

# 1.A. Arquitecturas y lenguajes de programación en clientes web

## 2.- Lenguajes de programación en clientes web.

### 2.3.- Seguridad.

JavaScript proporciona un gran potencial para diseñadores maliciosos que quieran distribuir sus scripts a través de la web. Para evitar esto los navegadores web en el cliente aplican **dos tipos de restricciones**:



- Por razones de seguridad cuando se ejecuta código de JavaScript éste lo hace en un "espacio seguro de ejecución" en el cuál **solamente** podrá **realizar tareas relacionadas** con la web, nada de tareas genéricas de programación como creación de ficheros, etc.
- Además los **scripts** están **restringidos** por la **política** de "mismo origen": la cuál quiere decir que los scripts de una web **no tendrán acceso** a información tal como **usuarios**, **contraseñas**, o **cookies** enviadas desde otra web. La mayor parte de los agujeros de seguridad son infracciones tanto de la **política de "mismo origen"** como de la política de "espacio seguro de ejecución".

Al mismo tiempo es importante entender las **limitaciones que tiene JavaScript** y que, en parte, refuerzan sus capacidades de seguridad. JavaScript no podrá realizar ninguna de las siguientes tareas:

**Modificar o acceder a las preferencias del navegador del cliente, las características de apariencia de la ventana principal de navegación, las capacidades de impresión, o a los botones de acciones del navegador.**

- **Lanzar** la ejecución de una aplicación en el ordenador del cliente.
- **Leer** o **escribir** ficheros o **directorios** en el ordenador del cliente (con la excepción de las cookies).
- **Escribir** directamente ficheros en el servidor.
- **Capturar** los datos **procedentes** de una transmisión en streaming de un servidor, para su retransmisión.
- Enviar e-**mails** a nosotros mismos de forma invisible sobre los visitantes a nuestra página web (aunque si que podría enviar datos a una aplicación en el lado del servidor capaz de enviar correos).
- **Interactuar directamente con los lenguajes de servidor.**
- Las páginas **web** almacenadas en **diferentes dominios** no **pueden** ser **accesibles** por JavaScript.
- JavaScript es incapaz de **proteger** el origen de las **imágenes** de nuestra **página**.
- **Implementar** multiprocesamiento o **multitarea**.
- Otro tipo de **vulnerabilidades** que podemos encontrar están relacionadas con el **XSS**. Este tipo de **vulnerabilidad** **viola la política de "mismo origen"** y ocurre **cuando un atacante es capaz de inyectar código malicioso en la página web presentada a su víctima**. Este código malicioso puede provenir de la base de datos a la cuál está accediendo esa víctima. Generalmente este tipo de errores se deben a fallos de **implementación de los programadores de navegadores web**.

Otro aspecto muy relacionado con la seguridad son los **defectos** o **imperfecciones** de los **navegadores web** o **plugins** utilizados. Éstas imperfecciones pueden ser empleadas por los atacantes para escribir **scripts maliciosos** que se puedan ejecutar en el **sistema operativo** del **usuario**.

El **motor de ejecución de JavaScript** es el encargado de **ejecutar el código de JavaScript en el navegador** y por lo tanto **es en él dónde recaerá el peso fuerte de la implementación de la seguridad**. Podríamos citar varios ejemplos de motores de JavaScript:

- **Active Script de Microsoft**: tecnología que soporta JScript como lenguaje de scripting. A menudo se considera compatible con JavaScript, pero Microsoft emplea múltiples características que no siguen los estándares **ECMA**.
- **El kit de herramientas Qt** (Biblioteca desarrollada por Trolltech (en aquel momento "Quasar Technologies")) C++ (C plus plus) también incluye un módulo intérprete de JavaScript.
- El **lenguaje de programación Java en su versión JDK 1.6** introduce un paquete denominada javax.script que permite la ejecución de JavaScript.
- Y por supuesto todos los **motores implementados** por los **navegadores web** como Mozilla, Google, Opera, Safari, etc. Cada uno de ellos **da soporte a alguna de las diferentes versiones de JavaScript**.

Hoy en día una de las características que más se resalta y que permite **diferenciar** a unos navegadores de otros, es **la rapidez con** la que sus **motores de JavaScript** pueden **ejecutar** las **aplicaciones**, y la **seguridad** y **aislamiento** que ofrecen en la ejecución de las aplicaciones en **diferentes** ventanas o **pestañas** de **navegación**.

Créditos de la imagen

Autoría: maxim2

Licencia: CC0 1.0 Universal Public Domain.