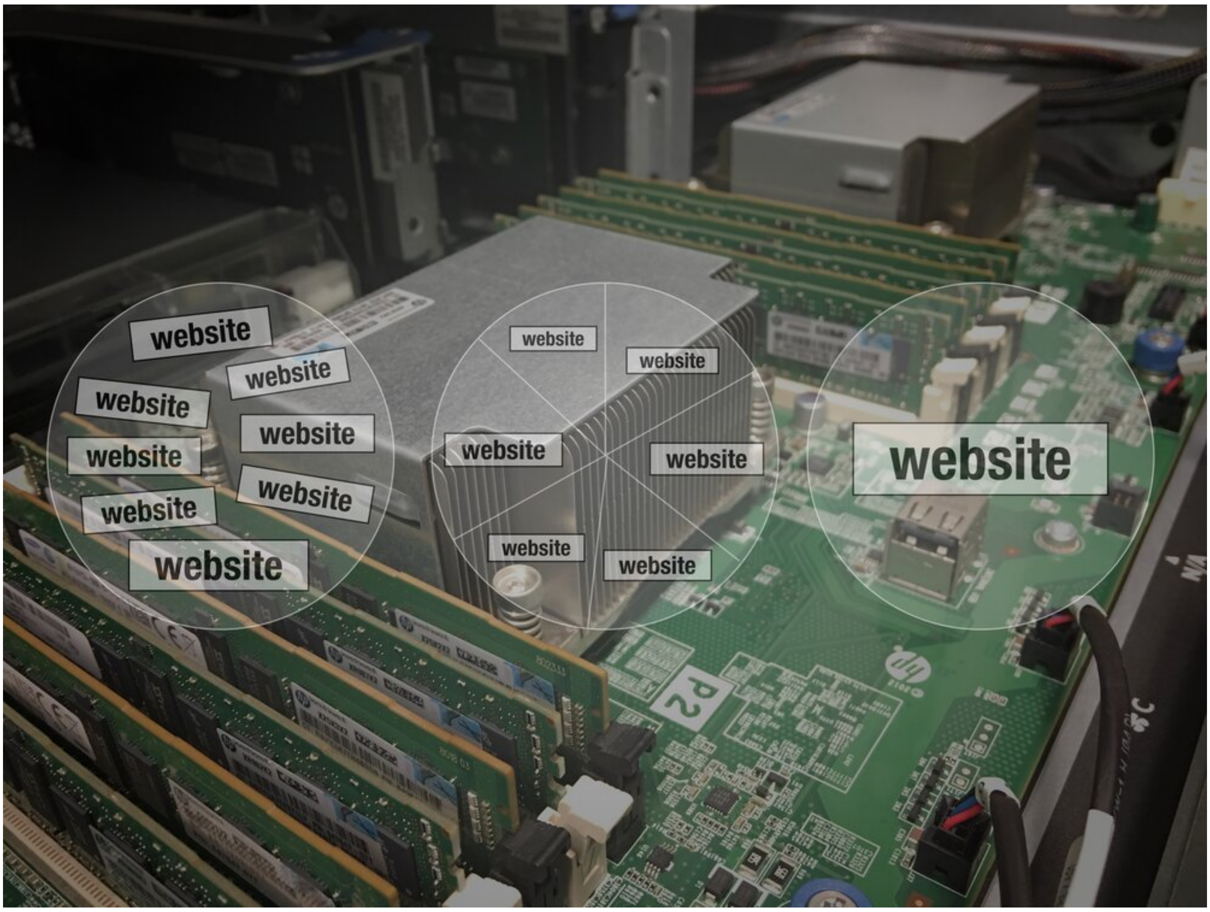
Understanding the security concerns in shared hosting

Considering open ports and unused network facing services

Willem L. Middelkoop

Feb. 28, 2019



People pay me to hack them, provided I'll explain how it was done, so future hacks can be prevented. As security consultant, I scan for weaknesses in my clients' apps, webshops and websites. Very often a hack starts by exploiting a security hole that is visible remotely. Read along to learn how hackers find security holes and what you can do to secure them.

To hack an app, webshop or website, hackers often target the servers that host it. To explain why hackers do this, you first have to understand what hosting is and what kinds of hosting there are.

What is hosting?

Hosting is a service that allows you to have your app, webshop or website be made available on the internet. Hosting is done using special computers called servers. When somebody types your website address in their browser, their device will connect to your server.

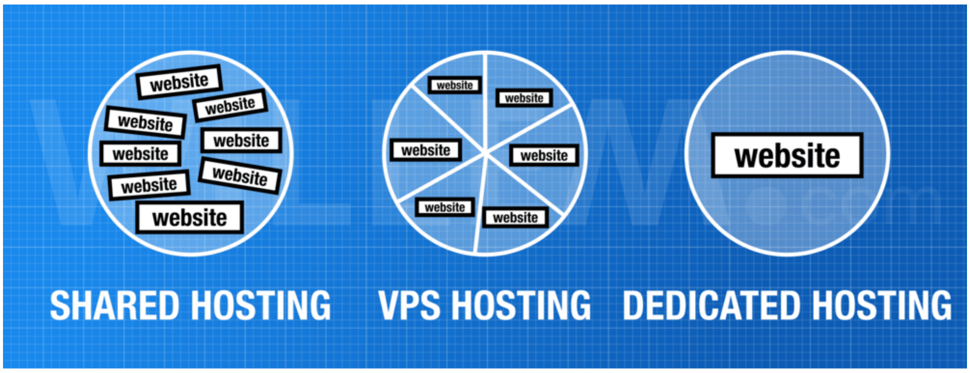
If hackers are able to take control over a server, they can access and manipulate all information that is on it. In addition, they can abuse the server's network and computational capacity to do bad things. You really don't want this...

A typical server in the datacenter, a physical machine that can host apps, webshops and websites

Different kinds of hosting

Your app, webshop or website can be hosted in different ways. Each kind of hosting has different concerns for security, but its relatively easy to understand as it all comes down to how the physical server (in the datacenter) is shared among the websites.

Web hosting companies usually operate multiple servers and divide their capacity among the number of websites that need hosting. One big server can easily host multiple websites, all depending on the amount of traffic the app, webshop or website has.



Different kinds of hosting: Shared hosting, VPS hosting and dedicated hosting visualised (a circle representing a physical server)

There are three different types of hosting:

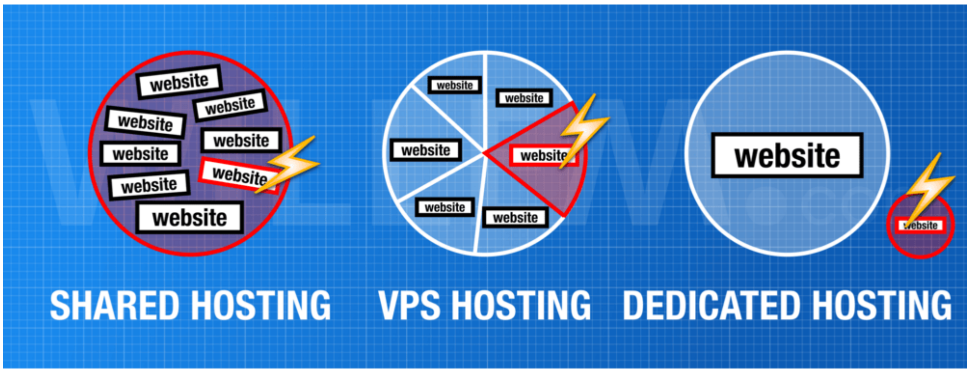
- **shared hosting**: The server runs multiple websites by sharing the operating system, memory, processor cores and hard disk storage. There are no hard divisions between the websites.
- **VPS hosting**: The physical server runs multiple virtual private servers (VPS) that all have their own operating system and their own share of memory, processor capacity and storage. A single VPS can be configured to run one or a couple of (related) websites. Because of the hard division between the VPS instances, it is very difficult for hackers to get from one VPS to another.
- **dedicated hosting**: The physical server runs only one website. Nothing is shared, all resources are dedicated to one app, webshop or website. Because of this physical division, you are not affected by hacks of any other website.

Warning: ”Cloud Hosting” is often rebranded shared hosting

It's important to understand that most modern ”Cloud Hosting” is actually *shared hosting* with a fancy name. Web design bureaus often configure their dedicated or virtual private server to sell shared hosting to their clients. So, unless you operate your own VPS or dedicated server, chances are you're on shared hosting.

Security concerns for shared hosting

The security risks of shared hosting come from its sharing basis. When one of the websites in the same server as yours is hacked, there is a high probability that your website will be affected as well. In this situation, security measures applied to your own website might not be enough to protect it against hackers.



Contagious effect of an hacked website (red indicating trouble)

Shared IP address

Furthermore, with shared hosting it usually means that all websites share the same IP address. You'll run into problems if any other website is involved in bad practice such as sending spam mails or hosting illegal content. This could cause your website to be blacklisted, blocked or downgraded in search engine rankings.

Performance

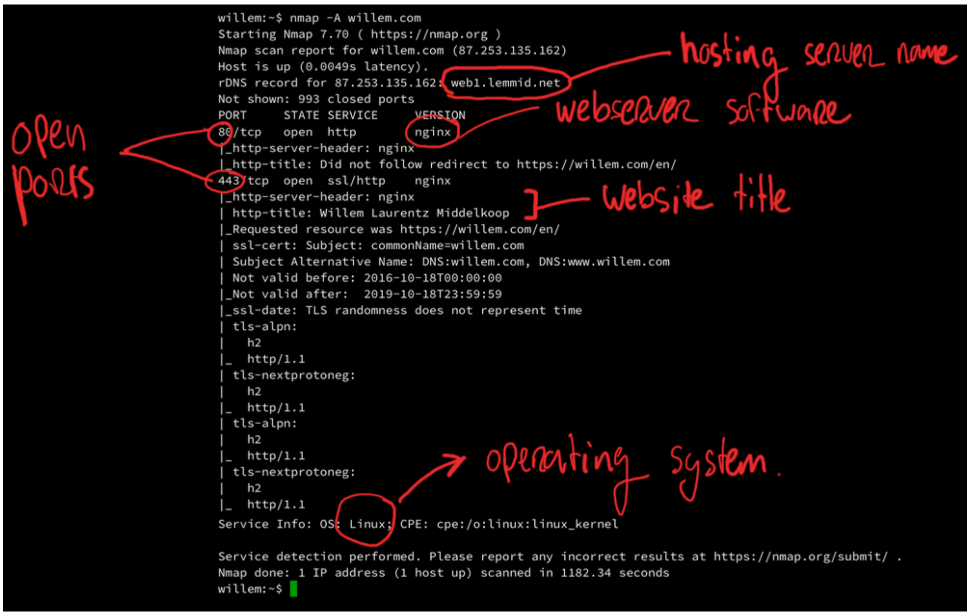
If you consider that hosting companies usually put hundredths - sometimes even thousands (!) - of websites on the same shared server, you'll understand why this increases the chance of being hacked. In addition to security issues, a shared hosting service also affects your website's performance as it has to compete with other websites over the same limited amount of server resources. If one of the other websites experiences some extreme traffic, it could slow down your app, webshop or website too!

Shared network facing services

Another problem with shared hosting is that usually the server has a lot of network facing services enabled, like a web, mail, FTP and database service. These services are available through open ports. It's bad form to have all ports open to everywhere because it exposes those services that are listening on those ports to exploits. Firewalls can limit what is allowed to connect a certain port, but in a shared hosting environment these restrictions are often not very tight (because of the many different things that are hosted on the same server).

Hacking an app, webshop or website

To hack your app, webshop or website a hacker can scan your hosting server for open ports, identifying the different services that run on the server. The unix program *nmap* is often used to do this. The hacker connects to the service listening on open ports to find out what program it is.



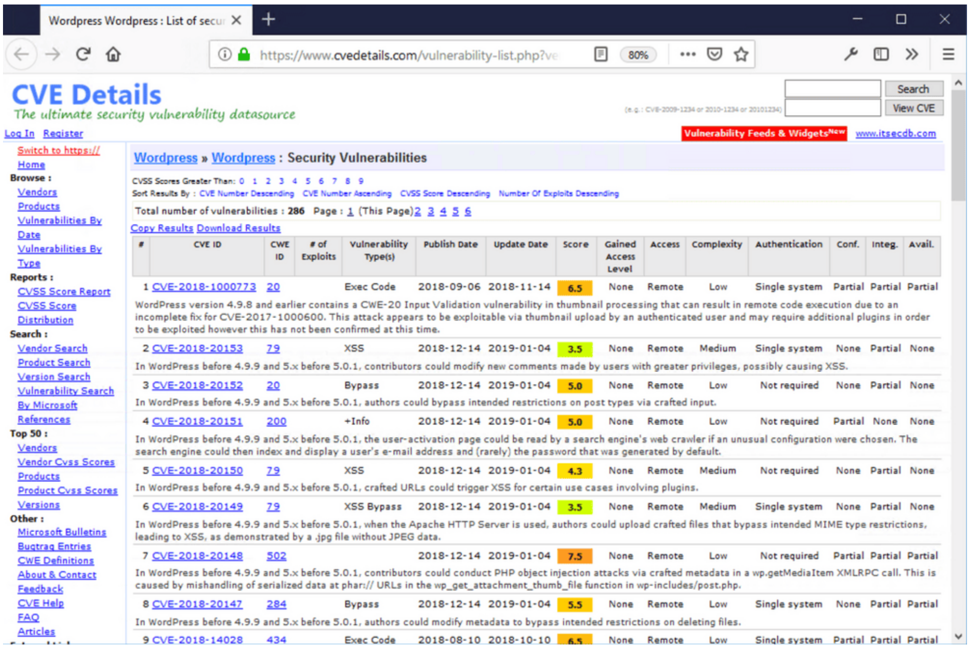
```
willem:~$ nmap -A willem.com
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for willem.com (87.253.135.162)
Host is up (0.0049s latency).
rDNS record for 87.253.135.162: web1.lemmid.net
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       nginx
|_http-server-header: 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:~$
```

Using nmap to scan a hosting server, identifying network facing services and open ports

This information can be used to check if running network services have any known security weaknesses. There are online libraries where these weaknesses can be looked up by software name and version. Finding a known weakness is as easy as a Google query. If an existing weakness is found, the hacker can use this to gain access to the server.

By checking the IP address of the hosting server, the hacker can determine if the server is shared with other apps, webshops or websites. It's possible (using reverse DNS lookups) to list all the websites hosted on the same server. While yours may be up to date and secure, others on the same server might run outdated software (with security weaknesses). Common website software is well documented, older versions of PHP and WordPress are known to have serious security problems.



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	CWE 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	3.5	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

Once a hacker knows what software your website uses, its easy to lookup known security holes using databases like cvedetails.com

Conclusion

The best way to secure your app, webshop or website is to limit its exposure to exploits as much as possible. Keeping your website software up to date is critical, but it might not be enough if your hosting is shared.

To prevent other hacks from affecting your app, webshop or website, you should consider hosting it on a dedicated physical or virtual server with its own IP address. You can then tighten security by filtering open ports and shutting down unused network facing services.

This way you reduce what cyber security experts call the ”attack surface”. The smaller it is, the easier it becomes to defend it - good luck and keep in mind that help is available!

Keep in mind that help is available - I know my way around servers and cyber security