Reporte Proyecto 2

Integrantes

Hernández Zacateco Aldo René

Soto Astorga Enrique Francisco

Gutiérrez Peto Emmanuel

Políticas de Seguridad de Contenido (CSP)

Es una capa de seguridad adicional que ayuda a detectar y mitigar cierto tipo de ataques, incluyendo Cross-Site Scripting (XSS) y ataques de inyección de datos. Estos ataques son usados para cualquier cosa desde el robo de datos hasta hasta la alteración de su sitio o la distribución de malware.

Mitigando cross site scripting

CSP hace posible a los administradores de servidores reducir o eliminar los vectores por los cuales un ataque XSS puede ocurrir especificando los dominios que el navegador web debe considerar orígenes válidos de scripts ejecutables. Un navegador web compatible con CSP entonces solo ejecutará scripts cargados en archivos fuente recibidos de aquellos dominios permitidos, ignorando todos los demás scripts (incluyendo scripts en línea y atributos HTML de manejo de eventos).

Como una última forma de protección, los sitios que no deseen permitir nunca la ejecución de scripts pueden optar por deshabilitar globalmente la ejecución de scripts.

Propuesta

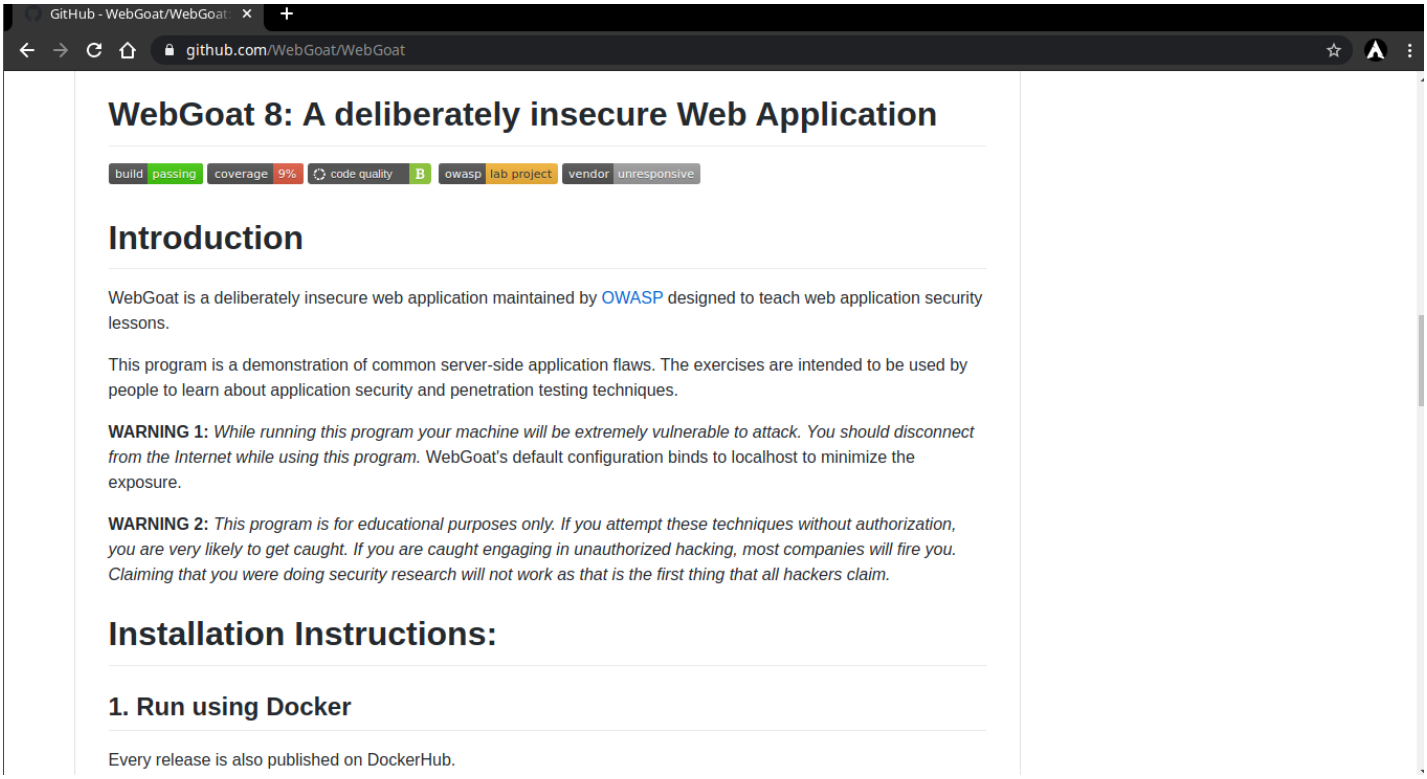
Una propuesta para resolver vulnerabilidades de la página web es sanitizar el html:

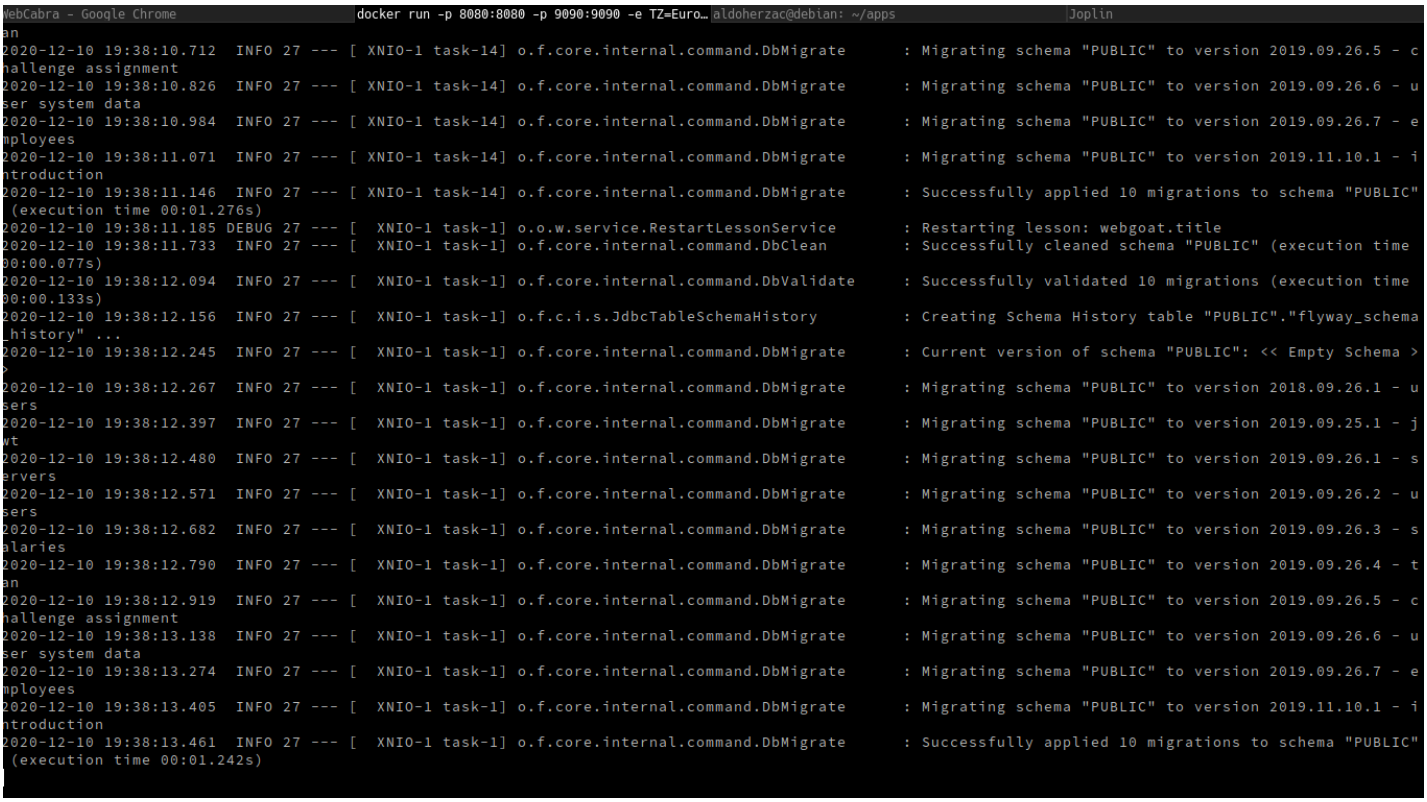
var regex = '(?:[^"'>]|"[^"]*"|'[^']*')*';

Y con esa regex debemos de implementar funciones que eliminene sus ocurrencias en los tags html

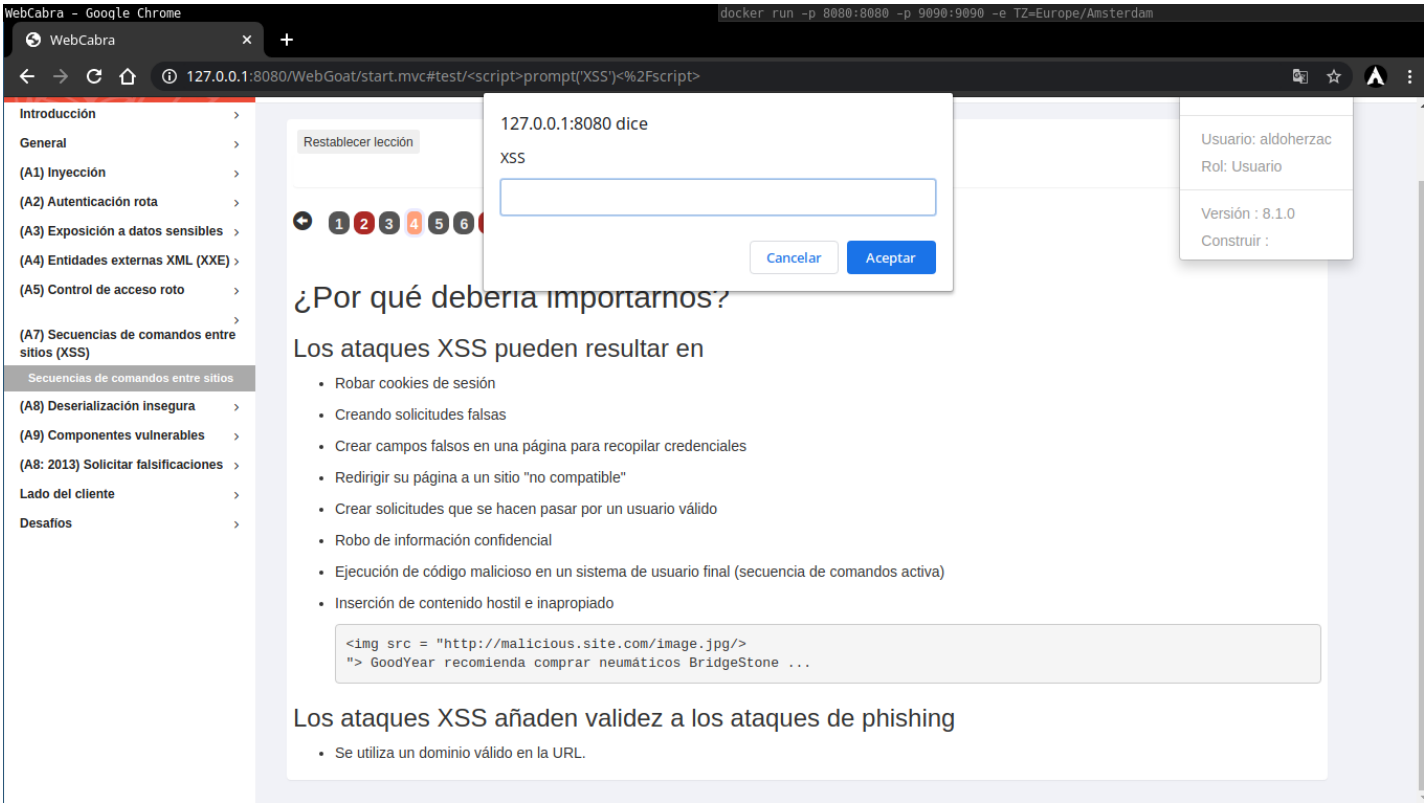
Página web vulnerable

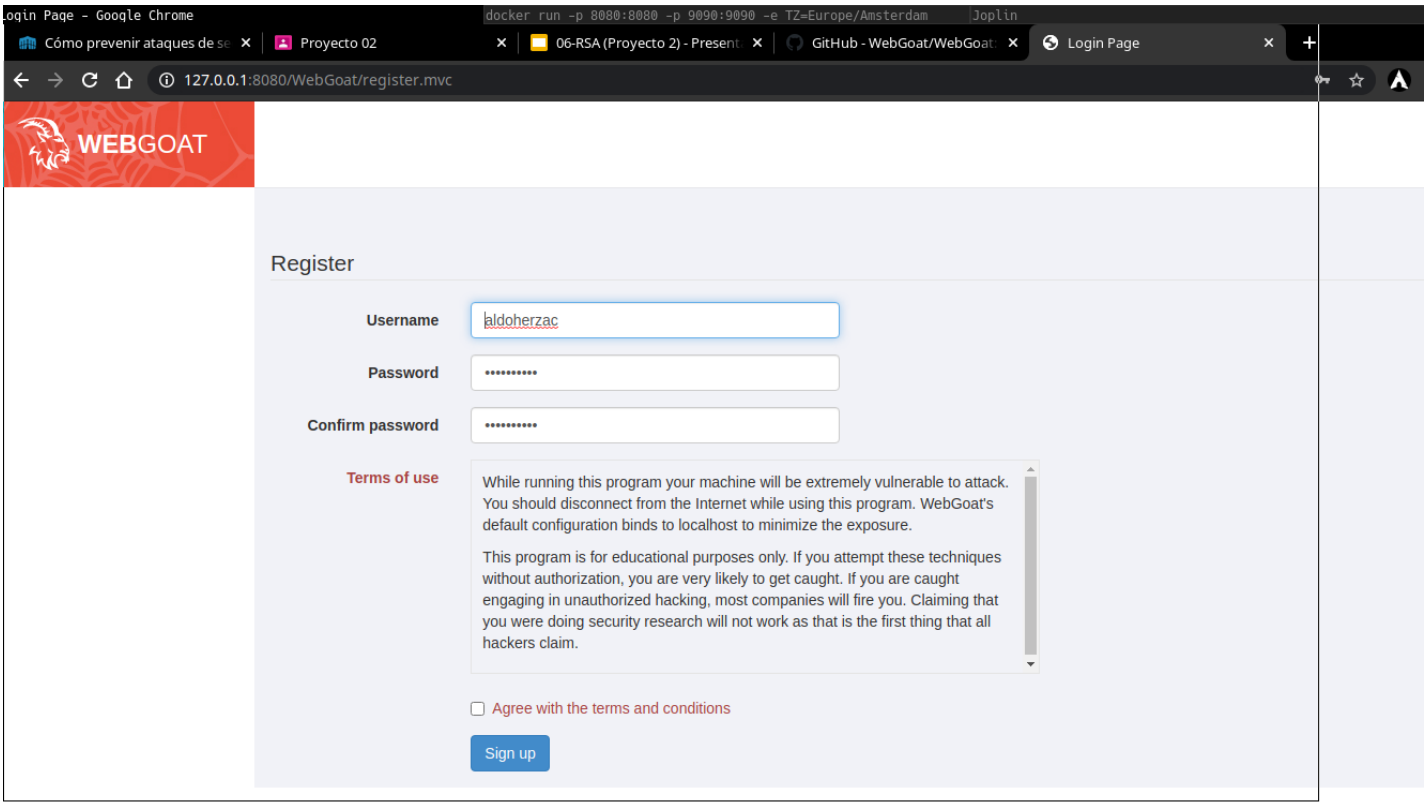
Clone un repositorio que contenia una pagina web de prueba que tiene varias vulnerabilidades.



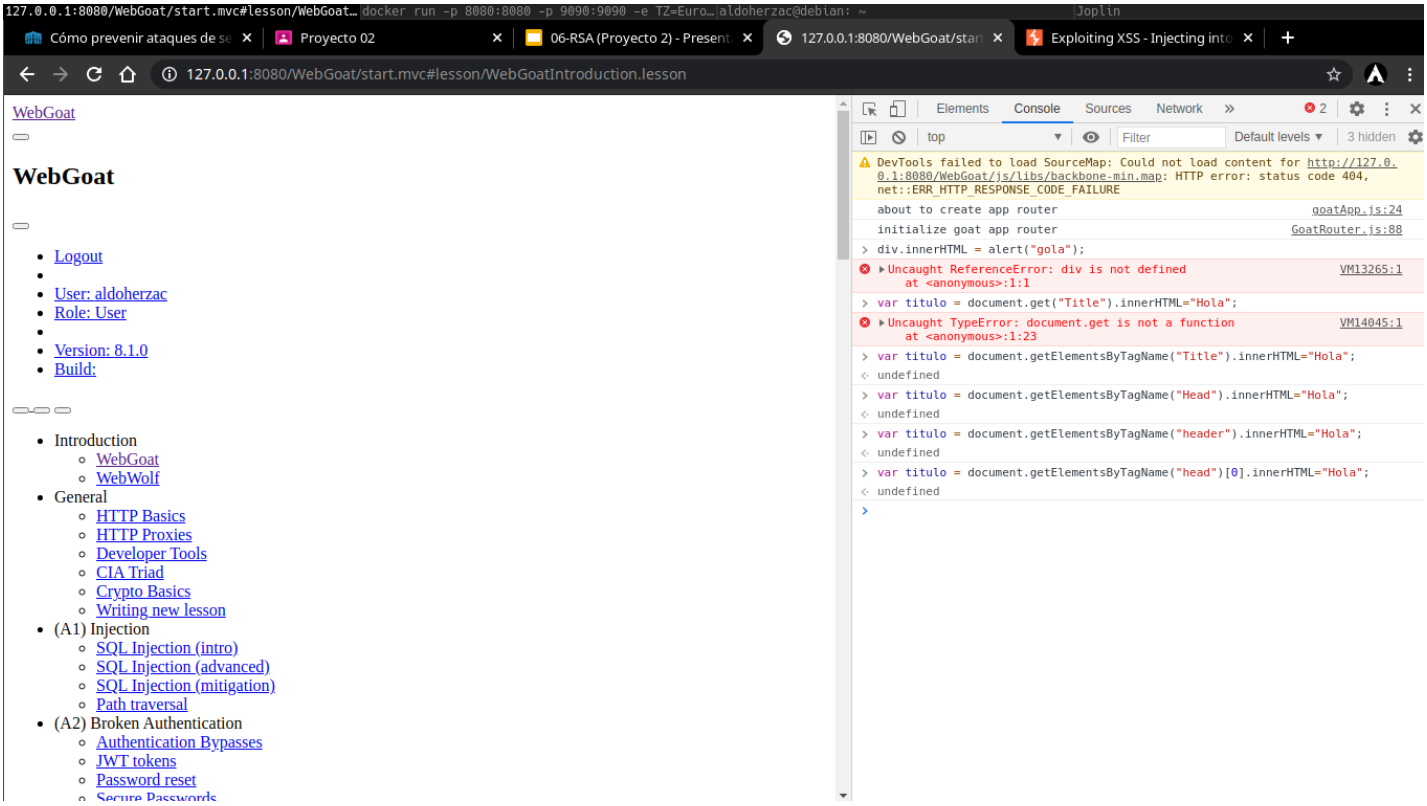


Y realizar un ataque XSS mediante la url que se ve en la imagen.





Modificamos el head:



Bibliografía

https://developer.mozilla.org/es/docs/Web/Security/CSP/Introducing_Content_Security_Policy#:~:text=Políticas de Seguridad de Contenido (CSP) es una capa de,ataques de inyección de datos.&text=Si el sitio no tiene,la política de mismo origen.