



Nombre Taller: Lab 13

XSS 0x01 - DOM-Based

Detalles Prácticos:

Descripción: En este laboratorio se logra redirigir automáticamente al usuario a una página externa
Nivel(Básico/Intermedio o avanzado)

Instructores: Rieradipe

Tabla de contenidos:

Introducción	Contexto del taller
	Objetivos generales y específicos
Materiales Necesarios	Software requeridos
	Recursos Adicionales
Metodología	Desglose paso a paso del proceso
	Prácticas recomendadas
Ejercicios Prácticos	Captura de solicitudes
	Análisis y pruebas
Resultados y Evaluación	Resultados esperados de las actividades
	Criterios de evaluación
Conclusión	Resumen de aprendizajes
	Preguntas y próximos pasos

Objetivo:

Identificar y explotar una vulnerabilidad de tipo DOM-Based XSS, logrando redirigir automáticamente al usuario a una página externa.

Análisis:

Comportamiento observado:

- Al introducir contenido en el campo de la lista y pulsar “Add”, el valor se refleja dinámicamente en el DOM sin tráfico de red asociado.
- Esto indica un procesamiento 100% en el cliente → posible vulnerabilidad DOM XSS

Punto vulnerable:

- Campo de entrada para agregar items a una lista (input)
- El contenido es inyectado directamente en el DOM usando probablemente **innerHTML**.

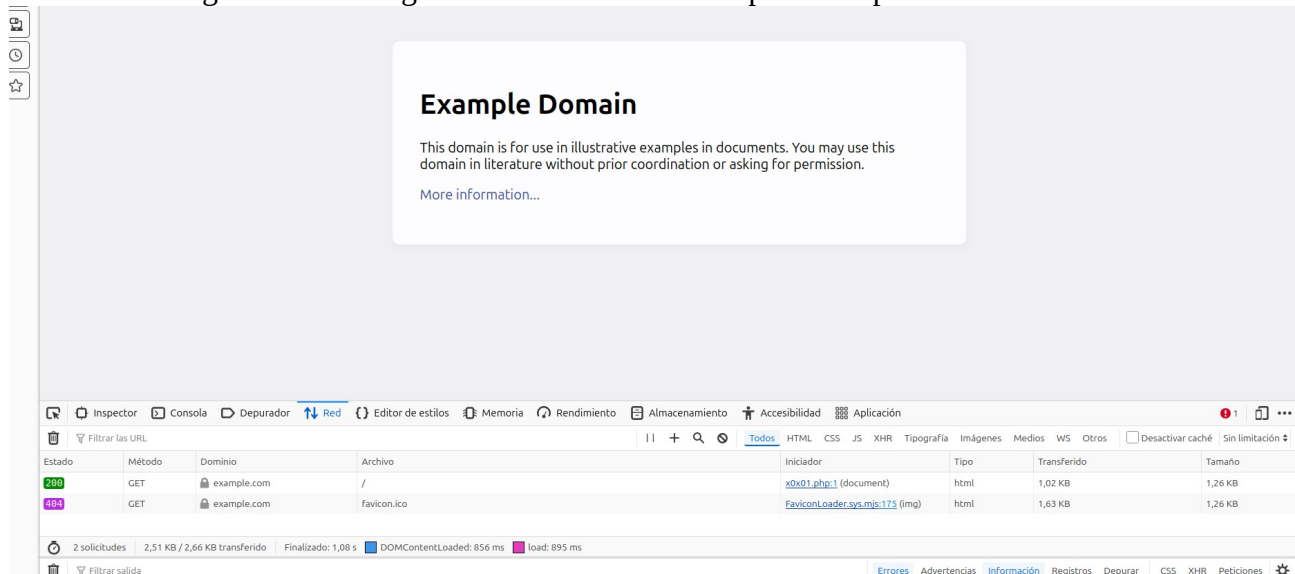
Explotación:

Payload utilizado:

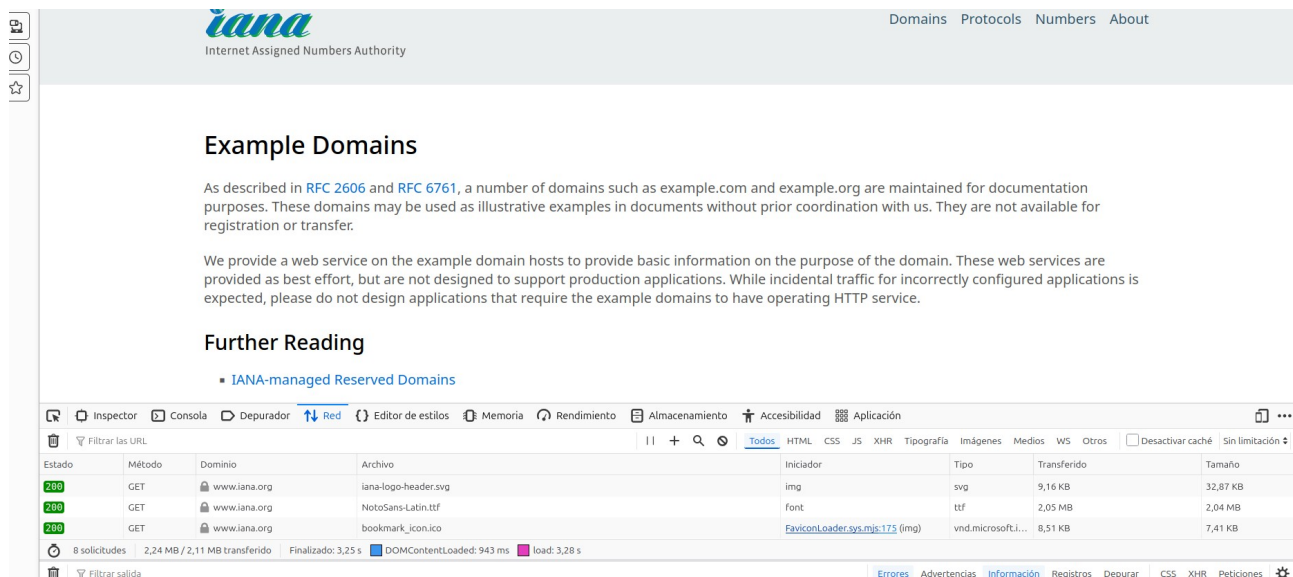
```
<img src=x onerror="location='https://example.com'">
```

Resultado:

- El navegador fue redirigido automáticamente a <https://example.com>



Aquí se puede ver que no hay tráfico ya que sucede todo desde el cliente.



Conclusión:

Se ha demostrado la existencia de una vulnerabilidad DOM-Based XSS **que permite ejecutar código malicioso** en el navegador. En este caso, se utilizó un evento onerror en una imagen para realizar redirección automática.

Recomendaciones:

Evita uso de innerHTML con datos no sanitizados

Usar .textContent o .setAttribute().

Incorporar una política CSP Content Security Policy

Utilizar librerías como DOMPurify
