

CMS Detector:

What CMS a Website is Using and the Best Tools to Find Out

TIPS

TOOLS

RECONNAISSANCE

[SECURITYTRAILS BLOG](#) · SEP 27 · SECURITYTRAILS TEAM

CMS Detector: What CMS a Website is Using and the Best Tools to Find Out

Reading time: 7 minutes

[Facebook](#) [Twitter](#) [LinkedIn](#)

Whether you're an online marketer doing market research, a developer, a security researcher or an SEO specialist, you must have asked yourself the question 'what CMS is this website using?' Or maybe you find yourself simply wanting to build a website—and you're interested in knowing which technology works best for different types of projects.

SEARCH BLOG

TABLE OF CONTENTS

What is a CMS?

What CMS is this site using?

Top 8 online CMS detectors

1. What CMS?
2. BuiltWith
3. Wappalyzer
4. W3Techs
5. Allora / Rescan.io

- 6. CMS Detector
- 7. Netcraft Site Report
- 8. OnlineWebTool — CMS Detector

Conclusion

Whatever the reason behind finding out which CMS or website builder a website is based on, there are different ways to perform this task, from using specially designed CMS detector tools, to looking into the source code from the browser, to still others. Today, we'll explore what a CMS is and what the best online CMS detector tools are, to find out which one a website is using.

What is a CMS?

A [CMS](#), or Content Management System, is a software that is used to build, manage and modify a website and its content. It's the best option for a less technical approach to website building, which doesn't require you to write the code for the website.

The content management system consists of two parts: a content management application or CMA; and content delivery application, the CDA. The CMA is the part you use to add and manage content on the website, the frontend interface; it's the part where other users can manage the content easily. In contrast, the CDA is the backend interface, where the content is stored and uploaded to the website.

Some of the most popular CMS examples are:

- WordPress
- Joomla
- Kinsta
- Magento
- Drupal
- Shopify
- Squarespace
- Wix

Detecting a CMS is an important part of any reconnaissance process; once you discover what CMS a target website is using, you can then perform vulnerability scanning. If, for example, it's a WordPress site, you can attempt to exploit known [WordPress security](#) vulnerabilities.

What CMS is this site using?

Detecting a CMS can be done many different ways, some slightly easier and quicker than others. It's simple to detect some of the most popular CMSs like WordPress, Joomla and Shopify but as there are many more platforms you should consider, it can get difficult using the basic checking in source code.

Before we dive into some specific CMS detector tools, let's explore some traditional ways of finding out which CMS a website is based on:

There are some obvious signs that a website owner hasn't removed, which could tell you the CMS they used:

- “Powered by”: Some websites might have a “Powered by” logo followed by the name of the CMS in their footer
- In the browser tab, there could be a favicon of the CMS (Joomla sites often have this favicon)

Since many website owners customize their website and do remove these tell-tale signs, you can also check their source code directly from your browser:

- A somewhat more timely option would be to use the “Find on page” shortcut and type in the names of the CMSs, which works well for Squarespace and WordPress (wp).
- Head tag might be your friend. There, search for the `<meta name=“generator” ...>` tag or x-powered-by header which will be followed by the CMS.
- Sometimes the generator tag is removed, so another option would be to type in some directories or tags specific for each CMS. For a WordPress website, “wp-content” or even just type in WordPress; Joomla will have a word “com_content” in their internal links; and Drupal will be “/sites/” or “/core/” folders, depending on the version.

All of these steps, besides being time consuming, aren’t that reliable—developers will often remove these tags or customize them to conceal the CMS they are using. Also, if they are not using any CMS it will take plenty of separate searches before you realize you were only shooting in the dark. This is where automated online CMS detector tools come to your rescue.

Follow us on Twitter to receive updates!



Follow @SecurityTrails

2,350 followers

Top 8 online CMS detectors

There are many CMSs you can use to build a website and there are also many CMS detector tools that help you find out about them. CMS detectors can even be paired with a [vulnerability scanner](#) to further your infosec investigation. We tested the most popular ones to give you a list of the 8 best online CMS detector tools available that help you answer the question: What CMS is this website using?

1. What CMS?

The creators of [this website](#) provide one of the best and most reliable CMS detector tools out there and it's all thanks to a minimal design that gives you exactly what its name implies: the CMS a website uses and additional information on the programming language, database OS and server. They are currently able to recognize 492 CMSs and are constantly updating their database to include even more.



2. BuiltWith

We love [BuiltWith](#) because it shows the most thorough outline of the technologies a website uses. You simply need to input the URL of the target website and it will show you numerous technology details including the CMS + CDN, analytics, used widgets, frameworks, hosting provider, SSL certificates and much more.

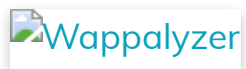
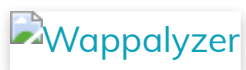
The reason it takes second place is because you do need to scroll through a large data list to find all the relevant information. However, it also has a feature that compares technology information with industry trends, in a pie chart:



3. Wappalyzer

[Wappalyzer](#) isn't really considered an online tool as it's a plugin for Chrome and Firefox browsers. It's considered the quickest, but also not as reliable as others mentioned on this list.

Once you've installed Wappalyzer, it will be bookmarked in the search tab. When you go to a website you want to inspect, just click the Wappalyzer button and it will reveal the CMS, web analytics, OS, programming languages, database and other technologies.



4. W3Techs

This highly reliable online CMS detector provides a comprehensive list of technologies on the target website. Simply navigate to the [W3Techs “Sites”](#) page and enter the URL.

From there, you’ll be able to access information on the CMS, programming languages, libraries, SSL, hosting provider, OS, TLD, geo location and much more.

It also offers installation as a bookmarklet, so you don’t even have to visit their website every time you need information on the websites you’re investigating.



5. Allora / Rescan.io

Allora.io has been integrated into [Rescan](#), but its features remain the same. It’s a trusted online detector that provides a free email analysis and lists out the CMS, framework, servers, OS, programming language, hosting provider, geo location, and more.

It’s easy to use. All you need is the website URL and with that, you can get all the related basic website technologies.



6. CMS Detector

[This website](#) is a well-known, straightforward online detector that will give you information about the CMS. It's the quickest ways to do so if you don't need any additional data.

Once you go to the website, simply type in the website URL, press Enter, and the results are there. While it's not 100 percent reliable and it doesn't offer any technology information, it's a speedy, handy tool when you're searching for the most well-known CMSs.



7. Netcraft Site Report

[Netcraft Site Report](#) will give you a wide range of information about the target website including the CMS, network information, hosting providers, SPF, DMARC, and other site technologies.

Other entries on this list may be more reliable, but it's one traditional tool that can come in handy.



8. OnlineWebTool — CMS Detector

Although the [OnlineWebTool](#) database isn't as large as some others—it detects around 100 popular CMSs—it offers not only standard CMS detection including technologies, it also provides a free website analysis that shows you the

website's ranking and safety along with some basic DNS records.

Keep in mind, however, that they say they're able to resolve around 30% of all user's requests. In other words, the scope of information you get might be limited.



Conclusion

There are many reasons you might need to know foundational technologies behind a website and including it in your reconnaissance process can be of great value. Specific CMSs have known vulnerabilities you might want to test, and online CMS detector tools are the fastest, most reliable ways to do so.

You might be old school and want to do it manually, but we're sure that using these free online tools, or cross-referencing a couple of them with your manual search, will yield the best results.

If you're ready to take a deeper dive and discover the entire external internet surface of your website or a target website, try out our [SurfaceBrowser™](#). [Schedule a demo](#) with our sales team to see all the features, information and security SurfaceBrowser™ can offer!

Sign up for our newsletter!

Email

name@company.com

Subscribe

< PREVIOUS NEXT >

Related Posts

What's My DNS? How to Find Domain DNS Records with our DNS Checker

Exploring the best ways to answer the question: What's my DNS?

Cybersecurity Red Team Versus Blue Team — Main Differences Explained

We've previously explored the Top 20 OSINT Tools available, and today we'll go through the list of top-used Kali Linux software.

Cybersecurity Fingerprinting Techniques and OS-Network Fingerprint Tools


We explore what a fingerprint is in cyber security, different types of

fingerprint techniques, and some of the most popular fingerprinting tools in use.

PRODUCTS

[DNS History](#)
[API](#)
[API Pricing](#)
[API Documentation](#)
[Feeds](#)

COMPANY

[Blog](#) 
[Our Story](#)
[Careers](#)
[Contact us](#)
[Product Manifesto](#)

RESOURCES

[Domain Stats](#)
[Data Bounty Program](#)
[Integrations](#)
[Fortune 500 Domains](#)
[Developer Hub](#)
[Service Status](#)

LATEST FROM OUR BLOG

- **NEW** [DNS Enumeration: Top DNS Recon Tools and Techniques](#)
- [5 Subdomain Takeover #ProTips](#)
- [CMS Detector: What CMS a Website is Using and the Best Tools to Find ...](#)
- [ASN Lookup Tools, Strategies and Techniques](#)
- [What is Reverse DNS? Top Tools for Performing a Reverse DNS Lookup](#)

SecurityTrails © 2019 · [Privacy Policy](#) · [Terms of Service](#)



 [Follow @SecurityTrails](#)