Laboratorio. Inspector

Contenido

1. Introducción

Este laboratorio nos guiará por el análisis de una aplicación web usando solo las herramientas integradas del navegador, aprenderemos a verificar manualmente una aplicación web en busca de vulnerabilidades de seguridad. Las herramientas y scripts de seguridad automatizados a menudo pasan por alto una gran cantidad de información y vulnerabilidades potencialmente peligrosas.

A continuación, se muestra un breve resumen de las herramientas que integran los navegadores modernos (Google Chrome o Firefox) que se utilizarán en este laboratorio:

- **Ver código fuente**: utilice su navegador para ver el código fuente legible de un sitio web.
- **Inspector de elementos**: aprenda a inspeccionar elementos de la página y realizar cambios para ver contenido normalmente bloqueados.
- **Fuentes**: inspecciona y controla el flujo de JavaScript de una página.
- **Red**: vea todas las solicitudes de red que realiza una página.
- **Aplicación - Cookies**: vea todas las cookies almacenadas en su equipo por un sitio web.

2. Explorar el sitio web

Como responsable de una auditoria de seguridad, su función es analizar un sitio web o una aplicación para descubrir características que puedan ser vulnerables e intentar explotarlas. A menudo, se trata de vulnerabilidades que requieren la interacción del usuario.

Encontrar secciones interactivas de un sitio web puede ser tan sencillo como observar un formulario de inicio de sesión o analizar el comportamiento de los scripts. Un buen punto de partida sería empezar por navegar por el sitio web y anotar las distintas páginas, áreas y funciones con un resumen de cada una.

Característica	URL	Resumen
Página de inicio	/index.php	En esta página aparece un resumen del sitio web y el equipo que lo componen.
Página de noticas	/noticias.php	En esta página aparecen las ultimas noticias. Se muestra un modal que impide la visualización a usuarios no premium.
Pagína de contacto	/contacto.php	En esta página aparece un formulario de contacto con tres campos, nombre, email y mensaje.

3. Ver el código fuente de una página

El código fuente de la página es el código legible por humanos que el servidor web devuelve a nuestro navegador/cliente cada vez que realizamos una solicitud.

El código devuelto se compone de HTML (lenguaje de marcado de hipertexto), CSS (hojas de estilo en cascada) y JavaScript, y es lo que le dice a nuestro navegador qué contenido mostrar, cómo mostrarlo y agrega un elemento de interactividad con JavaScript.

Para nuestros propósitos, ver **el código fuente de la página puede ayudarnos a descubrir más información sobre la aplicación web**.

¿Cómo puedo ver el código fuente de la página?

Mientras visualiza un sitio web, puede hacer **clic derecho** en la página y verá una opción en el menú que dice **Ver código fuente de la página** o pulsar **Ctrl+U**

La mayoría de los navegadores admiten colocar view-source: delante de la URL, por ejemplo, view-source:https://www.google.com/

Intente ver el código fuente de la página de inicio del sitio web del laboratorio. Lamentablemente, explicar todo lo que aparece está fuera del alcance de este laboratorio y deberá buscar cursos de diseño y desarrollo de sitios web para comprenderlo por completo. Nos centraremos en información que sea importante para nosotros.

En la parte superior de la página, verás que hay un código que comienza con <!-- y termina con --> , estos son comentarios. Los comentarios son mensajes que deja el desarrollador del sitio web, generalmente para explicar algo en el código a otros programadores o incluso notas/recordatorios para ellos mismos. Estos comentarios no están visibles en la web. Este comentario describe cómo la página de inicio es temporal mientras se desarrolla una nueva. Mira la página web en el comentario para obtener tu primera bandera.

¿Cuál es la bandera que puedes obtener en un comentario HTML?

Los enlaces a diferentes páginas se escriben en etiquetas de anclaje (son elementos HTML que comienzan con <a), y el enlace al que será dirigido se establece en el atributo href.

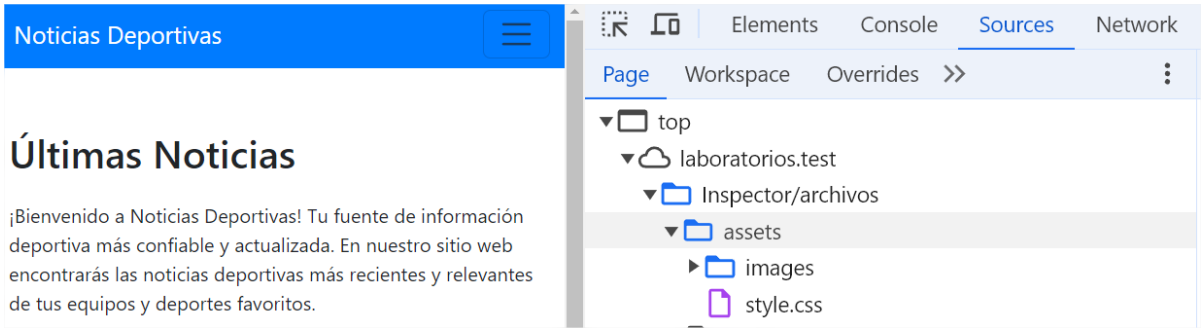
Por ejemplo, si miras en el pie de la página de inicio, hay un enlace oculto a una página llamada "secret.php". Mira este enlace para obtener otra bandera. Obviamente, no obtendrías una bandera en una situación real, pero puedes descubrir un área privada utilizada por la empresa, el personal o los clientes.

¿Cuál es la bandera que se encuentra en una página secreta?

Los archivos externos, como CSS, JavaScript e imágenes, se pueden incluir mediante el código HTML. En este ejemplo, notará que todos estos archivos se almacenan en el mismo directorio. Si visualiza este directorio en su navegador web, hay un error de configuración. Lo que debería aparecer es una página en blanco o

una página 403 Prohibida con un error que indique que no tiene acceso al directorio. En cambio, se ha habilitado la función de listado de directorios, que de hecho enumera todos los archivos del directorio. A veces, esto no es un problema y todos los archivos del directorio son seguros para que los vea el público, pero en algunos casos, los archivos de respaldo, el código fuente u otra información confidencial podrían almacenarse aquí.

Podemos utilizar la herramienta “Fuentes” (Ctrl+I) de nuestro navegador para listar directorios:



¿Cuál es la bandera que se encuentra en el directorio de recursos?

Ver el código fuente de la página puede darnos pistas sobre si usa un framework y, de ser así, qué framework e incluso qué versión. Conocer el framework y la versión puede ser una pista importante, ya que puede haber vulnerabilidades públicas en ese framework y es posible que el sitio web no esté usando la versión más actualizada. En la parte inferior de la página principal, encontrará un comentario sobre el framework y la versión que se está usando y un enlace al sitio web del framework. Al ver el sitio web del framework, observará que está desactualizado. Lea la ruta de cambios y use esta información para encontrar otra bandera.

¿Cuál es la bandera obtenida gracias a un framework desactualizado?

4. Inspector elementos

Todos los navegadores modernos incluyen herramientas para desarrolladores; se trata de un conjunto de herramientas que se utiliza para ayudar a los desarrolladores web a depurar aplicaciones web. Como pentester, podemos aprovechar estas herramientas para que nos proporcionen una mejor comprensión de la aplicación web. Nos centraremos específicamente en cuatro características del kit de herramientas para desarrolladores: **Inspector elementos**, **Fuente**, **Red y Aplicación**.

La forma de acceder a las herramientas para desarrolladores es diferente para cada navegador Por lo general, pude hacer clic con el segundo botón en la página, y en el menú desplegables elegir “Inspeccionar”. Puede intentar pulsar **Ctrl+I**.

El código fuente de la página no siempre representa lo que se muestra en una página web; esto se debe a que CSS, JavaScript y la interacción del usuario pueden cambiar el contenido y el estilo de la página, lo que significa que necesitamos una forma de ver lo que se ha mostrado en la ventana del navegador

en este momento exacto. El inspector de elementos nos ayuda con esto al proporcionarnos una representación en vivo de lo que está actualmente en el sitio web. Además de ver esta vista en vivo, también **podemos editar e interactuar con los elementos de la página**, lo que resulta útil para que los desarrolladores web puedan depurar problemas.

En el sitio web del laboratorio, haga clic en la sección de noticias, donde verá un modal que oculta las noticas a los usuarios no premium. El modal es un cuadro flotante que bloquea el contenido de la página. Con la herramienta “Elementos” de Inspeccionar puede seleccionar este modal y eliminarlo.

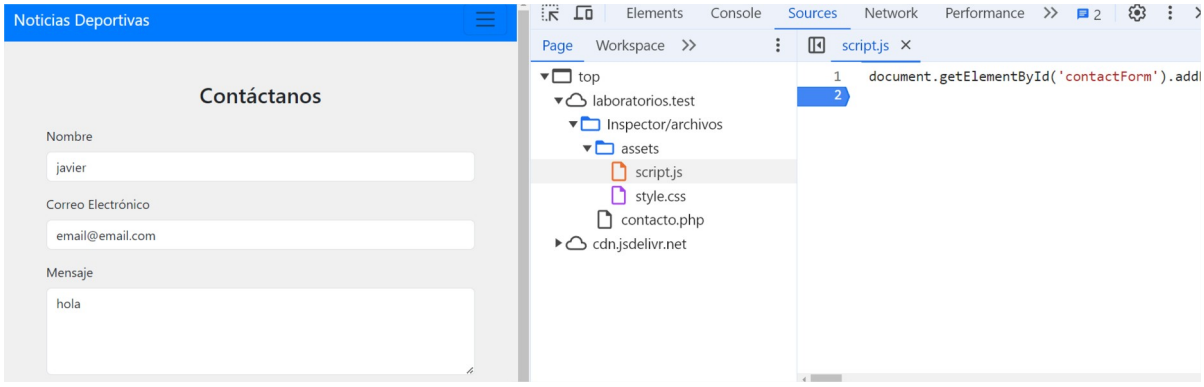
¿Cuál es la bandera que se encuentra en la página de noticias tras el modal?

5. Fuentes

Este panel de las herramientas para desarrolladores está pensado para depurar JavaScript. Pero, como pentesters, nos da la opción de profundizar en el código JavaScript. En Firefox y Safari, esta característica se llama Depurador, pero en Google Chrome se llama Fuentes.

En el sitio web del laboratorio, haz clic en la página de contacto; cada vez que se envía un formulario, notará un destello rápido en la pantalla. Vamos a utilizar el Depurador para averiguar qué es este destello y si contiene algo interesante.

En “Fuentes” verá una lista de todos los recursos que utiliza la página web actual. Si hace clic en la carpeta de assets, verá un archivo llamado script.js. Al hacer clic en este archivo, se muestran los contenidos del archivo JavaScript.

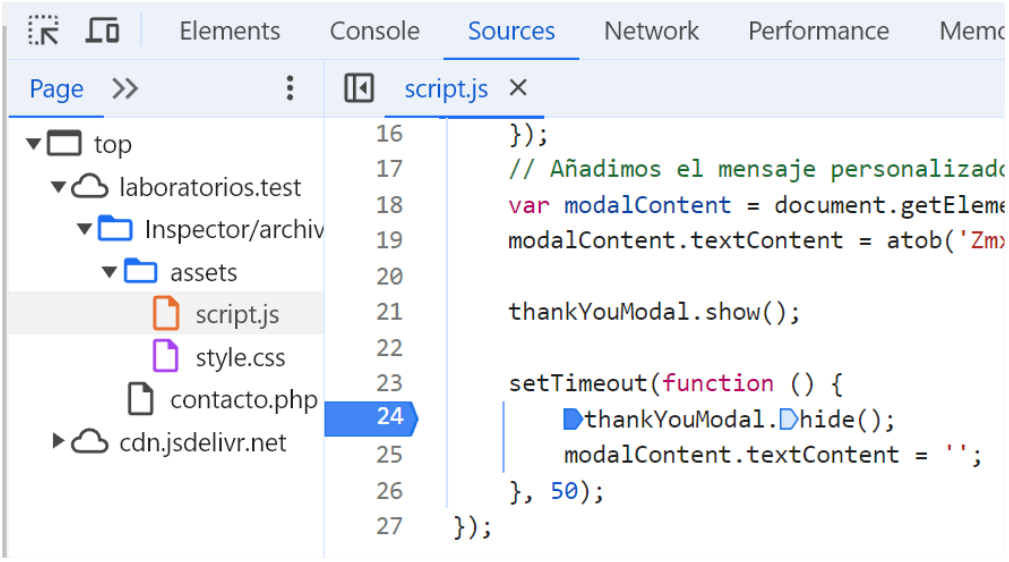


Si te desplazas hasta la parte inferior del archivo script.js, verás la línea:

```
setTimeout(function() {
    thankYouModal.hide();
    modalContent.textContent = '';
}, 50);
```

Este pequeño fragmento de JavaScript es lo que elimina la ventana emergente de la página. Podemos utilizar otra función del depurador llamada puntos de interrupción. Estos son puntos en el código en los que podemos obligar al navegador a que deje de procesar el código JavaScript y pause la ejecución actual. Si hace clic en el número de línea que contiene el código anterior, notará que se vuelve azul; ahora ha insertado un punto de interrupción en esta línea. Ahora

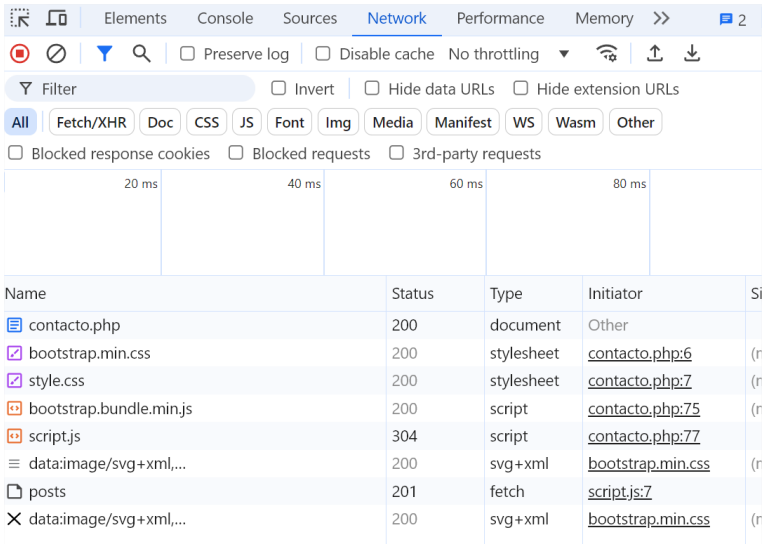
intente actualizar la página y notará que el mensaje permanece en la página en lugar de desaparecer pudiendo ver una bandera.



¿Cuál es la bandera que se muestra en un modal emergente al enviar el formulario de contacto?

6. Red

La pestaña de Red de las herramientas para desarrolladores se puede utilizar para realizar un seguimiento de cada solicitud externa que realiza una página web. Si hace clic en la pestaña de red y luego actualiza la página, verá todos los archivos que solicita la página. Intente hacer esto en la página de contacto; puede presionar el ícono de la papelera para eliminar la lista si se llena demasiado. Con la pestaña de red abierta, intente completar el formulario de contacto y presione el botón Enviar mensaje. Notará un evento en la pestaña de red, y este es el formulario que se envía en segundo plano utilizando un método llamado AJAX. AJAX es un método para enviar y recibir datos de red en segundo plano en una aplicación web sin interferir al cambiar la página web actual.



¿Cuál es la bandera que se obtiene en la petición AJAX al enviar el formulario de contacto?

Las peticiones de contenidos contienen una cabecera en la que se incluye información que puede sernos útil. Las cabeceras de respuesta son establecidas por el servidor y podemos obtener por ejemplo la versión de PHP que emplea.

¿Qué bandera se encuentra en la cabecera de respuesta de la página de inicio?

7. Aplicación - Cookies

Otra de las opciones que dispone las herramientas de desarrolladores de los navegadores, es la de consultar las cookies de los sitios webs. En la pestaña "Aplicación" podemos ver las cookies almacenadas.

¿Cuál es la flag que se encuentra en la cookie sesión_id del sitio web?