Nombre Taller:Lab 13

XSS 0x01 - DOM-Based

Detalles Prácticos:

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

Tabla de contenidos:

Objetivo:

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

Anślisis:

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.**

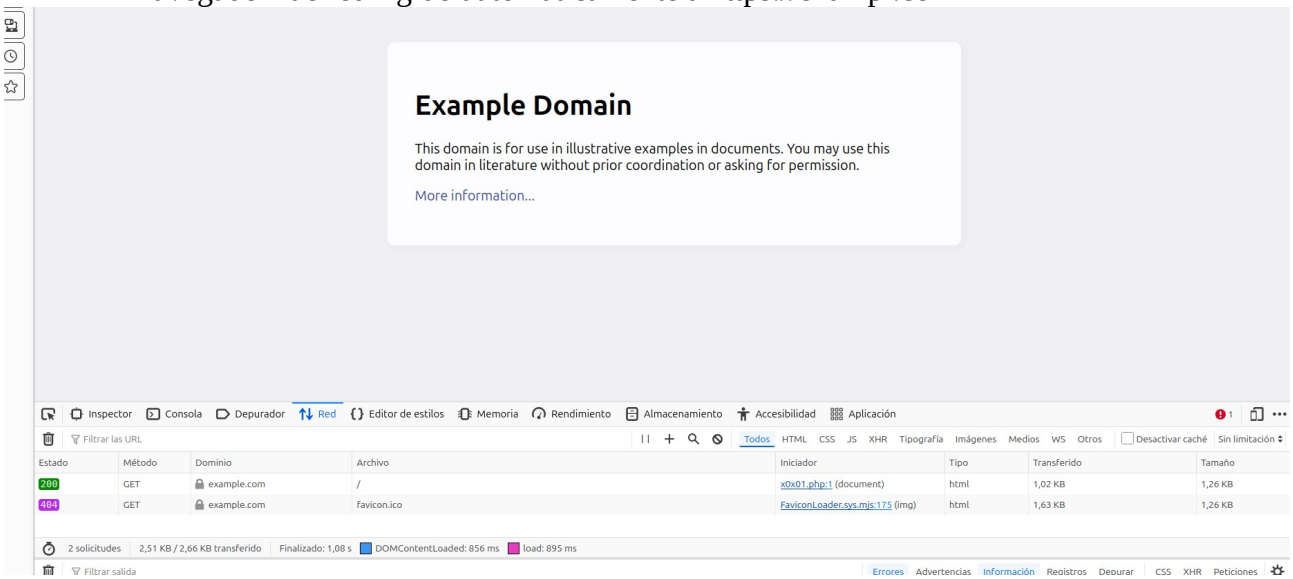
Explotación:

Payload utilizado:

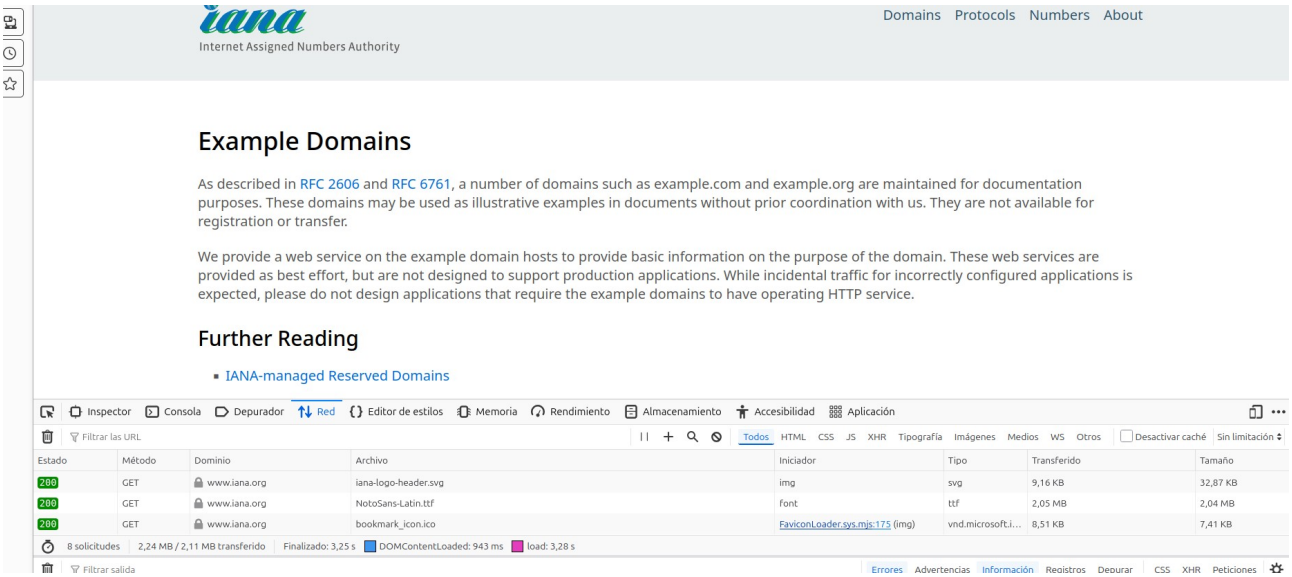
```
<img src=x onerror="location='https://example.com'">
```

Resultado:

- El navegador fue redirigido automáticamente a https://exampl.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 autómatica.

Recomendaciones:

Evita uso de innerHTML con datos no sanitizados
Usar .textContent o .setAttribute().
Incorporar una politica CSP Content Security Policy
Utilizar librerías como DOMPurify