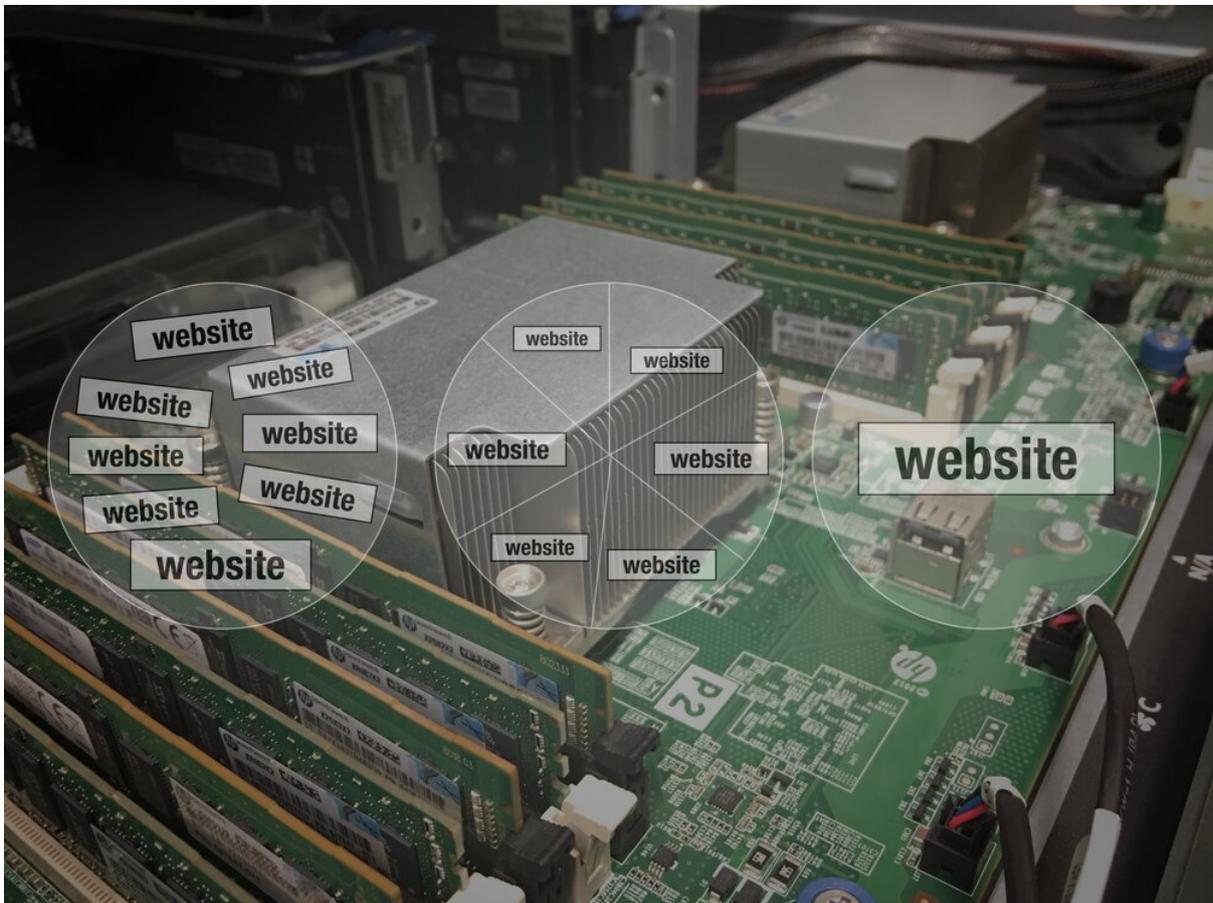


Comprensión de las preocupaciones de seguridad en el alojamiento compartido

Considerando los puertos abiertos y los servicios de red no utilizados

Willem L. Middelkoop

Feb. 28, 2019



Me pagan por hackear, con la condición de que explique cómo lo hice, para que se puedan prevenir futuros ataques. Como consultor de seguridad, busco vulnerabilidades en las aplicaciones, tiendas online y sitios web de mis clientes. Muy a menudo, un ataque comienza explotando una brecha de seguridad visible de forma remota. Sigue leyendo para aprender cómo los hackers encuentran las brechas de seguridad y qué puedes hacer para protegerlas.

Para hackear una aplicación, tienda web o sitio web, los hackers a menudo se dirigen a los servidores que la alojan. Para explicar por qué los hackers hacen esto, primero tienes que entender qué es el alojamiento y qué tipos de alojamiento existen.

¿Qué es el alojamiento?

El alojamiento es un servicio que te permite tener tu aplicación, tienda web o sitio web disponible en internet. El alojamiento se realiza utilizando ordenadores especiales llamados servidores. Cuando alguien escribe la dirección de tu sitio web en su navegador, su dispositivo se conectará a tu servidor.

Si los hackers pueden tomar el control de un servidor, pueden acceder y manipular toda la información que se encuentra en él. Además, pueden abusar de la red y la capacidad computacional del servidor para hacer cosas malas. Realmente no quieres esto...

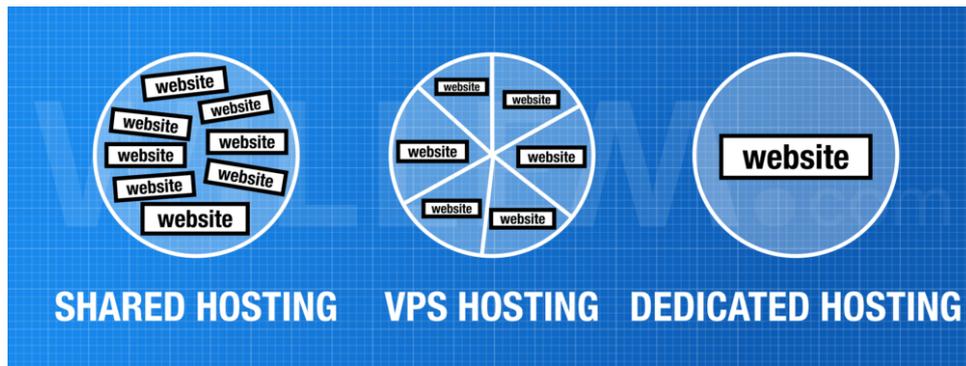


Un servidor típico en el centro de datos, una máquina física que puede alojar aplicaciones, tiendas online y sitios web

Diferentes tipos de alojamiento

Tu aplicación, tienda web o sitio web se puede alojar de diferentes maneras. Cada tipo de alojamiento tiene diferentes preocupaciones de seguridad, pero es relativamente fácil de entender, ya que todo se reduce a cómo se comparte el servidor físico (en el centro de datos) entre los sitios web.

Las empresas de alojamiento web suelen operar múltiples servidores y dividen su capacidad entre el número de sitios web que necesitan alojamiento. Un servidor grande puede alojar fácilmente múltiples sitios web, todo dependiendo de la cantidad de tráfico que tenga la aplicación, tienda web o sitio web.



Diferentes tipos de alojamiento: Alojamiento compartido, alojamiento VPS y alojamiento dedicado visualizados (un círculo que representa un servidor físico)

Hay tres tipos diferentes de alojamiento:

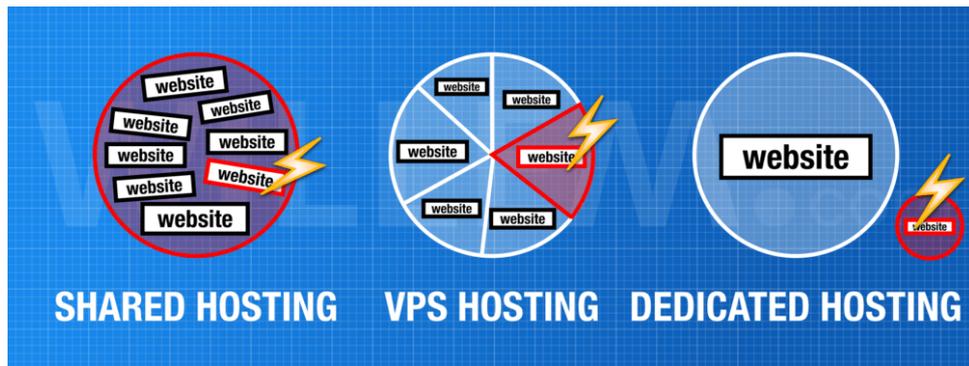
- **alojamiento compartido:** El servidor ejecuta múltiples sitios web compartiendo el sistema operativo, la memoria, los núcleos del procesador y el almacenamiento en disco duro. No hay divisiones rígidas entre los sitios web.
- **alojamiento VPS:** El servidor físico ejecuta múltiples servidores privados virtuales (VPS) que tienen su propio sistema operativo y su propia parte de memoria, capacidad del procesador y almacenamiento. Un solo VPS se puede configurar para ejecutar uno o un par de sitios web (relacionados). Debido a la división rígida entre las instancias de VPS, es muy difícil para los hackers pasar de un VPS a otro.
- **alojamiento dedicado:** El servidor físico ejecuta solo un sitio web. No se comparte nada, todos los recursos están dedicados a una aplicación, tienda web o sitio web. Debido a esta división física, no te verás afectado por los hacks de ningún otro sitio web.

Advertencia: "Alojamiento en la nube" a menudo es alojamiento compartido renombrado

Es importante entender que la mayoría del "Alojamiento en la nube" moderno es en realidad *alojamiento compartido* con un nombre elegante. Las agencias de diseño web a menudo configuran su servidor dedicado o privado virtual para vender alojamiento compartido a sus clientes. Por lo tanto, a menos que operes tu propio VPS o servidor dedicado, es probable que estés en un alojamiento compartido.

Preocupaciones de seguridad para el alojamiento compartido

Los riesgos de seguridad del alojamiento compartido provienen de su base de intercambio. Cuando uno de los sitios web en el mismo servidor que el tuyo es hackeado, hay una alta probabilidad de que tu sitio web también se vea afectado. En esta situación, las medidas de seguridad aplicadas a tu propio sitio web podrían no ser suficientes para protegerlo contra los hackers.



Efecto contagioso de un sitio web pirateado (rojo indica problemas)

Dirección IP compartida

Además, con el alojamiento compartido, generalmente significa que todos los sitios web comparten la misma dirección IP. Tendrás problemas si algún otro sitio web está involucrado en malas prácticas, como el envío de correos electrónicos no deseados o el alojamiento de contenido ilegal. Esto podría causar que tu sitio web sea incluido en la lista negra, bloqueado o degradado en las clasificaciones de los motores de búsqueda.

Rendimiento

Si consideras que las empresas de alojamiento suelen poner centenas, a veces incluso miles (!), de sitios web en el mismo servidor compartido, comprenderás por qué esto aumenta la posibilidad de ser hackeado. Además de los problemas de seguridad, un servicio de alojamiento compartido también afecta el rendimiento de tu sitio web, ya que tiene que competir con otros sitios web por la misma cantidad limitada de recursos del servidor. Si uno de los otros sitios web experimenta un tráfico extremo, ¡también podría ralentizar tu aplicación, tienda web o sitio web!

Servicios orientados a la red compartidos

Otro problema con el alojamiento compartido es que, por lo general, el servidor tiene muchos servicios orientados a la red habilitados, como un servicio web, de correo, FTP y de base de datos. Estos servicios están disponibles a través de puertos abiertos. Es una mala práctica tener todos los puertos abiertos a todas partes porque expone los servicios que están escuchando en esos puertos a exploits. Los firewalls pueden limitar lo que se permite conectar a un puerto determinado, pero en un entorno de alojamiento compartido, estas restricciones a menudo no son muy estrictas (debido a las muchas cosas diferentes que se alojan en el mismo servidor).

Hackear una aplicación, tienda web o sitio web

Para hackear tu aplicación, tienda web o sitio web, un hacker puede escanear tu servidor de alojamiento en busca de puertos abiertos, identificando los diferentes servicios que se ejecutan en el servidor. El programa unix *nmap* se utiliza a menudo para hacer esto. El hacker se conecta al servicio que escucha en los puertos abiertos para averiguar qué programa es.

```

willem:~$ nmap -A willem.com
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for willem.com (87.253.135.162)
Host is up (0.0049s latency).
rDNS record for 87.253.135.162: web1.lemmid.net
Not shown: 993 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http          nginx
|_ http-server-header: nginx
|_ http-title: Did not follow redirect to https://willem.com/en/
443/tcp    open  ssl/http      nginx
|_ http-server-header: nginx
|_ http-title: Willem Laurentz Middelkoop
|_ Requested resource was https://willem.com/en/
|_ ssl-cert: Subject: commonName=willem.com
|_ Subject Alternative Name: DNS:willem.com, DNS:www.willem.com
|_ Not valid before: 2016-10-18T00:00:00
|_ Not valid after: 2019-10-18T23:59:59
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_   h2
|_   http/1.1
|_   tls-nextprotoneg:
|_     h2
|_   http/1.1
|_   tls-alpn:
|_     h2
|_   http/1.1
|_   tls-nextprotoneg:
|_     h2
|_   http/1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1182.34 seconds
willem:~$

```

Handwritten annotations:
 - "open ports" points to the 80 and 443 ports.
 - "hosting server name" points to "web1.lemmid.net".
 - "webserver software" points to "nginx".
 - "website title" points to "Willem Laurentz Middelkoop".
 - "operating system" points to "OS: Linux".

Usando nmap para escanear un servidor de alojamiento, identificando servicios orientados a la red y puertos abiertos

Esta información se puede utilizar para comprobar si los servicios de red en ejecución tienen alguna debilidad de seguridad conocida. Hay bibliotecas en línea donde se pueden buscar estas debilidades por nombre y versión del software. Encontrar una debilidad conocida es tan fácil como una consulta de Google. Si se encuentra una debilidad existente, el hacker puede utilizarla para obtener acceso al servidor.

Al verificar la dirección IP del servidor de alojamiento, el hacker puede determinar si el servidor se comparte con otras aplicaciones, tiendas web o sitios web. Es posible (utilizando búsquedas inversas de DNS) enumerar todos los sitios web alojados en el mismo servidor. Si bien el tuyo puede estar actualizado y seguro, otros en el mismo servidor pueden ejecutar software obsoleto (con debilidades de seguridad). El software común de sitios web está bien documentado, las versiones anteriores de PHP y WordPress son conocidos por tener serios problemas de seguridad.

WordPress WordPress : List of secur X +

https://www.cvedetails.com/vulnerability-list.php?ve

CVE Details
The ultimate security vulnerability datasource

Log In Register

Switch to https://
Home

Browse :
Vendors
Products
Vulnerabilities By
Date
Vulnerabilities By
Type

Reports :
CVSS Score Report
CVSS Score
Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft
References

Top 50 :
Vendors
Vendor Cves Scores
Products
Product Cves Scores
Versions

Other :
Microsoft Bulletins
Bugtraq Entries
CVE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles

WordPress » WordPress : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 286 Page : 1 (This Page) 2 3 4 5 6

Copy Results Download Results

#	CVE ID	CVE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-1000773	20		Exec Code	2018-09-06	2018-11-14	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
WordPress version 4.9.8 and earlier contains a CWE-20 Input Validation vulnerability in thumbnail processing that can result in remote code execution due to an incomplete fix for CVE-2017-1000600. This attack appears to be exploitable via thumbnail upload by an authenticated user and may require additional plugins in order to be exploited however this has not been confirmed at this time.														
2	CVE-2018-20153	79		XSS	2018-12-14	2019-01-04	3.5	None	Remote	Medium	Single system	None	Partial	None
In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could modify new comments made by users with greater privileges, possibly causing XSS.														
3	CVE-2018-20152	20		Bypass	2018-12-14	2019-01-04	5.0	None	Remote	Low	Not required	None	Partial	None
In WordPress before 4.9.9 and 5.x before 5.0.1, authors could bypass intended restrictions on post types via crafted input.														
4	CVE-2018-20151	200		*Info	2018-12-14	2019-01-04	5.0	None	Remote	Low	Not required	Partial	None	None
In WordPress before 4.9.9 and 5.x before 5.0.1, the user-activation page could be read by a search engine's web crawler if an unusual configuration were chosen. The search engine could then index and display a user's e-mail address and (rarely) the password that was generated by default.														
5	CVE-2018-20150	79		XSS	2018-12-14	2019-01-04	4.3	None	Remote	Medium	Not required	None	Partial	None
In WordPress before 4.9.9 and 5.x before 5.0.1, crafted URLs could trigger XSS for certain use cases involving plugins.														
6	CVE-2018-20149	79		XSS Bypass	2018-12-14	2019-01-04	5.5	None	Remote	Medium	Single system	None	Partial	None
In WordPress before 4.9.9 and 5.x before 5.0.1, when the Apache HTTP Server is used, authors could upload crafted files that bypass intended MIME type restrictions, leading to XSS, as demonstrated by a .jpg file without JPEG data.														
7	CVE-2018-20148	502			2018-12-14	2019-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could conduct PHP object injection attacks via crafted metadata in a wp_getMediaItem XMLRPC call. This is caused by mishandling of serialized data at phar:// URLs in the wp_get_attachment_thumb_file function in wp-includes/post.php.														
8	CVE-2018-20147	284		Bypass	2018-12-14	2019-01-04	5.5	None	Remote	Low	Single system	None	Partial	Partial
In WordPress before 4.9.9 and 5.x before 5.0.1, authors could modify metadata to bypass intended restrictions on deleting files.														
9	CVE-2018-14028	434		Exec Code	2018-08-10	2018-10-10	6.5	None	Remote	Low	Single system	Partial	Partial	Partial

Una vez que un hacker sabe qué software usa tu sitio web, es fácil buscar agujeros de seguridad conocidos usando bases de datos como cvedetails.com

Conclusión

La mejor manera de proteger tu aplicación, tienda web o sitio web es limitar su exposición a exploits tanto como sea posible. Mantener el software de tu sitio web actualizado es fundamental, pero puede que no sea suficiente si tu alojamiento es compartido.

Para evitar que otros hacks afecten a tu aplicación, tienda web o sitio web, deberías considerar alojarla en un servidor físico o virtual dedicado con su propia dirección IP. Luego puedes reforzar la seguridad filtrando los puertos abiertos y cerrando los servicios orientados a la red que no se utilizan.

De esta manera, reduces lo que los expertos en ciberseguridad llaman la "superficie de ataque". Cuanto más pequeña sea, más fácil será defenderla: ¡buena suerte y ten en cuenta que [hay ayuda disponible!](#)



Ten en cuenta que hay ayuda disponible: conozco los servidores y la ciberseguridad