

Escáner de eructos

Una característica esencial de las herramientas de proxy web son sus escáneres web. Burp Suite viene con **Burp Scanner**un poderoso escáner para varios tipos de vulnerabilidades web, que utiliza **Crawler**para construir la estructura del sitio web y **Scanner**para el escaneo pasivo y activo.


Burp Scanner es una característica exclusiva de Pro y no está disponible en la versión comunitaria gratuita de Burp Suite. Sin embargo, dado el amplio alcance que cubre Burp Scanner y las funciones avanzadas que incluye, lo convierte en una herramienta de nivel empresarial y, como tal, se espera que sea una función paga.

Alcance objetivo

Para iniciar un escaneo en Burp Suite, contamos con las siguientes opciones:

- 1. Comience a escanear en una solicitud específica del historial de proxy
- 2. Iniciar un nuevo escaneo en un conjunto de objetivos
- 3. Inicie un escaneo de elementos dentro del alcance

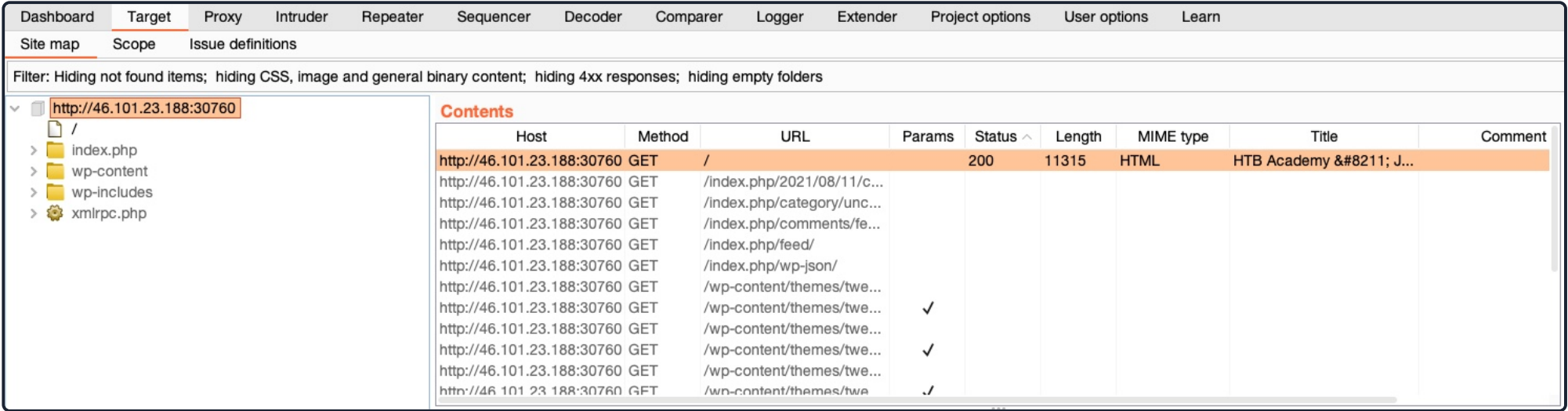
Para iniciar un escaneo en una solicitud específica del historial de proxy, podemos hacer clic con el botón derecho en él una vez que lo ubiquemos en el historial y luego seleccionar **Scan**para poder configurar el escaneo antes de ejecutarlo, o seleccionar **Passive/Active Scan**para iniciar rápidamente un escaneo con las configuraciones por defecto:

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options	Learn
Intercept	HTTP history	WebSockets history	Options									
Filter: Hiding CSS, image and general binary content												
# 	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title		
15	http://142.93.35.92:30269	GET	/			200	11297	HTML		HTB Academy – J...		
13	http://142.93.35.92:30269	http://142.93.35.92:30269/	s/comment-reply.min.js?...	✓		200	3274	script	js			
12	http://142.93.35.92:30269	Add to scope	1/08/11/customer-supp...			200	16348	HTML		Customer Support – J...		
11	http://142.93.35.92:30269					404	457	HTML	ico	404 Not Found		
9	http://142.93.35.92:30269	Scan	s/wp-emoji-release.min.j...	✓		200	18473	script	js			
8	http://142.93.35.92:30269	Do passive scan	s/wp-embed.min.js?ver=...	✓		200	1716	script	js			
6	http://142.93.35.92:30269	Do active scan	emes/twentytwentyone/...	✓		200	1417	script	js			

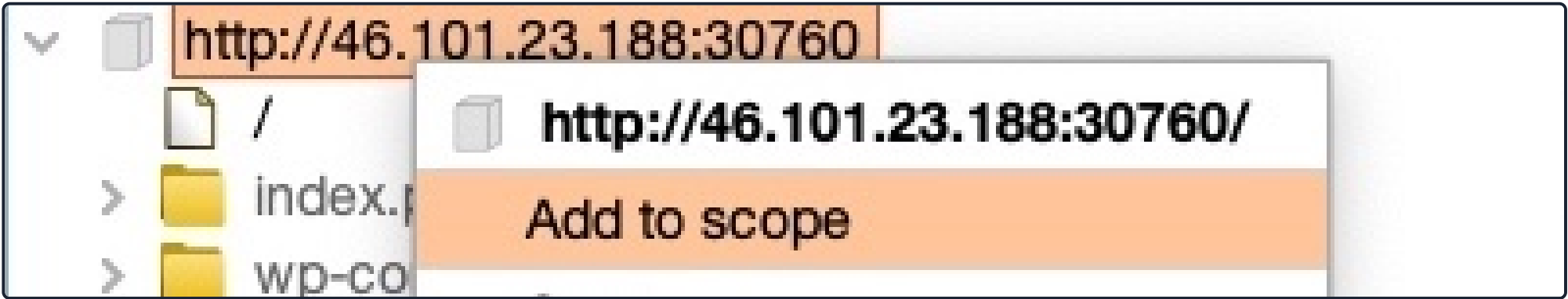
También podemos hacer clic en el **New Scan**botón de la **Dashboard**pestaña, que abriría la **New Scan**ventana de configuración para configurar un escaneo en un conjunto de objetivos personalizados. En lugar de crear un escaneo personalizado desde cero, veamos cómo podemos utilizar el alcance para definir correctamente lo que se incluye/excluye de nuestros escaneos usando el archivo **Target Scope**. Se **Target Scope**puede utilizar con todas las funciones de Burp para definir un conjunto personalizado de objetivos que se procesarán. Burp también nos permite limitar Burp a elementos dentro del alcance para ahorrar recursos ignorando cualquier URL fuera del alcance.

Nota: escanearemos la aplicación web del ejercicio que se encuentra al final de la siguiente sección. Si obtiene una licencia para usar Burp Pro, puede generar el objetivo al final de la siguiente sección y seguir hasta aquí.

Si vamos a (**Target>Site map**), mostrará una lista de todos los directorios y archivos que burp ha detectado en varias solicitudes que pasaron por su proxy:

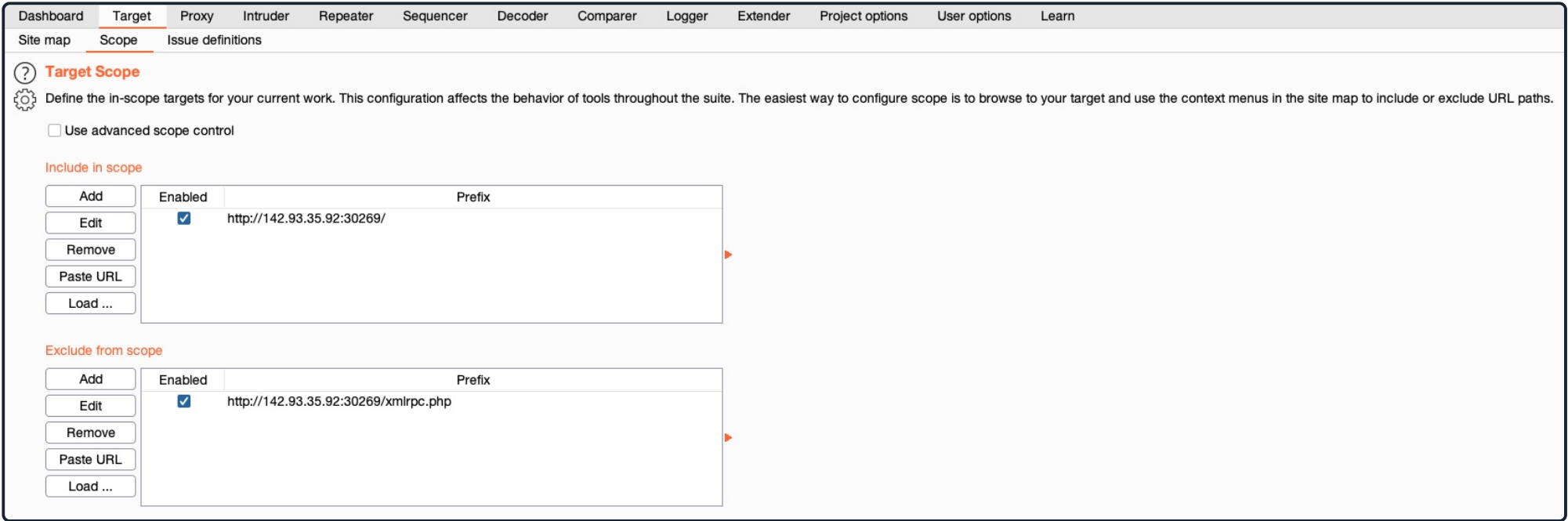


Para agregar un elemento a nuestro alcance, podemos hacer clic derecho sobre él y seleccionar **Add to scope**:



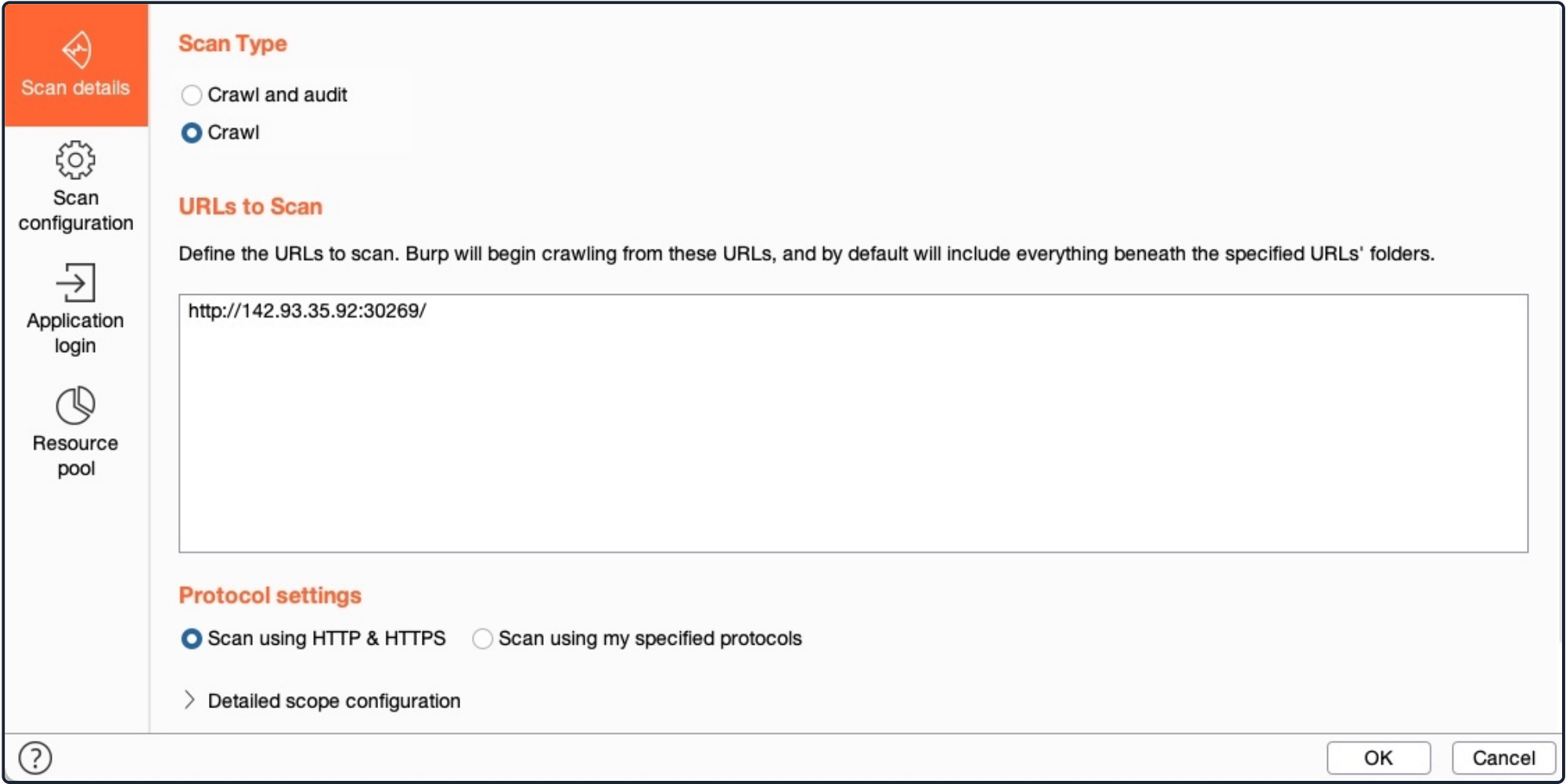
Nota: Cuando agregue el primer elemento a su alcance, Burp le dará la opción de restringir sus funciones solo a los elementos dentro del alcance e ignorar cualquier elemento fuera del alcance.

También es posible que debamos excluir algunos elementos del alcance si escanearlos puede ser peligroso o puede finalizar nuestra sesión 'como una función de cierre de sesión'. Para excluir un elemento de nuestro alcance, podemos hacer clic derecho en cualquier elemento dentro del alcance y seleccionar **Remove from scope**. Finalmente, podemos ir a (**Target>Scope**) para ver los detalles de nuestro alcance. Aquí, también podemos agregar/eliminar otros elementos y usar el control de alcance avanzado para especificar los patrones de expresiones regulares que se incluirán/excluirán.



Tractor

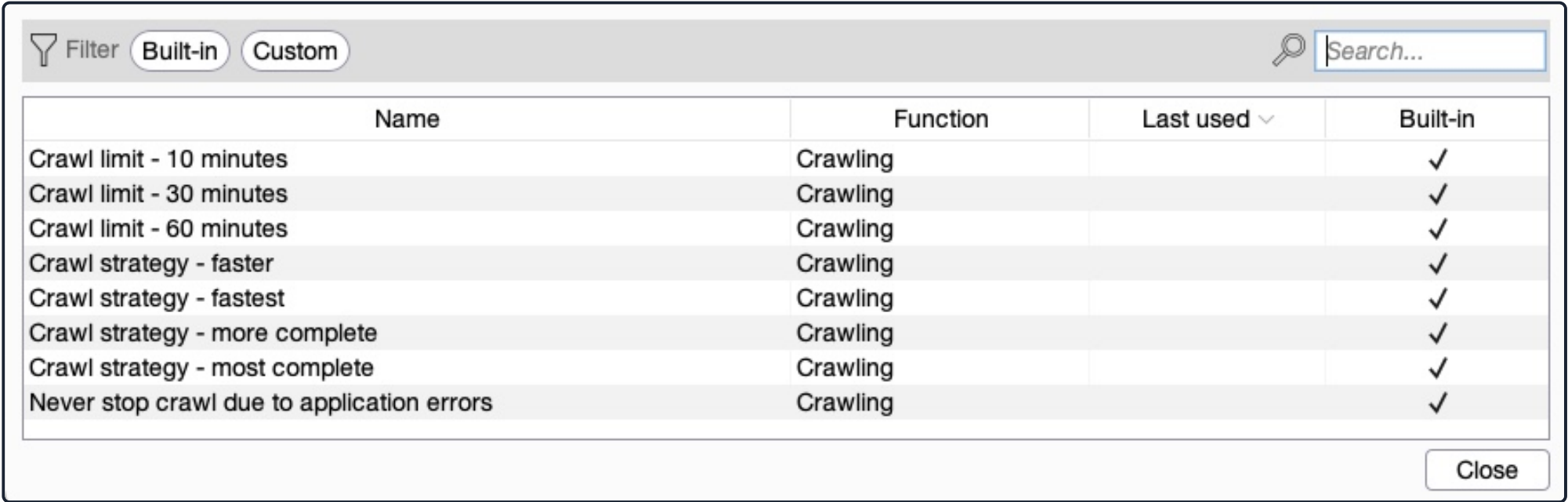
Una vez que tengamos nuestro alcance listo, podemos ir a la **Dashboard** pestaña y hacer clic en **New Scan** para configurar nuestro escaneo, que se completará automáticamente con nuestros elementos dentro del alcance:



Vemos que Burp nos da dos opciones de escaneo: **Crawl and Audit** y **Crawl**. Un Web Crawler navega por un sitio web accediendo a cualquier enlace que se encuentre en sus páginas, accediendo a cualquier formulario y examinando cualquier solicitud que haga para crear un mapa completo del sitio web. Al final, Burp Scanner nos presenta un mapa del objetivo, mostrando todos los datos de acceso público en un solo lugar. Si seleccionamos **Crawl and Audit**, Burp ejecutará su escáner después de su Crawler (como veremos más adelante).

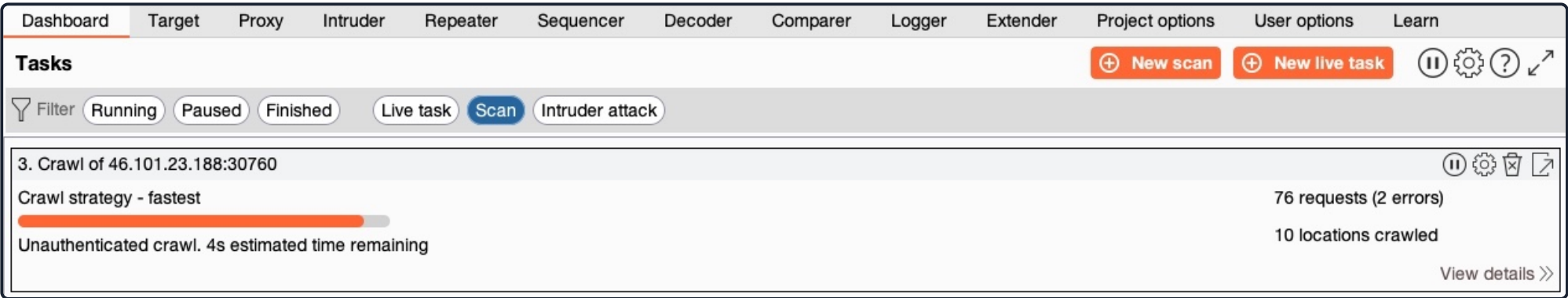
Nota: Un escaneo de rastreo solo sigue y mapea los enlaces que se encuentran en la página que especificamos, y cualquier página que se encuentre en ella. No realiza un análisis de fuzzing para identificar páginas a las que nunca se hace referencia, como lo harían dirbuster o ffuf. Esto se puede hacer con Burp Intruder o Content Discovery, y luego se puede agregar al alcance, si es necesario.

Seleccionemos **Crawl** como inicio y vayamos a la **Scan configuration** pestaña de configurar nuestro escaneo. Desde aquí, podemos optar por hacer clic en **New** para crear una configuración personalizada, lo que nos permitiría establecer configuraciones como la velocidad o el límite de rastreo, si Burp intentará iniciar sesión en cualquier formulario de inicio de sesión y algunas otras configuraciones. En aras de la simplicidad, haremos clic en el **Select from library** botón, que nos brinda algunas configuraciones preestablecidas entre las que podemos elegir (o configuraciones personalizadas que definimos previamente):



Seleccionaremos la **Crawl strategy - fastest** opción y continuaremos hasta la **Application login** pestaña. En esta pestaña, podemos agregar un conjunto de credenciales para que Burp intente en cualquier formulario/campo de inicio de sesión que pueda encontrar. También podemos registrar un conjunto de pasos realizando un inicio de sesión manual en el navegador preconfigurado, de modo que Burp sepa qué pasos seguir para obtener una sesión de inicio de sesión. Esto puede ser esencial si estuviéramos ejecutando nuestro análisis con un usuario autenticado, lo que nos permitiría cubrir partes de la aplicación web a las que Burp no tendría acceso de otro modo. Como no tenemos ninguna credencial, lo dejaremos vacío.

Con eso, podemos hacer clic en el **Ok** botón para iniciar nuestro escaneo de rastreo. Una vez que comienza nuestro escaneo, podemos ver su progreso en la **Dashboard** pestaña debajo **Tasks**:



También podemos hacer clic en el **View details** botón de las tareas para ver más detalles sobre el análisis en ejecución o hacer clic en el ícono de ajustes para personalizar aún más nuestras configuraciones de análisis. Finalmente, una vez que se complete nuestro escaneo, veremos **Crawl Finished** en la información de la tarea, y luego podemos volver a (**Target>Site map**) para ver el mapa del sitio actualizado:

<div><div>http://46.101.23.188:30760</div><div><div>devtools</div><div>index.php</div><div>2021</div><div>author</div><div>category</div><div>comments</div></div></div>	Contents							
	Host	Method	URL	Params	Status ^	Length	MIME type	Title
	http://46.101.23.188:30760	GET	/		200	11315	HTML	HTB Academy – J...
	http://46.101.23.188:30760	GET	?s=126723	✓	200	11390	HTML	Search Results for R...
	http://46.101.23.188:30760	GET	?s=204965	✓	200	11390	HTML	Search Results for R...
	http://46.101.23.188:30760	GET	?s=564658	✓	200	11390	HTML	Search Results for R...
	http://46.101.23.188:30760	GET	?s=609701	✓	200	11390	HTML	Search Results for R...
	http://46.101.23.188:30760	GET	?s=763331	✓	200	11390	HTML	Search Results for R...

Escáner pasivo

Ahora que el mapa del sitio está completamente construido, podemos seleccionar escanear este objetivo en busca de posibles vulnerabilidades. Cuando elegimos la **Crawl and Audit** opción en el **New Scan** cuadro de diálogo, Burp realizará dos tipos de escaneos: A **Passive Vulnerability Scan** y an **Active Vulnerability Scan**.

A diferencia de un Active Scan, un Passive Scan no envía nuevas solicitudes, sino que analiza el origen de las páginas ya visitadas en el objetivo/alcance y luego intenta identificar **potential** vulnerabilidades. Esto es muy útil para un análisis rápido de un objetivo específico, como etiquetas HTML faltantes o posibles vulnerabilidades XSS basadas en DOM. Sin embargo, sin enviar ninguna solicitud para probar y verificar estas vulnerabilidades, un escaneo pasivo solo puede sugerir una lista de posibles vulnerabilidades. Aún así, Burp Passive Scanner proporciona un nivel de **Confidence** para cada vulnerabilidad identificada, lo que también es útil para priorizar vulnerabilidades potenciales.

Comencemos intentando realizar solo un escaneo pasivo. Para hacerlo, podemos volver a seleccionar el objetivo en (**Target>Site map**) o una solicitud en Burp Proxy History, luego hacer clic derecho sobre él y seleccionar **Do passive scan** o **Passively scan this target**. El escaneo pasivo comenzará a ejecutarse y su tarea también se puede ver en la **Dashboard** pestaña. Una vez finalice el escaneo, podemos hacer clic en **View Details** para revisar las vulnerabilidades identificadas y luego seleccionar la **Issue activity** pestaña:

Details Audit items Issue activity Event log Logger									
Filter High Medium Low Info Certain Firm Tentative									
#	Task	Time	Action	Issue type	Host	Path	Insertion point	Severity	Confidence
9	7		Issue found	Cookie without HttpOnly flag set	http://142.93.35.92:32729	/wp-comments-post.php		Information	Certain
8	7		Issue found	Frameable response (potential Clickjacking)	http://142.93.35.92:32729	/index.php/author/academy/		Information	Firm
7	7		Issue found	Cross-domain Referer leakage	http://142.93.35.92:32729	/		Information	Certain
6	7		Issue found	Frameable response (potential Clickjacking)	http://142.93.35.92:32729	/index.php/2021/08/11/customer-support/		Information	Firm

Alternativamente, podemos ver todos los problemas identificados en el **Issue activity** panel de la **Dashboard** pestaña. Como podemos ver, muestra la lista de vulnerabilidades potenciales, su gravedad y su confianza. Por lo general, queremos buscar vulnerabilidades con **High** severidad y **Certain** confianza. Sin embargo, debemos incluir todos los niveles de severidad y confianza para aplicaciones web muy sensibles, con un enfoque especial en la **High** severidad y **Confident/Firm** la confianza.

Escáner activo

Finalmente llegamos a la parte más poderosa de Burp Scanner, que es su Active Vulnerability Scanner. Un escaneo activo ejecuta un escaneo más completo que un escaneo pasivo, de la siguiente manera:

1. Comienza ejecutando un rastreo y un fuzzer web (como dirbuster/ffuf) para identificar todas las páginas posibles

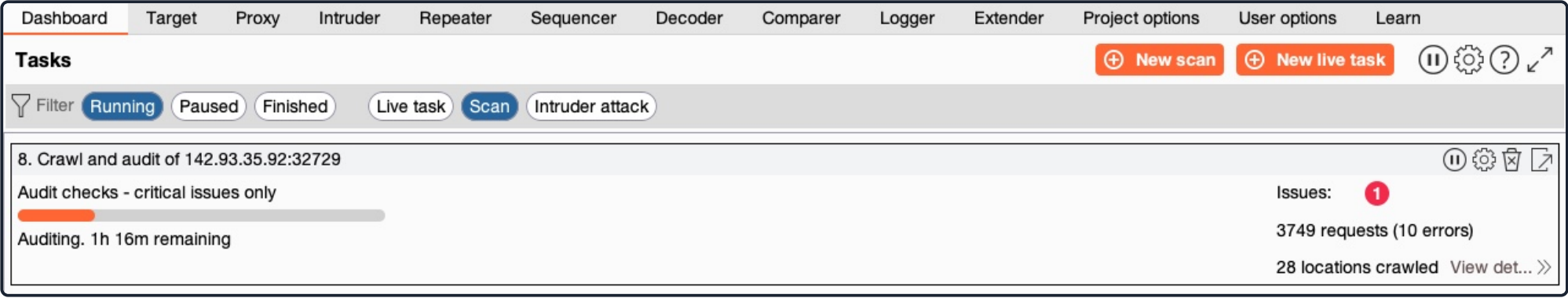
2. Ejecuta un escaneo pasivo en todas las páginas identificadas
3. Comprueba cada una de las vulnerabilidades identificadas del Escaneo Pasivo y envía solicitudes para verificarlas
4. Realiza un análisis de JavaScript para identificar más vulnerabilidades potenciales.
5. Analiza varios puntos de inserción y parámetros identificados para buscar vulnerabilidades comunes como XSS, inyección de comandos, inyección SQL y otras vulnerabilidades web comunes.

El escáner Burp Active se considera una de las mejores herramientas en ese campo y se actualiza con frecuencia para buscar vulnerabilidades web recientemente identificadas por el equipo de investigación de Burp.

Podemos iniciar un Escaneo activo de manera similar a como comenzamos un Escaneo pasivo seleccionando **Do active scan** desde el menú contextual en una solicitud en Burp Proxy History. Alternativamente, podemos ejecutar un escaneo en nuestro alcance con el **New Scan** botón en la **Dashboard** pestaña, lo que nos permitiría configurar nuestro escaneo activo. En esta ocasión, seleccionaremos la **Crawl and Audit** opción que realizaría todos los puntos anteriores y todo lo que hemos comentado hasta ahora.

También podemos establecer las configuraciones de Rastreo (como discutimos anteriormente) y las configuraciones de Auditoría. Las configuraciones de Auditoría nos permiten seleccionar qué tipo de vulnerabilidades queremos escanear (predeterminado en todas), dónde el escáner intentaría insertar sus cargas útiles, además de muchas otras configuraciones útiles. De nuevo, podemos seleccionar un preset de configuración con el **Select from library** botón . Para nuestra prueba, dado que estamos interesados en **High** las vulnerabilidades que pueden permitirnos obtener control sobre el servidor backend, seleccionaremos la **Audit checks - critical issues only** opción. Finalmente, podemos agregar detalles de inicio de sesión, como vimos anteriormente con las configuraciones de rastreo.

Una vez que seleccionamos nuestras configuraciones, podemos hacer clic en el **Ok** botón para iniciar el escaneo, y la tarea de escaneo activo debe agregarse en el **Tasks** panel en la **Dashboard** pestaña:



El análisis ejecutará todos los pasos mencionados anteriormente, por lo que tardará mucho más en finalizar que nuestros análisis anteriores, según las configuraciones que hayamos seleccionado. A medida que se ejecuta el análisis, podemos ver las diversas solicitudes que está realizando haciendo clic en el **View details** botón y seleccionando la **Logger** pestaña, o yendo a la **Logger** pestaña en Burp, que muestra todas las solicitudes que pasó o realizó Burp:

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options	Learn
Capture filter: Logger memory limit set to 100MB Capturing requests up to 1MB; capturing responses up to 1MB												
View filter: Showing all items												
#	Time	Tool	Method	Host	Path	Query	Param count	Status	Length	S		
3495		Scanner	GET	142.93.35.92	/index.php/search/18508...		0	404	11066	123		
3494		Scanner	GET	142.93.35.92	/index.php47320044'%2...		0	404	457	109		
3493		Scanner	GET	142.93.35.92	/index.php/search/18508...		0	404	11066	121		
3492		Scanner	GET	142.93.35.92	/index.php')waitfor%20d...		0	404	457	108		
3491		Scanner	GET	142.93.35.92	/index.php/search/18508...		0	404	11066	124		
3490		Scanner	GET	142.93.35.92	/index.php/search/18508...		0	404	11066	122		
3489		Scanner	GET	142.93.35.92	/index.php'%20waitfor%...		0	404	457	110		
3487		Scanner	GET	142.93.35.92	/index.php'%2b(select*fr...		0	404	457	109		
3486		Scanner	GET	142.93.35.92	/wp-includes/js/wp-embe...	ver=5.8	1	404	457	107		
3483		Scanner	GET	142.93.35.92	/wp-content/themes/twe...	ver=1.4	1	404	457	108		
3482		Scanner	GET	142.93.35.92	/wp-content/themes/twe...	ver=1.4	1	404	457	108		
3481		Scanner	GET	142.93.35.92	/wp-content/themes/twe...	ver=1.4	1	404	457	107		

Una vez que se realiza el escaneo, podemos mirar el **Issue activity** panel en la **Dashboard** pestaña para ver y filtrar todos los problemas identificados hasta el momento. Del filtro arriba de los resultados, seleccionemos **Highly Certain** veamos nuestros resultados filtrados:

Details		Audit items		Issue activity		Event log		Logger	
Filter		High		Medium		Low		Info	
		Certain		Firm		Tentative			
#	Task	Time		Action		Issue type		Host	
10	8			Issue found		OS command injection		http://142.93.35.92:32729	

Vemos que Burp identificó una **OS command injection** vulnerabilidad, que se clasifica con una **High** gravedad y **Firm** confianza. Como Burp confía firmemente en que existe esta vulnerabilidad grave, podemos leer sobre ella haciendo clic en ella y leyendo el aviso que se muestra y ver la solicitud enviada y la respuesta recibida, para poder saber si la vulnerabilidad se puede explotar o cómo plantea un problema. amenaza en el servidor web:

AdvisoryRequestResponse

!

OS command injection

Issue:OS command injection

Severity:High

Confidence:Firm

Host:http://142.93.35.92:32729

Path:

Issue detail

The parameter appears to be vulnerable to OS command injection attacks. It is possible to use the pipe character (|) to inject arbitrary OS commands and retrieve the output in the application's responses.

The payload |echo 7lyf4yq3fl h8zqfsgedv||a #| |echo 7lyf4yq3fl h8zqfsgedv||a #| |echo 7lyf4yq3fl h8zqfsgedv||a # was submitted in the parameter. The application's response appears to contain the output of the injected command.

Informes

Finalmente, una vez que se hayan completado todos nuestros escaneos y se hayan identificado todos los problemas potenciales, podemos ir a (**Target>Site map**), hacer clic con el botón derecho en nuestro objetivo y seleccionar (**Issue>Report issues for this host**). Se nos pedirá que seleccionemos el tipo de exportación para el informe y qué información nos gustaría incluir en el informe. Una vez que exportamos el informe, podemos abrirlo en cualquier navegador web para ver sus detalles:

Burp Scanner Report

Burp Suite

Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			Total
		Certain	Firm	Tentative	
Severity	High	0	1	0	1
	Medium	0	0	0	0
	Low	1	0	0	1
	Information	2	3	0	5

Como podemos ver, el informe de Burp está muy organizado y se puede personalizar para incluir solo problemas seleccionados por gravedad/confianza. También muestra detalles de prueba de concepto sobre cómo explotar la vulnerabilidad e información sobre cómo remediarla. Estos informes se pueden utilizar como datos complementarios para los informes detallados que preparamos para nuestros clientes o los desarrolladores de aplicaciones web al realizar una prueba de penetración web o se pueden almacenar para nuestra futura referencia. Nunca debemos simplemente exportar un informe de cualquier herramienta de penetración y enviarlo a un cliente como entrega final. En cambio, los informes y los datos generados por las herramientas pueden ser útiles como datos de apéndice para los clientes que pueden necesitar los datos de escaneo sin procesar para los esfuerzos de remediación o para importarlos a un tablero de seguimiento.


 Hoja de trucos

Tabla de contenido

Empezando

Introducción a los servidores proxy web	✓
Configuración	✓


Proxy web

Configuración de proxy	✓
 Interceptar solicitudes web	
Interceptar respuestas	✓
Modificación Automática	✓
 Repetición de solicitudes	
 Decodificación de codificación	
 Herramientas de proxy	

fuzzer web

-  Intruso eructar
-  Fuzzer ZAP

Escáner web

- [Escáner de eructos](#)
-  Escáner ZAP
- Extensiones

Evaluación de habilidades

-  Evaluación de habilidades: uso de servidores proxy web

Mi estación de trabajo

DESCONECTADO

 Instancia de inicio

∞ / Quedan 1 engendros