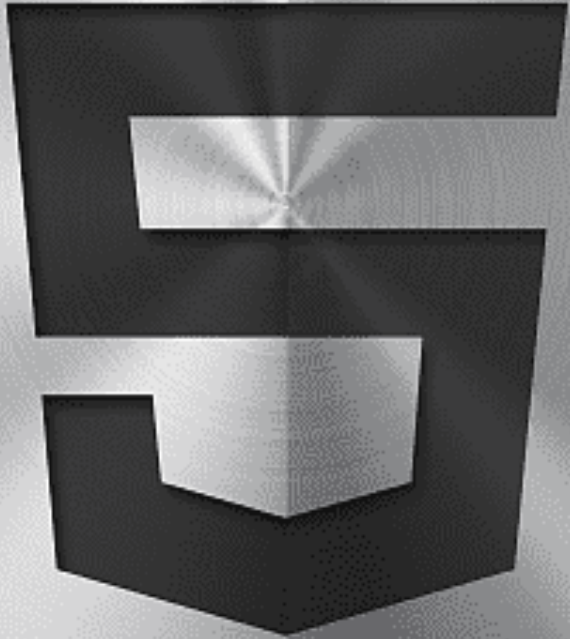


HTML



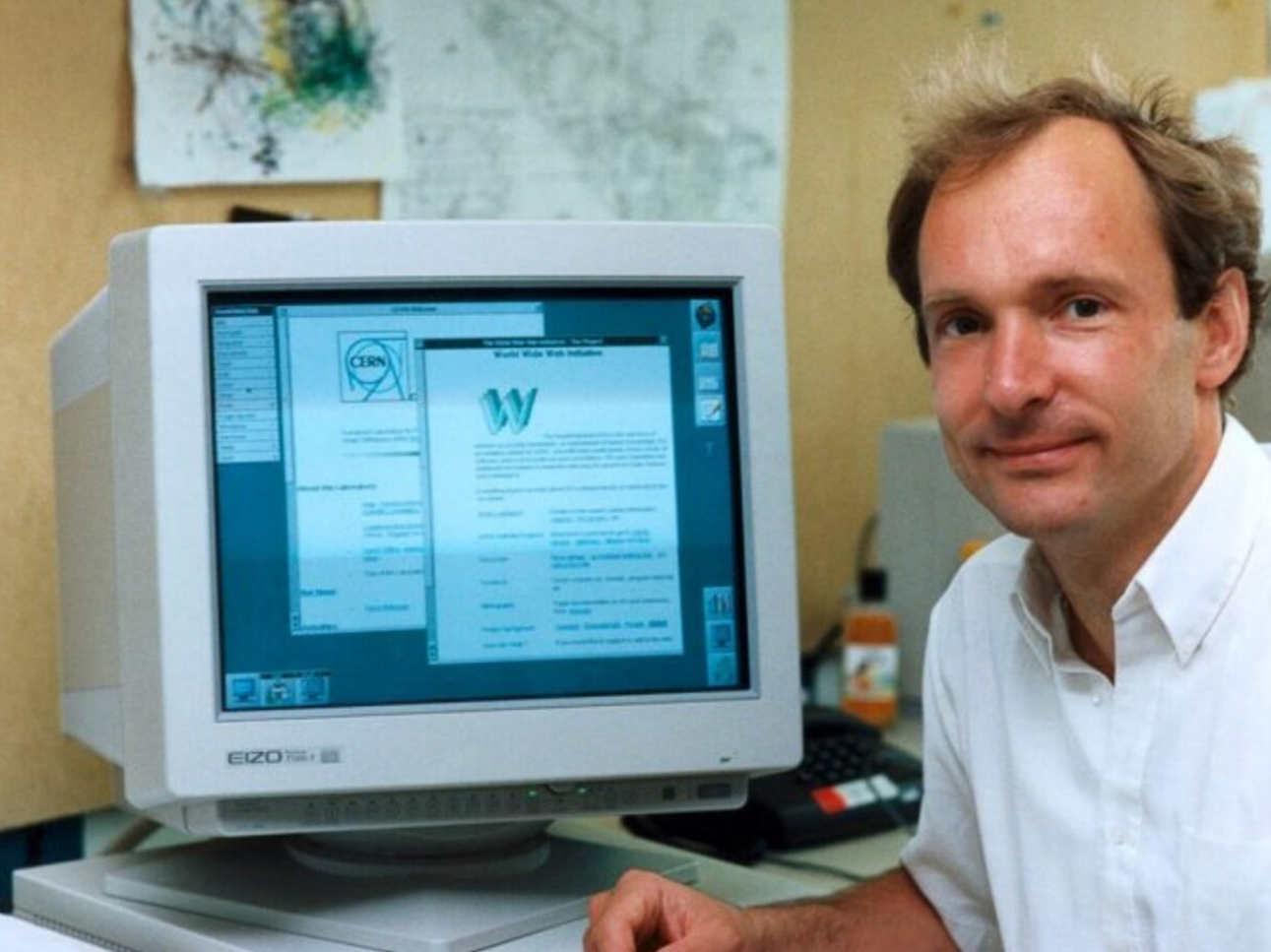
HTML5

Tahir Farooq

Índice

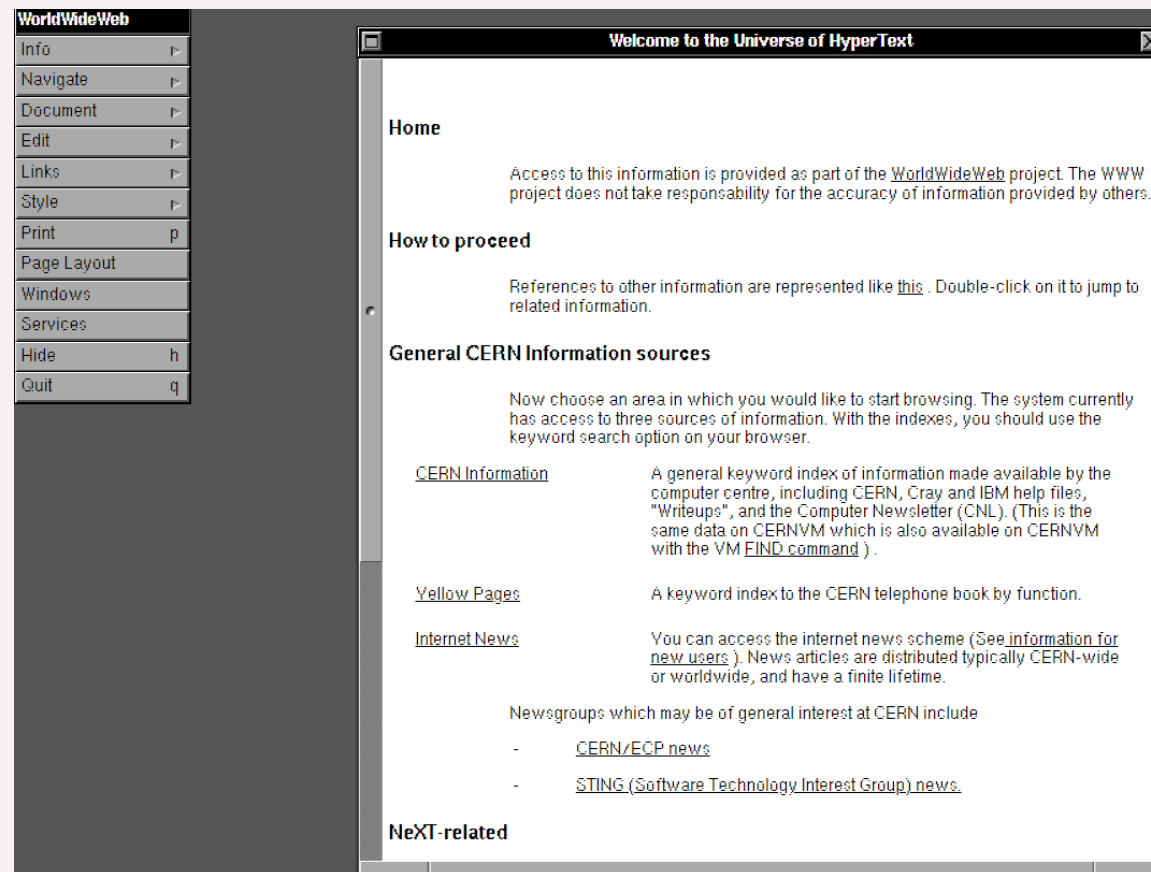
- Historia
- Introducción HTML5
- Desglose HTML5
- Conclusiones



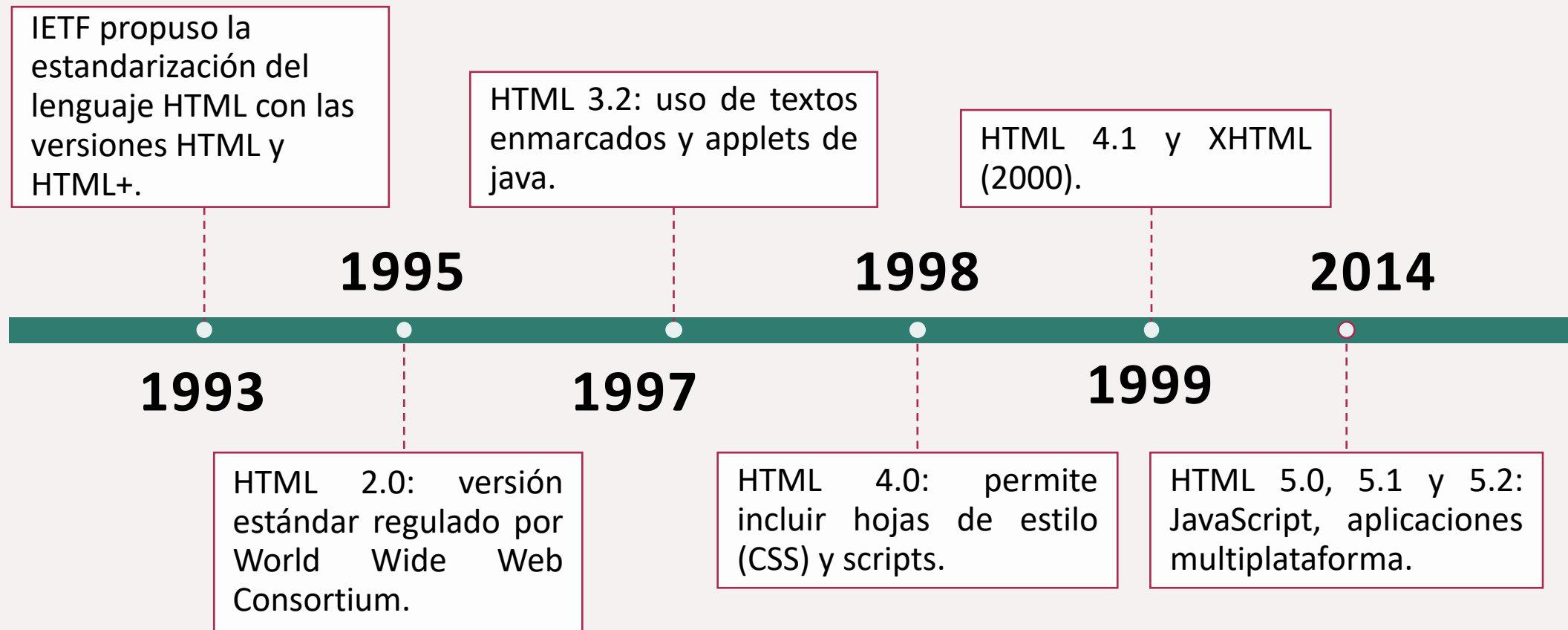


- HTML (Lenguaje de Marcas de Hipertexto) se creó en 1980 por el físico Tim Berners Lee.
- HTML Tags se publicó en 1991.
- Se creó el primer navegador web: Nexus.

Historia



Historia



Historia

Introducción

HTML5

HTML5 es un lenguaje de marcado que sirve para definir la estructura y los contenidos de una página web. Actualmente, se usa junto a otras tecnologías como CSS o JavaScript para dar diseño visual/auditivo para una variedad de dispositivos.



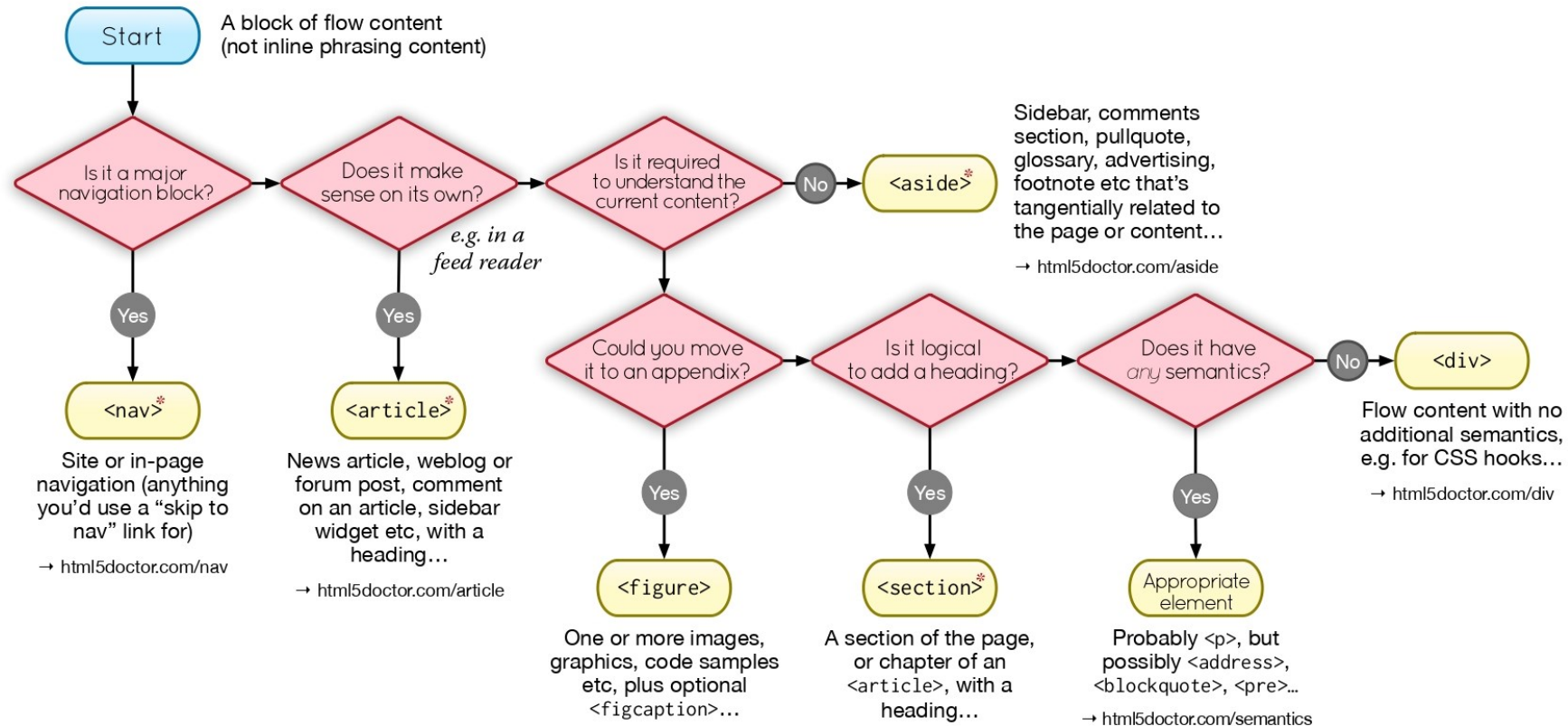
HTML5

- Uso de etiquetas semánticas.
- APIS desarrolladas en otros lenguajes de programación: videojuegos, accesos a base de datos, geolocalización.
- Provee soporte de audio y video nativo.
- Utiliza Local Storage para almacenar datos temporales.
- Aparición del elemento Canvas.

HTML5

En un documento HTML:

- Etiqueta `<!DOCTYPE>`: Indica la declaración del tipo de documento y del estándar en el que la página ha sido creada ya sea HTML o XHTML.
- Elemento `html`: es el elemento raíz del documento.
- Elementos `head` y `body`: para englobar la información de la página y del contenido, respectivamente.





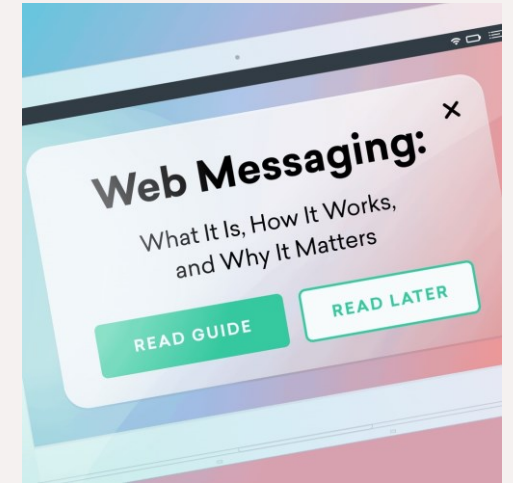
XSS



CORS



Local Storage



Web Messaging

Desglose HTML5

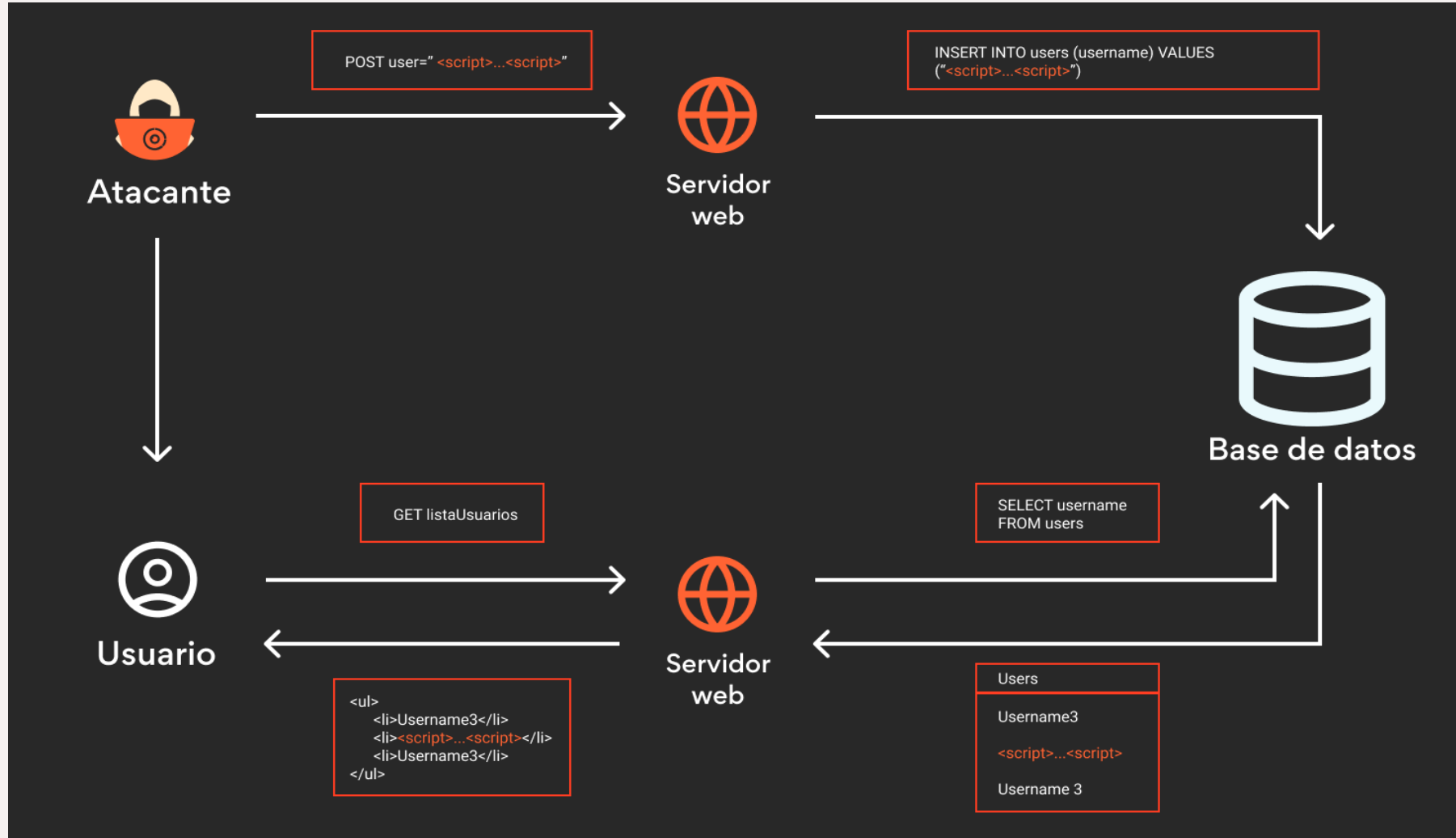
XSS



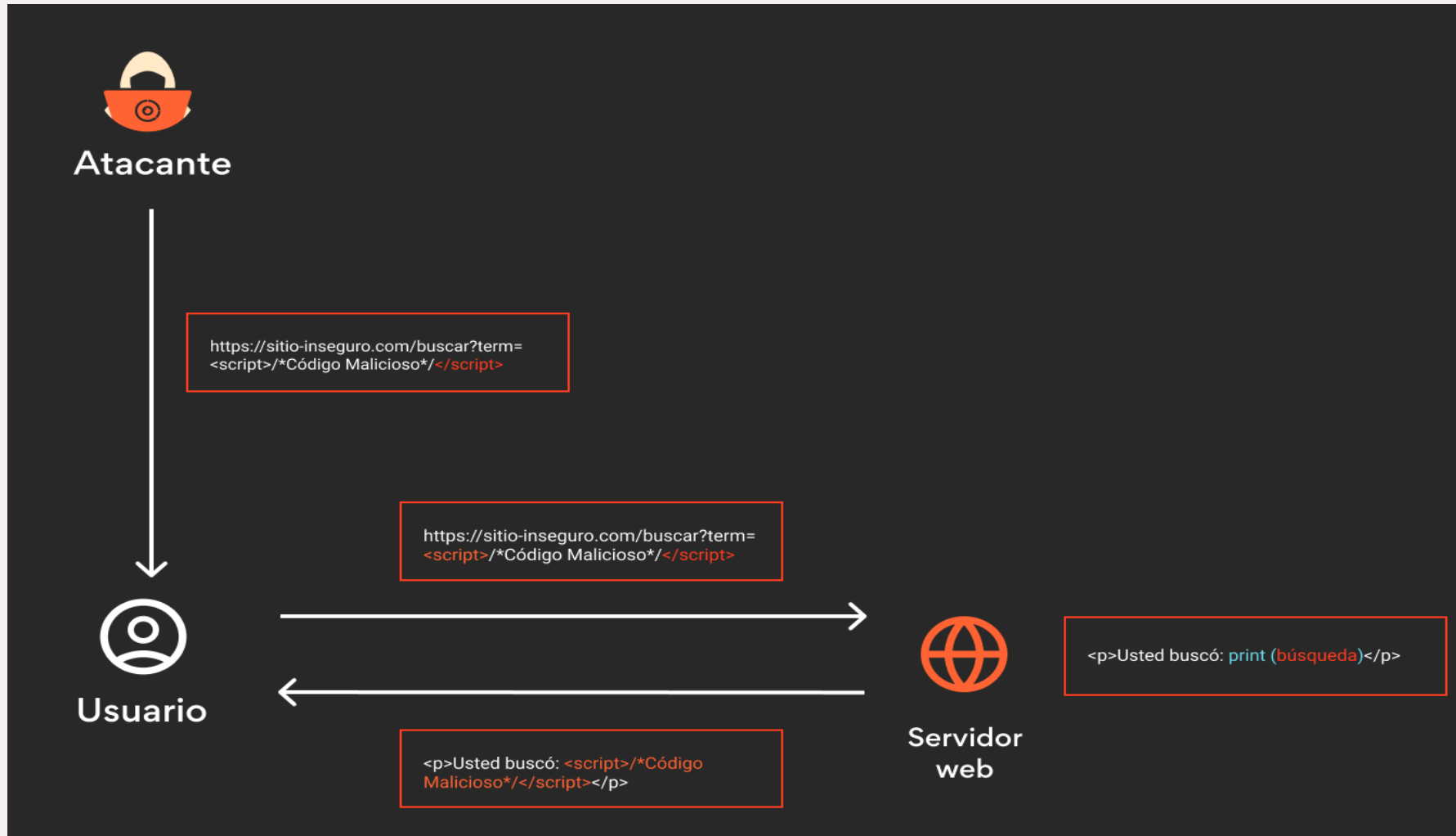
Cross-Site-Scripting (XSS) es una vulnerabilidad que aprovecha un atacante para ejecutar scripts en la parte del cliente.

- Tipos:
 - **Directo**
 - **Reflejado**
 - **Basado en DOM**
- 

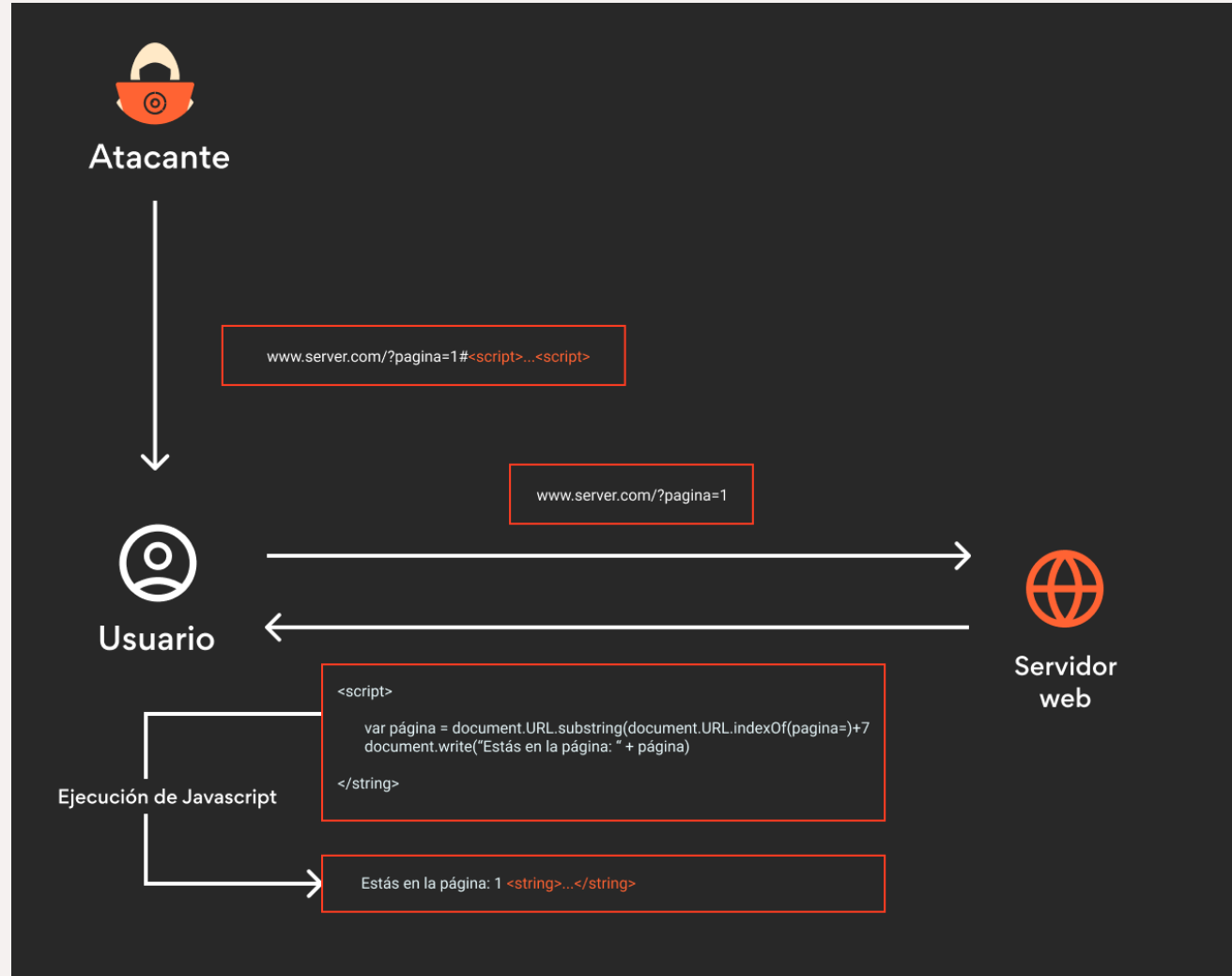
XSS Directo



XSS Reflejado



XSS Basado en DOM



CORS

¿Qué es?

- Cross-Origin Resource Sharing (CORS)
- Mecanismo basado en cabeceras HTTP.
- Permite indicar a un servidor los orígenes externos que pueden acceder a sus recursos.
- Ejemplo: “Access-Control-Allow-Origin: <http://www.ejemplo.com>”

CORS

¿Porqué es peligroso?

- Access-Control-Allow-Origin: *
- Access-Control-Allow-Origin: null
- Access-Control-Allow-Origin: sufijos de ejemplo.com

Local Storage

- Objeto JavaScript que permite guardar datos en el cliente de forma local.
- No tienen fecha de expiración.
- Aumenta las velocidades de transmisión.
- Vulnerable a XSS.

Web Messaging



- Permite a documentos de diferentes dominios comunicarse de una forma segura.
- EventListner para recibir el mensaje.
- Validar su origen para comprobar la integridad de este y procesar solo los mensajes de dominios conocidos.
- Validar el contenido del mensaje.



Conclusiones

- HTML y su evolución a lo largo de los años.
- HTML5.
- Consecuencia de malas configuraciones en HTML y la falta de validaciones de seguridad.
- Owasp: Top 10.

Gracias por vuestra atención

Tahir Farooq

