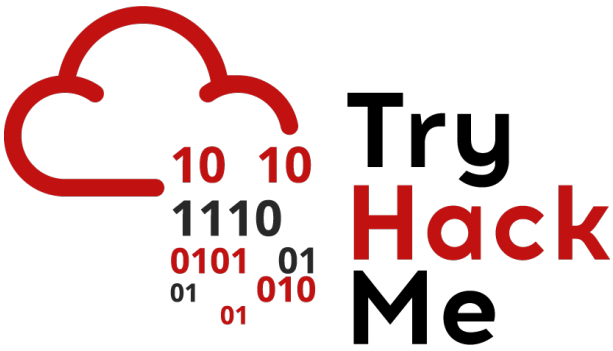
Writeup: Sala *How Websites Work*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

En esta sala aprenderemos sobre los conceptos básicos sobre el funcionamiento de los sitios web. A lo largo de varias tareas interactivas, vamos a conocer sobre la estructura del front-end y back-end, el uso de HTML y JavaScript, y cómo ciertas prácticas inseguras pueden exponer datos o permitir inyecciones de código malicioso.

2. Sala

2.1. Tarea 1 - Cómo trabajan los sitios web

En esta primera tarea vamos a introducirnos a como funcionan los sitios web, además, como al acceder a uno de ellos el navegador realiza una solicitud al servidor y este responde con la información necesaria para renderizar la página. Por último, se destacan dos componentes principales los cuales son

- **Front-End** (Lado del cliente)
- **Back-End** (Lado del servidor)

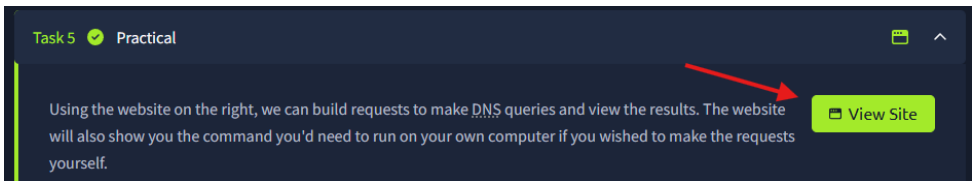
Una vez que aprendemos sobre este tema, podemos pasar a responder la siguiente pregunta.

Pregunta: What term best describes the component of a web application rendered by your browser?
Respuesta: **Front End**

2.2. Tarea 2 - HTML

En esta tarea vamos a aprender sobre los fundamentos de **HTML**, un lenguaje de marcado de Hipertexto que estructura el contenido de las páginas web.

Para resolver esta tarea debemos realizar actividades prácticas, para ello, lo primero que tendremos que hacer es desplegar el sitio haciendo clic en **View Site** en el lado superior.



Una vez desplegado el sitio vamos a resolver las siguientes actividades:

One of the images on the cat website is broken - fix it, and the image will reveal the hidden text answer!

Para resolver este primer ejercicio tenemos que fijarnos bien en las etiquetas **<img>** y nos daremos cuenta que nos hace falta la extensión **.jpg**, la solución es sencilla, simplemente añadimos la extensión correspondiente y le damos clic a **Render HTML Code**, posterior a eso, cargara la imagen con el texto de respuesta a la actividad.

HTML Code

Render HTML Code

```
<!DOCTYPE html>
<html>
    <head>
        <title>TryHackMe HTML Editor</title>
    </head>
    <body>
        <h1>Cat Website!</h1>
        <p>See images of all my cats!</p>
        <img src='img/cat-1.jpg'>
        <img src='img/cat-2.'>
        <!-- Add dog image here -->
    </body>
</html>
```

HTML Code

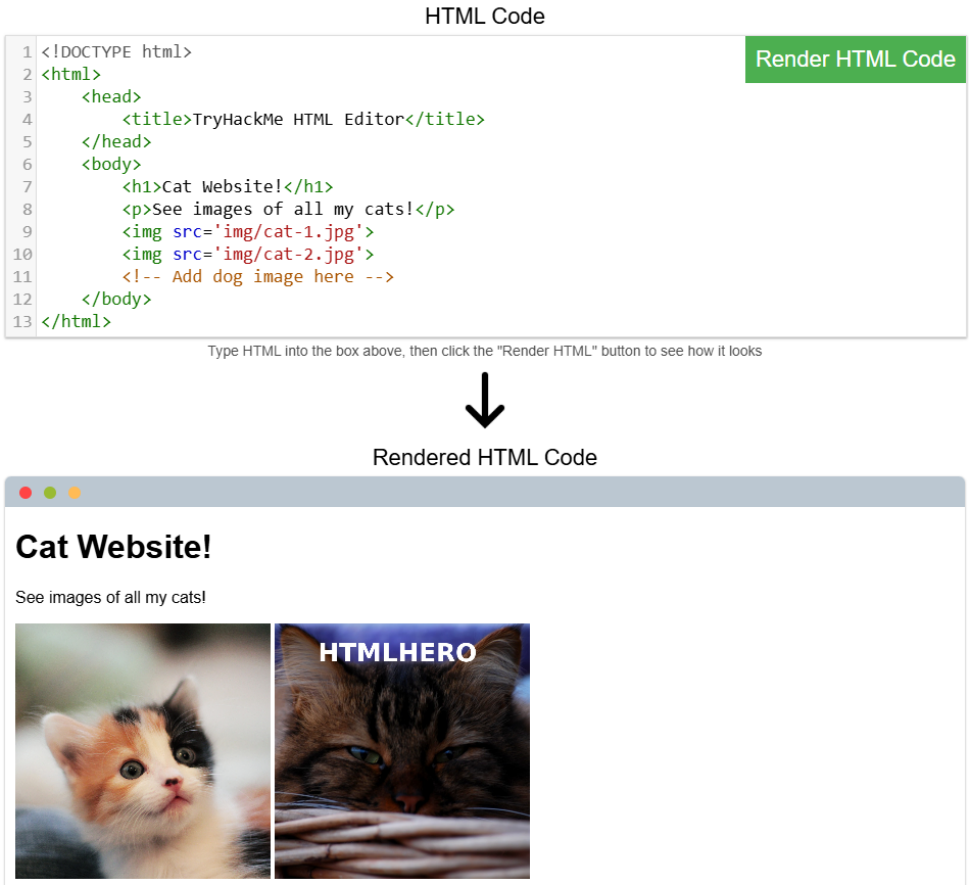
Render HTML Code

```
<!DOCTYPE html>
<html>
    <head>
        <title>TryHackMe HTML Editor</title>
    </head>
    <body>
        <h1>Cat Website!</h1>
        <p>See images of all my cats!</p>
        <img src='img/cat-1.jpg'>
        <img src='img/cat-2.'>
        <!-- Add dog image here -->
    </body>
</html>
```

HTML Code

Render HTML Code

```
<!DOCTYPE html>
<html>
    <head>
        <title>TryHackMe HTML Editor</title>
    </head>
    <body>
        <h1>Cat Website!</h1>
        <p>See images of all my cats!</p>
        <img src='img/cat-1.jpg'>
        <img src='img/cat-2.jpg'>
        <!-- Add dog image here -->
    </body>
</html>
```



Respuesta: HTMLHERO

Add a dog image to the page by adding another img tag (<img>) on line 11. The dog image location is img/dog-1.png. What is the text in the dog image?

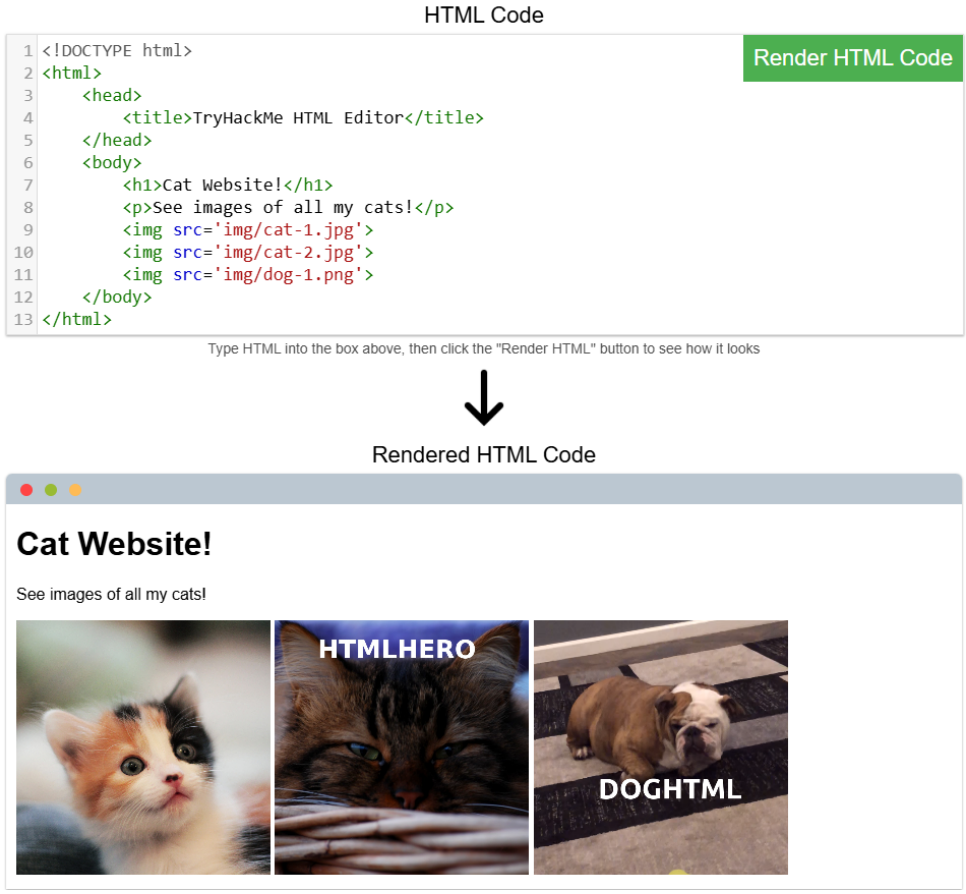
Ahora nos toca resolver esta última actividad para completar la tarea, para ello, debemos volver al código HTML e insertar una nueva etiqueta **<img>** con la dirección de la imagen según el texto (**img/dog-1.png**).

HTML Code

Render HTML Code

```
<!DOCTYPE html>
<html>
    <head>
        <title>TryHackMe HTML Editor</title>
    </head>
    <body>
        <h1>Cat Website!</h1>
        <p>See images of all my cats!</p>
        <img src='img/cat-1.jpg'>
        <img src='img/cat-2.jpg'>
        <img src='img/dog-1.png'>
    </body>
</html>
```

Una vez que añadimos la etiqueta con la ruta correspondiente, haremos clic en **Render HTML Code** y renderizara la imagen con el texto de respuesta.

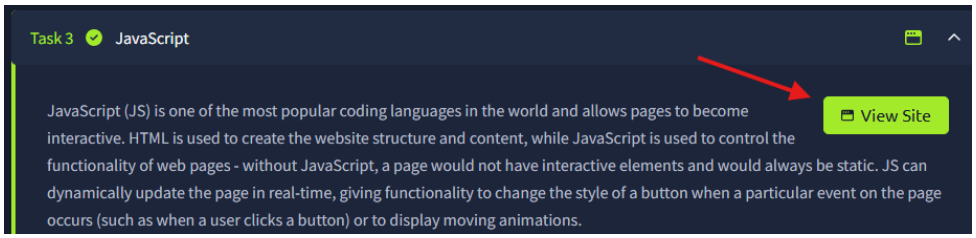


Respuesta: DOGHTML

2.3. Tarea 3 - JavaScript

Conoceremos los fundamentos de JavaScript, el cual permite crear páginas web interactivas y dinámicas. Este lenguaje se destaca por su capacidad para manipular dinámicamente el contenido de una página web.

Para completar esta tarea, debemos resolver una actividad con los fundamentos aprendidos de JavaScript. Para ello, lo primero que haremos es desplegar el sitio haciendo clic en **View Site**.



Una vez desplegado, deberemos realizar la siguiente actividad:

Add JavaScript that changes the demo element's content to "Hack the Planet"

Para completar esta actividad, deberemos usar lo aprendido sobre manipular elementos e insertar contenido HTML. Entonces, debemos escribir el siguiente código JavaScript **document.getElementById("demo").innerHTML = "Hack The Planet"**, este código nos permitira obtener el elemento HTML por medio de su id e insertar el texto correspondiente según la actividad.

HTML + Javascript Code

Render HTML+JS Code

```
<!DOCTYPE html>
<html>
    <head>
        <title>TryHackMe Editor</title>
    </head>
    <body>
        <div id="demo">Hi there!</div>
        <script type="text/javascript">
            // add your JavaScript here
        </script>
    </body>
</html>
```

HTML + Javascript Code

Render HTML+JS Code

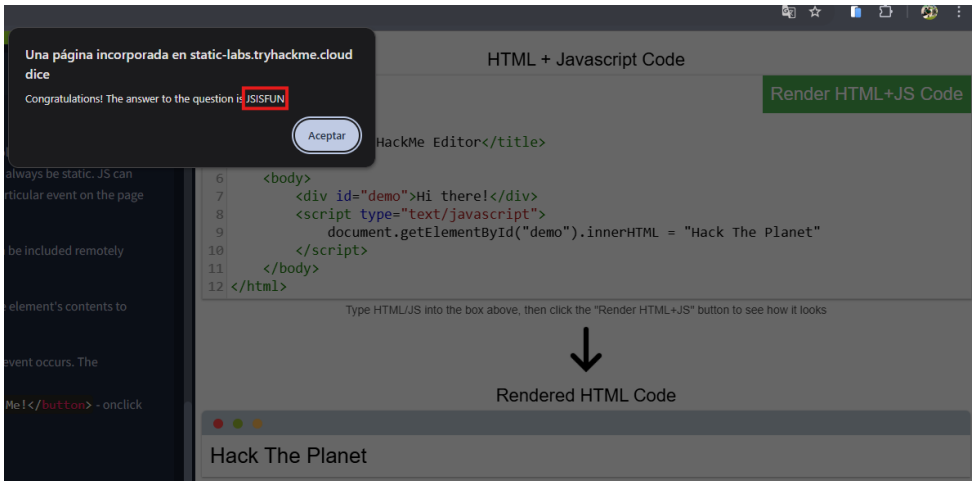
```
<!DOCTYPE html>
<html>
    <head>
        <title>TryHackMe Editor</title>
    </head>
    <body>
        <div id="demo">Hi there!</div>
        <script type="text/javascript">
            // add your JavaScript here
        </script>
    </body>
</html>
```

HTML + Javascript Code

Render HTML+JS Code

```
<!DOCTYPE html>
<html>
    <head>
        <title>TryHackMe Editor</title>
    </head>
    <body>
        <div id="demo">Hi there!</div>
        <script type="text/javascript">
            document.getElementById("demo").innerHTML = "Hack The Planet"
        </script>
    </body>
</html>
```

Después de escribir el código, hacemos clic en **Render HTML+JS Code** y procederá a renderizar el sitio, posterior a eso, nos saltará una alerta con la respuesta de la actividad.



Respuesta: JSISFUN

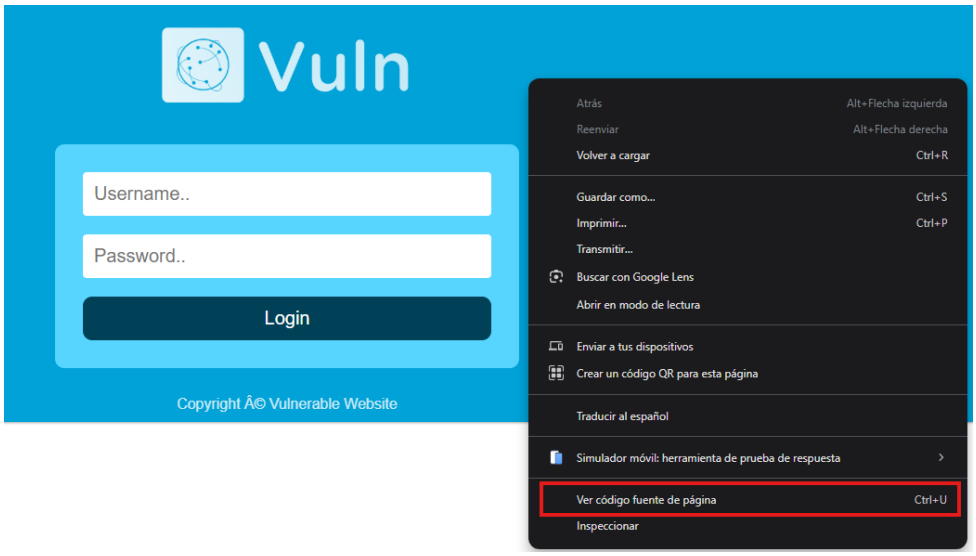
2.4. Tarea 4 - Exposición de datos confidenciales

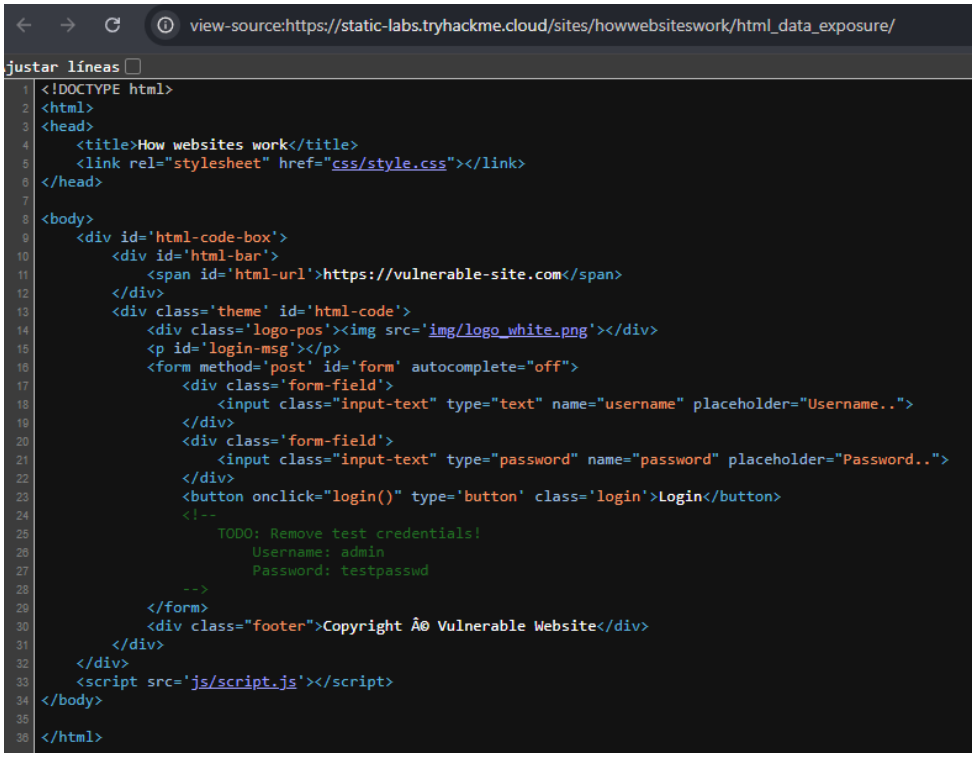
Esta tarea aborda la exposición de datos confidenciales, una vulnerabilidad común cuando los desarrolladores dejan información sensible en el código fuente de una página web.

Para resolver esta tarea, deberemos ingresar al siguiente enlace haciendo clic aquí. Una vez que nos encontremos en la página, debemos realizar la siguiente actividad:

Pregunta: View the website on this link. What is the password hidden in the source code?

Para resolver la actividad, debemos ir al código fuente de la página haciendo clic derecho y luego, otra vez clic en la sección **Ver código fuente de página** o usando la combinación de teclas **Ctrl + U**.





Una vez que nos encontremos en el codigo fuente, notaremos que hay un comentario HTML con unas credenciales de acceso que son usuario y contraseña.

```
<body>
    <div id='html-code-box'>
        <div id='html-bar'>
            <span id='html-url'>https://vulnerable-site.com</span>
        </div>
        <div class='theme' id='html-code'>
            <div class='logo-pos'><img src='img/logo_white.png'></div>
            <p id='login-msg'></p>
            <form method='post' id='form' autocomplete="off">
                <div class='form-field'>
                    <input class="input-text" type="text" name="username" placeholder="Username..">
                </div>
                <div class='form-field'>
                    <input class="input-text" type="password" name="password" placeholder="Password..">
                </div>
                <button onclick="login()" type='button' class='login'>Login</button>
                <!
                    TODO: Remove test credentials!
                        Username: admin
                        Password: testpasswd
                -->
            </form>
            <div class="footer">Copyright Â© Vulnerable Website</div>
        </div>
    </div>
    <script src='js/script.js'></script>
</body>
```

Con esto, logramos encontrar la respuesta de la actividad.

Respuesta: testpasswd

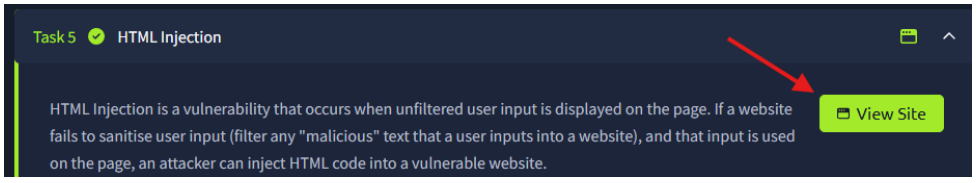
2.5. Tarea 5 - Inyección de HTML

Aprenderemos sobre la vulnerabilidad de inyección HTML, que ocurre cuando una aplicación web no valida adecuadamente las entradas del usuario, permitiendo la inserción de código HTML malicioso.

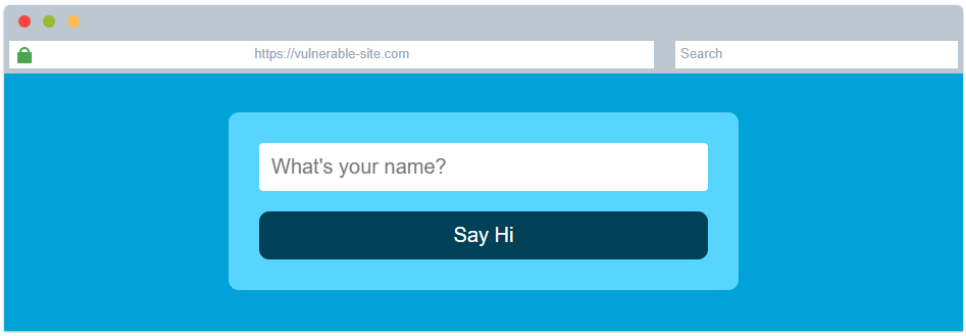
Para lograr resolver esta última tarea de la sala, debemos usar lo aprendido de inyección HTML para resolver la siguiente actividad:

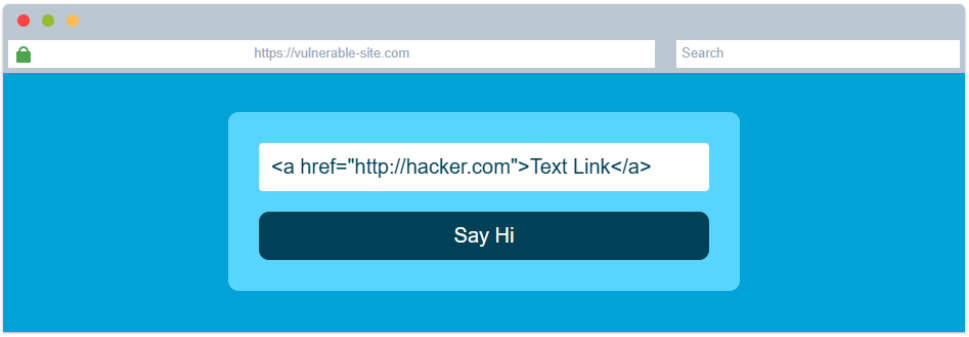
View the website on this task and inject HTML so that a malicious link to http://hacker.com is shown.

Lo primero que haremos es desplegar el sitio haciendo clic en **View Site** en el lado superior.

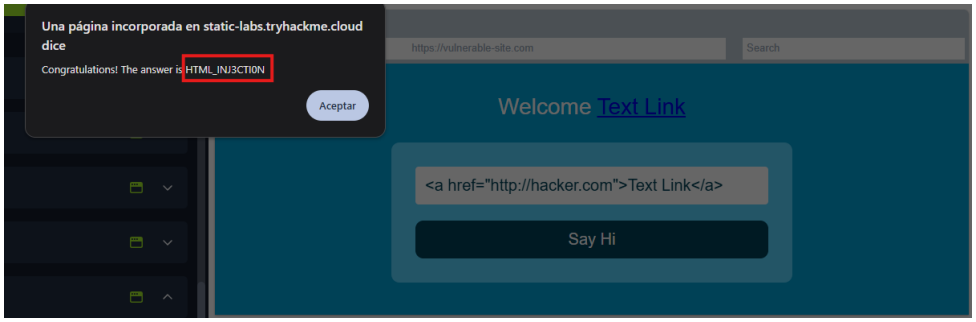


Una vez en el sitio, debemos ingresar por medio de la entrada de texto un código HTML malicioso que permita al usuario redirigirse al sitio **http://hacker.com**. Para ello, usaremos la etiqueta **<a>** para ingresar un contenido que al hacer clic en él, logrará enviar al usuario al sitio que necesitamos. El código que ingresaríamos sería el siguiente: **Texto**





Después que escribimos el código en la entrada de texto, haremos clic en **Say Hi** para enviarlo y proceder a que se muestre en pantalla, posterior a eso, nos saltara una alerta con la respuesta de la actividad.



Respuesta: HTML_INJ3CTI0N

3. Conclusión sobre la Sala

Esta sala ha logrado cumplir el objetivo de introducir los fundamentos del desarrollo web desde una perspectiva de seguridad. A lo largo de las tareas, se aprende cómo funciona la interacción entre el cliente y el servidor, cómo estructurar contenido con HTML, cómo usar JavaScript para dinamismo y cómo prácticas inseguras pueden exponer información sensible o permitir inyecciones de código.