Web Tech Report 2011

Part 2: Top 1000 Corporations

Forbes Fortune 1000 Analysis

HackerTarget.com LLC
Everyone is a Target

peter <at> hackertarget.com
http://hackertarget.com

Table of Contents

Web Tech Report

Technologies in use by the worlds leading web sites

Introduction

A handful of technologies power the worlds leading websites. These technologies are the bridge between end users and information. They are also the bridge between attackers and the data.

This report is Part 2 of a series that aims to provide a snap shot of technology that is currently used by the worlds leading websites. Part 1 was based on the Alexa Top 1 Million websites, this second report focus on the largest US Corporations.

Weak technology decisions, poorly managed patching and systems management deficiencies allow attackers easy access to back-end databases and systems.

Not paying attention will lead to customers, employees and business all put at risk.

About

HackerTarget.com is a leading provider of on-line security scanning services. Utilizing open source tools, advanced security testing is made available to anyone wanting to test their external facing Internet Services for security vulnerabilities or other issues.

Port Scanning, Vulnerability Testing, Web Server analysis, SQL Injection, CMS fingerprinting and open source intelligence gathering are the core automated tools.

All scan options are available for free (limited to 4 / day), additional scans are available for a minimal cost.

In depth security assessment consulting services are also available.

Methodology

The Top corporations were selected from the Forbes Fortune 1000 top US companies by revenue. These companies have the big money, what technology decisions do you make when you can afford to purchase anything?

During February 2011 HackerTarget.com compiled a list of corporate websites based on the Fortune 1000 list downloaded from aggdata.com.

We then spidered the root web page of each of those sites using the fingerprinting tool WhatWeb.

Redirects from sites that responded with a 302 were followed and a total of 999 “HTTP 200 OK” pages were analyzed.

Intensity of the analysis was set to a minor level, meaning the only active scanning of the target sites was to download the HTML from the page and examine the resulting code and HTTP headers.

The data in this report is based on these sites that responded with a 200 OK HTTP Response. No attempt was made to access sub-domains or subdirectories to include additional blogs / forums and other minor parts of the site. Blogs and Forum statistics are only from sites that are based on those systems from the root page.

The nature of this data means that there is no way this report can be 100% accurate. Server administrators can hide and alter these responses for security reasons. HackerTarget.com LLC makes no guarantee on the accuracy of this report.

Generally technologies with less than 0.1% sites detected have not been included in the results.

External References

http://hackertarget.com

http://en.wikipedia.org/wiki/List_of_HTTP_status_codes

http://www.morningstarsecurity.com/research/whatweb

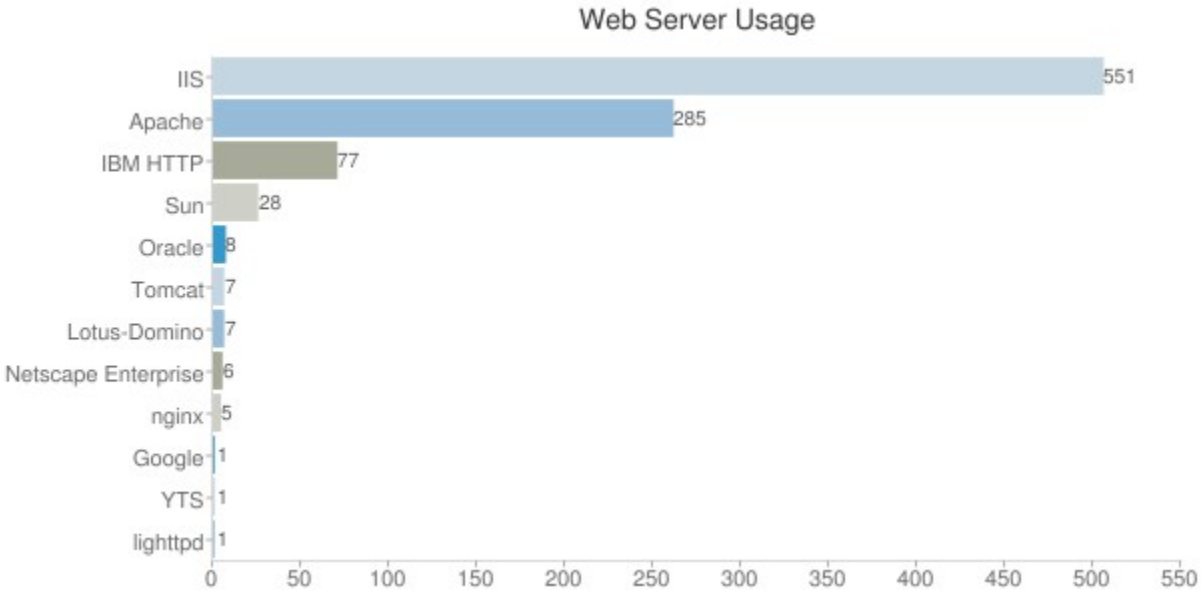
http://www.alexa.com

Web Servers

The web servers in use has been collated from HTTPServer header responses primarily however some servers have also been counted from the X-Powered-By header.

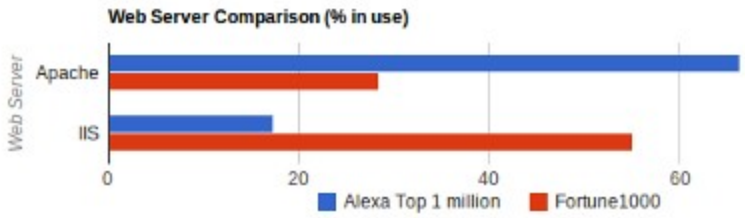
There is a clear preference towards proprietary solutions in these results. Apache is lagging well behind Microsoft IIS. Sun, IBM and Oracle all have strong results.

More information regarding web server popularity can be found at the Netcraft Web Server Survey page.



Foot Notes

The following chart compares Apache vs IIS in popularity, showing a clear difference between the Alexa Top 1 million sites and the Fortune 1000 Web Sites.



External References

http://news.netcraft.com/archives/category/web-server-survey/

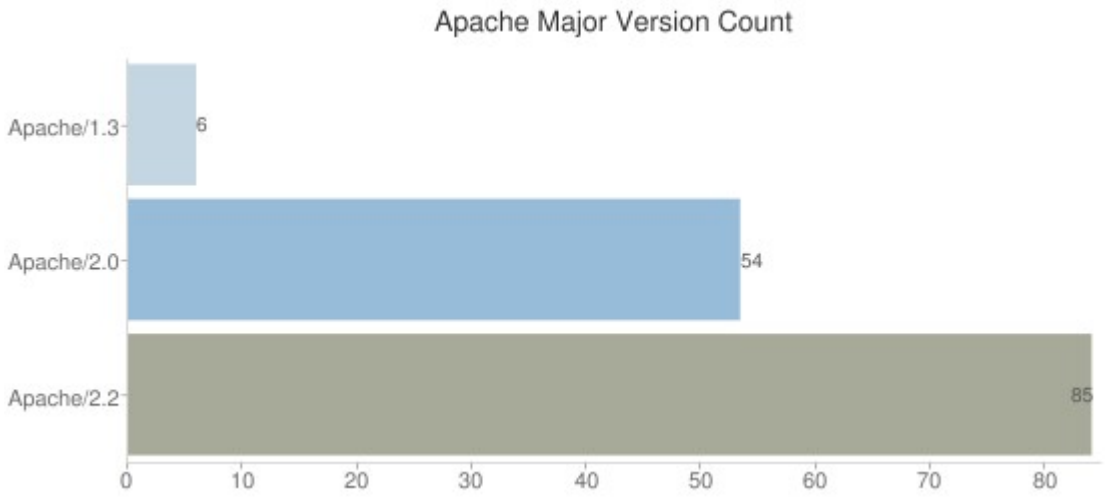
http://hackertarget.com/2011/03/web-tech-2011-report/

Apache Server Versions

This data has been collected from the HTTPServer Header.

While this is an indication of the Apache version distribution, the majority of Apache sites do not advertise the exact version number.

Apache version 1.3 is deprecated and no longer maintained.



Foot Notes

Apache has a large list of point releases for each of these versions.

External References

http://httpd.apache.org/ABOUT_APACHE.html

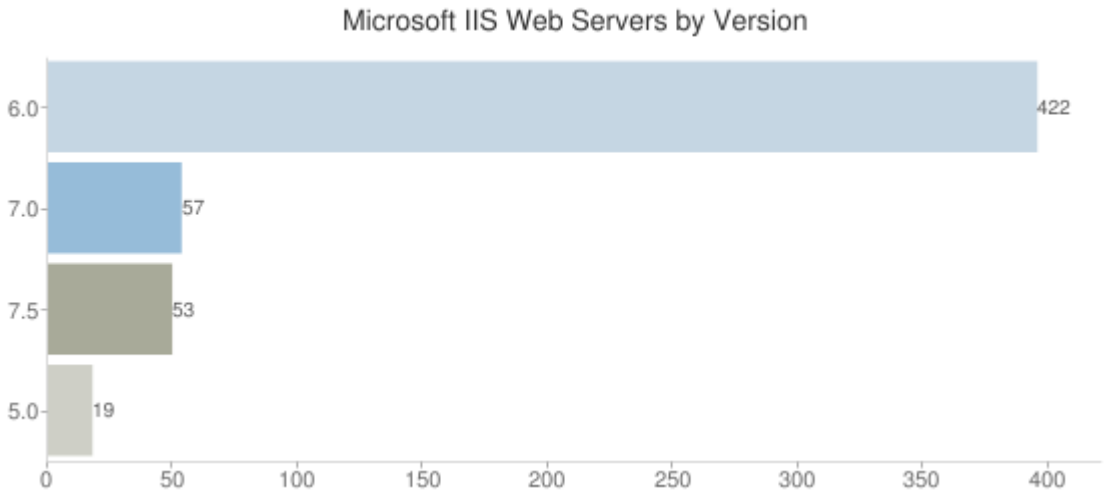
Microsoft IIS Server Versions

This data has been collected from the HTTPServer Header.

IIS 6.0 is clearly the most popular.

IIS 5.0 will be running on Windows 2000 servers that became unsupported in July 2010.

Generally IIS 6.0 was the first version released by Microsoft where Security started to become a priority.



Foot Notes

External References

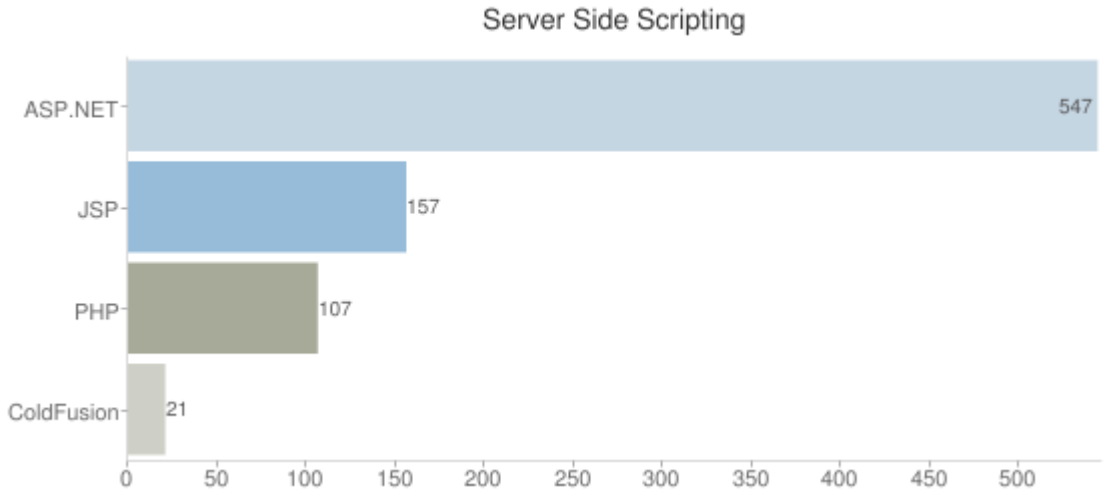
http://en.wikipedia.org/wiki/Internet_Information_Services

http://en.wikipedia.org/wiki/Windows_2000

Server Side Scripting

Numbers for ASP closely resemble the numbers for Microsoft IIS web servers, while the Apache Servers are broken up between PHP and JSP.

Compared to the Alexa Top 1 Million PHP usage there is a clear indication that the Largest American Corporations have not embraced PHP as a Server Side Scripting Language.



Foot Notes

JSP (Java) pages have been detected using the detection of cookies containing JSESSIONID and JSP in the HTTPServer Header.

ColdFusion has been detected through the detection of CFID in the page cookie.

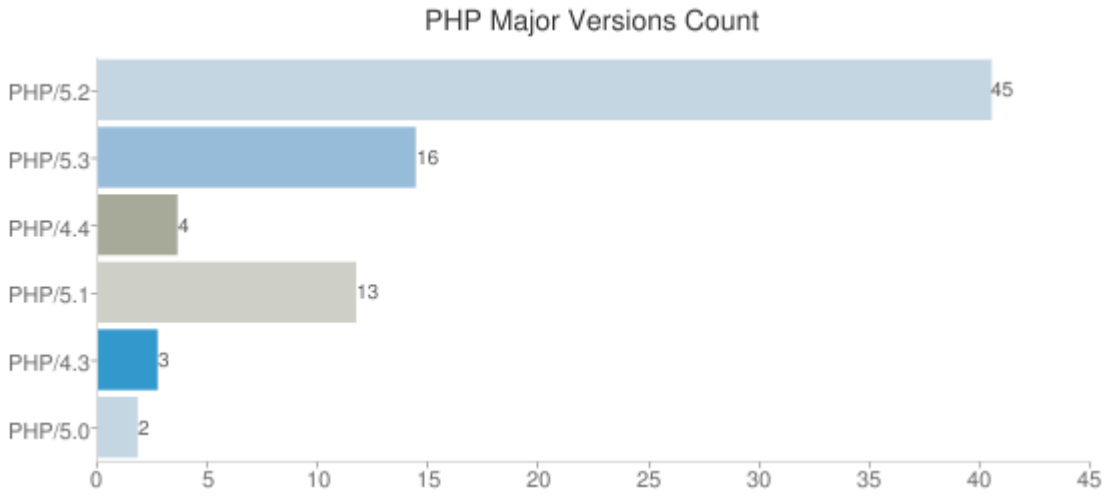
External References

http://hackertarget.com/2011/03/web-tech-2011-report/

PHP Version

This data has been collected from the HTTPServer and X-Powered-By Header.

Only major versions have been counted.

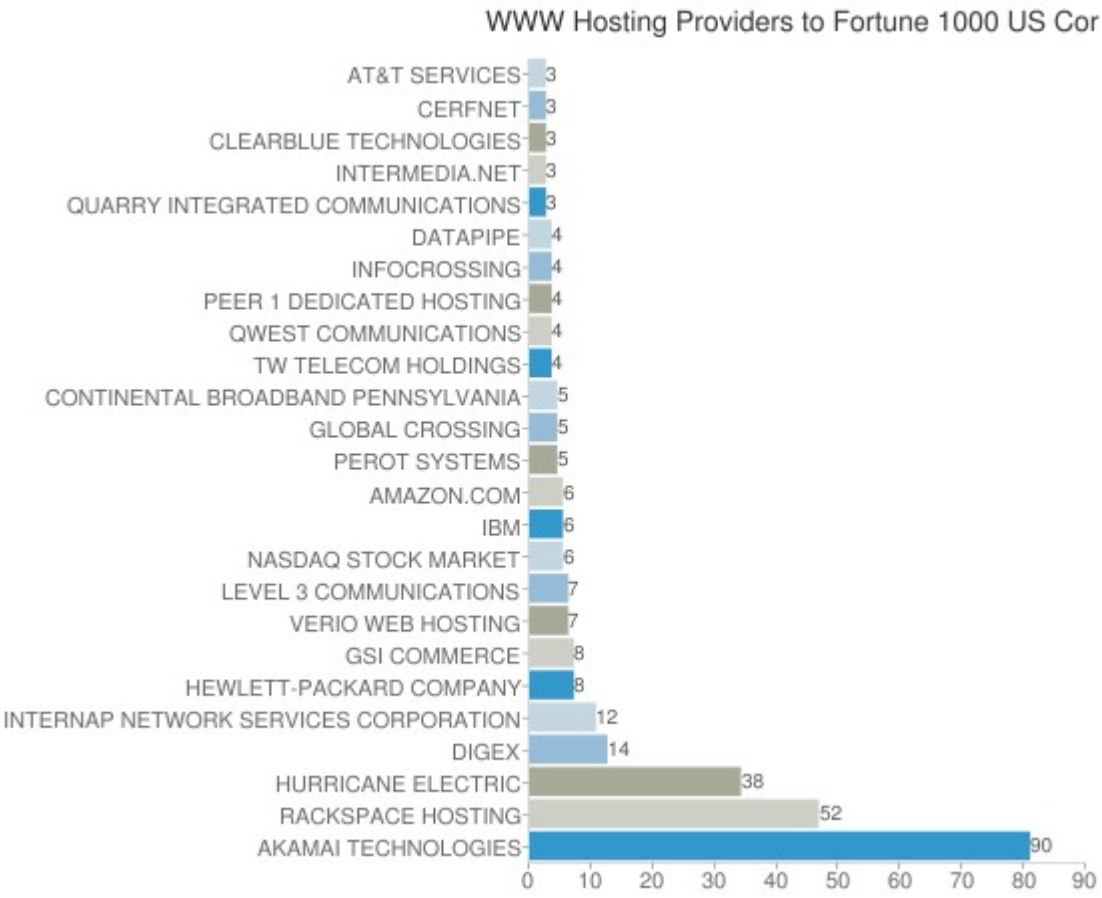


External References

http://php.net/releases/index.php

Web Hosting

Most web sites appear to be hosted within the corporations own net blocks. This could be correlated with the high Microsoft IIS web server counts. Logically sites are hosted on company managed servers in house and are managed by the companies IT staff who are working in a primarily Microsoft based environment.



Results of 2 or below have been omitted. These are mostly corporate owned Net Blocks where the sites are hosted in house or in the corporations data center space.

Numbers were calculated by determining the net block owner of the web sites resolved IP address.

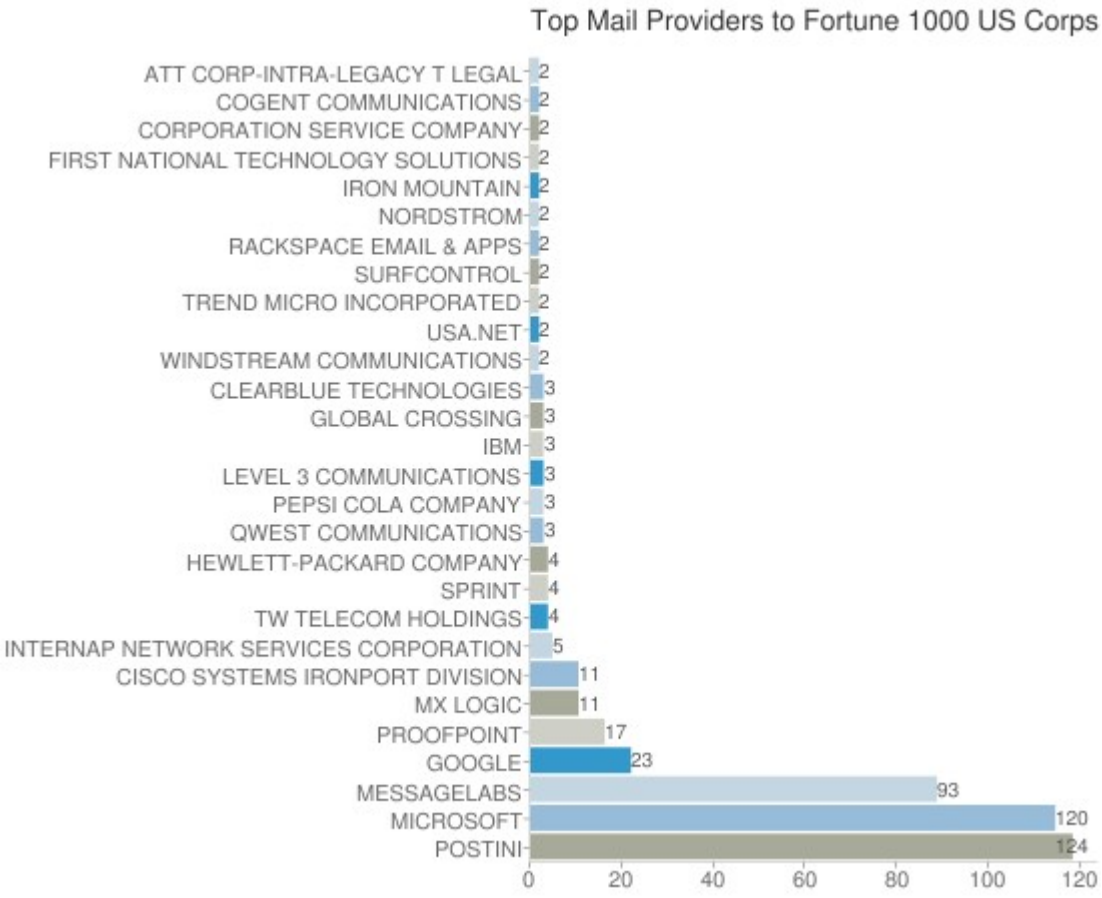
External References

http://en.wikipedia.org/wiki/Web_hosting_service

Mail Hosting

Mail service has been outsourced much more than web hosting. Likely due to the effectiveness of “cloud based” SPAM and content filtering of email.

Google owned Positini leads the charge just ahead of Microsoft and Messagelabs (now owned by Symantec).



Footnotes

These numbers were calculated by determining the net block owner of the IP of the registered MX record for each domain.

Counts of 1 were usually hosted in-house and are not included in the above chart.

External References

http://en.wikipedia.org/wiki/Postini

http://en.wikipedia.org/wiki/MessageLabs

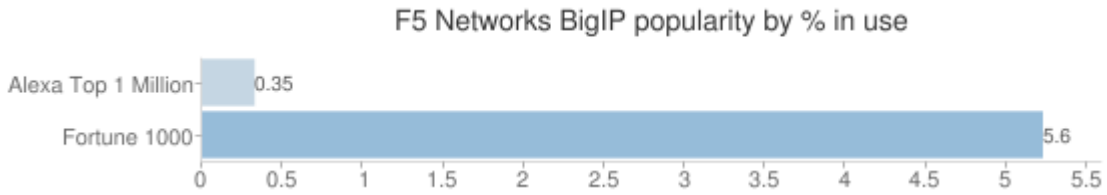
F5 Load Balancers

F5 Networks sell a range of load balancing devices known as BigIP.

Once again the following chart shows that the large corporations are willing to put up the money for these proprietary systems.

Many of the top sites in the Alexa Top 1 Million will be using apache or other open source load balancing alternatives, these are difficult to count separately.

For those who are unaware the F5 BigIP systems were originally developed on a BSD core, they are now running Linux under the hood.



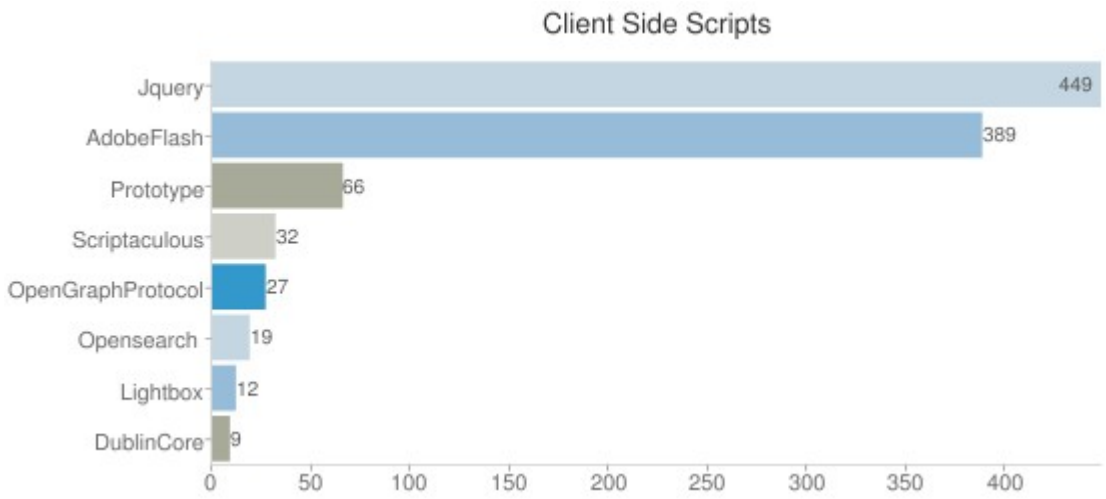
External References

http://en.wikipedia.org/wiki/F5_Networks

Client Side Scripting

Javascript libraries and Adobe Flash are both very popular.

HTML5 was also discovered on 24 pages, it will be interesting to see how these numbers change once HTML5 usage becomes more widespread.



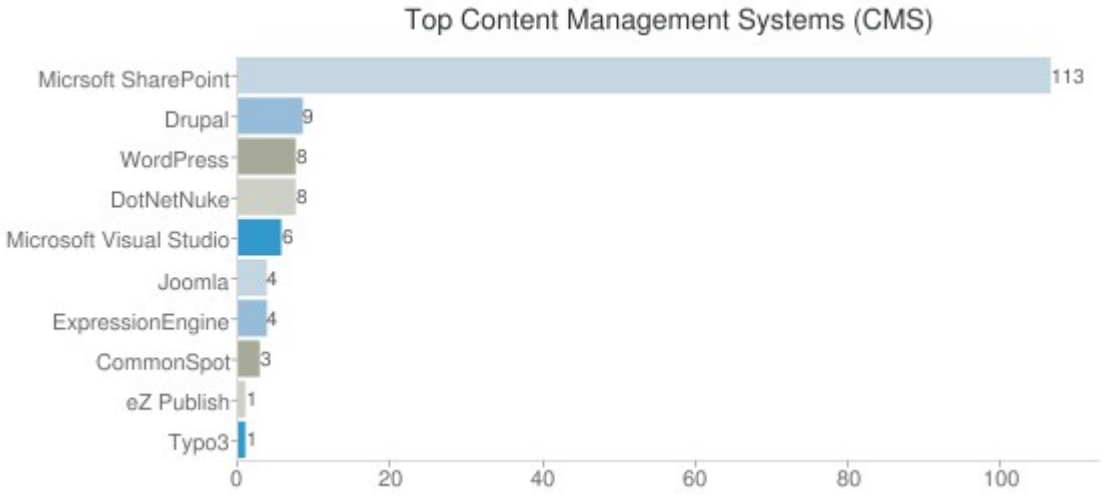
External References

http://en.wikipedia.org/wiki/JQuery

Content Management Systems

The most popular “content management system” in use is Microsoft SharePoint. 113 results puts this at 11% of the total sites.

Unlike the results seen the top 1 million most popular sites, open source based sites such as WordPress are rarely in use. Drupal does have a stronger showing in these results when compared to WordPress.



External References

http://en.wikipedia.org/wiki/Microsoft_SharePoint

http://en.wikipedia.org/wiki/WordPress

http://en.wikipedia.org/wiki/Drupal

Conclusion

These results show a clear preference by the largest corporations to purchase proprietary solutions from the worlds largest technology companies.

Whether these proprietary solutions are as good as the open source alternatives is a debate that continues to rage, however the fact the most popular websites in the world rely on open source technologies in the majority of cases is an indication that there is clearly an alternative to the proprietary systems preferred by the large corporations.

Analysis of “cloud based” providers for Web Hosting and Email shows a clear move towards cloud based mail filtering services. Hosted Web services do not appear to be as popular with most corporate web sites being hosted in house.

From a security perspective proprietary and open source solutions both continue to be attacked and compromised on a regular basis. It is possible to achieve a robust secure system no matter what technology you decide on; the key is best practice management, ongoing maintenance and monitoring.

HackerTarget.com recommends the following:

- Ensure all software is up to date and patched including all web based applications such as content management systems (don't forget the plugins!).
- Use strong passwords on administrator accounts
- Limit password reuse between different accounts and environments
- If the application allows it move the administration panel url to an undisclosed location.
- Implement well documented web server lock down configurations.
- Perform regular security scanning as part of your overall security strategy.