Práctica de Laboratorio - Secuencias de Comandos entre Sitios

Objetivos

En esta práctica de laboratorio, realizará ataques XSS reflejados y XSS almacenados contra DVWA (aplicación web vulnerable) a niveles de seguridad bajos, medios y altos.

- Part 1: Realizar explotaciones de secuencias de comandos entre sitios reflejados

Aspectos básicos/Situación

En esta práctica de laboratorio, realizará pruebas de penetración de una aplicación web para determinar si se ha diseñado de forma segura.

DVWA (Damn Vulnerable Web Application!) es una aplicación web PHP/MySQL. Está diseñada para ser vulnerable a ataques comunes para permitir que los profesionales de seguridad prueben sus habilidades y herramientas, y que los estudiantes y profesores aprendan y comprendan la seguridad de las aplicaciones web en un entorno legal.

DVWA ofrece cuatro niveles de seguridad: bajo, medio, alto e imposible. Cada nivel de seguridad requiere diferentes habilidades para realizar explotaciones. Los niveles de seguridad reflejan diferentes niveles de seguridad que los desarrolladores pueden codificar en sus aplicaciones. En esta práctica de laboratorio, realizará exploits en tres de los niveles de seguridad, Bajo, Medio y Alto, lo que le permitirá ajustar sus ataques para comprometerlos.

Recursos necesarios

- Maquina Virtual Kali (Kali VM) personalizada para el curso de Pirata Ético
- Acceso a Internet

Instrucciones

Parte 1: Realizar explotaciones de secuencias de comandos entre sitios reflejados

Un ataque XSS reflejado es aquel en el que un script malicioso se refleja en el navegador del usuario desde un servidor web. El script se activa a través de un enlace en el que la víctima hace clic. Esto enviará una solicitud al sitio web que tiene una vulnerabilidad que permite la ejecución del script malicioso.

Paso 1: Inicie sesión en DVWA.

a. Desde la VM Kali Linux, abra un navegador y navegue hasta la aplicación DVWA.

b. Ingrese la siguiente URL en el navegador http://10.6.6.13.

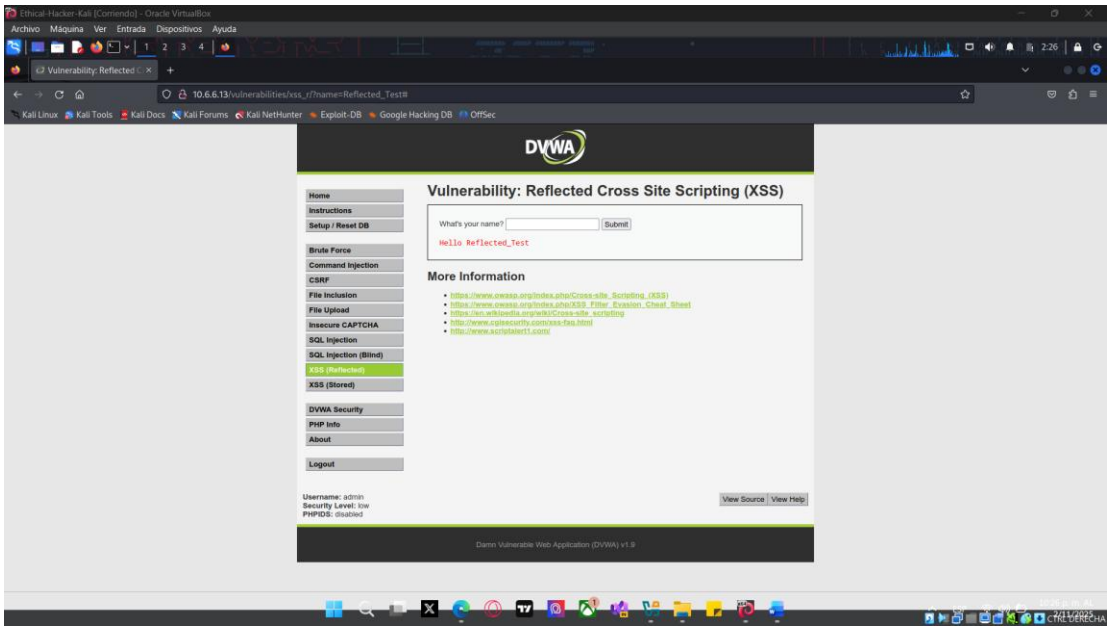
c. En la solicitud de inicio de sesión, introduzca las credenciales: **admin**/**password**.

Paso 2: Realizar un ataque XSS reflejado con un nivel de seguridad bajo.

a. Seleccione **DVWA Security** en el menú de la izquierda y seleccione **Low** en el menú desplegable Nivel de seguridad. Haga clic en **Submit** (Enviar).

b. Seleccione **XSS (Reflected)** en el menú de la izquierda.

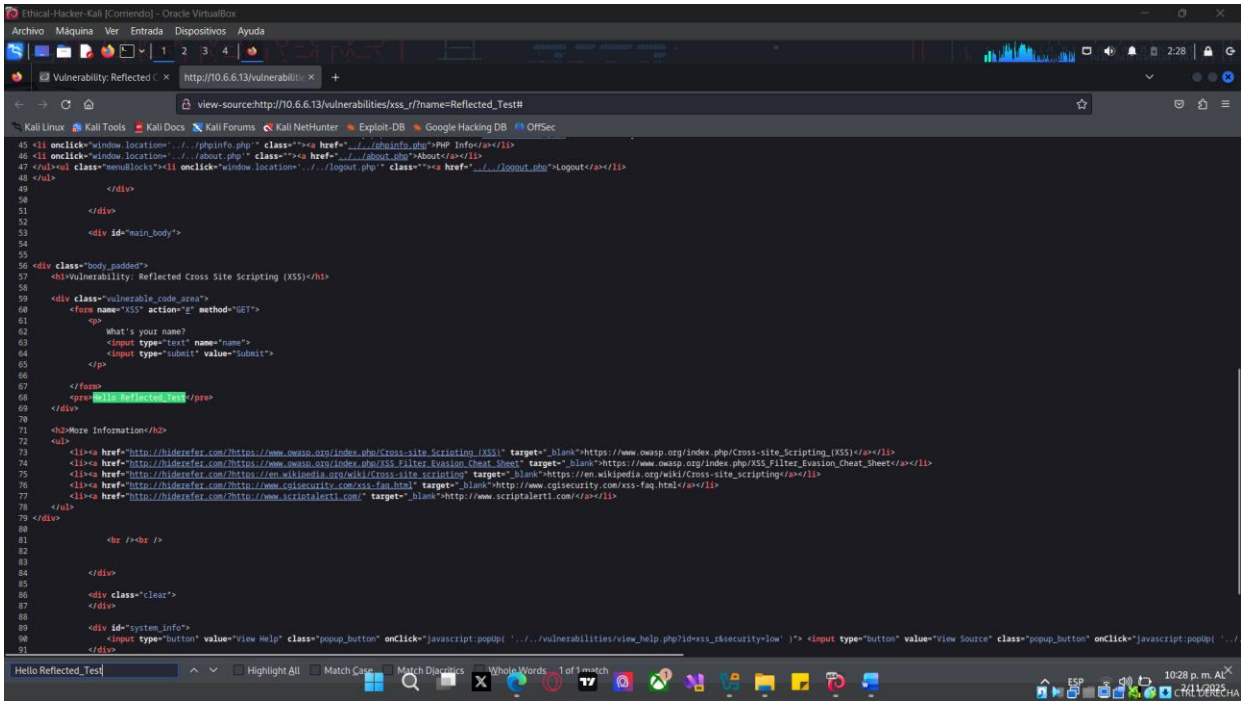
c. Escriba la cadena **Reflected_Test** en **What's your name?** y haga clic en **Submit**.



Verá aparecer el mensaje **Hello Reflected_Test**.

d. Ingrese **CTRL+U** en el teclado para ver el código fuente de la página.

e. Busque la cadena **Hello Reflected_Test** ingresando CTRL+F para abrir un cuadro de búsqueda.



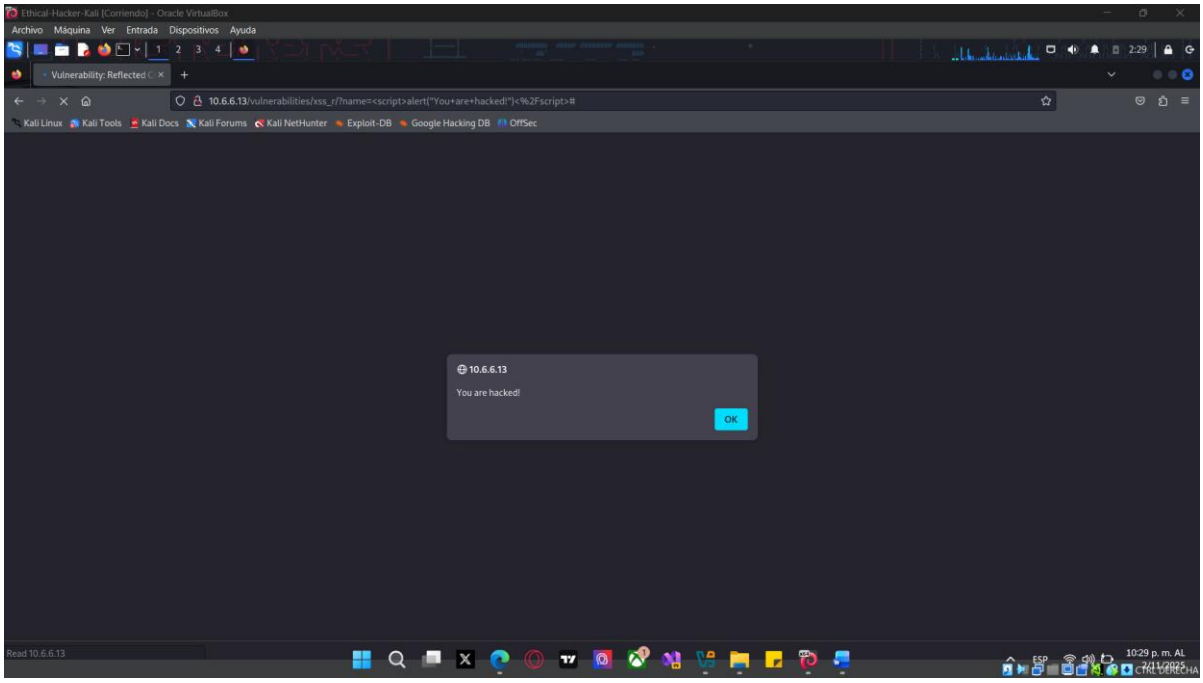
La presencia de la cadena en el código fuente HTML de la página indica que los valores ingresados en un campo de texto de respuesta del usuario se insertan en el código fuente de la página. Esto indica al atacante que la página puede ser vulnerable a los ataques XSS reflejados.

f. Cierre la ventana de código fuente y vuelva a la página Reflected XSS Vulnerability.

g. Ingrese la siguiente carga útil en el campo **What's your name?** y haga clic en **Submit**.

```
<script>alert("You are hacked!")</script>
```

Aparecerá un cuadro emergente de alerta con las palabras **You are hacked!**. Esto significa que el sitio es vulnerable a ataques XSS reflejados y hemos aprovechado la vulnerabilidad con éxito.



h. Seleccione y copie la URL de la página comprometida. Abra una nueva pestaña del navegador, pegue la URL en el campo URL y presione <Enter> .

Debería ver aparecer la misma página web mostrando el cuadro emergente **You are hacked**!. Esto significa que si un usuario abre la URL, se ejecutará un script malicioso. El cuadro emergente se usa para simular un script malicioso en esta práctica de laboratorio.

En un compromiso de piratería ética, intentaría insertar un script de prueba simple en los campos de entrada para ver si el script se ejecuta. Si es así, el sitio web es vulnerable a los ataques XSS reflejados. Luego, podría distribuir el enlace en un ataque de suplantación de identidad (phishing) para determinar el nivel de conocimiento de la seguridad entre los empleados de sus clientes.

Paso 3: Realizar un ataque XSS reflejado en el nivel de seguridad medio.

Intentará el mismo ataque, pero esta vez el nivel de seguridad del sitio web será medio.

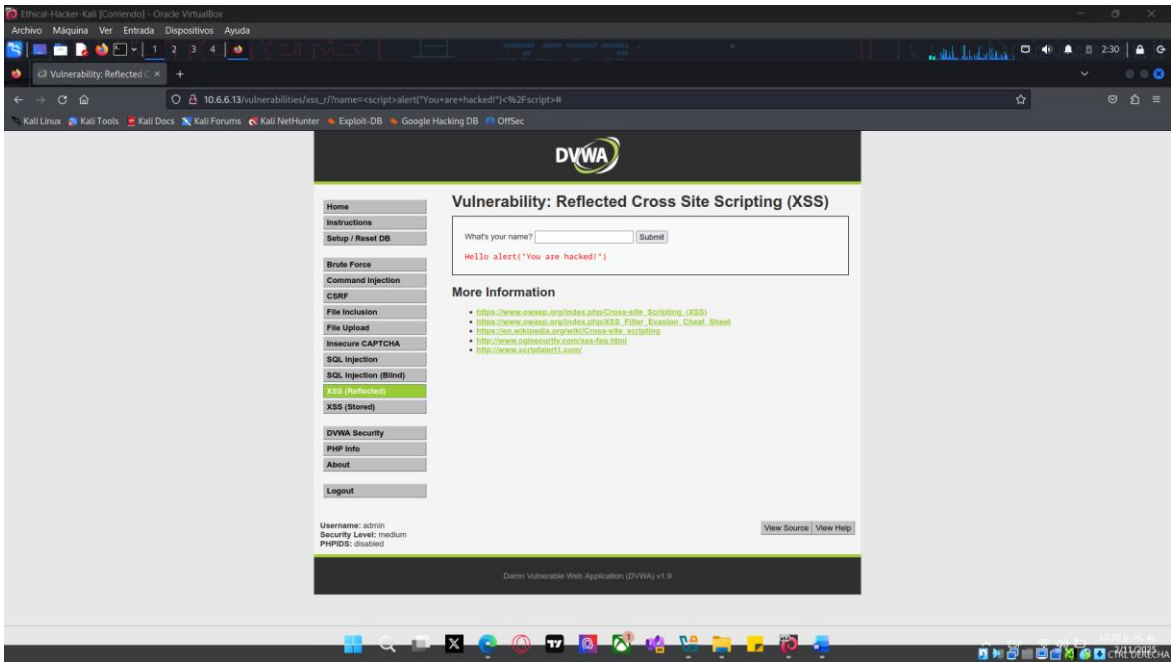
a. Seleccione **DVWA Security** en el menú de la izquierda y seleccione **Medium** en el menú desplegable Nivel de seguridad. Haga clic en **Submit** (Enviar).

b. Seleccione **XSS (Reflected)** en el menú de la izquierda.

c. Nuevamente, ingrese la siguiente carga útil en **What's your name?** y haga clic en **Submit**.

```
<script>alert("You are hacked!")</script>
```

Verá una respuesta de saludo, pero esta vez no aparecerá ninguna ventana emergente. Esto indica que el script no se ejecutó. Tenga en cuenta que el script se muestra como texto literal.



Podemos analizar el código en el backend del sitio web para investigar el motivo.

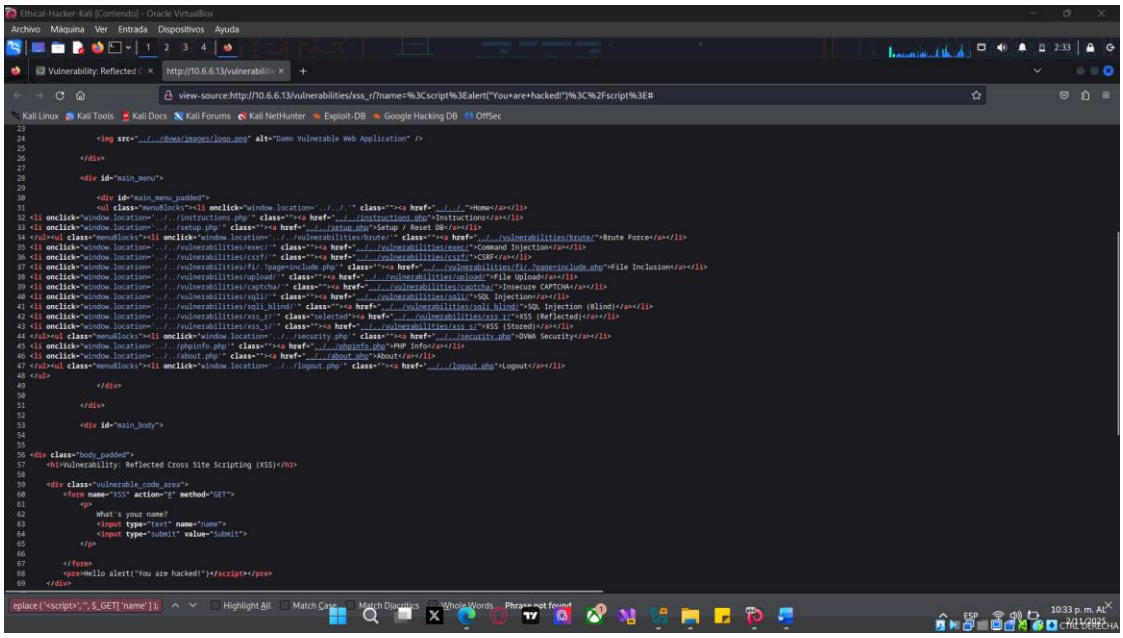
d. Haga clic en el botón **View Source** en la parte inferior derecha de la página y revise el código PHP.

Nota: En un servidor web real, no tendríamos acceso a este código fuente de backend, pero aquí en DVWS sí.

e. Tenga en cuenta la línea:

```
$name = str_replace ( '<script>', '', $_GET[ 'name' ] );
```

Este código fuente crea un filtro, con la función **str_replace()** , que elimina la etiqueta **<script>** en nuestra carga útil y la reemplaza con un valor nulo. Esto hace que el script de carga útil sea ineficaz, por lo que el ataque falló y no se muestra ninguna ventana emergente. Dado que este script solo filtra <script> en minúsculas, podemos intentar evitar el filtro utilizando una etiqueta diferente en la carga útil. Utilizaremos **<ScRipt>**.

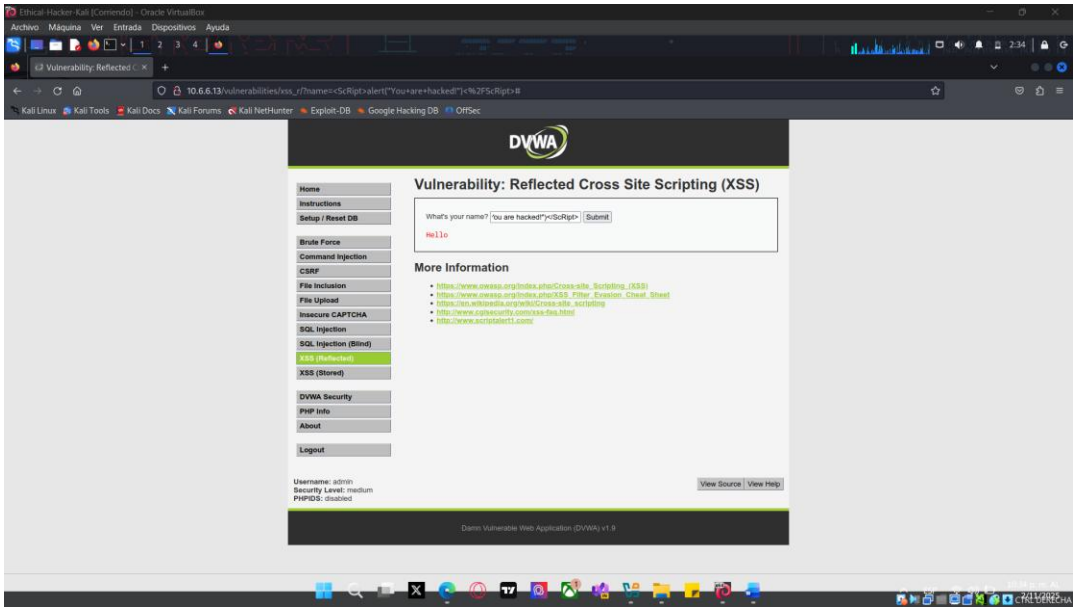


f. Cierre la ventana de código fuente y vuelva a la página Reflected XSS Vulnerability.

g. Ingrese la siguiente carga útil en el campo **What's your name?** y haga clic en **Submit**.

```
<ScRipt>alert("You are hacked!")</ScRipt>
```

¿Apareció la alerta emergente? Si esto es correcto, ¿por qué?



La ventana emergente apareció porque la carga útil con la etiqueta <ScRipt> pudo eludir el filtro. Esto significa que el sitio sigue siendo vulnerable a los ataques XSS reflejados incluso en el nivel de seguridad medio.

Paso 4: Paso 4: Realizar un ataque XSS reflejado en un nivel de seguridad alto.

Se intentará el mismo ataque, pero esta vez el nivel de seguridad del sitio web será alto.

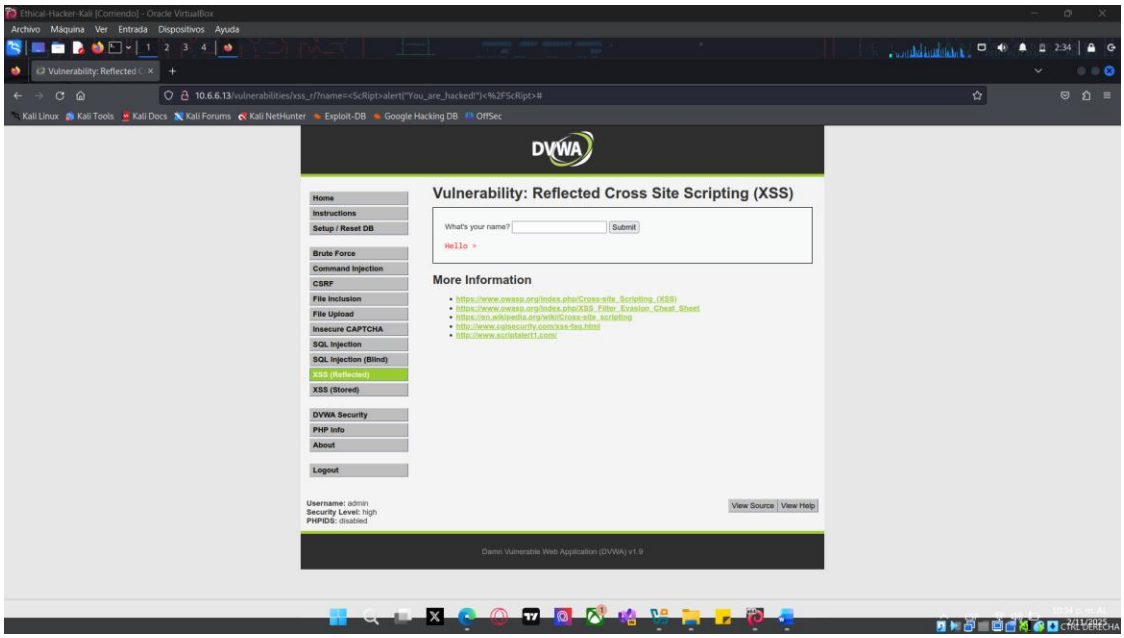
a. Seleccione **DVWA Security** en el menú de la izquierda y seleccione **High** en el menú desplegable Nivel de seguridad. Haga clic en **Submit** (Enviar).

b. Seleccione **XSS (Reflected)** en el menú de la izquierda.

c. Ingrese la siguiente carga útil en el campo **What's your name?** y haga clic en **Submit**. (Tenga en cuenta el uso de guiones bajos para reemplazar espacios).

```
<ScRipt>alert("You_are_hacked!")</ScRipt>
```

Hay un mensaje de saludo y no hay un cuadro emergente de alerta. Nuevamente, podemos analizar el código fuente del back-end para investigar.

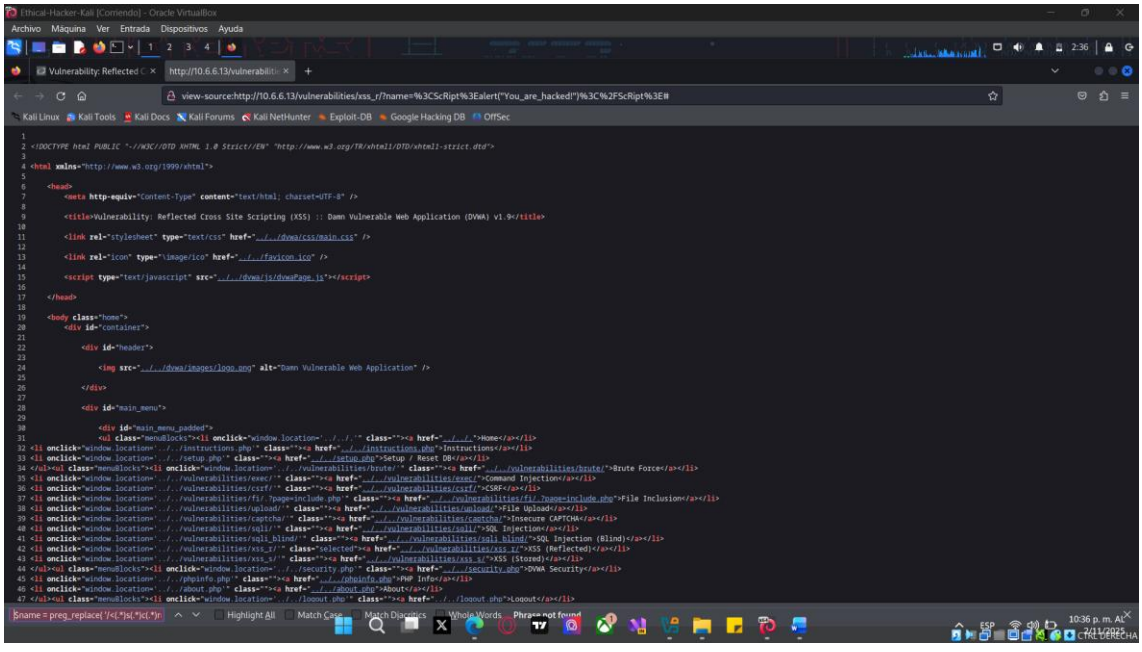


d. Haga clic en el botón **View Source** y revise el código PHP.

Tenga en cuenta la siguiente línea:

```
$name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $_GET[ 'name' ] );
```

En este código, el desarrollador utilizó una expresión regular para reemplazar cualquier forma de la etiqueta **<script>** , sin importar qué mayúsculas y minúsculas se utilicen, con un valor nulo.



¿Qué carácter del script se omitió de la expresión regular? ¿Cómo lo sabe?

Se omitió el carácter “>”. Aún puedes verlo en la salida para la entrada What's your name? enviada.

e. Para evitar este filtro, debemos utilizar otra etiqueta HTML en lugar de **<script>** para atacar el sitio.

Cierre la ventana de código fuente y vuelva a la página Reflected XSS Vulnerability.

f. Ingrese la siguiente carga útil en el campo **What's your name?** y haga clic en **Submit**. (Tenga en cuenta el uso de guiones bajos para reemplazar espacios).

```
<img src=x onerror=alert("You_are_hacked!")>
```

Esta vez aparecerá el cuadro emergente XSS. Hemos pasado por alto con éxito el filtro y hemos explotado la vulnerabilidad XSS reflejada en DVWA en seguridad de alto nivel.

Revise el texto que ingresó en el formulario web. ¿Cómo funcionó?

Obligó a ocurrir un error al intentar cargar una imagen inexistente. El error se detectó con onerror y se activó la respuesta de alerta para mostrar el cuadro de alerta.