EUSKO JAURLARITZA
GOBIERNO VASCO

nº 50
Diciembre de 2014

Aurrera!

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

- Las distribuciones de Linux
  Pág. 2
- Comprometiendo aplicaciones Web: XSS
  Pág. 6
- Alboan:
  Lehendakaritza libera el software de OpenIrekia
  Pág. 10
- Breves:
  50 números del boletín Aurrera
  LibreCon 2014 en Bilbao
  Pág. 12

14 años, 50 ejemplares, más de 100 artículos y una gran variedad de temas tratados. Este es el resumen en cifras del camino realizado hasta ahora por el boletín Aurrera! que tienes en tus manos.

> *«Aurrera! (¡adelante!), es una expresión muy utilizada en nuestro pueblo para dar ánimos a alguien a la hora de avanzar o acometer algo. Podemos encontrarle una doble connotación: en cuanto a superación de las dificultades mediante el esfuerzo y en cuanto a seguir un camino que lleva hacia delante, y que a veces se hace duro realizar.»*

Con estas mismas palabras empezaba nuestro boletín Aurrera! su camino allá por octubre del año 2000.

La verdad es que han sido muchos los esfuerzos que ha requerido y también algunas las felicitaciones que hemos recibido.

A través de estas líneas, queremos agradecer a todas aquellas personas que a lo largo del tiempo (de una manera u otra) han colaborado con nuestro Gabinete Tecnológico en la elaboración de los artículos, así como aquellas que nos han enviado sus sugerencias y/o aportaciones (e incluso sus críticas constructivas), todas las cuales siempre han sido bienvenidas. Sin olvidarnos del Servicio de Reprografía del Gobierno Vasco, así como del Servicio Oficial de Traductores del IVAP (IZO).

Esperando poder seguir contando con el apoyo y ánimo de todas ellas, continuaremos divulgando todas aquellas iniciativas y/o proyectos que los Departamentos y Organismos Autónomos lleven a cabo en el ámbito de las nuevas tecnologías.

Mila esker (muchas gracias)

Las distribuciones de Linux

Seguramente muchas de las personas que habitualmente nos leen hayan oído hablar en alguna ocasión de Linux[1] y sus famosas distribuciones, pero al no tener un perfil informático «avanzado» no sepan a qué se refiere. Pues bien, a través de este artículo queremos explicar qué es una distribución, por qué surgieron y cuáles son sus principales características.

Una distribución[2] de Linux (también conocidas por el diminutivo «distro») es un conjunto de software basado en el núcleo Linux, el cual **incluye una serie de paquetes o programas** adicionales (procesador de texto, hoja de cálculo, reproductor de video, herramientas para gestión administrativa, documentación, un administrador de ventanas, un entorno de escritorio, etc.), cuyo objetivo es dar respuesta a las necesidades de los usuarios finales.

Cabe recordar que a lo largo de la historia han existido y existen distribuciones que están soportadas por empresas, es decir, con un objetivo comercial, como pueden ser, entre otras, Fedora (soportada por la empresa Red Hat), openSuSE (Novell), Ubuntu (Canonical); aunque también hay distribuciones mantenidas por la «Comunidad», como son Debian y Gentoo.

Debido a ello, y con el paso de los años, han ido surgiendo ediciones o distribuciones que estaban orientadas al sector doméstico, mientras que otras se centraban en el sector empresarial.

ANTECEDENTES

Antes de que apareciesen las primeras distribuciones de Linux, si una persona quería usar Linux en su ordenador ésta debía tener unos mínimos conocimiento sobre Unix[3], ya que debía saber cuales eran las «bibliotecas» y programas ejecutables necesarios para arrancar el sistema, por ejemplo.

De hecho, las distribuciones de Linux empezaron a aparecer poco después de que fuese publicado el núcleo de Linux, allá por 1991. La razón fue que en aquel momento a los programadores les interesaba más desarrollar un sistema operativo en lugar de aplicaciones, interfaces para los usuarios o un paquete de software determinado.

Entre las primeras distribuciones que se lanzaron podemos mencionar las siguientes: MCC Interim Linux (la cual se podía descargar de un servidor público FTP de la Universidad de Mánchester, en febrero de 1992); TAMU (creada por estudiantes de la Universidad de Texas A&M); Softlanding Linux System (también conocida como SLS); Yggdrasil Linux creó el primer CD-ROM de una distribución Linux; etc.

«Actualmente existen más de 300 distribuciones de GNU/Linux»

Desde aquellos primeros momentos, algunos usuarios vieron que Linux podía ser una alternativa válida a los sistemas operativos MSDOS de Microsoft en la plataforma de ordenadores personales o PCs, MacOS en Apple Macintosh y las versiones bajo licencia (bajo pago) de UNIX. La mayoría de estos primeros usuarios se habían ido familiarizando con el entorno UNIX porque lo usaban en sus empresas o centros educativos (Universidades, etc.)

Las primeras distribuciones surgieron para facilitar al usuario «medio» el usar Linux en sus ordenadores, evitando de esta forma tener que instalar (y en muchos casos compilar) los paquetes que eran necesarios utilizar. Las distribuciones se han popularizado tanto que incluso hoy en día son usadas por los usuarios «expertos».

Si bien, históricamente, Linux estuvo mejor posicionado en el mercado de los servidores, distribuciones centradas en la facilidad de instalación y uso, tales como Fedora, Mandriva, OpenSuSE, Knoppix y Ubuntu, entre otras, han

DICCIONARIO

[1] **Linux:** es un sistema operativo libre, basado en Unix. De hecho, es uno de los principales ejemplos de software libre y código abierto. El núcleo de este sistema operativo fue desarrollado en 1991 por el finlandés Linus Torvalds.

[2] **Distribución:** es el resultado de unir un núcleo (*kernel*), *drivers* y aplicaciones. Todo ello nos permite interactuar con la máquina u ordenador. Tanto las aplicaciones como el entorno gráfico varían de una distribución a otra. Algunas distribuciones usan como entorno de escritorio, por ejemplo, el llamado KDE, otras utilizan Xfce, etc.

[3] **Unix:** es el sistema operativo creado por la empresa AT&T a mediados de los 70. Los sistemas GNU/Linux y BSD se basan en la filosofía de Unix. También OSX de Mac es un sistema tipo Unix. Por ello, se puede decir que es la base de Linux y demás sistemas operativos similares.

logrado una mayor aceptación en el mercado doméstico.

TIPOS DE DISTRIBUCIONES

Linux, como ya es sabido, es un sistema operativo de libre distribución, por lo que actualmente se pueden encontrar en muchas páginas webs de Internet todos los ficheros y programas necesarios para su funcionamiento. De todas formas, la tarea de reunir todos esos ficheros y programas, así como instalarlos en nuestro sistema y configurarlos, puede requerir de un trabajo bastante complicado y no apto para muchas personas (por motivos técnicos o por no disponer del tiempo suficiente). Por ese motivo, en su momento surgieron las llamadas «distribuciones de Linux». Algunas empresas y organizaciones, por ejemplo, se dedican a hacer ese trabajo por nosotros y, posteriormente, lo ponen a nuestra disposición.

«Las primeras distribuciones surgieron para facilitar al usuario "medio" el usar Linux en sus ordenadores»

En estos casos, suelen ser los programadores de las distintas distribuciones los que realizan ese esfuerzo de recopilar lo mejor del software libre disponible en cada momento y mejorar los procesos de instalación, todo ello con el fin de facilitar la vida al usuario «medio». En definitiva, recopilan el mejor software disponible, mejoran la detección de dispositivos y los entornos gráficos, implementan procesos de instalación automatizados, etc.

Actualmente, y como consecuencia de todo ello, existen más de 300 distribuciones de GNU/Linux y su número va en aumento, puesto que cada vez resulta más fácil hacer una distribución propia a partir de ya las existentes. Esto puede sorprender o desorientar a los usuarios de Windows que están acostumbrados a una única interfaz para todas sus versiones. No obstante esta diversidad permite que distintos usuarios puedan usar GNU/Linux de acuerdo con sus necesidades específicas.

En general, las distribuciones Linux pueden ser:

- ✓ Comerciales o no comerciales
- ✓ Ser completamente libres o incluir software privativo
- ✓ Diseñadas para ser usadas en el ámbito doméstico o en las empresas
- ✓ Diseñadas para servidores, escritorios o dispositivos empotrados (embebidos)
- ✓ Orientadas a usuarios con pocos conocimientos informáticos o para usuarios avanzados
- ✓ De uso general o para dispositivos altamente especializados, como un cortafuegos, un enrutador o un clúster de servidores

Hoy en día, podemos encontrar distribuciones que no requieren ninguna instalación, las cuales reciben el nombre de «*Live*», «Live CD» o «Live DVD». Éstas consisten en una distribución que va almacenada en un medio extraíble, por ejemplo un CD o un DVD, la cual puede ser ejecutada directamente desde este dispositivo sin necesidad de instalar nada en el disco duro del ordenador, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

Precisamente esta característica hace que este tipo de distribuciones sean ideales para ser usadas en demostraciones, procesos de recuperación, cuando haya que utilizar una máquina que no es nuestra o como medio de instalación para una distribución estándar. Tal es así que, hoy en día, casi todas las distribuciones tienen una versión *Live*.

A continuación incluimos una breve descripción de las distribuciones de Linux más importantes, así como sus principales características[4]:

- **Ubuntu:** distribución basada en Debian que se centra en el usuario final y se caracteriza por su facilidad de uso. Es muy popular y dispone de un amplio soporte por parte de la Comunidad. El entorno de escritorio por defecto es GNOME. Otra característica es que realiza publicaciones de nuevas versiones de forma regular (cada seis meses). Esta distribución incluye una serie de paquetes cuidadosamente seleccionados de Debian, y conserva su sistema de mantenimiento de paquetes que le permite instalar y desinstalar programas de un modo fácil. A diferencia de otras distribuciones que vienen con un gran número de programas que normalmente no se usan, Ubuntu incluye un

DICCIONARIO

[4] **Principales características** de las distribuciones de Linux: (se incluye información general de cada distribución: creador, fecha de lanzamiento y última versión). http://es.wikipedia.org/wiki/Anexo:Comparativa_de_distribuciones_Linux

Otra página web que reúne noticias, análisis, capturas de pantalla, lanzamientos o desarrollos, y establece un ranking de popularidad, es **DistroWatch**: http://distrowatch.com

número reducido de aplicaciones básicas y de gran calidad. Es la distribución que probablemente mejor soporte ofrece para el hardware más reciente. Cada versión de Ubuntu se distribuye en dos modalidades: estación de trabajo (*workstation*) y servidor (*server*). Asimismo ofrece soporte gratuito durante 18 meses. Las versiones LTS[5] son especiales y tienen 3 años de soporte para la edición *desktop* y 5 para la edición *server*. Debido a sus características, Ubuntu ha sido la base de otras distribuciones, como pueden ser, Guadalinex (promovida por la Junta de Andalucía), MoLinux (Castilla-La Mancha), etc.

- **RedHat Enterprise**: distribución creada por la compañía RedHat[6]. Se caracteriza por ser una distribución de muy alta calidad, contenidos y soporte a los usuarios por parte de la empresa que la distribuye. Aunque en este caso es necesario el pago de una licencia de soporte. Está enfocada principalmente a las empresas. Ofreció soporte hasta la versión 9 momento en que decidió concentrar sus esfuerzos en el desarrollo de la versión corporativa RedHat Enterprise Linux y delegó la versión común a Fedora Core, un proyecto abierto e independiente de Red Hat. Actualmente RedHat Enterprise Linux es una distribución comercial orientada a grandes servidores.

- **Fedora**: Fedora Core, es una distribución enteramente libre, patrocinada por RedHat y desarrollada/soportada por su Comunidad. Se caracteriza por ser fácil de instalar y ofrecer una buena calidad. Esta «distro» es generalista y está enfocada a una amplia variedad de personas o perfiles.

- **Knoppix**: distribución basada en Debian y desarrollada por Klaus Knopper en Alemania. Destaca de manera especial la detección automática de hardware. Se realizan actualizaciones con frecuencia, pero una vez ha adquirido cierta estabilidad, suelen pasar varios meses hasta que llega una nueva versión.

- **Debian**: esta distribución inició su andadura de la mano de Ian Murdock en 1993. En el proyecto de desarrollo colabora un gran equipo de programadores, que es dirigido de una forma muy rígida. Tal es así que en cualquier momento del proceso de desarrollo existen tres versiones del producto: «estable», «en pruebas» e «inestable». Cuando aparece una nueva versión de un paquete, por ejemplo, se sitúa en el apartado «inestable» para llevar a cabo las primeras pruebas; si las pasa, el paquete pasa al apartado «pruebas», donde se realiza un exhaustivo test que puede durar varios meses. Todo ello hace que esta distribución sea posiblemente la más estable y confiable de todas las existentes, aunque no la más actualizada. Por todo ello, los expertos recomiendan la versión «estable» para servidores con funciones críticas. De todas formas, muchas personas prefieren usar en sus ordenadores las versiones de «pruebas» o «inestable» ya que están más actualizadas. Por otro lado, y según muchas personas, el proceso de instalación es un poco más complicado si lo comparamos con otras «distros». Para compensar este aspecto, se ofrece el instalador de paquetes «apt-get» de Debian. Algunas distribuciones que se han basado en Debian son: Knoppix, Gnoppix, Linspire, GnuLinex (promovida por la Junta de Extremadura), etc.

«Las distribuciones de Linux empezaron a aparecer poco después de que fuese publicado el núcleo de Linux, allá por 1991»

- **SuSE Linux Enterprise**: desarrollada en Alemania, es una de las principales distribuciones de GNU/Linux existentes a nivel mundial. Entre sus principales virtudes se encuentra el que sea una de las más sencillas de instalar y administrar, gracias, principalmente, a que cuenta con varios asistentes gráficos para realizar las diversas tareas. Ofrece muy buena calidad en cuanto a contenidos y soporte por parte de la empresa que la distribuye, Novell, aunque es necesario el pago de una licencia de soporte. En su momento, Novell, anunció su

DICCIONARIO

[5] **LTS:** son las siglas en inglés de *Long Term Support* (en castellano «Soporte a Largo Plazo»).

Si una versión de Ubuntu es LTS, significa que es una versión que tendrá soporte durante más tiempo que una versión «normal».

Las versiones LTS de Ubuntu tienen soporte durante 5 años.

Las LTS suelen ser versiones más estables que el resto.

[6] **RedHat:** es posiblemente la compañía de linux más popular del mundo. Fue fundada en 1995 por Bob Young y Marc Ewing.

intención de crear la comunidad abierta OpenSuse para complementar los desarrollos de SuSe Linux Enterprise (en una estrategia similar a la llevaba a cabo por Red Hat con Fedora). Se caracteriza por estar enfocada principalmente a las empresas. La distribución destaca por su instalador y la herramienta de configuración YaST. La documentación que viene con las versiones comerciales, es considerada como la más completa y útil.

- **OpenSuSE**: versión libre de la distribución comercial SuSE que se caracteriza por ser fácil de instalar.
- **Slackware**: esta distribución, creada por Patrick Volkerding en 1993, es una de las primeras que salió al mercado, por lo que es una de las más veteranas de las distribuciones GNU/Linux actualmente disponibles. Su principal característica ha sido siempre apostar por la simplicidad y la estabilidad. La interface del programa de instalación es de texto, y necesita un mayor conocimiento de Linux que la mayoría de las otras distribuciones.
- **Gentoo**: esta distribución está inspirada en BSD-ports. Los expertos no recomiendan trabajar con esta «distro» si no tenemos una buena conexión a internet y un ordenador mínimamente potente, así como cierta experiencia a la hora de trabajar con sistemas Unix.
- **KUbuntu**: distribución basada en Ubuntu que se centra en el usuario final y destaca por su facilidad de uso. La gran diferencia con Ubuntu es que el entorno de escritorio por defecto es KDE.
- **Mandriva**: esta distribución fue creada en 1998 con el objetivo de acercar el uso de Linux a todas las personas, por lo que se caracteriza por la facilidad de uso. Mandriva Linux, antes llamada Mandrake Linux (rebautizada tras una fusión empresarial) originalmente era una derivación francesa de RedHat.

Como hemos visto e lo largo del artículo, existe una gran cantidad de distribuciones, cada una con sus propias características, por lo que si nos decidimos a usar alguna de ellas lo más recomendable es saber para qué la queremos y, a continuación, ir a la página web[7] correspondiente para bajarnos una. ❑

DICCIONARIO

[7] **Página web** dónde poder descargar cada una de las distribuciones:
www.ubuntu.com
www.redhat.com
www.es.debian.org
www.opensuse.com
www.suse.com
www.slackware.com
www.gentoo.org
www.kubuntu.com
www.mandrivalinux.org
www.mandriva.com
www.novell.com/linux
http://fedora.redhat.com

La distribución KZnux

El proyecto de alfabetización digital **KZgunea**, nació en 2001 y es la red de centros públicos gratuitos para la formación y el uso de las TIC de Euskadi. Desde su inicio, KZgunea ha apostado por el uso y la formación en herramientas libres ofreciendo cursos como OpenOffice, tratamiento de imágenes digitales con GIMP, Audacity…

En 2011, KZgunea crea **KZnux**, una distribución basada en Ubuntu y que se adapta específicamente a las necesidades del servicio y, sobre todo, a las de las personas usuarias. Tras superar algunos hándicaps durante la migración del sistema operativo, como puede ser el de la infraestructura y, quizás la más importante, la aceptación del nuevo entorno por parte del usuario final y después de varias versiones, KZnux se ha convertido en una realidad que se puede probar en cualquiera de los más de 260 centros KZgunea repartidos por todo el territorio de la Comunidad Autónoma de Euskadi.

La buena aceptación del nuevo sistema operativo y la inclinación que desde KZgunea se ha adoptado en favor del software libre, fueron los detonantes para crear un módulo formativo específico llamado «Software Libre», que toma tanta importancia como los módulos «Redes Sociales» o «Internet Básico» en el plan formativo.

De cara al futuro, KZgunea se mantendrá en una constante de mantenimiento y mejora de su plan formativo en herramientas *opensource* y, por supuesto, en su sistema operativo KZnux.

www.kzgunea.net

Comprometiendo aplicaciones Web: XSS

En el área de la seguridad de aplicaciones Web nos encontramos con diferentes técnicas que comprometen estas aplicaciones; dentro del conjunto de estas vulnerabilidades de seguridad Web, y entre las más relevantes, está la conocida como **ataque por inyección de *scripts* (XSS)**, vamos a ver en qué consiste.

En primer lugar, vamos a explicar qué es, en el ámbito de la seguridad, una **vulnerabilidad o fallo de seguridad**: es una debilidad de un sistema de información, o de sus procedimientos de seguridad, o de sus controles internos, etc., que podría ser utilizada para producir un incidente de seguridad, de tal modo que la posibilidad de que una vulnerabilidad se explote constituye una **amenaza**, y si esta amenaza se materializa sobre un activo (recurso del sistema de información o relacionado con este), es cuando el incidente de seguridad es un hecho, ya que se produce un **daño**.

Diariamente se publican multitud de fallos de seguridad (vulnerabilidades) en lo que respecta a los entornos Web, tanto relativos a productos como a aplicaciones.

De hecho, existe una base de datos denominada WHID, *Web Hacking Incidents Database*, de WASC[8], en donde se publican los incidentes de seguridad más relevantes; uno de sus objetivos es concienciar sobre la seguridad de los entornos Web, así como proporcionar información para su análisis estadístico (la idea básica es que las incidencias de seguridad queden registradas de una manera pública, que se asocien a vulnerabilidades de seguridad de aplicaciones Web, y que se solucionen). Esta base de datos asocia a cada incidente de seguridad un código único que incluye el año en el que se produjo el incidente, junto con un número correlativo por año.

Los expertos recomiendan que se consulte dicha web para conocer el estado del arte en lo que respecta a los ataques e incidentes de seguridad.

INYECCIÓN DE SCRIPTS (XSS)

Hay que destacar la relevancia en la actualidad de los ataques por inyección de scripts, pero, ¿en qué consiste? Se entiende por «inyección de scripts» distintas técnicas que comparten el mismo sistema de explotación, que consiste en incluir (inyectar) pequeños programas (*scripts*) que tienen por objeto que el navegador de la persona usuaria atacada ejecute el código "inyectado" cuando acceda a la página alterada.

Básicamente se puede decir que consiste en incluir un código de programa HTML, *Javascript*[9] o *VBScript*[10] en una aplicación Web, y de esta forma causar una acción indebida en el navegador de la persona usuaria que ejecuta dicho código; esto es posible gracias a que el código HTML se **interpreta en el navegador** de la persona usuaria, y no en el servidor, por ello es un ataque que compromete la seguridad de la persona usuaria más que la seguridad del servidor. Esta última característica, el que no se comprometa la seguridad del servidor, que sea un «ataque del lado del cliente», ha hecho que este tipo de ataques no sean considerados o tenidos muy en cuenta, propagándose la idea de que no pueden comprometer la seguridad de un sitio Web, cosa que no es cierta.

Otra denominación del ataque «inyección de

DICCIONARIO

[8] **WASC:** *Web Application Security Consortium*, Consorcio para la seguridad de aplicaciones Web, que proporciona una detallada clasificación de amenazas en aplicaciones Web.

[9] **JavaScript:** es un lenguaje de programación que se utiliza para crear páginas Web dinámicas (lenguaje para crear acciones), donde aparecen texto, animaciones...es un lenguaje de programación interpretado, esto es, se ejecuta directamente, sin tener que compilar sus líneas de código. También se le llama ECMAScript. Como repetimos en el artículo, se ejecuta en el lado del cliente, no en el del servidor.

[10] **VBScript:** es un lenguaje de programación desarrollado por Microsoft, similar a JavaScript, pero que sólo funciona con navegadores de Microsoft.

scripts» es su traducción al inglés: «*Cross Site Scripting*» o XSS, o secuencias de comandos en sitios cruzados. XSS permite a los atacantes ejecutar secuencias de comandos en el navegador de la víctima, por ello estos pueden realizar diversas acciones: secuestrar las sesiones de usuario, redirigir a la persona usuaria hacia sitios web maliciosos, ejecutar aplicaciones en el navegador de la persona usuaria sin que esta sea consciente (troyano)...

¿Cómo se pueden realizar este tipo de acciones (incluir código fuente en una página)? Simplemente hay que buscar un punto de entrada (cualquier sitio que devuelva datos ingresados por el usuario). El caso más común es utilizar los formularios de entrada, o el campo «buscar», que aparecen en muchos sitios web; por ejemplo, cuando incluimos un texto en el campo «buscar», la cadena que hemos incluido puede aparecer en el código fuente del sitio web en cuestión (si se puede visualizar mediante la acción «ver código fuente de la página»), es decir, la cadena de texto que hemos escrito en el campo «buscar» está incluida (*inyectada*) en el código fuente de la página, formando parte de ella, lista para ser interpretada por el navegador; **después de enviar la información al servidor, esta será incluida en el código fuente de alguna página, lista para ser interpretada por los navegadores de las personas usuarias que la ejecutan, gracias a la utilización de diferentes trucos y técnicas para que el navegador interprete este código de la forma deseada (ya que el código malicioso suele estar dentro de los atributos de otras etiquetas)**. La vulnerabilidad existe cuando es posible que se incluya código en la página, que esta se envíe al servidor, y a partir de ahí realizar los ataques. Resumiendo, el atacante envía cadenas de textos que son *scripts* (secuencias de comandos) de ataque, que se almacenan en las páginas web del servidor, y que posteriormente se ejecutarán en el intérprete del navegador de la persona usuaria.

Determinados filtros anti ataques por inyección de *scripts* pueden impedir que se utilicen caracteres tales como comilla simple (’), comilla doble(“), símbolos de *mayor que* (>) y *menor que* (<), símbolo de barra (/) y espacio ( ), que sirven para escribir pequeños programas de código; si se pueden introducir estos caracteres, tenemos muchas posibilidades de encontrar fallos de *Cross Site Scripting* (XSS).

Este tipo de ataques se aprovechan de la falta de **sistemas que filtren y verifiquen la entrada** de datos en los campos habilitados a tal efecto.

QUÉ SE PUEDE ATACAR CON ESTE TIPO DE VULNERABILIDADES

En este tipo de ataques la aplicación Web envía los datos proporcionados por el usuario al navegador, en la parte cliente, siendo el problema que si estos datos no se validan ni se codifican, esto permite a un atacante ejecutar código en el navegador de la persona usuaria, pudiendo realizar, entre otras, las siguientes acciones: robo de sesiones (ver

DICCIONARIO

[11] ***Document.cookie***: es un «objeto» del lenguaje JavaScript; en JavaScript podemos acceder a las *cookies* a través de la propiedad *cookie* de este objeto (*document*). Esta propiedad permite acceder a todas las *cookies* de una página Web, pero para acceder a una *cookie* concreta, es necesario analizar la cadena para localizar su valor.

Qué son las «sesiones» y qué es la «gestión de usuarios»

Cuando una persona usuaria ingresa en un sitio Web, se le asigna un identificador único; como ya adelantamos en el boletín Aurrera número 49 (artículo «¿Qué es eso de los *cookies*?») el problema que presentan las sesiones HTTP de Internet (funcionamiento basado en un protocolo de comunicación «sin estado» -*stateless*-), es que no son capaces de mantener información persistente entre diferentes peticiones; ya que no existe un vínculo físico permanente entre los dos extremos de esa comunicación; por ello, el proceso de persistencia del identificador único se debe hacer desde el servidor (almacenar de forma temporal el identificador hasta que la relación *persona usuaria - sitio Web* finalice), almacenando dicho identificador tanto en el propio servidor Web, como en el equipo de la persona usuaria (esta última acción se realiza a través de los *cookies*). Es aconsejable que la gestión de sesiones se realice empleando identificadores de sesión no predecibles, para que no puedan ser adivinados mediante técnicas de «fuerza bruta».

Debe quedar claro que lo que se conoce como «sesiones» no tiene ninguna relación con la «gestión de usuarios» o «mecanismos de autentificación», en este último caso, existe un identificador asociado a una persona usuaria, y es totalmente independiente del gestor de sesiones.

recuadro inferior) -acceder al objeto *document.cookie*[11] y enviarlo a un servidor web controlado por la persona atacante y de este modo secuestrar la sesión de la víctima-, así como la modificación de los contenidos de la Web (***defacement***[12]) y de su configuración, ***phishing*** (obtención de datos de una persona usuaria), ataques por denegación de servicio o DoS (forzar el uso intensivo de recursos), gusanos XSS, re-direccionamiento de páginas Web, etc.

Como hemos visto, las posibilidades de este tipo de ataques son realmente amplias, por ejemplo, una vez comprobado que podemos ejecutar código en la página Web, podemos realizar multitud de acciones: cerrar la sesión de usuario automáticamente, borrar todos sus mensajes, mandar mensajes automáticamente para conseguir las *cookies* de sesión de las personas usuarias, modificar el contenido de ese sitio, etc.

Resumiendo, **un sitio Web es vulnerable cuando no se asegura que todas las entradas de datos que son introducidas por los usuarios son codificadas adecuadamente**, o si **durante el ingreso no se verifica que los datos son seguros antes de incluirlos en la página de salida**.

Además de todo lo dicho anteriormente, la exposición pública de que un determinado sitio Web sufre este tipo de vulnerabilidad afecta negativamente al negocio asociado a dicho sitio (imagen negativa percibida por las personas clientes).

TIPOS DE VULNERABILIDADES XSS

Principalmente existen dos tipos:

1. **Ataques no persistentes o reflejados**: cuando el servidor genera una página en función de la información proporcionada; por ejemplo, una búsqueda, cuando los datos no son validados por el navegador y se incluyen en el código fuente de la página. Un ejemplo sencillo de este tipo de ataque: se envía el enlace (la URL) modificado a través de las Redes Sociales (la página Web no se ha modificado, sólo el enlace, en donde se ha inyectado código), además, para que «no se vea la modificación» se suele acortar la URL (utilizando programas específicos que realizan esta tarea).
2. **Ataques persistentes o almacenados**: en este caso la inyección se realiza en una página estática, la información proporcionada por el atacante se almacena en la base de datos, en el sistema de archivos… para, posteriormente, ser mostrada a otras personas usuarias que visiten la página, de ahí que se llame «persistente». Un caso práctico simple: una página Web en la que la persona atacante introduce un «post»[13] con código inyectado (que se almacena en la página Web), para que, cuando entre otra persona usuaria a dicha página Web, le re-direccione a otra página Web distinta a la que ha accedido.

«La seguridad debe ser tomada como un elemento clave en lo que respecta al ciclo de vida del desarrollo de elementos software en el ámbito Web»

MEDIDAS DE PROTECCIÓN

Como hemos comentado anteriormente, se pueden utilizar filtros anti-ataques por inyección de *scripts*; otra limitación, que sirve como **medida de protección**, es que el código introducido no pueda ser superior a un número determinado de caracteres o que el tipo de datos y su longitud se corresponden con los datos que se esperan; también puede ser útil filtrar determinados comandos, como pueden ser: *script, form, object, applet, img*…

Otra medida recomendable es utilizar los navegadores actualizados, esto es, con las últimas versiones disponibles de los mismos, e indicar a estos que no ejecuten este tipo de códigos.

DICCIONARIO

[12] ***Defacement***: se refiere al cambio producido, de una forma intencionada, por un atacante, en una página Web, a través de la obtención de algún tipo de acceso a la misma, por supuesto sin autorización del dueño de dicha página. A los autores de este tipo de acciones se les conoce por el nombre de *defacer*.

[13] ***Post***: es sinónimo de entrada o artículo que se publica en un blog ordenado de manera cronológica.

Aun así, si bien con el uso de herramientas automatizadas para la detección de vulnerabilidades XSS (como, por ejemplo, *Appscan, Webinspect, Acunetix* y *Burp Suite*) se pueden detectar ciertas vulnerabilidades, hay que tener en cuenta que cada aplicación «construye» sus páginas Web de salida de una forma diferente, utilizando diferentes intérpretes en el navegador, lo que supone dificultar la detección automática; por todo ello, además de utilizar herramientas automáticas de detección de vulnerabilidades XSS, se debe revisar el código de una forma manual (es la forma más elemental de detección), y también es aconsejable realizar pruebas de penetración.

¿CÓMO CONSEGUIR UNA WEB SEGURA?

Hay dos puntos importantes en lo que respecta al diseño y desarrollo de aplicaciones Web, por un lado está el propio entorno de desarrollo Web, que debe estar asegurado en lo que respecta a las vulnerabilidades de seguridad, y, por otro lado, la propia aplicación Web, que se programa en función del lenguaje de programación elegido. Además, debemos tener en cuenta que las aplicaciones Web suelen ser públicas, están desarrolladas para diferentes entornos, usan puertos conocidos, y se utiliza HTTP, que es el protocolo para realizar transacciones en la Web.

En la actualidad se están realizando trabajos para conseguir una **lista unificada** de clasificación de vulnerabilidades Web. También existen aplicaciones Web vulnerables desarrolladas por empresas dedicadas a la seguridad, para que puedan ser probadas por las herramientas automáticas de detección de vulnerabilidades, y, de este modo, valorar su comportamiento en este ámbito.

En cualquier caso, queda claro que **la concienciación y la formación en el área de la seguridad Web son dos elementos fundamentales**, sino imprescindibles, para conseguir aplicaciones Web seguras y fiables. Para alcanzar un nivel de seguridad óptimo es imprescindible implicar tanto a administradores de sistemas como a desarrolladores de aplicaciones Web, así como realizar auditorías de seguridad (utilizando test de caja negra y test de caja blanca[14]). ❑

Proyecto abierto de seguridad en aplicaciones Web: OWASP Foundation

Open Web Application Security Project (OWASP) es un proyecto abierto de seguridad en aplicaciones Web, básicamente es una organización internacional abierta, sin ánimo de lucro, nacida en el año 2001, dedicada a permitir a las organizaciones realizar el desarrollo, adquisición y mantenimiento de aplicaciones Web fiables y seguras.

Todas las herramientas, documentos, foros y delegaciones del OWASP son libres y abiertas a cualquiera interesado en mejorar la seguridad de las aplicaciones. Desde OWASP abogan por un enfoque de la seguridad en las aplicaciones como un problema tecnológico, de procesos, y que involucra a la gente, porque los enfoques más efectivos respecto a la seguridad de aplicaciones incluyen mejoras en todas estas áreas. Desde OWASP se crean documentación y herramientas abiertas y gratuitas, se organizan foros virtuales y conferencias con el objeto de difundir el conocimiento y mejorar la seguridad en el ámbito de las aplicaciones Web.

Existen delegaciones repartidas por todo el mundo. Las actividades de OWASP se financian a través de patrocinadores, donaciones y con la aportación de una cuota anual por parte de sus miembros.

Esta organización publica una lista anual denominada **OWASP Top 10** que se enfoca en la identificación de los diez riesgos más serios para una amplia gama de organizaciones, respecto a las aplicaciones Web; muchos de estos riesgos son fáciles de encontrar y fáciles de explotar. En la lista publicada en el año 2013 **los ataques por inyección de código (XSS) aparecen en el número tres**. También desarrolla la guía de pruebas de OWASP, conjunto de pruebas que aplicadas sobre las aplicaciones Web sirven para detectar vulnerabilidades en las mismas.

http://www.owasp.org (en inglés)

DICCIONARIO

[14] **Test de caja negra y test de caja blanca:** los test de caja negra son realizados desde «fuera», y consisten en simular los ataques de un *hacker*, con los recursos que estos utilizan; los test de caja blanca se realizan desde «dentro», y en ellos los auditores recaban toda la información posible para, de este modo, evaluar la seguridad del entorno sometido al test. También suelen hacerse test denominados de **caja gris**, que es una combinación de los dos test anteriores.

ALBOAN:

Lehendakaritza libera el software de OpenIrekia

«Lehendakaritza facilita el código fuente de Irekia a través del portal "Opendata" (en su apartado "OpenApps")»

El pasado mes de octubre, Lehendakaritza liberaba la última versión del **código fuente** de su plataforma de Gobierno Abierto «Irekia», poniéndolo, de esta forma, a disposición de todas aquellas personas y/o entidades que quieran implantarlo en su ámbito de actuación.

DE IREKIA A OPENIREKIA

En enero de 2010 Lehendakaritza puso en marcha la iniciativa conocida como «Irekia». Este proyecto tenía (y tiene) como objetivos hacer que la Administración Pública vasca sea más **transparente**, así como hacer que la opinión de la ciudadanía sea más relevante.

Para alcanzar ambos objetivos la Dirección responsable del proyecto habilitó en su momento un portal web (denominado *Irekia*), el cual está integrado en la estructura de euskadi.eus.

Irekia basa su funcionamiento en dos ideas:

1. **Transparencia**. Ésta es considerada como el primer pilar de cualquier Gobierno Abierto. Por ello, a través de Irekia se hace pública la actualidad del Gobierno Vasco, su agenda de eventos, el material audiovisual y la hemeroteca. Todo ello con el objetivo de reforzar aún más la relación con la ciudadanía.
2. **Participación y colaboración.** Bajo esta idea, Irekia cuenta con dos espacios: por un lado, las «*Propuestas del Gobierno*», pensado para que la ciudadanía aporte sus comentarios y dudas a las propuestas, anteproyectos de ley o iniciativas que los Departamentos del Gobierno publican; y, por otro lado, las «*Propuestas ciudadanas*», un espacio donde cualquier persona puede crear sus propias propuestas sobre los asuntos que a cada uno le resulte de interés.

Actualmente, todas las aportaciones son analizadas y puestas en conocimiento de las personas del Gobierno con responsabilidades en cada materia para que tengan conocimiento de las mismas y, aquellas ideas que puedan ser aprovechadas por el Ejecutivo, pasen a formar parte del material de los grupos de trabajo que preparan, diseñan y elaboran las diferentes iniciativas y propuestas legislativas.

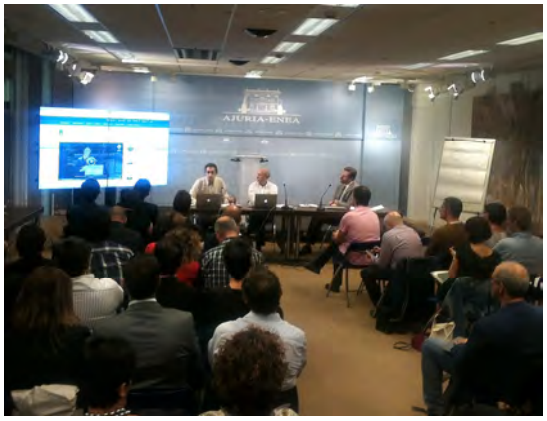
Desde el punto de vista de los usuarios finales, indicar que estos pueden acceder a los contenidos multimedia a través de un navegador web o desde dispositivos móviles, incluyendo las correspondientes aplicaciones nativas para iOS y Android.

EL CÓDIGO FUENTE DE IREKIA

El software que soporta la web de Irekia se viene liberando desde sus primeras versiones bajo la denominación de «OpenIrekia–Gobierno Abierto», y se pone a disposición de la **ciudadanía**, **empresas**, **organizaciones** y, por supuesto, de otras **instituciones y administraciones públicas**, facilitando, de esta manera, la **reutilización libre y gratuita del software**. Lo cual evita que las administraciones públicas que quieran poner en marcha una plataforma de Gobierno Abierto

tengan que realizar nuevas inversiones económicas de dinero público.

Siguiendo el compromiso del Gobierno Vasco de apertura y colaboración, Lehendakaritza facilita el **código fuente** de Irekia a través del portal «*OpenData*» (dentro del apartado *OpenApps,* donde se están publicando todas las aplicaciones del Gobierno Vasco). De esta forma, mediante la distribución libre y gratuita del citado software, la plataforma Irekia queda al alcance de la ciudadanía, empresas, organizaciones, así como de otras instituciones. En este sentido, indicar que varias Administraciones ya se han basado en la plataforma OpenIrekia para poner en marcha su portal de «Gobierno Abierto».



ASPECTOS TÉCNICOS

La plataforma OpenIrekia liberada (desarrollada con el lenguaje de programación Ruby 2.1) ha sido preparada para ser implantada sobre un servidor con sistema operativo Ubuntu Linux 14.04 LTS, servidor web Apache 2.4, servidor de aplicaciones Phusion Passenger, base de datos PostgreSQL 9.3, motor de búsqueda Elastic Search 1.3 (java 7) y hace uso del *framework* de desarrollo RubyOnRails 4.1 .

Para facilitar que cualquier persona y/o entidad pueda probar las características y comprobar el funcionamiento de Irekia, Lehendakaritza ha habilitado tres opciones para descargar el software:

1. **Tradicional**: consiste en la instalación completa del sistema. Se instala Ubuntu 14.04 LTS Server y después se realiza la instalación completa del propio servicio web.
2. **Emulación en local**: consiste en descargar una máquina virtual completa para VMware donde la imagen contiene el sistema operativo, todos los componentes de software y OpenIrekia ya instalados y listos para iniciar.
3. ***Web Service***: (máquina virtual en *Amazon Web Services*) Para desarrollo en un servidor accesible en internet es posible iniciar copia de todo el sistema con el sistema operativo, todos los componentes de software y OpenIrekia ya instalados en el servicio de hosting en la nube de Amazon, *Amazon Web Services*.

En cuanto a la licencia utilizada, señalar que el código fuente está liberado bajo la Licencia Pública de la Unión Europea «*European Union Public Licence* (EUPL)».

Esta licencia, desarrollada en el seno de la Unión Europea, nació con la intención de ser la licencia bajo la cual se liberasen los programas y aplicaciones desarrolladas por la Administración Pública y con la característica específica de ser compatible con otras licencias denominadas libres, como la GNU *General Public License* (GNU/GPL). Una licencia de estas características dota de mayor seguridad jurídica a las aplicaciones así liberadas y fomentan la interoperabilidad de los servicios de la Administración Electrónica. ❑

«La plataforma *OpenIrekia* está desarrollada para ser usada en un servidor con Ubuntu»

[+info]:

Web de Irekia:

http://irekia.euskadi.eus

Licencia EUPL:

http://www.osor.eu/eupl

ALBOAN

¡¡BREVES!!

nº 50

Diciembre de 2014

50 números del boletín Aurrera

En octubre del año 2000 se publicaba el primer ejemplar del Boletín divulgativo «Aurrera!».

Desde entonces han pasado ya casi 15 años y un total de 50 números. Por ello, y con motivo del ejemplar número 50, la Dirección de Informática y Telecomunicaciones, a través del Gabinete Tecnológico del Gobierno Vasco, ha decidido elaborar este año un libro para conmemorar dicho aniversario.

Este libro, que consta de 128 páginas, está integrado por una selección de los artículos más significativos que a lo largo de los últimos años se han publicado en el boletín Aurrera! Una vez seleccionados, los distintos artículos han sido agrupados en una serie de capítulos que son los siguientes:

1. El euskera
2. La Web
3. Los sistemas corporativos
4. La eAdministración
5. Los planes y/o proyectos
6. Las personas
7. El software libre
8. La seguridad

El libro se encuentra disponible tanto en castellano como en euskera.

Para todas aquellas personas que estén interesadas en tener acceso a los distintos ejemplares del boletín Aurrera publicados hasta la fecha, así como al contenido del propio libro, informaros que todos ellos están disponibles, en formato PDF, en la siguiente página web:

Web en Euskadi.eus:
http://www.euskadi.eus/informatica

LibreCon 2014 en Bilbao

El pasado mes de noviembre (los días 11 y 12), tuvo lugar en el Palacio Euskalduna de Bilbao (Bizkaia) el evento «**LibreCon 2014**», Congreso Nacional de Software Libre y Tecnologías Abiertas.

Dicho evento, que fue organizado por **ASOLIF** (Federación Nacional de Empresas de Software Libre) y **ESLE** (Asociación de Empresas de Software Libre de Euskadi), contó con la asistencia de casi 1.500 personas procedentes de 600 empresas, administraciones públicas y otras organizaciones.

A lo largo de los dos días que duró el evento se llevaron a cabo más de 60 conferencias, jornadas, ponencias y talleres prácticos, centradas en campos del comercio, las finanzas, la educación, la industria o los servicios en las administraciones públicas. A este respecto indicar que el Gobierno Vasco estuvo presente con un stand. Así mismo, el Gobierno Vasco, EJIE y KZgunea tuvieron la oportunidad de dar a conocer las principales características de sus proyectos con varias ponencias: «*El Software Libre en el Gobierno Vasco*», «*Hadoop Big Data: Plataforma de almacenamiento masivo y distribuido en un contexto de Big Data en la red corporativa de Gobierno Vasco*» y «*Plataforma de eLearning de KZgunea*», respectivamente.

El objetivo de LibreCon era dar visibilidad a este sector y demostrar cómo las tecnologías abiertas generan empleo y son un motor de competitividad.

Web de LibreCon: http://www.librecon.io
Web de ESLE: http://www.esle.eu
Web de ASOLIF: http://www.asolif.es