¿Mi Sitio Web Esta Preparado Para Cualquier Ataque De Hackers?

La cuestión de la **seguridad del sitio web** ha sido una prioridad para los diseñadores y desarrolladores web durante mucho tiempo. Prevenir los métodos de ataques en los sitios web se ha transformado en toda una profesión, gracias al abanico de **posibilidades que existen para atacar un sitio web**. No solo las grandes bases de datos bancarios son el blanco ideal para el hacker, también existen las diversas bases de datos que pueden ser extraídas de grandes sitios web, como foros o comunidades, y esto es tan solo ejemplo de lo que se podrían lograr los hackers con sus ataques. En este punto de seguro te preguntarás: ¿**Mi Sitio Web Esta Preparado** Para Cualquier Ataque De Hackers?

Cualquier sitio web, llamese **blog, sitio de noticias, foro, tienda virtual ó una pagina web corporativa**, pueden y seguramente serán atacadas por un hacker. Ahora, como un diseñador ó desarrollador de paginas web, tienen la tarea de no sólo crear páginas web llamativas visualmente, sino también, mantenerlas protegidas los atacantes que deseen extraer información ó simplemente hacer alguna maldad.

Existen una cantidad de **formas para hackear un sitio web**. Por esto, muchas medidas se deben implementar para prevenir estas desafortunadas situaciones. Sin embargo, no hay ningún método infalible de prevenir y erradicar las intrusiones de piratas informáticos. En este artículo, conocerá las medidas que podría tomar para hacer que su sitio web este preparado para los posibles ataques conocidos.

Métodos comunes de Hacking

Como se ha mencionado, son diversos los métodos que un atacante puede usar para atacar un sitio web. Por este motivo, le explicaremos los métodos mas comunes que usan los atacantes, y por supuesto, sus respectivas medidas para evitar dicha intrusión.

Inyección SQL

El ataque de inyección SQL, es sin duda uno de los ataques mas graves para un sitio ó aplicación web. Este ataque va dirigido a campos de consulta ó ingreso de datos, incluso, podria llegar a ser usado directamente en el cuadro de la URL del navegador. Un ataque de este tipo, puede dar acceso a información de la base de datos al intruso.

Los ataques de **inyección SQL** se producen cuando un hacker intenta pegar comandos SQL en sus campos de la página web. En el caso de que un dato contenga una comilla simple (‘) al final de un nombre de usuario, su base de datos podría ver esto como una consulta SQL construida. Debido a esto, se podría **recibir datos de una consulta SQL**.

Los hackers no pueden entrar a su sitio web utilizando esta

consulta, pero el método les permitirá tener **acceso a su nombre de base de datos, tablas y campos claves**. A partir de estos datos, el hacker puede utilizar la información que tiene que usar comandos SQL en los otros campos de su sitio web. Con este método, recogerán los datos necesarios para usar en una intrusión.

¿Cómo Defender Mi Web Contra El SQL injection?

- Asegurarnos en el manejo de tipos de datos correctos.
- Consultas parametrizadas
- Permisos para las consultas
- Considere el uso de un ORM

En un anterior articulo, dimos algunos consejos de como manejar la información sensible de las bases de datos ;)

Cross Site Scripting (XSS)

Este ataque es comúnmente conocido como XSS, Cross Site Scripting es uno de los hacks más difíciles de tratar. En los últimos años, Microsoft, MySpace y Google han tenido dificultades para hacer frente a dichos casos. Este ataque roba las sesiones que cree un usuario al momento de loguearse, por ende, puede tomar toda la información personal de dicho usuario.

Este tipo de ataques esta oculto en la ventanas emergentes que pueden aparecer en los sitios web, con estas ventanas se pretenden atrapar al usuario mientras se muestra un mensaje como el de una chica sexy invitando a tener una conversación privada, por ejemplo. Al momento de caer el usuario, se vera en la URL de navegación algo como lo siguiente:

[html]%63%61%74%69%6f%6e%3d%274%74%70%3a%2f%2f%77%7…[/html]

En algún momento, puede pensar que no ha pasado nada. Estos enlaces pueden ayudar a robar cookies de sesión (suena como usted está siendo intimidado), posiblemente, puede conducir al robo de su información personal.

¿Cómo evito que este hack suceda?

- Nunca ingrese datos personales en lugares sospechosos.
- Desconfie de las ventanas emergentes.
- Evita el ingreso de datos en funciones Javascript que sean dudosas.

Autorización Bypass

Este ataque es sencillo y bastante fácil de usar. Trabaja de la siguiente manera:

- Ver el código fuente del sitio web.
- Copiar el código en el bloc de notas.
- Eliminar la autorización JavaScript y cambiar algunos enlaces.
- Guardar el archivo del bloc de notas.
- Abrir el archivo en el navegador, iniciar sesión y pulsar Enter.
- Voila. Ya tienes acceso!

Cómo determinar si mi sitio web es vulnerable?

- ¿Los procesos de su servidor se ejecutan en la raíz, administrador, sistema local o en otras cuentas privilegiadas?

- ¿Tiene acceso su aplicación web a la base de datos a través de SA o de otras cuentas?
- ¿Su aplicación tiene la capacidad de acceder a la base de datos a través de las cuentas con más privilegios?
- ¿Las máquinas virtuales del servidor de aplicaciones se ejecutan con AllPermission o FullTrust en J2EE y. Entornos de red?
- ¿Se puede limitar el acceso a los recursos web utilizando capacidades de la plataforma?

Si alguna de las anteriores es afirmativa, entonces, su sitio web podría ser vulnerable.

¿Cómo puedo proteger a mi sitio web?

- Los entornos de desarrollo siempre tienen que usar los permisos mas bajos posibles.
- Asegúrese de usar cuentas creadas con permisos limitados para las consultas que se desean realizar.
- Limite sus cuentas de usuario de suficientes privilegios correspondientes a sus tareas.

Los siguiente enlaces mostraran información complementaria para este ataque:

- CMS Wire
- Defencly
- HackyShacky

Medidas De Seguridad Comunes Para Evitar Ataques

Mantenga Siempre Sus Plugins Y Software Actualizados

Un plugin desactualizado, es una puerta de entrada para los ataques, ya que los atacantes aprovechan los fallos de seguridad en el código del software ó complementos que todavía no han sido desactualizados. Anteriormente se ha visto esto, solo tienes que estas pendiente de las actualizaciones y así evitar intrusiones por un descuido tuyo.

Use Contraseñas Seguras

El uso de contraseñas seguras es muy importante. No puede tener una idea acerca de esto, pero los hackers están continuamente tratando de romper o robar sus contraseñas . Así que, ¿cómo elaboramos una contraseña bastante fuerte?

Método Salt

El método Salt es una gran manera de mantener su contraseña segura. De acuerdo con el principio, debería reemplazar letras o números en caracteres especiales de acuerdo a su propia regla. Ponemos esto como un ejemplo.

- Reemplace todas las ‘a’ con @
- Reemplace todas las ‘s’ con $
- Reemplace cualquier espacio con %
- Reemplace cualquier ‘o’ con 0
- Reemplace cualquier ‘i’ con !

Así que con esto, podemos hacer nuestra contraseña pase de ‘whoisjohngalt’ a esto ‘wh0!$j0hngalt’.

Método de Business Insider

Business Insider publicó recientemente un método para crear contraseñas seguras que pueden ser muy fáciles de recordar. Según la revista, debe hacer una contraseña más larga, ya que los ordenadores llevaran mas tiempo para adivinarla.

El principio básico de este método, es usar una palabra larga, conformada por palabras que no tengan que ver directamente con usted.

Usar Las Herramientas Para Webmasters De Google

Google provee un grupo de herramientas para los administradores de sitios web, entre estas herramientas, podemos encontrar una que nos notificara sobre contenido malicioso en nuestro sitio web. En caso de que no pueda eliminarlos y seas hackeado, Google le ayudará a poner en lista negra dicho elemento de la web. Esto le proporciona tiempo para deshacerse del malware más rápido. El servicio también incluye los detalles del problema que Google está detectando.

No Mostrar El Número De Versión De WordPress

Ademas de la plataforma que administra el contenido de su sitio web, debe evitar que se conozca la versión de esta. Hacer esto evitará que puedan explotar los fallos de seguridad en su sitio. Se puede quitar el número de versión de WordPress editando el archivo functions.php de tu sitio, para esto agregamos el siguiente código:

[php]

```
function wpbeginner_remove_version() {
return »;
}
add_filter(‘the_generator’, ‘wpbeginner_remove_version’);
```

[/php]

Cambiar El Valor De register_globals A register_globals=off

Este parámetro de configuración es bastante peligroso, ya que al tenerlo activado, estamos permitiendo que se puedan crear variables globales en e servidor y posteriormente, puedan ser usadas para realizar algún ataque. Esta modificación debemos de realizarla desde el php.ini.

Mejora La Seguridad Del .htaccess

Normalmente, el valor predeterminado del .htaccess es abierto y sin ninguna restricción. Sin embargo, podemos configurarlo al punto de evitar ataques por inyeccion SQL, ataques por URL y otros mas. Hay un montón de maneras de modificar su htaccess, pero vamos a nombrar las más útiles (como siempre, recuerde hacer copia de seguridad).:

[text]

RewriteEngine On

RewriteBase /

RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK) [NC]RewriteRule ^(.*)$ – [F,L]RewriteCond %{QUERY_STRING} \.\.\/ [NC,OR]RewriteCond %{QUERY_STRING} boot\.ini [NC,OR]RewriteCond %{QUERY_STRING} tag\= [NC,OR]RewriteCond %{QUERY_STRING} ftp\: [NC,OR]RewriteCond %{QUERY_STRING} http\: [NC,OR]RewriteCond %{QUERY_STRING} https\:

```
[NC,OR]RewriteCond %{QUERY_STRING} (\|%3E) [NC,OR]RewriteCond
%{QUERY_STRING}      mosConfig_[a-zA-Z_]{1,21}(=|%3D)
[NC,OR]RewriteCond  %{QUERY_STRING}  base64_encode.*\(.*\)
[NC,OR]RewriteCond                    %{QUERY_STRING}
^.*(\[|\]|\(|\)||ê|&quot;|;|\?|\*|=$).*   [NC,OR]RewriteCond
%{QUERY_STRING}    ^.*(&quot;|'|&amp;lt;|&amp;gt;|\|{||).*
[NC,OR]RewriteCond  %{QUERY_STRING}  ^.*(%24&amp;amp;x).*
[NC,OR]RewriteCond                    %{QUERY_STRING}
^.*(%0|%A|%B|%C|%D|%E|%F|127\.0).*    [NC,OR]RewriteCond
%{QUERY_STRING}    ^.*(globals|encode|localhost|loopback).*
[NC,OR]RewriteCond                    %{QUERY_STRING}
^.*(request|select|insert|union|declare).*   [NC]RewriteCond
%{HTTP_COOKIE} !^.*wordpress_logged_in_.*$

RewriteRule ^(.*)$ – [F,L]

[/text]
```

Finalmente

Sin duda alguna, el no prevenir ataques en nuestros sitios web, nos da la inseguridad propia para no poder dormir bien. Es por esto, que el poner en practica los anteriores consejos, nos hará ser capaces de relajarnos y pensar en como mejorar nuestro sitio, no en la seguridad, sino en el contenido u otras características ;) Deseas compartir algo mas con respecto a este tema? Déjalo en un comentario :)