Bases de datos y sus vulnerabilidades más comunes

El mundo de la informática es vulnerable de sufrir algún tipo de ataque por terceras personas, con la intención de propagar algún tipo de malware o robar información importante de la víctima. Por todo esto, es fundamental tomar las medidas que sean necesarias para mantener a buen recaudo la información. Dentro de todo esto, las bases de datos son uno de los sistemas que más sufren este tipo de ataques, en gran medida a que es ahí donde en la mayoría de las ocasiones está almacenada la información. Para acceder a ella, los hackers buscan cualquier tipo de vulnerabilidad que no haya sido controlada para acceder al sistema y hacerse con aquello que les sea de interés.

A lo largo de este White Paper indagaremos sobre algunas de las vulnerabilidades más comunes que nos podemos encontrar en las bases de datos y que en muchos casos son la fuente de todos los problemas de seguridad.

La seguridad en las bases de datos

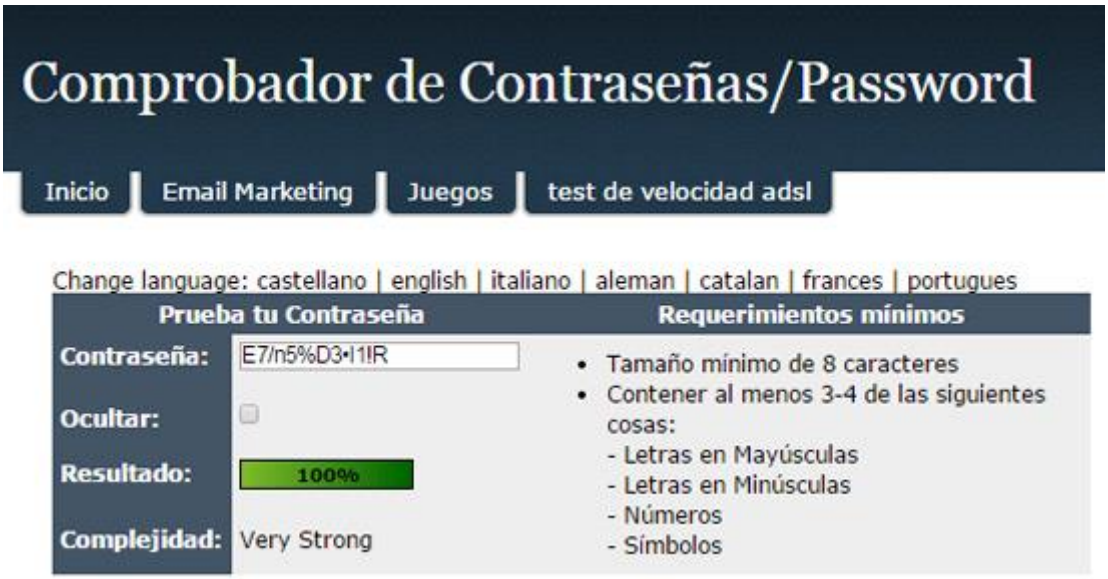
La mayoría de información sensible del mundo está almacenada en sistemas gestores de bases de datos como MySQL, Oracle, Microsoft SQL Server entre otros. Toda esa información es la que hace que los hackers centren todo su esfuerzo en poder acceder a esa información por medio de alguna de las muchas vulnerabilidades que nos podemos encontrar referente a estos gestores, vulnerabilidades que o bien pueden ser debidos a problemas de seguridad en el software, en este caso es necesario tener siempre actualizada a la última versión para corregir posibles problemas de seguridad, y otras veces a la forma en la que está configurado su acceso o bien problemas en la programación de la aplicación, problemas que pueden causar el conocido ataque SQL Injection, uno de los ataques más comunes cuando de bases de datos se trata.

Hasta este momento, gran parte del esfuerzo para mejorar la seguridad de cualquier servicio informático se centraba en asegurar los perímetros de las redes por medio de firewalls, IDS / IPS y antivirus, pero cada vez las organizaciones están poniendo más esfuerzos en la protección de la seguridad de las bases de datos protegiéndolos de intrusiones y cambios no autorizados.

Vulnerabilidades más comunes en bases de datos

A continuación repasaremos cuales son las vulnerabilidades más habituales que nos podemos encontrar a la hora de trabajar con bases de datos.

1.- Nombre de usuario/password en blanco o bien hacer uso de uno débil
Hoy en día no es raro encontrarnos pares de datos usuario/password del tipo admin/12345 o similar. Esta es la primera línea de defensa de entrada a nuestra información y debemos optar por el uso de algo más complejo que sea complicado de conseguir por parte de cualquier atacante.



A la hora de generar una contraseña para un usuario que estemos creando es recomendable usar tanto letras como números, así como de caracteres especiales tipo ¡, ¿, %... y con una longitud superior a 8 caracteres. De esta forma nos estamos asegurando de que la contraseña sea lo suficientemente fuerte para que no pueda ser adivinada por ningún proceso automático. En esta entrada de nuestro blog podéis ver consejos para crear una contraseña segura.

2. Preferencia de privilegios de usuario por privilegios de grupo
En ocasiones muchos usuarios reciben más privilegios sobre la base de datos de los que realmente necesitan, lo que a la larga se puede convertir en un importante problema. Es recomendable modificar los privilegios otorgados a los usuarios que estarán en contacto con la información con el fin de que no puedan realizar modificaciones más allá de las autorizadas.

Si por ejemplo un usuario sólo realizará consultas a la base de datos pero no podrá modificar ningún registro ni insertar nada nuevo, no tiene sentido que le ofrezcamos esos privilegios, ya que lo que estamos haciendo es abrir una puerta para un eventual ataque.

3. Características de bases de datos innecesariamente habilitadas
Cada instalación de base de datos viene con una serie de paquetes o módulos adicionales de distintas formas y tamaños que en muy pocas ocasiones todos ellos son utilizadas por las compañías, lo que las convierten en una posible puerta de entrada para sufrir algún tipo de ataque si en esos paquetes se descubre cualquier problema de seguridad. Para reducir riesgos, es recomendable que los usuarios detecten esos paquetes que no se utilizan y se desactiven del servidor donde estén instalados. Esto no sólo reduce los riesgos de ataques, sino que también simplifica la gestión de parches ya que únicamente será de máxima urgencia actualizar aquellos que hagan referencia a un módulo que estemos utilizando.

4.- Desbordamiento de búfer
Se trata de otro de los medios favoritos utilizados por los piratas y que se dan por el exceso de información que se puede llegar a enviar por medio del ingreso de información mediante el uso de formularios, es decir, se recibe mucha más información de lo que la aplicación espera. Por poner un ejemplo, si se espera la entrada de una cuenta bancaria que puede ocupar unos 25 caracteres y se permite la entrada de muchos más caracteres desde ese campo, se podría dar este problema.

5.- Bases de datos sin actualizar
Como ocurre con cualquier tipo de aplicación que tengamos instalada en nuestra máquina, es necesario ir actualizando la versión de nuestra base de datos con las últimas versiones lanzadas al mercado, ya que en ellas se solucionan aquellos problemas de seguridad detectados, por lo que pondremos más barreras a los posibles atacantes.

Para ello es muy importante estar informados de todos las noticias relacionadas con la base de datos que estemos utilizando para saber en todo momento si algo nuevo ha sido lanzado al mercado que pueda solucionar cualquier brecha de seguridad.

6.- Datos sensibles sin cifrar
Aunque pueda ser algo obvio, a la hora de la verdad no todo el mundo cifra la información más importante que se almacena en base de datos. Esto es una buena práctica para que en caso de hackeo, sea complicado para el atacante poder recuperar esa información.

Por poner un ejemplo, las contraseñas de acceso a un sitio por parte de los usuarios podrían ser cifradas utilizando el algoritmo MD5. De esta forma una contraseña del tipo “YUghd73j%” en base de datos se almacenaría con el siguiente valor “993e65b24451e0241617d6810849c824”. Como podéis ver, se trata de un valor que poco o nada tiene que ver con el original.

7. Inyecciones SQL
Un ataque de este tipo puede dar acceso a alguien a una base de datos completa sin ningún tipo de restricción, pudiendo llegar incluso a copiar y modificar los datos.

El funcionamiento de este tipo de vulnerabilidades es similar al que puede ocurrir en los portales web, donde una mala limpieza de los datos de entrada puede hace que ejecuten código no deseado en la base de datos, pudiendo coger el control de la plataforma. Muchos proveedores ofrecen soluciones para este

tipo de situaciones, pero para que surjan efecto es necesario realizar la actualización de la aplicación a la última versión estable disponible que exista en cada momento.

Recomendaciones para proteger una base de datos

A continuación veremos algunas interesantes recomendaciones a tener en cuenta para proteger nuestras bases de datos de posibles vulnerabilidades.

1.- Identificar su sensibilidad
Una cosa hay que tener claro, y es que no se puede asegurar aquello que no se conoce. Con esto queremos decir que es importante conocer la sensibilidad de nuestro sistema de bases de datos para saber cómo actuar y mejorar de esta forma su seguridad. Para ello podemos hacer uso de herramientas de identificación que nos ayuden a encontrar posibles agujeros por donde podríamos ser atacados.

2.- Evaluación de las vulnerabilidades y la configuración
Evalúe la configuración de tu base de datos para descartar posibles agujeros de seguridad. Esto incluye la verificación de la forma en la que ésta fue instalada y la de tu sistema operativo. Por ejemplo podríamos verificar los privilegios de los distintos grupos de usuarios respecto a las acciones de ejecutar, leer y escribir en bases de datos.

3.- Audita
Una vez que hayamos creado una configuración que creamos que puede ser totalmente segura, realicemos actividades de auditoría para asegurarnos que no te desvías de tu objetivo. Por ejemplo, se podría poner algún tipo de alarma para que nos avisara de cualquier cambio que se pudiera dar en dicha configuración.

4.- Monitoriza toda acción relacionada con la base de datos
Monitorizar la actividad que se lleva a cabo en nuestra base de datos nos puede dar algún tipo de pista en caso de estar siendo utilizada de forma indebida o para la detección de intrusos.

5.- Control de acceso y gestión de derechos
No todos los datos son igual de importantes y no todos los usuarios son creados igual. Es necesario establecer una jerarquía y garantizar que cada tipo de usuario sólo pueda realizar las acciones que se le permiten en la base de datos, para garantizar de esa forma la integridad de la información.

En el caso de los datos confidenciales, como pueden ser todo tipo de contraseñas, es recomendable utilizar algún tipo de cifrado de datos para que la información no sea legible a simple vista.

En este White Paper hemos visto las principales vulnerabilidades que nos podemos encontrar sobre las bases de datos, vulnerabilidades que nos pueden dar más de un quebradero de cabeza si no tomamos las medidas necesarias para paliarlas.