos minutos nuestro escáner envió alrededor de 17000 solicitudes a la aplicación web e incluso descartó varias vulnerabilidades según su nivel de gravedad.

¿Y si queremos ver la versión detallada?

Para hacerlo, simplemente haga clic en la sección Ver detalles ubicada en la parte inferior de la tarea definida y, por lo tanto, será redirigido a una nueva ventana con todos los detalles refinados que contiene.



¡¡Fresco!! Revisemos los elementos auditados.

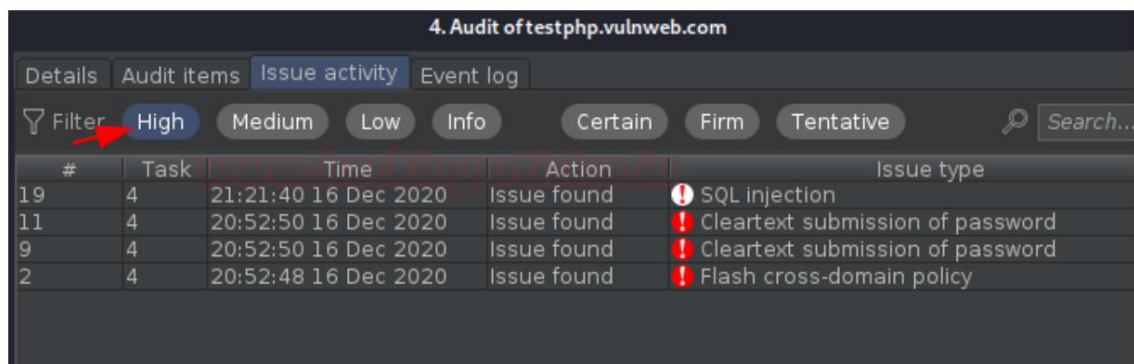
Y cuando lleguemos a la pestaña Elementos de auditoría, accederemos a la versión detallada de las secciones auditadas, donde obtendremos los estatutos, las fases activa y pasiva, las solicitudes por URL y mucho más.

Details	Audit items	Issue activity	Event log										
URL	Status	Passive ph...	Active phases	JavaScript ph...	Issues	Requests	Errors	Insertion point					
/	Scanning	1 2	1 2 3 4 5	1 2 3	1	560		3					
/AJAX/index.php	Errors: request tim...	1 2	1 2 3 4 5	1 2 3		1254	2	6					
/Mod_Rewrite_Shop/	Scanning	1 2	1 2 3 4 5	1 2 3	1	656	1	4					
/Mod_Rewrite_Shop/BuyProduct-1/	Errors: unknown h...	1 2	1 2 3 4 5	1 2 3		773	2	5					
/Mod_Rewrite_Shop/BuyProduct-2/	Scanning	1 2	1 2 3 4 5	1 2 3		26		5					
/Mod_Rewrite_Shop/BuyProduct-3/	Scanning	1 2	1 2 3 4 5	1 2 3		26		5					
/Mod_Rewrite_Shop/Details/color-printer/3/	Errors: request tim...	1 2	1 2 3 4 5	1 2 3		1281	4	7					
/Mod_Rewrite_Shop/Details/network-attached-sto...	Scanning	1 2	1 2 3 4 5	1 2 3		1230	1	7					
/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	Errors: request tim...	1 2	1 2 3 4 5	1 2 3		1332	1	7					
/Mod_Rewrite_Shop/RateProduct-1.html	Errors: request tim...	1 2	1 2 3 4 5	1 2 3	2	1043	3	5					
/Mod_Rewrite_Shop/RateProduct-2.html	Errors: request tim...	1 2	1 2 3 4 5	1 2 3		769	1	5					
/Mod_Rewrite_Shop/RateProduct-3.html	Errors: request tim...	1 2	1 2 3 4 5	1 2 3	2	1066	1	5					
/artists.php	Errors: unknown h...	1 2	1 2 3 4 5	1 2 3		206	1	5					
/artists.php	Errors: request tim...	1 2	1 2 3 4 5	1 2 3	1	584	2	6					
/artists.php	Scanning	1 2	1 2 3 4 5	1 2 3	1	504		6					
/artists.php	Errors: request tim...	1 2	1 2 3 4 5	1 2 3	1	590	1	6					
/cart.php	Scanning	1 2	1 2 3 4 5	1 2 3		477		5					
/cart.php	Scanning	1 2	1 2 3 4 5	1 2 3	1	424		8					
/cart.php	Scanning	1 2	1 2 3 4 5	1 2 3		362		8					
/cart.php	Scanning	1 2	1 2 3 4 5	1 2 3		236		8					
/cart.php	Scanning	1 2	1 2 3 4 5	1 2 3		171		8					
/cart.php	Scanning	1 2	1 2 3 4 5	1 2 3									

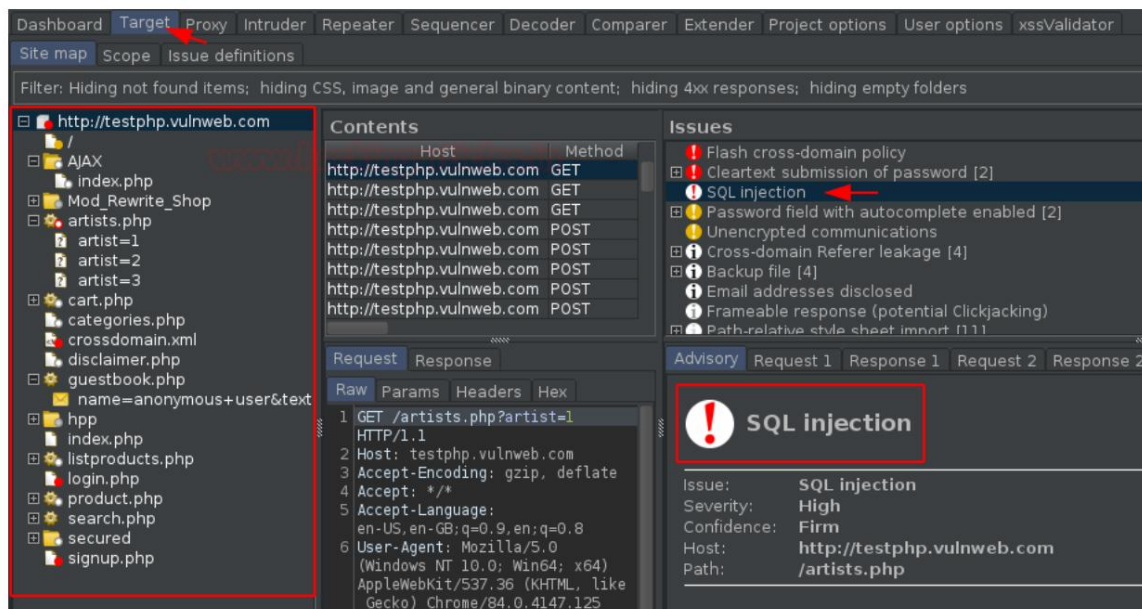
Además, incluso podemos consultar los problemas detallados que se han encontrado en la aplicación web.

Details		Audit items		Issue activity		Event log		
Filter		High	Medium	Low	Info	Certain	Firm	Tentative
#	Task	Time	Action	Issue type		Host	Path	
21	4	21:26:08 16 Dec 2020	Issue found		Path-relative style sheet import	http://testphp.vulnweb.com	/artists.php	
20	4	21:24:24 16 Dec 2020	Issue found		Path-relative style sheet import	http://testphp.vulnweb.com	/cart.php	
19	4	21:21:40 16 Dec 2020	Issue found		SQL injection	http://testphp.vulnweb.com	/artists.php	
18	4	21:20:33 16 Dec 2020	Issue found		Path-relative style sheet import	http://testphp.vulnweb.com	/AJAX/index.php	
17	4	21:19:52 16 Dec 2020	Issue found		Backup file	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/RateProduct-3.htm	
16	4	21:19:52 16 Dec 2020	Issue found		Backup file	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/RateProduct-3.htm	
15	4	21:19:41 16 Dec 2020	Issue found		Backup file	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/RateProduct-1.htm	
14	4	21:19:41 16 Dec 2020	Issue found		Backup file	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/RateProduct-1.htm	
13	4	20:59:28 16 Dec 2020	Issue found		Path-relative style sheet import	http://testphp.vulnweb.com	/	
12	4	20:52:50 16 Dec 2020	Issue found		Password field with autocomplete enabled	http://testphp.vulnweb.com	/signup.php	
11	4	20:52:50 16 Dec 2020	Issue found		Clear text submission of password	http://testphp.vulnweb.com	/signup.php	
10	4	20:52:50 16 Dec 2020	Issue found		Password field with autocomplete enabled	http://testphp.vulnweb.com	/login.php	
9	4	20:52:50 16 Dec 2020	Issue found		Clear text submission of password	http://testphp.vulnweb.com	/login.php	
8	4	20:52:50 16 Dec 2020	Issue found		Cross-domain Referer leakage	http://testphp.vulnweb.com	/http/	
7	4	20:52:50 16 Dec 2020	Issue found		Cross-domain Referer leakage	http://testphp.vulnweb.com	/	
6	4	20:52:50 16 Dec 2020	Issue found		Cross-domain Referer leakage	http://testphp.vulnweb.com	/	

Aunque incluso podremos filtrarlos según sus niveles de gravedad definidos.



No solo estas cosas, en la pestaña de destino, algo nos está esperando, es decir, los Problemas y el Aviso también se mencionan allí, pero si miramos el árbol desafiado en el panel izquierdo podemos ver algunas cosas coloridas. Los puntos principalmente rojos y grises indican que estas URL tienen vulnerabilidades existentes altas e informativas, respectivamente.



Sin embargo, en la imagen a continuación, con la opción Asesoramiento de Inyección SQL, hay un panel específico para Solicitud y Respuesta, revisemos y determinemos cómo el escáner confirma que existe una Inyección SQL.

Advisory Request 1 Response 1 Request 2 Response 2 Request 3 Response 3

SQL injection Compare responses

Issue: SQL injection
Severity: High
Confidence: Firm
Host: http://testphp.vulnweb.com
Path: /artists.php

Issue detail

The **artist** parameter appears to be vulnerable to SQL injection attacks. The payloads **71972544 or 4095=04095** and **90514291 or 9068=9069** were each submitted in the artist parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

Additionally, the payload **(select*from(select(sleep(20)))a)** was submitted in the artist parameter. The application took **20156** milliseconds to respond to the request, compared with **0** milliseconds for the original request, indicating that the injected SQL command caused a time delay.

The database appears to be MySQL.

Issue background

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe

Mientras navegamos hacia la tercera solicitud, recibimos una consulta SQL basada en tiempo inyectada en el campo "artista =".

Y cuando compartimos esta solicitud con el navegador, obtuvimos un retraso de unos 20 segundos, lo que confirma que las vulnerabilidades descargadas con el escáner se pueden activar.

Advisory Request 1 Response 1 Request 2 Response 2 Request 3 Response 3

Raw Params Headers Hex

```

1 GET /artists.php?artist=(select*from(select(sleep(20)))a) HTTP/1.1
2 Host: testphp.vulnweb.com
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/84.0.4147.125 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Referer: http://testphp.vulnweb.com/artists.php
10
11

```

Quizás te preguntes: Bueno, tengo la vulnerabilidad, pero no soy consciente de ello: ¿qué más puedo conseguir o cómo podría encadenarla para dar un golpe crucial?

Por lo tanto, para resolver este problema, tenemos una sección de definición de problema, donde simplemente podemos revisar la vulnerabilidad definida o capturada.

Issue Definitions

This listing contains the definitions of all issues that can be detected by Burp Scanner.

Name	Typical severity	Type index
OS command injection	High	0x00100100
SQL injection	High	0x00100200
SQL injection (second order)	High	0x00100210
ASP.NET tracing enabled	High	0x00100280
File path traversal	High	0x00100300
XML external entity injection	High	0x00100400
LDAP injection	High	0x00100500
XPath injection	High	0x00100600
XML injection	Medium	0x00100700
ASP.NET debugging enabled	Medium	0x00100800
HTTP PUT method is enabled	High	0x00100900
Out-of-band resource load (HTTP)	High	0x00100a00
File path manipulation	High	0x00100b00
PHP code injection	High	0x00100c00
Server-side JavaScript code injection	High	0x00100d00
Perl code injection	High	0x00100e00
Ruby code injection	High	0x00100f00
Python code injection	High	0x00100f10
Expression Language injection	High	0x00100f20
Unidentified code injection	High	0x00101000
Server-side template injection	High	0x00101080
SSI injection	High	0x00101100
Cross-site scripting (stored)	High	0x00200100
HTTP request smuggling	High	0x00200140
Web cache poisoning	High	0x00200180
HTTP response header injection	High	0x00200200
Cross-site scripting (reflected)	High	0x00200300
Client-side template injection	High	0x00200308
Cross-site scripting (DOM-based)	High	0x00200310

OS command injection

Description

Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed, and inject arbitrary further commands that will be executed by the server.

OS command injection vulnerabilities are usually very serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be possible to use the server as a platform for attacks against other systems. The exact potential for exploitation depends upon the security context in which the command is executed, and the privileges that this context has regarding sensitive resources on the server.

Remediation

If possible, applications should avoid incorporating user-controllable data into operating system commands. In almost every situation, there are safer alternative methods of performing server-level tasks, which cannot be manipulated to perform additional commands than the one intended.

If it is considered unavoidable to incorporate user-supplied data into operating system commands, the following two layers of defense should be

Definición de configuraciones de auditoría

De manera similar a la opción de rastreo, también podemos configurar esta auditoría simplemente regresando al panel de control "Nuevo escaneo" haciendo clic derecho en la URL definida y presionando Escanear.

New scan

Scan Type

- ☐ Crawl and audit
- ☐ Crawl
- ☒ Audit selected items

Items to Scan

- ☐ Add to task
- ☒ Create new task

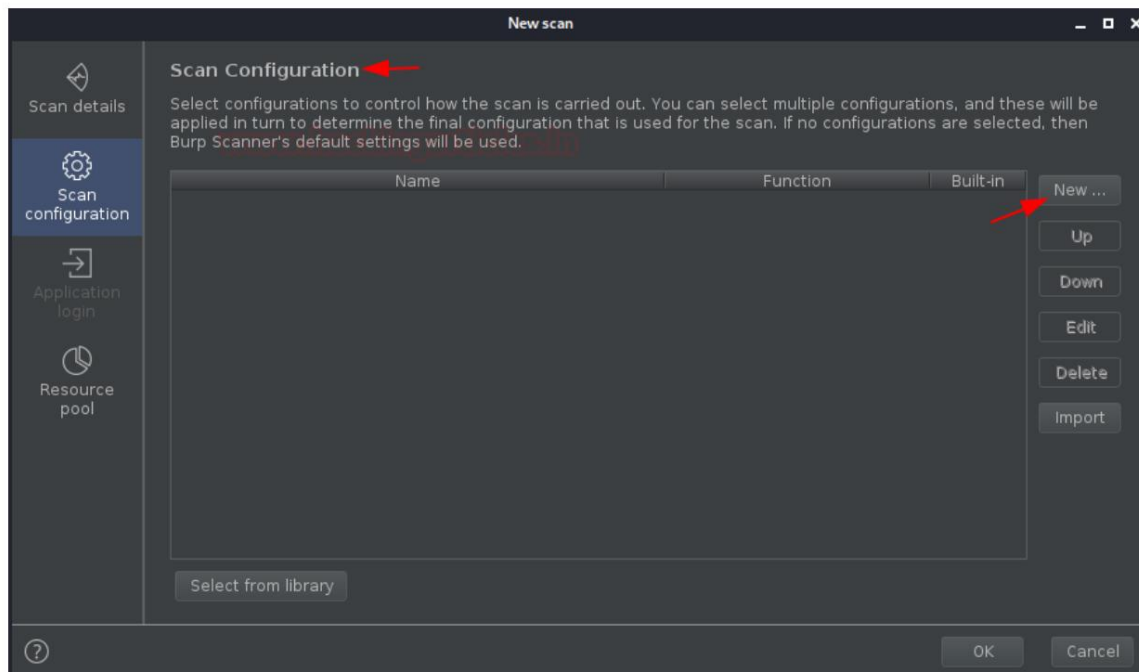
Items to Scan

- http://testphp.vulnweb.com/
- http://testphp.vulnweb.com/AJAX/index.php
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/
- http://testphp.vulnweb.com/artists.php
- http://testphp.vulnweb.com/artists.php
- http://testphp.vulnweb.com/artists.php
- http://testphp.vulnweb.com/artists.php
- http://testphp.vulnweb.com/cart.php
- http://testphp.vulnweb.com/categories.php
- http://testphp.vulnweb.com/disclaimer.php

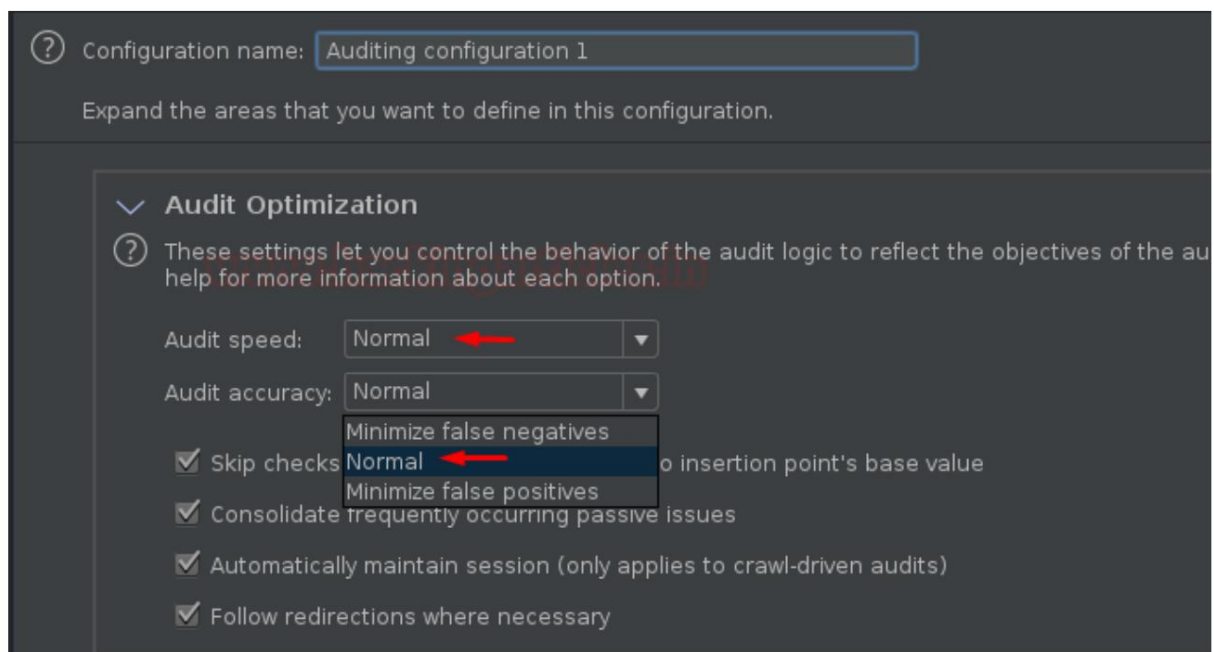
OK Cancel

Aquí, en la imagen de arriba, si nos desplazamos hacia abajo, obtendremos la misma opción para configurar la URL fuera de alcance que estaba en la sección Rastrear.

Ahora, avanzando con las configuraciones de escaneo, presione el botón "Nuevo" como hicimos antes.



Al establecer el nombre de la configuración por defecto y manipular la precisión de la auditoría a la normalidad, puede definirla según sus necesidades.



Ahora llega a la sección más importante para definir los problemas reportados seleccionando el "Tipo de escaneo". Aquí, para completar el escaneo más rápido, simplemente elijo la opción de escaneo activo ligero, pero puedes optar por cualquiera de las siguientes:

- Pasivo: estos problemas se detectan simplemente inspeccionando el comportamiento de las solicitudes de la aplicación y respuestas.
- Luz activa: aquí detecta problemas al realizar una pequeña cantidad de solicitudes adicionales benignas.


- Medio activo: estos son problemas que se pueden detectar al realizar solicitudes que la aplicación podría razonablemente considerarse malicioso.
- Intrusivo activo: estos problemas se detectan realizando solicitudes que conllevan un mayor riesgo de dañar la aplicación o sus datos. Por ejemplo, inyección SQL.
- Análisis de JavaScript: estos son problemas que se pueden detectar analizando el JavaScript que ejecuta la aplicación en el lado del cliente.

Issues Reported

? These settings control which issues Burp will check for. You can select issues by scan type or individually. If you see the detection methods that are used for some types of issues.

☒ Select by scan type:

☐ Passive

☒ Light active 

☐ Medium active

☐ Intrusive active

☐ JavaScript analysis

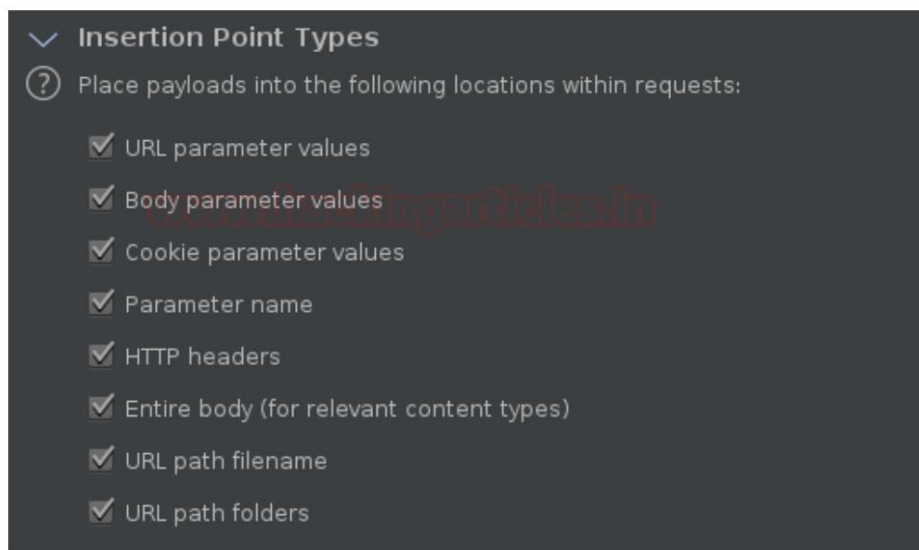
☐ Select individual issues:

Filter **Passive** **Light** **Medium** **Intrusive** **JavaScript**

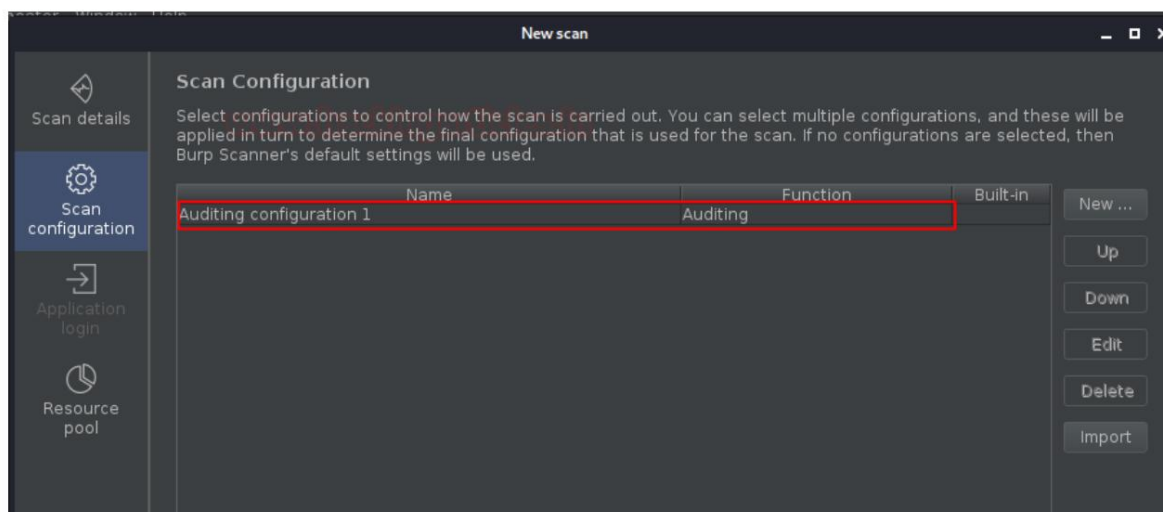
Enabled	Name	Passive	Light	Medium	Intrusive	JavaScript	Typical severity
<input checked="" type="checkbox"/>	OS command injection			•			High
<input checked="" type="checkbox"/>	SQL injection				•		High
<input checked="" type="checkbox"/>	SQL injection (second order)				•		High
<input checked="" type="checkbox"/>	ASP.NET tracing enabled			•			High
<input checked="" type="checkbox"/>	File path traversal				•		High
<input checked="" type="checkbox"/>	XML external entity injection			•			High
<input checked="" type="checkbox"/>	LDAP injection				•		High
<input checked="" type="checkbox"/>	XPath injection				•		High
<input checked="" type="checkbox"/>	XML injection				•		Medium
<input checked="" type="checkbox"/>	ASP.NET debugging enabled			•			Medium
<input checked="" type="checkbox"/>	HTTP PUT method is enabled				•		High
<input checked="" type="checkbox"/>	Out-of-band resource load (HTTP)			•			High

Es posible que conozca el concepto de puntos de inserción, ya que son las secciones más importantes para que la vulnerabilidad sea atacada. Son ubicaciones dentro de las solicitudes donde se inyectan las cargas útiles.

Sin embargo, el escáner del eructo también audita los puntos de inserción, por lo que también podría manipularse en esta fase.



Ahora que hemos terminado con la configuración y presionamos el botón "Guardar", nuestra auditoría personalizada aparece en el panel de control del Nuevo escaneo.



Sin embargo, la opción de inicio de sesión en la aplicación está deshabilitada en esta sección ya que no existe una necesidad específica de iniciar sesión en una aplicación solo para realizar pruebas de vulnerabilidad.

Por lo tanto, ahora sabemos qué sigue, es decir, presionar el botón Aceptar y pasar al tablero. Y tan pronto como lleguemos allí, obtendremos el resultado según nuestra configuración con aproximadamente 2700 solicitudes.

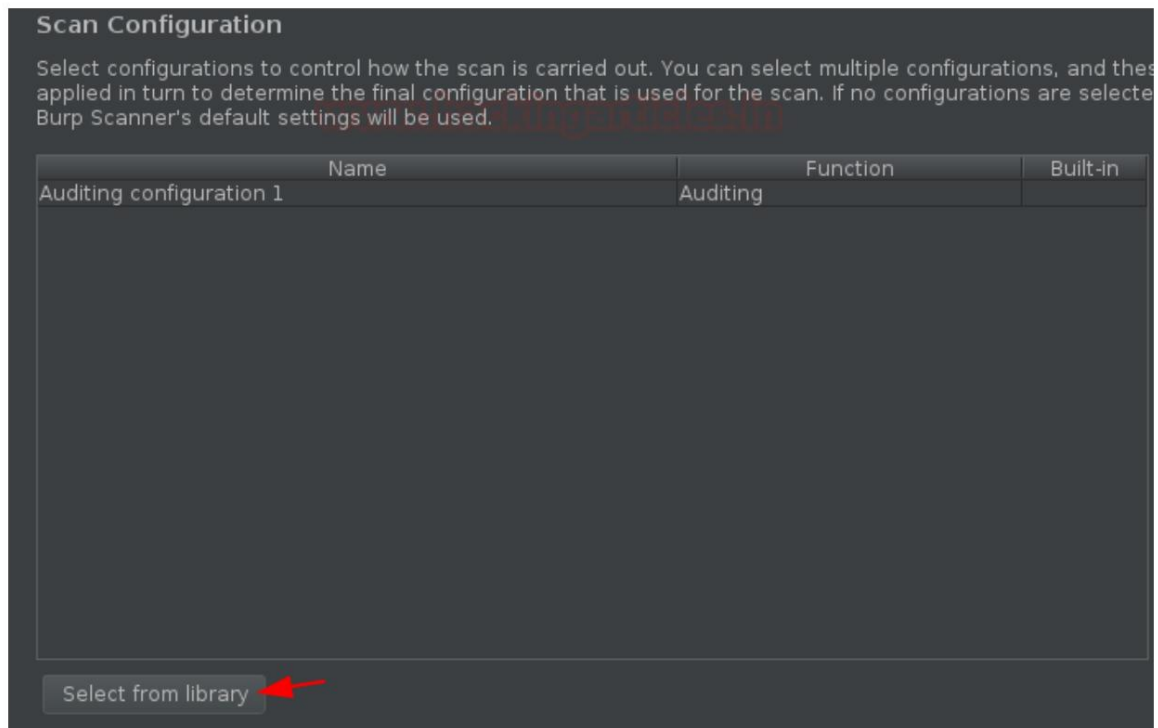
Pero esta vez, el problema principal es sólo "1"

The screenshot shows the Burp Suite interface. On the left, the 'Tasks' panel lists three tasks: 1. Live passive crawl from Proxy (all traffic), 2. Live audit from Proxy (all traffic), and 4. Audit of testphp.vulnweb.com. Task 4 is highlighted, showing 'Auditing configuration 1' with 'Issues: 1' and '2687 requests (0 errors)'. The 'Audit finished.' status is also visible. On the right, the 'Issue activity' panel shows a list of issues found, including 'Path-relative style sheet import' and 'Input returned in response (reflector)'.

Ahora, si volvemos a la pestaña Destino y seleccionamos cualquier solicitud del panel izquierdo y hacemos clic derecho allí, obtendremos 2 opciones en lugar de "1", es decir, la última personalización que configuremos entrará en esta y si compartimos alguna solicitud dentro de él, comenzará a auditarse en consecuencia.

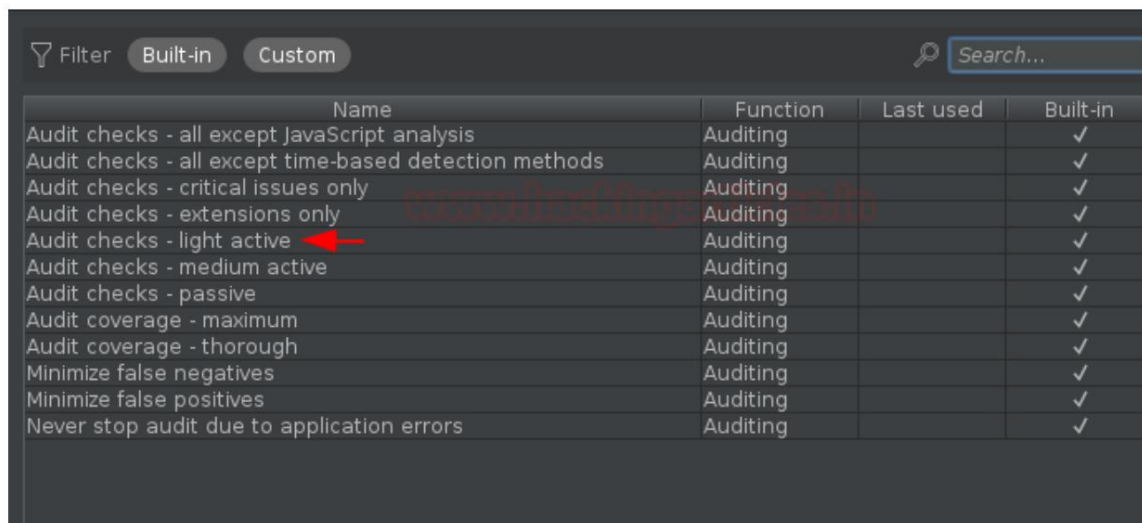
The screenshot shows the Burp Suite interface with a selected request in the 'Contents' panel. The context menu is open, showing options like 'Add to scope', 'Scan', 'Passively scan this branch', 'Actively scan this branch', 'Engagement tools', 'Compare site maps', and 'Expand branch'. The 'Scan' option is highlighted, and a red box highlights the 'Open scan launcher' and 'Add to task: 4. Auditing configuration 1' options.

De esta manera, volveremos a optar por el iniciador de escaneo abierto para verificar las otras funciones también. A medida que regresamos, nos da la bienvenida nuestra auditoría personalizada anterior, pero en la parte inferior, hay una opción "Seleccionar de la biblioteca", haga clic allí y verifique lo que ofrece.

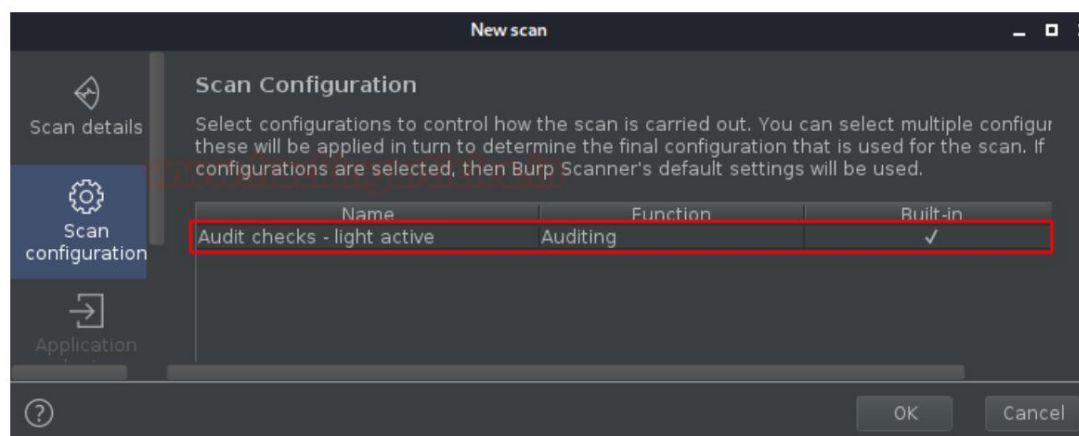


Entonces, ¿no fue un poco confuso configurar la auditoría manipulando cada opción que tiene?

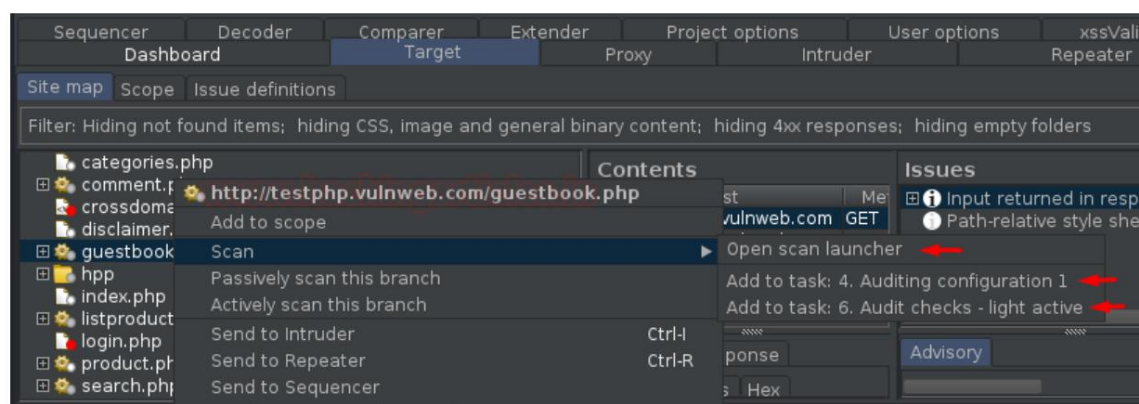
Por lo tanto, para deshacernos de esto, la suite Burp ofrece una excelente característica adicional para optar por una verificación de auditoría incorporada, donde simplemente debemos seleccionar cualquiera y continuar.



Y cuando seleccionamos uno, nuestra opción volverá a aparecer en el panel de Nuevo escaneo.



¡Presiona "Aceptar" y verifica el resultado en el tablero! Además, ahora, si navegamos a la pestaña Destino y hacemos clic derecho en cualquier solicitud, obtendremos 3 opciones en lugar de 2.



Rastreo y escaneo con un escenario avanzado

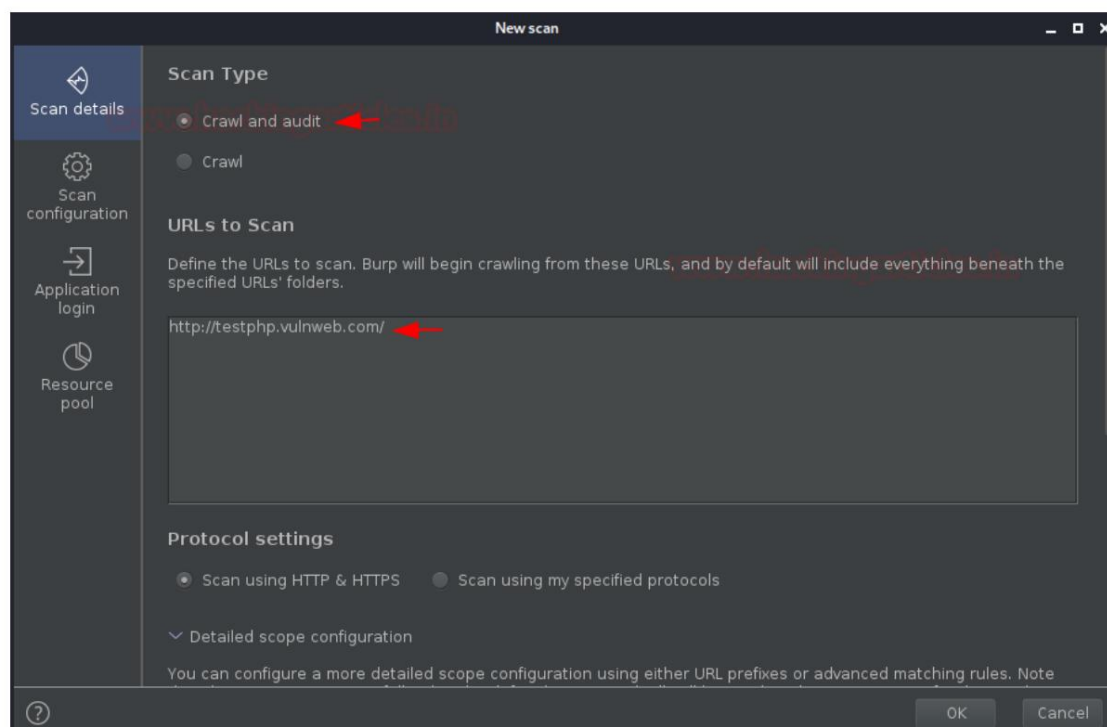
Hasta ahora, hemos usado el escáner y el rastreador individualmente, pero ¿qué pasa si queremos hacer ambas cosas juntas? Para resolver este problema también, los creadores de la suite Burp nos brindan una oportunidad de escaneo de extremo a extremo, donde nuestra suite Burp:

1. Primero rastree la aplicación y descubra los contenidos y las funcionalidades que contiene.
2. Además, comenzará a auditarlo en busca de vulnerabilidades.

Por lo tanto, para hacer todo esto, todo lo que necesita es una "URL".

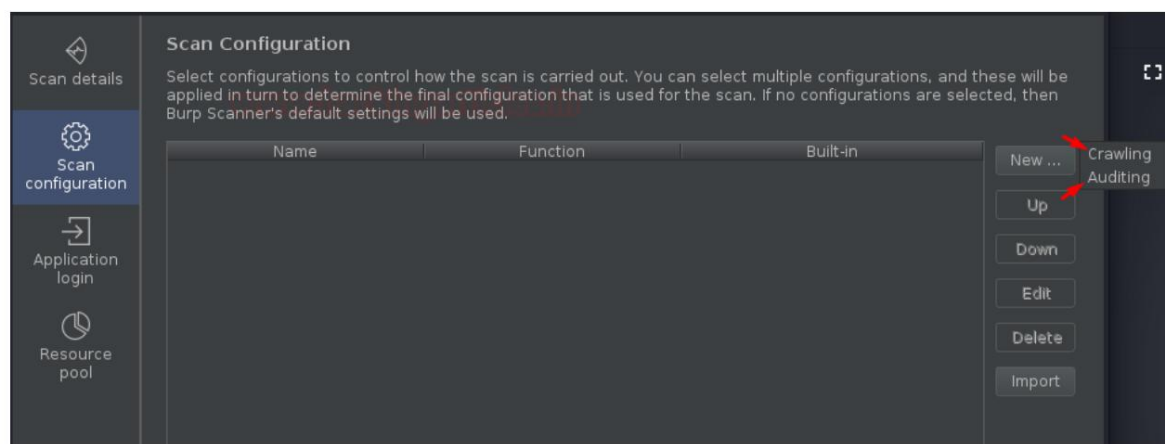
Veamos cómo podemos hacerlo.

De vuelta en el panel, seleccione "Nuevo escaneo" y ahora, esta vez, opte por "Rastrear y auditar", mencione además la URL que contiene.



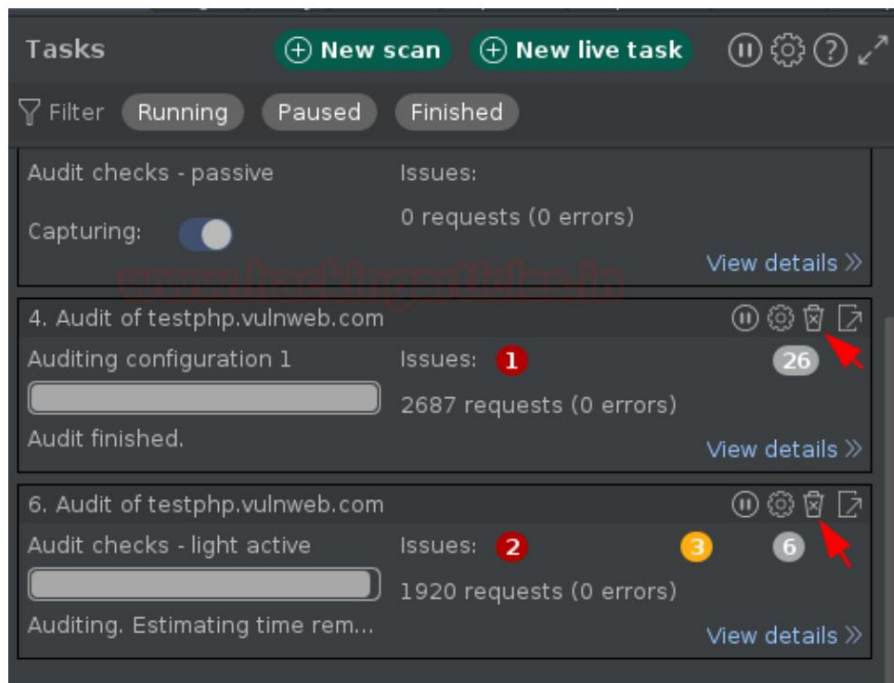
¡¡Excelente!! Ahora revisemos las opciones de Configuración de escaneo, a medida que nos movemos allí y cuando hacemos clic en el botón "Nuevo", en lugar de redirigirnos al menú de personalización, nos pregunta dónde ir, para optimización de rastreo o configuración de auditoría.

Sin embargo, todas las opciones internas son iguales.

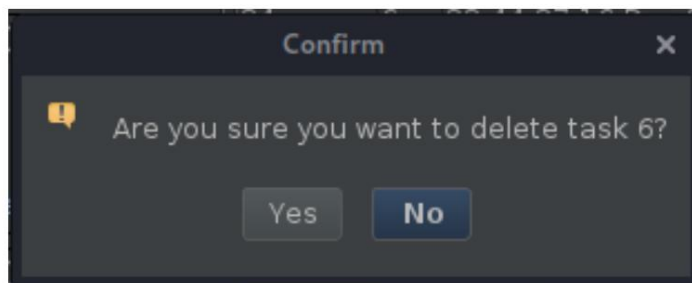


Eliminar las tareas definidas

Más bien no sólo saber cómo empezar o configurar las cosas, sino que también debemos ser conscientes de cómo finalizarlas todas. De esta manera hagamos clic en el ícono del Cubo de basura definido como una opción de Tarea, para eliminar nuestras tareas completadas o incompletas.



Y mientras lo hacemos, aparece la ventana emergente de confirmación como



ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

