17-6-2015

SECURITY WORM

DEPARTAMENTO DE ELECTRÓNICA E INFORMÁTICA

Autores:
Ernesto González Pradas
Jorge Guzmán Ovejero
Ismael Pérez Roldan

Tutor del proyecto:
Samuel Arranz

Índice

1.- Nombre del proyecto y resumen del mismo

¿Qué es Security Worm?

La empresa consiste en el análisis de los metadatos de los archivos que introduzca el usuario, bien sean, imágenes, documentos, vídeos, etc.

Security Worm S.L., cuya localización se encuentra en la calle Ronda de Atocha 55, Madrid.

La actividad que genera esta empresa es analizar o borrar los metadatos de los archivos introducidos por los usuarios en un tiempo determinado. Para ello usamos distintas tecnologías software, herramientas que nos permitirán mostrar por pantalla todos los metadatos analizados.

Los metadatos

Metadatos son los datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos, llamado recurso. El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos. Por ejemplo, en una biblioteca se usan fichas que especifican autores, títulos, casas editoriales y lugares para buscar libros. Así, los metadatos ayudan a ubicar datos.

Para varios campos de la informática, como la recuperación de información o la web semántica, los metadatos en etiquetas son un enfoque importante para construir un puente sobre el intervalo semántico.

Resumen del proyecto

Podrá haber dos tipos de usuarios, los usuarios free o gratuitos, los cuales tendrán derecho a subir archivos de imágenes para ser analizados, y los usuarios premium, que tendrán derecho a subir archivos de cualquier extensión para poder ser analizados, y si quieren borrar los metadatos.

Los clientes a los que va destinado este tipo de producto, son aquellos a los que les interesa extraer información adicional de los archivos. Por ejemplo, una persona le entrega un documento y esta, quiere saber si lo ha escrito esa persona que se lo entregó u otra.

2.- Herramientas Utilizadas

Para poder llevar a cabo este proyecto nos hemos servido de varias herramientas informáticas las cuales explicaremos a continuación. Estas son las herramientas que hemos utilizado para el desarrollo del proyecto:

- **SUBLIME TEXT.** Sublime Text es un editor de código multiplataforma, ligero y con pocas concesiones a las florituras. Es una herramienta concebida para programar sin distracciones. Su interfaz de color oscuro y la riqueza de coloreado de la sintaxis, centra nuestra atención completamente.

Sublime Text permite tener varios documentos abiertos mediante pestañas, e incluso emplear varios paneles para aquellos que utilicen más de un monitor. Dispone de modo de pantalla completa, para aprovechar al máximo el espacio visual disponible de la pantalla.
El programa cuenta “de serie” con 22 combinaciones de color posibles, aunque se pueden conseguir más. Para navegar por el código cuenta con Minimap, un panel que permite moverse por el código de forma rápida.

- **NOTEPAD ++.** Notepad++ es un editor de texto y de código fuente libre con soporte para varios lenguajes de programación. De soporte nativo a Microsoft Windows. Se parece al Bloc de notas en cuanto al hecho de que puede editar texto sin formato y de forma simple. No obstante, incluye opciones más avanzadas que pueden ser útiles para usuarios avanzados como desarrolladores y programadores. Se distribuye bajo los términos de la Licencia Pública General de GNU.

- **MARIADB.** MariaDB es un sistema de gestión de bases de datos derivado de MySQL con licencia GPL. Es desarrollado por Michael (Monty) Widenius (fundador de MySQL) y la comunidad de desarrolladores de software libre. Introduce dos motores de almacenamiento nuevos, uno llamado Aria -que reemplaza con ventajas a MyISAM- y otro llamado XtraDB -en sustitución de InnoDB. Tiene una alta compatibilidad con MySQL ya que posee las mismas órdenes, interfaces, APIs y bibliotecas, siendo su objetivo poder cambiar un servidor por otro directamente.1 Este SGBD surge a raíz de la compra de Sun Microsystems -compañía que había comprado previamente MySQL AB2 - por parte de Oracle. MariaDB es un fork directo de MySQL que asegura que permanecerá una versión de este producto con licencia GPL. Monty decidió crear esta variante porque estaba convencido de que el único interés de Oracle en MySQL era reducir la competencia que MySQL daba al mayor vendedor de bases de datos relacionales del mundo que es Oracle.

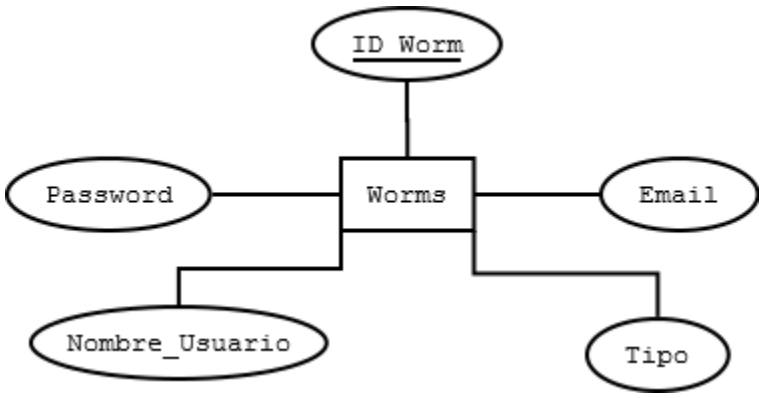
- **WINSCP.** WinSCP es una aplicación de Software libre. WinSCP es un cliente SFTP gráfico para Windows que emplea SSH. El anterior protocolo SCP también puede ser empleado. Su función principal es facilitar la transferencia segura de archivos entre dos sistemas informáticos, el local y uno remoto que ofrezca servicios SSHNewbie. El código fuente de WinSCP y las descargas están hospedadas en SourceForge.

- **PUTTY.** Putty es un cliente SSH, Telnet, rlogin, y TCP raw con licencia libre. Disponible originalmente sólo para Windows, ahora también está disponible en varias plataformas Unix, y se está desarrollando la versión para Mac OS clásico y Mac OS X. Otra gente ha contribuido con versiones no oficiales para otras plataformas, tales como Symbian para teléfonos móviles. Es software beta escrito y mantenido principalmente por Simon Tatham, open source y licenciado bajo la Licencia MIT.

Estas y otras herramientas que hemos utilizado en la parte de desarrollo web, como por ejemplo bootstrap, o PDInfo en la parte de Raspberry Pi las explicaremos en sus apartados correspondientes.

3.- Bases de datos, planteamiento y desarrollo.

Modelo Entidad/Relación



Las Tablas

Field	Type	Null	Key	Default	Extra
ID_Worm	int(11)	NO	PRI	NULL	auto_increment
Email	varchar(50)	NO	UNI	NULL	
Password	varchar(255)	NO		NULL	
Nombre_Usuario	varchar(50)	NO		NULL	
Tipo	tinyint(1)	NO		NULL	

4.- Desarrollo web y sus contenidos

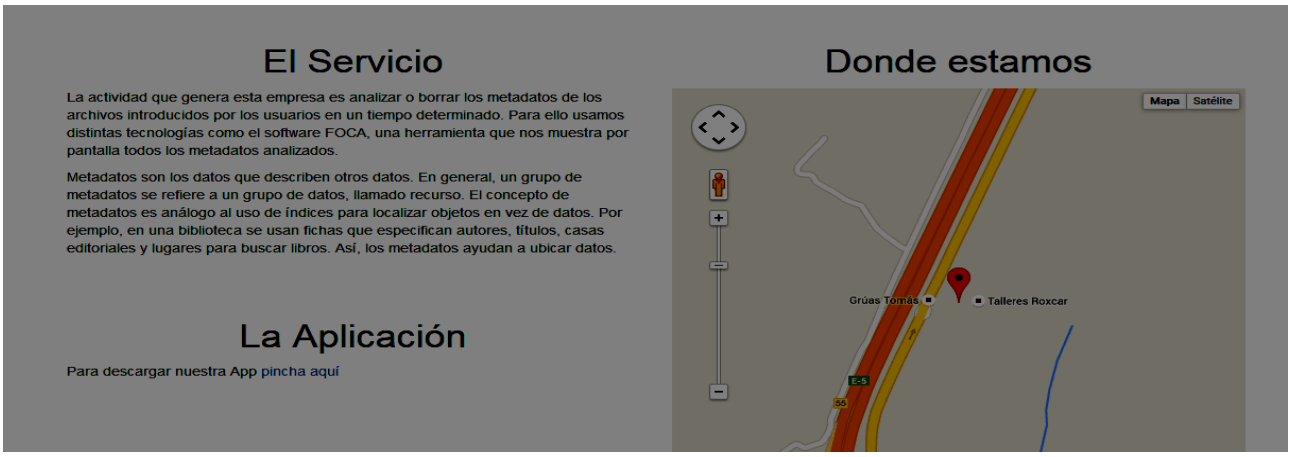
Sección Pública (Página principal, Quienes somos…)

- Página principal:

En la página principal, encontramos de forma visual muy intuitiva como utilizar los servicios de Security Worm en tres pasos:

- ¿Quiénes somos?

Explicamos brevemente a los componentes de este proyecto, su historial académico, que es Security Worm, donde estamos localizados, y un enlace para descargar nuestra aplicación para el móvil.



- Registrarse

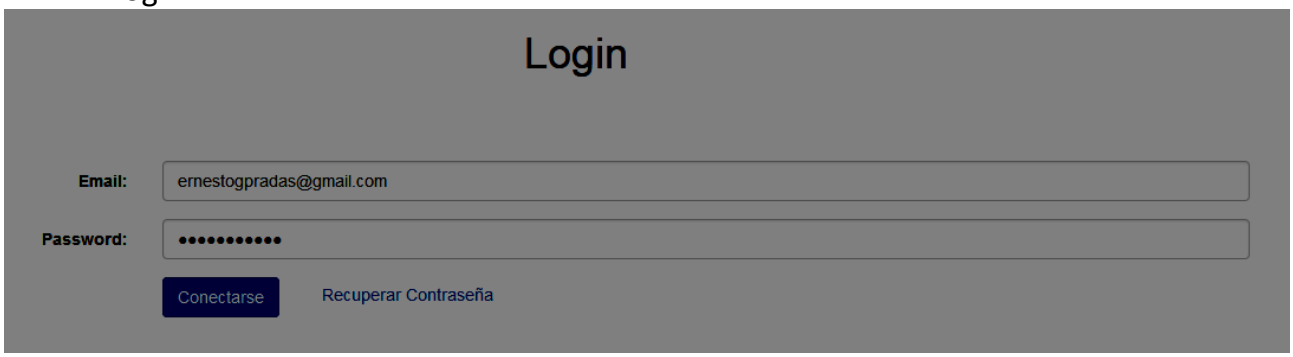
Los usuarios se pueden registrar de dos formas en la página, una de forma Premium y la otra de forma Gratuito:

Premium:

Gratuito:

Sección Privada (PHP, Javascript)

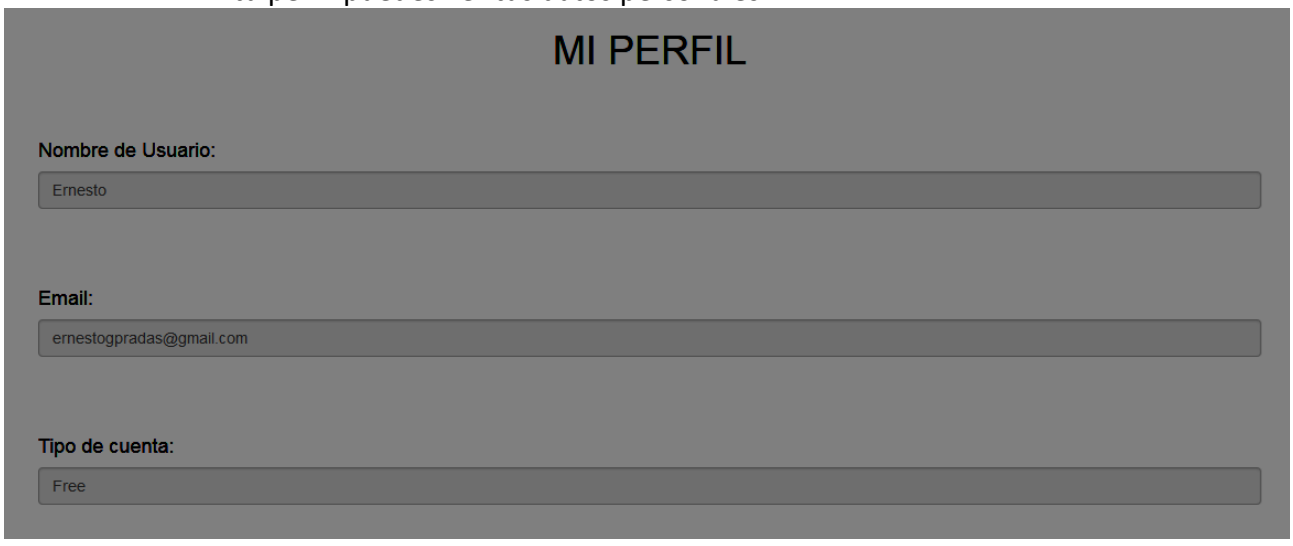
-Login



Una vez registrados, los usuarios pueden loguearse en esta pantalla:

- Perfil

En tu perfil puedes ver tus datos personales:

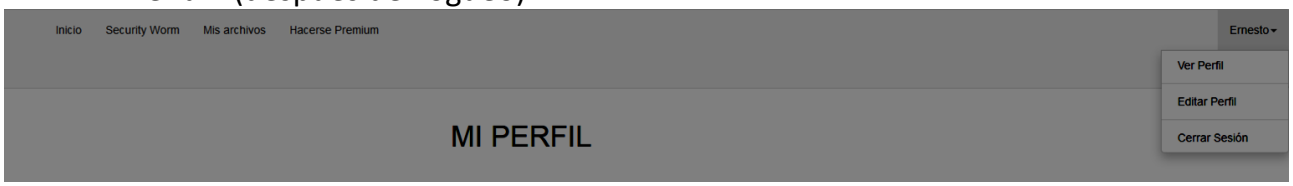


- Mis archivos

En esta pestaña podemos subir un archivo y analizar los metadatos a la par que mantenemos un historial:

- Menú 1 (antes del logueo)

- Menú 2 (después del logueo)



Bootstrap:

Ya que como una parte muy importante de nuestro trabajo ha sido el estudio y aprendizaje de este lenguaje de programación, a continuación, antes de explicar cómo hemos utilizado Bootstrap en nuestro proyecto, voy a citar de Wikipedia los Orígenes, Características, Estructura, Función y Uso de dicha herramienta.

Origen

Bootstrap fue desarrollado por Mark Otto y Jacbod Thornton de Twitter, como un marco de trabajo (framework) para fomentar la consistencia a través de herramientas internas. Antes de Bootstrap, se usaban varias librerías para el desarrollo de interfaces de usuario, las cuales guiaban a inconsistencias y a una carga de trabajo alta en su mantenimiento.

El primer desarrollo en condiciones reales ocurrió durante la primera "Semana de Hackeo" (Hackweek) de Twitter."5 Mark Otto mostró a algunos colegas como acelerar el desarrollo de sus proyectos con la ayuda de la herramienta de trabajo. Como resultado, decenas de temas se han introducido en el marco de trabajo.

En agosto del 2011, Twitter liberó a Bootstrap como código abierto. En febrero del 2012, se convirtió en el proyecto de desarrollo más popular de GitHub.

Características

Bootstrap tiene un soporte relativamente incompleto para HTML5 y CSS 3, pero es compatible con la mayoría de los navegadores web. La información básica de compatibilidad de sitios web o aplicaciones está disponible para todos los dispositivos y navegadores. Existe un concepto de compatibilidad parcial que hace disponible la información básica de un sitio web para todos los dispositivos y navegadores. Por ejemplo, las propiedades introducidas en CSS3 para las esquinas redondeadas, gradientes y sombras son usadas por Bootstrap a pesar de la falta de soporte de navegadores antiguos.

Desde la versión 2.0 también soporta diseños sensibles. Esto significa que el diseño gráfico de la página se **ajusta dinámicamente**, tomando en cuenta las características del dispositivo usado (Computadoras, tabletas, teléfonos móviles).

Bootstrap es de código abierto y está disponible en GitHub. Los desarrolladores están motivados a participar en el proyecto y a hacer sus propias contribuciones a la plataforma.

Estructura y Función

Bootstrap es modular y consiste esencialmente en una serie de hojas de estilo LESS que implementan la variedad de componentes de la herramienta. Una hoja de estilo llamada bootstrap.less incluye los componentes de las hojas de estilo. Los desarrolladores pueden adaptar el mismo archivo de Bootstrap, seleccionando los componentes que deseen usar en su proyecto.

Los ajustes son posibles en una medida limitada a través de una hoja de estilo de configuración central. Los cambios más profundos son posibles mediante las declaraciones LESS.

Desde la versión 2.0, la configuración de Bootstrap también tiene una opción especial de "Personalizar" en la documentación. Por otra parte, los desarrolladores eligen en un formulario los componentes y ajustes deseados, y de ser necesario, los valores de varias opciones a sus necesidades. El paquete consecuentemente generado ya incluye la hoja de estilo CSS pre-compilada.

Sistema de cuadrilla y diseño sensible

Bootstrap viene con una disposición de cuadrilla estándar de 940 píxeles de ancho. Alternativamente, el desarrollador puede usar un diseño de ancho-variable. Para ambos casos, la herramienta tiene cuatro variaciones para hacer uso de distintas resoluciones y tipos de dispositivos: teléfonos móviles, formato de retrato y paisaje, tabletas y computadoras con baja y alta resolución (pantalla ancha). Esto ajusta el ancho de las columnas automáticamente.

Entendiendo la hoja de estilo CSS

Bootstrap proporciona un conjunto de hojas de estilo que proveen definiciones básicas de estilo para todos los componentes de HTML. Esto otorga una uniformidad al navegador y al sistema de anchura, da una apariencia moderna para el formateo de los elementos de texto, tablas y formularios.

Componentes reusables

En adición a los elementos regulares de HTML, Bootstrap contiene otra interfaz de elementos comúnmente usados. Ésta incluye botones con características avanzadas (e.g grupo de botones o botones con opción de menú desplegable, listas de navegación, etiquetas horizontales y verticales, ruta de navegación, paginación, etc.), etiquetas, capacidades avanzadas de miniaturas tipográficas, formatos para mensajes de alerta y barras de progreso.

Plugins de JavaScript

Los componentes de JavaScript para Bootstrap están basados en la librería jQuery de JavaScript. Los plugins se encuentran en la herramienta de plugin de jQuery. Proveen elementos adicionales de interfaz de usuario como diálogos, tooltips y carruseles. También extienden la funcionalidad de algunos elementos de interfaz existentes, incluyendo por ejemplo una función de auto-completar para campos de entrada (input). La versión 2.0 soporta los siguientes plugins de JavaScript: Modal, Dropdown, Scrollspy, Tab, Tooltip, Popover, Alert, Button, Collapse, Carousel y

Typeahead.

Uso

Para usar Bootstrap en una página HTML, el desarrollador solo debe descargar la hoja de estilo Bootstrap CSS y enlazarla en el archivo HTML.

Si el desarrollador también quiere usar los componentes de JavaScript, éstos deben estar referenciados junto con la librería jQuery en el documento HTML.

Bootstrap en Security Worm

Utilizando la herramienta Bootstrap, hemos conseguido que nuestra página se ajuste automáticamente a cualquier tipo de resolución de pantalla, ya sea en un ordenador, una tablet o un móvil.

Para ello hemos ido metiendo en nuestro código HTML las siguientes etiquetas en diferentes cajas a lo largo de todo el proyecto.

Como por ejemplo esta:

```
<html>
  <head></head>
  <body>
    <div class="navbar navbar-default"></div>
    <div class="body-container">
      <div class="container">
        ::before
        <div class="col-xs-12 col-sm-12 col-md-12 col-lg-12">
          <center>
            <img class="col-xs-4 col-sm-4 col-md-12 col-lg-12" src="images/paso1.png"></img>
          </center>
          <center></center>
          <center></center>
        </div>
        ::after
      </div>
    </div>
    <br \=""></br>
```

5.- Raspberry Pi

Como servidor usamos una Raspberry Pi modelo B+, con un overclock a 950 MHz para aumentar el rendimiento. Puesto que el overclock puede aumentar la temperatura de nuestra Raspberry Pi hemos desarrollado un script que nos muestra por pantalla la temperatura actual del procesador, así podremos controlar que nuestra Raspberry Pi no se calienta demasiado.

El contenido del script se encuentra en:

sudo /opt/vc/bin/vcgencmd measure_temp

Puesto que nuestro servidor web está alojado en nuestra Raspberry Pi utilizamos **No-IP**, el cual convierte nuestra IP dinámica en una IP estática y comprueba cada 5 minutos si esta ha cambiado. En el caso de que cambie, se actualizará nuestra IP, además, afiliará nuestra IP a un nombre de dominio, en nuestro caso, **securityworm.ddns.net.**

Además, hubo que abrir los puertos 80(web) y 8969(ssh) e instalar el software de NO-IP en nuestra Raspberry Pi.

En cuanto al apartado de seguridad en nuestra Raspberry Pi, modificamos el fichero de configuración de ssh para que el usuario root no pueda acceder y modificamos el puerto de ssh a 8969 en lugar de 22. Además, eliminamos el usuario pi, puesto que es el usuario por defecto en

todas las distribuciones de Raspbian y creamos un usuario con los mismos permisos que “pi”.

Para la lectura de los metadatos utilizamos tres herramientas:

- **PDINFO.-** para analizar documentos pdf,
- **EXITFOOL.-**para imágenes y documentos generados por Microsoft office. Esta es una herramienta Open Source, escrita en Perl y multiplataforma, soporta varios formatos, entre ellos están EXIF, GPS, IPTC, XMP, JFIF, ID3 y otras más.
- **Librerías php->phpmailer.-** para el envío de mails vía php desde Gmail.
- **LIBEXTRACTOR.-**para extraer los metadatos de los demás tipos de documentos. Es una biblioteca utilizada para extraer los metadatos de cualquier tipo de archivo. Está diseñado para realizar una extracción real, y para ser trivialmente prorrogables por enlaces con extractores externos para tipos de archivo adicionales. Actualmente, libextractor soporta los siguientes formatos: HTML, PDF, PS, OLE2 (DOC, XLS, PPT), OpenOffice(sxw), StarOffice (sdw), DVI, MAN, FLAC, MP3 (ID3v1 and ID3v2), NSF(E) (NES music), SID (C64 music), OGG, WAV, EXIV2, JPEG, GIF, PNG, TIFF, DEB, RPM, TAR(.GZ), ZIP, ELF, S3M (Scream Tracker 3), XM (eXtended Module), IT (Impulse Tracker), FLV, REAL, RIFF (AVI), MPEG, QT and ASF. También algunos MIME pueden ser detectados.

6.- Pruebas

Las comprobaciones que se hicieron durante la realización de la aplicación web fueron las siguientes:

1. Comprobación de los resultados de analizar los metadatos con el programa FOCA (WINDOWS) tienen los mismos resultados que analizarlos con los paquetes Exiftool, Libextractor y Pdfinfo.
2. Estudio de puertos para facilitar la conexión a la Raspberry Pi de forma externa.
3. Estudio de lenguaje de programación usado para la creación de la página web, y tras mirar los pros y los contras, decidimos hacerlo mediante Bootstrap y PHP orientado a objetos.

7.- Conclusiones

1. Adquirir nuevos recursos para optimizar el código de la web.
2. Cumplir el objetivo inicial del proyecto.
3. Investigar nuevos paquetes para su uso en el proyecto.
4. Crear trabajo en equipo a distancia.
5. Aprender la gran cantidad de datos que los archivos tienen ocultos.

8.- Aspectos a mejorar

Los aspectos a mejorar son los siguientes:

1. Mejor equipo para el proceso de envío de los correos y analizar los metadatos más rápido para el usuario.
2. Mejora de la seguridad existente en la Raspberry Pi.
3. Encriptación más segura para el almacenamiento y envío de los archivos.