CMS y LMS vulnerables a ataques de sus administradores de bases de datos.

CMS and LMS vulnerable to attacks by their database administrators.

Ing. Alexis Ramón Domínguez Arrojo

Ingeniero Informático, Miembro de la Federación de Radioaficionados de Cuba. Desarrollador de software y administrador de redes de la Empresa de Mantenimiento a los Grupos Electrógenos de Fuel-Oil. Plaza de la Revolución, La Habana, Cuba
Email:cl2ada@frcuba.cu

Dr. **Ing. Juan Carlos Sepúlveda Peña.**

Dr. en Ciencias Informáticas, Ingeniero en Control Automático, Profesor Titular de la Facultad de Informática del Instituto Superior Politécnico José Antonio Echeverría. Calle 114 e/ 119 y 127, Marianao, La Habana, Cuba
Email: jcarlos@ceis.cujae.edu.cu

Dr. Ing. Yulier Núñez Musa·

Dr. en Ciencias Informáticas, Profesor Titular de la Facultad de Informática del Instituto Superior Politécnico José Antonio Echeverría. Calle 114 e/ 119 y 127, Marianao, La Habana, Cuba.
Email: jnunezm@ceis.cujae.edu.cu

RESUMEN

En la era de la Internet se utilizan cada vez más diversas tecnologías para llevar la información y el conocimiento a personas de todo el mundo. Algunas de ellas son los Sistemas para la Gestión del Aprendizaje como Moodle; los blogs, los sitios y portales web, basándose buena parte de estos en populares Sistemas Gestores de Contenidos como Joomla, Wordpress y Drupal. Estas tecnologías tienen en común la necesidad de usar un Sistema Gestor de Base de Datos para su funcionamiento en general, lo que incluye el uso de tablas para almacenar datos de los usuarios que tendrán acceso al sistema e información necesaria para su autenticación. Estos sistemas son administrados por personas que poseen elevados números de privilegios y que pueden explotar las vulnerabilidades presentes en Joomla, Wordpress, Drupal y Moodle para apropiarse de la cuenta de un usuario determinado para realizar actos perjudiciales con el nombre de dicha cuenta; esto lo logra al suplantar el *password* que existe en la base de datos (que él administra) asociado a un usuario por un nuevo *password* generado por él, sin que el usuario víctima lo note y pueda impedirlo. De ahí que el objetivo del artículo sea demostrar la existencia de dichas vulnerabilidades y como pueden ser explotadas por este tipo de personas con la intención de hacer daño, alertando de esta manera a los usuarios y a los desarrolladores de estas tecnologías para que tomen medidas al respecto. Los autores dan una propuesta de solución a esta situación.

PALABRAS CLAVES: Base de datos, sistema gestor de base de datos, sistemas gestores de contenidos, sistemas para la gestión del aprendizaje, vulnerabilidades.

ABSTRACT

In the era of the Internet the information and knowledge, utilize to people of whole more and more various carryout technologies the world. Some there are Learning Management Systems like Moodle; sites and portals Web, having a base good part of these in popular Content Management Systems like Joomla, Wordpress and Drupal. These technologies have the need to use Data Base Management Systems for his functioning in general jointly that includes the use of tables to store data of the users that will have

access to the system and necessary information for its authentication. People administrate the systems that they possess elevated numbers of privileges and that the present vulnerabilities in Joomla, Wordpress, Drupal and Moodle to take possession of the account of a user determined can exploit to accomplish nuisances under the name of the aforementioned account. This achieves it taking some my place the password that exists in database (that he administrates) once a user for a new password generated by him was associated, without than the user victim note it and may impede him. So that the objective of the article be to demonstrate the existence of the aforementioned vulnerabilities and as they can be exploited by this people's type with the intention of being harmful, alerting this way the users and to the developers of these technologies in order that they take measures to the respect. The authors give a proposal of solution to this situation.

KEY WORDS: Databases, data base management systems, content management systems, learning management systems, vulnerabilities.

1- INTRODUCCIÓN

Con el surgimiento de la Internet y la Web 2.0[1] es común ver como sitios y portales web, así como blogs[2] y diferentes aplicaciones inundan el ciberespacio[3] [1]. Gran parte de estas tecnologías se desarrollan utilizando Sistemas de Gestión de Contenidos[4] (CMS, por sus siglas en inglés) por las ventajas y beneficios que estos proveen [2]. Algunos de los CMS libres más conocidos y utilizados son: Joomla, Drupal y Wordpress [3].

También se han vuelto populares en Internet los Ambientes Educativos Virtuales o Sistemas de Gestión de Aprendizaje[5] (LMS, por sus siglas en inglés) por las ventajas que estos ofrecen a los diferentes usuarios de diferentes regiones del mundo [4]. Uno de los sistemas libres más conocido y utilizado es el Ambiente de Aprendizaje Dinámico y Modular Orientado a Objetos (Moodle, por sus siglas en inglés) [5].

Estas tecnologías tienen en común la necesidad de usar un Sistema Gestor de Base de Datos[6] (SGBD) para su funcionamiento en general, lo que incluye el uso de tablas[7] para almacenar datos de los usuarios que tendrán acceso al sistema e información necesaria para su autenticación[8]. También requieren por lo general de un servicio *hosting*[9] para mantener los sitios o blogs en línea (*online*) [21].

Es usual leer noticias de ataques y hackeos realizados de manera externa a diferentes sitios webs y blogs que se sustentan en las tecnologías anteriores [6]. Acerca de esta variante de ataques y la forma

[1] Sistema global de hipertexto que utiliza Internet como su mecanismo de transporte. En un sistema de hipertextos, el usuario navega haciendo clic sobre hipervínculos, que despliegan otros documentos (que también contiene hipervínculos) [1].

[2] Espacio personal de escritura en Internet, similar a un diario en línea, es decir, un sitio que una persona usa para escribir periódicamente, en el que toda la escritura y el estilo se manejan vía Web [1].

[3] Espacio cibernético. Espacio telemático por el que circula la información en las redes. Coloquialmente, suele denominarse "navegar por el ciberespacio" a la acción de consultar Internet [18].

[4] Sistema de software para ordenador que permite organizar y facilitar la creación de documentos y otros contenidos de modo cooperativo. Con frecuencia es una aplicación web usada para gestionar sitios y contenidos web [17].

[5] Sistema de software online que permite administrar, distribuir, monitorear, evaluar y apoyar las diferentes actividades previamente diseñadas y programadas dentro de un proceso de formación completamente virtual o de formación semipresencial [19].

[6] Software de aplicación que controla los datos en una base de datos, incluyendo la organización global, el almacenamiento, la recuperación, la seguridad e integridad de los datos [1].

[7] Objeto de una base de datos que almacena datos como una colección de filas y columnas [1].

[8] Proceso que se utiliza para comprobar que una entidad o un objeto es quien dice ser [1].

[9] Servicio de hospedaje, acción de alojar un documento web en los servidores de internet para difundirlo [1].

de cómo resolverlos existen diversas fuentes que abordan el tema [7], lo inusual son noticias referentes a ataques internos y relacionadas con las personas que poseen un número elevado de privilegios y atiende las bases de datos[10] en las que se soportan los sistemas: el administrador de la base de datos. De acá que el objetivo de este artículo sea dar a conocer las vulnerabilidades presentes en el LMS Moodle y en los CMS: Joomla, Drupal y Wordpress, que pueden ser aprovechadas por estos administradores con la finalidad de causar daños en las personas o en los datos. En el artículo se da una propuesta de solución a esta situación

2- MATERIALES Y MÉTODOS.

Para instalar de forma local los CMS: Joomla, Drupal y Wordpress, así como el LMS Moodle se requiere de un servidor web[11], un intérprete[12] para el lenguaje de script PHP[13] y un SGBD. Para el desarrollo de la investigación se instaló el software XAMPP (disponible en https://www.apachefriends.org/es/index.html), (paquete de instalación gratuito) que consiste principalmente de un SGBD (MySQL o MariaDB), el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl; el nombre proviene del acrónimo de X (para cualquiera de los diferentes sistemas operativos), Apache, MySQL, PHP, Perl [8]. De este software también se utilizó el módulo adicional que instala para la administración de la base de datos: phpMyAdmin.

CMS

Joomla

Joomla es un CMS premiado y reconocido mundialmente, que ayuda a construir sitios web y aplicaciones en línea potentes. Es una solución de código abierto y está disponible libremente para cualquiera que desee utilizarlo. Es software libre distribuido bajo Licencia Pública General GNU [9]. Ha sido un gran éxito desde hace varios años y ahora es popular con millones de usuarios en todo el mundo. Es fácil de instalar, fácil de gestionar y muy confiable [10].

Cuando se instala Joomla hay que llenar algunos campos referentes a la configuración del sistema. Es en este momento donde se le da el nombre a la base de datos que se creará, se escribe el nombre de usuario y contraseña de la misma, así como el prefijo de las tablas que esta contendrá. El nombre de la tabla que almacena los nombres de usuarios y sus contraseñas tiene la siguiente estructura: **prefijodetabla_users**, donde el nombre del campo donde se almacena la contraseña es ***password*** y el nombre del campo donde se almacena el nombre de usuario es ***username*.**

Wordpress

Wordpress es un CMS que se puede utilizar para crear fantásticas webs, blogs o aplicaciones. Se dice que WordPress es, al tiempo, gratis y de un precio incalculable. WordPress lo crean y mantienen cientos de voluntarios de la comunidad y hay miles de plugins[14] y temas disponibles para transformar la web en cualquier cosa que se pueda imaginar [11]. Más de 60 millones de personas han elegido WordPress, existiendo más de 64 millones de sitios basados en este CMS [12]. Es un proyecto de código abierto, desarrollado en PHP y MySQL, bajo Licencia Pública General v2 [13].

[10] Conjunto de información o de datos relacionados que se encuentran agrupados o estructurados, fiables y homogéneos, organizados, independientemente de su utilización e implementación, en una computadora, accesibles en tiempo real [1].

[11] Máquina conectada a la red en la que están almacenadas físicamente las páginas que componen un sitio Web. //Dícese también del programa que sirve dichas páginas [1].

[12] Traductor de un lenguaje de programación, el cual convierte el código fuente de un programa de alto nivel -línea por línea- en enunciados del lenguaje máquina [1].

[13] Lenguaje de programación de código abierto y de distribución gratuita [1].

[14] Pequeño programa que añade funcionalidades a otro programa, habitualmente de mayor tamaño [1].

Cuando se instala Wordpress se introduce información en campos referentes a la configuración de este CMS, acá es donde se escribe el nombre de la base de datos, el nombre de usuario y contraseña de la misma, así como el prefijo de las tablas que esta contendrá. El nombre de la tabla que almacena los nombres de usuarios y sus contraseñas tiene la siguiente estructura: prefijodetabla_users, donde el nombre del campo donde se almacena la contraseña es user_pass y el nombre del campo donde se almacena el nombre de usuario es user_login.

Almacenamiento de las contraseñas de Joomla y Wordpress. **Variantes de suplantación[15].**

Luego de la instalación de las versiones estables de los CMS Joomla y Wordpress: 3.6.0 (de 2016) y 4.5.3 (22 de junio2016) respectivamente, usando MySQL (versión 5.5.25a) como SGBD y phpMyAdmin (versión 3.5.2), se pudo constatar que estos CMS guardan las contraseñas asociadas a los usuarios, en la base de datos usando el algoritmo criptográfico MD5[16]. No guardan la contraseñas en texto claro, sino que le aplican una función *hash*[17] a éstas y el valor resultante es lo que almacenan; protegiéndolas de esta forma por si es comprometida la base de datos por un ataque externo, para que no puedan ser utilizadas por los atacantes.

Conociendo lo anterior, el administrador de la base de datos puede crearse un *password* en texto claro, luego aplicarle el algoritmo MD5 y así obtener el valor *hash* de su nueva contraseña, *hash* que puede suplantar en cualquier campo de contraseña asociado a cualquier usuario de la base de datos que él administra. Con esta acción es capaz de adentrarse en el sitio web o blog que utiliza la base de datos que él administra usando un nombre de usuario real, pero que no le corresponde a él, pudiendo utilizarlo para cometer acciones perjudiciales y así incriminar al verdadero usuario al que corresponde ese perfil. Esta acción la puede repetir ilimitadamente si antes de suplantar o sobreescribir el *password* que existe asociado al usuario (que va a ser víctima) con el nuevo *password* (generado por él) copia en un fichero[18] el *password* existente, para así poder restaurarlo una vez cometa la suplantación y el usuario víctima no se entere, pues al autenticarse la víctima en el sistema lo haría de forma rutinaria y no se enteraría de que su cuenta (asociada a su nombre de usuario) fue utilizado por otra persona que no fue él.

Otra vía para realizar la suplantación de *password* es editar en el phpMyAdmin el usuario al que se quiere victimizar, salvar el *hash* del *password* existente, luego en el campo *password* introducir la nueva contraseña (en textoclaro, que será utilizada para acceder al sistema usando este nombre de usuario) y seleccionar en el *combobox*[19] *¨password¨* el tipo de dato[20] (en este caso MD5), para que así quede guardada en el nuevo tipo. Otra variante es copiar el *hash* del *password* asociado a un usuario del que se conoce la contraseña en texto claro y sobrescribirlo en el campo del *password* del usuario que va a ser víctima. Luego de aplicar alguna de las variantes anteriores solo resta autenticarse en el sitio web o blog utilizando el nombre de usuario de la víctima y el *password* que se generó y se suplantó por la contraseña original de la víctima. A continuación se describe una de las variantes con un ejemplo real.

Ejemplo:

Nombre de usuario (que será víctima) en la base de datos: *ale2*

Hash del *password* del usuario ale2 existente en la base de datos:

---

[15] Sustituir una cosa por otra, especialmente de forma fraudulenta [20].

[16] Esquema de hash unívoco de 128 bits. Un esquema de hash es un método para transformar los datos, por ejemplo, una contraseña, de manera que el resultado sea único y no se pueda devolver a su forma original [1].

[17] Función computable mediante un algoritmo que tiene como entrada un conjunto de elementos, que suelen ser cadenas y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija [1].

[18] Unidad significativa de información que puede ser manipulada por el sistema operativo de una computadora. Ejemplo: contraseña.txt [1].

[19] Cuadro de lista descendente. En una interfaz gráfica de usuario, elemento de un cuadro de diálogo que ayuda al usuario a escoger un ítem desde una lista de posibles alternativas [1].

[20] Especifica el rango de valores que puede contener una variable o una constante y se almacena esa información en la memoria de la computadora [1].

$2y$10$Wwgg0KMN/jAcMwYtIKQq5.CcG3fSns8zg57qtER/qDwtoW50F4p3S

Password en texto claro al que se le aplicará el algoritmo criptográfico MD5 para suplantar por el *password* de ale2: *Esto sí es una prueba de MD5*

Hash MD5 resultante: *02306f485f385f6ed9ab6626052a633d*

Luego de generar el *hash* MD5 que se suplantará, este se copia en caché[21], entonces hay que autenticarse como administrador en el software desde el que se administra la base de datos (phpMyAdmin, en esta investigación), seleccionar la base de datos en la que se encuentra el usuario que será víctima, seleccionar la tabla de la base de datos en la que se almacenan los nombres de usuarios y sus respectivas contraseñas, en el caso de Joomla y Wordpress: *prefijodtabla_users*, luego doble clic en el campo que almacena el *hash* del *password* del usuario ale2, se borra el *hash* existente y finalmente se pega el *hash* MD5 que se generó. Esto permitirá autenticarse en el sitio o blog con el usuario ale2 y el *password ¨Esto sí es una prueba de MD5¨*.

Drupal

Drupal es un CMS que se utiliza para crear sitios web dinámicos y con gran variedad de funcionalidades. Es un software libre distribuido bajo la Licencia Pública General, escrito en PHP, que cuenta con una amplia y activa comunidad de usuarios y desarrolladores que colaboran conjuntamente en su mejora y ampliación [14]. Esta ampliación es posible gracias a que se trata de un sistema modular con una arquitectura consistente, que permite que los módulos creados por cualquier desarrollador puedan interactuar con el núcleo del sistema y con los módulos creados por otros miembros de la comunidad. Con Drupal es posible implementar una gran variedad de sitios web: un blog personal o profesional, un portal corporativo, una tienda virtual, una red social o comunidad virtual [15].

Cuando se instala Drupal hay que llenar algunos campos referentes a la configuración del sistema. Es en este momento donde se escribe el nombre de la base de datos, el nombre de usuario y contraseña de la misma, así como el prefijo de las tablas que esta contendrá. El nombre de la tabla que almacena los nombres de usuarios y sus respectivos *password*s tiene la siguiente estructura: **users_field_data**, donde el nombre del campo donde se almacena la contraseña es **pass** y el nombre del campo donde se almacena el nombre de usuario es **name.**

Versión 6.20

Al instalar la versión 6.20 del CMS Drupal usando MySQL (versión 5.5.25a) como SGBD y phpMyAdmin (versión 3.5.2) para la administración de la base de datos se pudo comprobar que esta versión del CMS presenta las mismas vulnerabilidades que Joomla y Wordpress (referido a la manera de salvar el *password* asociado a los usuarios en la base de datos), por lo que se aplicaron las mismas variantes de suplantación descritas en la sección anterior y se obtuvieron los mismos resultados.

Versión 7

Al instalar la versión 7 de Drupal usando MySQL (versión 5.5.25a) como SGBD y phpMyAdmin (versión 3.5.2) para la administración de la base de datos, se procedió a ejecutar los mismos procedimientos que se usaron con la versión 6.20, pero en esta ocasión no se lograron los mismos resultados. A partir de esta versión se usa SHA512 como algoritmo criptográfico y no MD5 como en las versiones anteriores para almacenar las contraseñas en la base de datos, por lo que no fue posible suplantar las contraseñas de los usuarios desde el phpMyAdmin puesto que en el *combobox* del tipo de dato asociado al campo *password* no aparece SHA512, solo MD5 y SHA.

Se probó además generar un *password* con SHA512 y sustituirlo en el campo *password* de un usuario seleccionado para ser víctima, lográndose la sustitución del *password*, pero no la utilización del nombre de usuario para cometer actos perjudiciales, ya que al intentar la autenticación con el *password* al que se

[21] Proceso que consiste en almacenar, de forma temporal, los valores de datos utilizados recientemente en un bloque especial de la memoria para agilizar el acceso posterior [1].

le aplicó el SHA512 dio error de inicio de sesión[22]. La variante que se encontró, fue que el administrador de la BD se creara una cuenta (usuario y password) desde el sistema y luego desde la BD que administra asociada a ese sistema, copiar el *hash* de ese *password* generado y suplantarlo por el *hash* existente del usuario víctima, lográndose de esta manera la autenticación en el sistema con la nueva contraseña generada y no con la del verdadero usuario, apropiándose de esta manera nuevamente de un nombre de usuario cualquiera para cometer actos dañinos.

Versión 8.1.8

Luego de la instalación de la versión estable 8.1.8 (del 3 de agosto de 2016) de Drupal usando MariaDB (versión 10.1.9) como SGBD y phpMyAdmin (versión 4.5.1), se efectuaron las mismas pruebas que se realizaron con la versión 7, obteniéndose los mismos resultados. Por lo que a la fecha de publicarse este artículo se mantiene la vulnerabilidad.

LMS

Moodle

Moodle es un sistema gratuito para gestión del aprendizaje en línea también conocido como Entorno Virtual de Aprendizaje (Virtual Learning Environment = VLE, por sus siglas en inglés) [16]. Es apropiado para todas las edades y todos los sectores. Generalmente se usa en-línea, pero también en una computadora sin internet o en una intranet dentro de una organización. Está diseñado para proporcionarles a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados. El número de usuarios de Moodle a nivel mundial es de más de 79 millones de usuarios, entre usuarios académicos y empresariales, convirtiéndose en la plataforma de aprendizaje más ampliamente utilizada del mundo [5].

Cuando se instala Moodle se introduce información en campos referentes a la configuración de este LMS, acá es donde se escribe el nombre de la base de datos, el nombre de usuario y contraseña de la misma, así como el prefijo de las tablas que esta contendrá. El nombre de la tabla que almacena los nombres de usuarios y sus contraseñas tiene la siguiente estructura: **prefijodetabla_users**, donde el nombre del campo donde se almacena la contraseña es ***password*** y el nombre del campo donde se almacena el nombre de usuario es ***username***.

Luego de la instalación de Moodle 3.1.1 (versión liberada el 11 Julio de 2016) usando MySQL (versión 5.6.16) como SGBD y phpMyAdmin (versión 4.1.12) se pudo constatar que se pueden utilizar las mismas variantes usadas con Joomla y WordPress para lograr el mismo objetivo.

3- RESULTADOS Y DISCUSIÓN

Luego de las pruebas aplicadas a los CMS: Joomla, Wordpress y Drupal y al LMS: Moodle queda demostrado la carencia de un mecanismo por parte de estas tecnologías para impedir que el administrador de las bases de datos, en las que se soportan estos sistemas pueda realizar la suplantación no autorizada de identidad de un usuario cualquiera. Estas acciones tienen graves consecuencias, por ejemplo, se pueden victimizar periodistas de renombre, ya que al apropiarse de su nombre de usuario se pueden escribir comentarios ofensivos respecto a cualquier tema, manchando así la imagen de esta persona y creando grandes conflictos intelectuales, políticos y morales; pues esta persona no tiene forma de demostrar que no ha sido la que ha publicado ese tema, pues a su verdadero nombre está asociado ese nombre de usuario, al que aparece asociado ese comentario o *post*.

En el caso de Moodle siempre existe la competencia entre estudiantes. Un alumno pudiera sobornar al administrador de la base de datos para obtener un *password* (válido por un corto tiempo, pues luego el administrador restauraría el original) asociado al nombre de usuario de su compañero rival y apropiarse así del perfil del mismo, entonces podría mandar trabajos de baja puntuación para desacreditarlo y poder tener mejores notas, ganándose una beca o un puesto de trabajo que en realidad no le pertenecía, por ejemplo.

[22] Espacio de trabajo que se abre en una computadora o sistema donde determinado usuario realiza su trabajo [1].

En las pruebas realizadas se demostró además que el usuario víctima no posee ningún sistema de alerta para darse cuenta de que su cuenta fue utilizada por una persona que no fue él, solamente el LMS: Moodle posee registros de la actividad de autenticación dando como datos la fecha y la hora de la primera y la última vez que se accedió al sitio, así como la dirección IP y la acción realizada. Si el usuario de Moodle tiene como costumbre revisar esta sección podría darse cuenta de que alguien accedió desde su sesión, pero si es olvidadizo o sencillamente no revisa esta sección, no se dará por enterado de que su cuenta fue usada por otra persona no autorizada.

4- CONCLUSIONES

Los CMS: Joomla, Wordpress y Drupal y el LMS: Moodle necesitan de un SGBD para su funcionamiento en general, lo que incluye el uso de una base de datos conformada por tablas, que entre otras informaciones almacenan datos de los usuarios que tendrán acceso al sistema e información necesaria para su autenticación. Estas bases de datos son administradas por personas con un alto nivel de privilegios, que pueden realizar la suplantación no autorizada de identidad de un usuario cualquiera existente en la base de datos que administren. En el artículo se ejemplificaron además las acciones perjudiciales que pueden llevar a cabo estos administradores de bases de datos al explotar las vulnerabilidades presentes en estas tecnologías y las posibles variantes que pueden emplear para lograr con éxito las suplantaciones de identidad.

Está claro que los administradores de bases de datos por lo general son personas serias y responsables, que no deben verse involucradas en acciones como las descritas, pero a fin de cuentas son seres humanos que pueden ser sobornados, amenazados, extorsionados, etc. Si se contrata un servicio de *hosting* para algún sitio que se basa en estos CMS o LMS, hay que tener en cuenta que los administradores por lo general pertenecen a empresas foráneas y responden a los intereses de estas, por lo que no son confiables. Existen casos de personas altamente confiables que han dado al traste con este tema, como es el caso del reconocido administrador de sistemas Edward Snowden, por lo que no es conveniente que un administrador tenga tales privilegios. Además es injusto que los usuarios no se enteren de que es lo que ha sucedido con su cuenta o perfil al ser usada por una persona ajena, se viola de esta manera la privacidad de los datos de esta persona así como la integridad de los mismos.

Se denuncia en el artículo la existencia de un problema de seguridad y se dan muestras de la magnitud del mismo. De esta manera se alerta a los usuarios y desarrolladores de estas tecnologías para que trabajen de conjunto en la búsqueda de una solución. Los autores del artículo proponen el desarrollo de un *plugin* para cada una de estas tecnologías como una posible solución a los problemas antes descritos. Se analizaron varios de estos pequeños programas pero ninguno logra resolver la situación y los que pudieran ayudar de alguna forma son de pago.

5- REFERENCIAS BIBLIOGRÁFICAS

1. NÚÑEZ CAMALLEA, Noel Luis; COUTIN ABALO, Ronald**.** *Diccionario de Informática.* La Habana : Editorial Científico-Técnica, 2005. ISBN 959-05-0391-8.

2. AUTORES, Colectivo de. *¿Qué es un CMS y qué ventajas tiene?* [en línea]. Internetya Soluciones Web [ref. de 6 de Septiembre de 2016]. Disponible en Web: http://www.internetya.co/que-es-un-cms-y-que-ventajas-tiene/.

3. AUTORES, Colectivo de. *2016 Best Content Management System Software Review* [en línea]. TopTenReviews [ref. de 6 de Septiembre de 2016]. Disponible en Web: http://www.toptenreviews.com/business/internet/best-content-management-system-software/.

4. AUTORES, Colectivo de. *Sistemas de Gestión de Aprendizaje(LMS) y GROUPWARE* [en línea] [ref. de 6 de Septiembre de 2016]. Disponible en Web: http://sistemadegestiondeaprendizaje.blogspot.com/p/ventajas.html.

5. AUTORES, Colectivo de. Moodle. *Acerca de Moodle*[en línea] [ref. de 5 de Septiembre de 2016]. Disponible en web: https://docs.moodle.org/all/es/Acerca_de_Moodle.

6. AUTORES, Colectivo de. *Cómo los Sitios Web Son Hackeados y Cuál Malware Se Usa* [en línea]. Informe de Sitios Web Hackeados (2016 / T1) [ref. de 6 de Septiembre de 2016]. Disponible en Web: https://sucuri.net.

7. VERIZON**.** *Informe sobre investigaciones de brechas en los datos de 2014* [en línea] [ref. de 6 de Septiembre de 2016.] Disponible en Web: https://www.verizon.com.

8. APACHE, Friends**.** *XAMPP Apache + MariaDB + PHP + Perl* [en línea] [ref. de 5 de Septiembre de 2016]. Disponible en Web: https://www.apachefriends.org/es/about.html.

9. AUTORES, Colectivo de**.** *Joomla!* [en línea] [ref. de 5 de Septiembre de 2016]. Disponible en Web: https://www.joomla.org/about-joomla.html.

10. GRAF, Hagen**.** *Joomla! 3 en 10 sencillos pasos.* s.l. : Cocoate, 2012.

11. AUTORES, Colectivo de. *WordPress.ORG Español* [en línea] [ref. de 5 de Septiembre de 2016]. Disponible en web: https://es.wordpress.org/.

12. AUTORES, Colectivo de. *Wordpress.com* [en línea] [ref. de 6 de Septiembre de 2016]. Disponible en Web: https://www.wordpress.com.

13. AUTORES, Colectivo de. *About WordPress* [en línea]. WordPress.ORG [ref. de 5 de 2016 de 2016]. Disponible en Web: https://wordpress.org/about/.

14. BUITRAGO, Jorge**.** *¿Qué es Drupal? ¿Para qué se usa?* [en línea] [ref. de 5 de Septiembre de 2016]. Disponible en Web: https://groups.drupal.org/node/148379 .

15. DRUPAL, Colectivo de Drupal. *About Drupal* [en línea] [ref. de 5 de Septiembre de 2016]. Disponible en Web: https://www.drupal.org/about.

16. AUTORES, Colectivo de. Moodle. *Acerca de Moodle-FAQ* [en línea] [ref. de 5 de Septiembre de 2016]. Disponible en Web: https://docs.moodle.org/all/es/Acerca_de_Moodle_FAQ.

17. WHITE, Steve**.** *Joomla! User Manual.* [Documento(pdf)] s.l. : Joomla! Spanish, 2006.

18. AMOROSO FERNÁNDEZ, Yarina. *Diccionario Ilustrado y Comentado de Criminalidad Tecnológica .* La Habana : s.n., 2005.

19. CAÑELLAS MAYOR, Alicia. *LMS y LCMS: Funcionalidades y beneficios* [en línea] [ref. de 5 de Septiembre de 2016]. Disponible en Web: http://www.centrocp.com/lms-y-lcms-funcionalidades-y-beneficios/.

20. PAZ ARIAS, Battaner. *Diccionario de uso del español de América y España.* Aribau. Editorial SPES, 2003. ISBN: 84-8332-483-0.

21. BARREIRO, Andrea. *¿Qué es el hosting web y para qué sirve*? [en línea] [ref. de 20 de Septiembre de 2016]. Disponible en Web: https://www.hosteurope.es/blog/que-es-el-hosting-web-y-para-que-sirve/.