UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

The Vulnerable Web An Analysis of Content Management Systems on the Internet

Trabajo Fin de Máster

Presentado por: Garceau Aranda, Xavier

Director: Martínez Herráiz, José Javier

Ciudad: Madrid
Fecha: 2017-02-05

1 Abstract

In this work, we aim to analyze the presence of Content Management Systems on the Internet. We build empiric data on what proportion of the Web uses these software platforms, by fingerprinting known CMSs and their versions. We then analyze the versions of the most important CMSS (WordPress, Drupal and Joomla) to define what proportion of websites are running outdated and vulnerable code.

While the proportion of websites found to be vulnerable may be low, this is most likely attributable to the benchmark we set to consider a website as such. This work provides empiric data and a reproducible methodology, in a field that is severely lacking of both.

Keywords:

Content Management Systems, Outdated Software, Known Vulnerabilities, Internet, Web

2 Resumen

El objetivo de este trabajo es de analizar la prevalencia de Sistemas de Gestión de Contenido en el Internet. Recopilamos datos empíricos sobre la proporción del Web que usa estas plataformas de software, identificando CMSs conocidos y sus versiones. A continuación analizamos las versiones de los CMSs más importantes (WordPress, Drupal y Joomla) para definir qué proporción de los sitios web están ejecutando código desactualizado y vulnerable.

Si bien la proporción de sitios web que se consideran como vulnerables es baja, esto es atribuible a los criterios de referencia establecidos para considerar un sitio web como tal. Este trabajo proporciona datos empíricos y una metodología reproducible, en un campo que es severamente en falta de ambos.

Palabras Clave:

Sistema de Gestión de Contenidos, Software Desactualizado, Vulnerabilidades, Internet, Web

3 Table of Contents

4 Table of Figures

5 Table of Tables

6

7 Introduction

While developing good software is hard, the need for on-demand web applications is ever-growing. The reality is that not everyone has the knowledge, time or funds to develop custom applications. That is where Content Management Systems (CMSs) shine. With their ease of use, extensibility and features, they are the perfect solution when custom code is not an option.

But these qualities come at a cost. While custom code may have more bugs and software vulnerabilities, when a vulnerability is found in a CMS the number of websites affected is much greater. Also, custom plugins that are trivial to install may be responsible for introducing vulnerabilities. While these plugins are used by a large amount of websites, they aren't subject to the same scrutiny. These two aspects are made worst by the fact that it is generally possible to fingerprint CMSs and their versions through many different techniques.

Two other prevalent issues are that CMSs are often used by individuals with lesser technical knowledge and are not always kept up to date, either because the owner of the application, disables automatic updates, doesn't have a process for software maintenance or is scared that the new version may not be compatible with custom code

All of this said and while many high-profile vulnerabilities are thought to have an important impact on the security of the Internet, there is very little real data on this matter. This work aims to uncover what proportion of websites are running on the three major CMSs, WordPress, Drupal and Joomla. By fingerprinting the versions these applications are running, we will then define metrics to assess what percentage of these websites are exposed to known vulnerabilities. All of these steps will follow a defined and reproducible methodology, on which future work can be done.

8 Review of Literature

In this chapter, we will study the current knowledge including substantive findings, as well as theoretical and methodological contributions to the topic at hand. We will be focusing on the role of CMSs on the Internet and the vulnerabilities related to this type of software.

8.1 CMS Usage Statistics

The first thing we need to establish is what proportion of the Internet is running on CMSs. This will enable us to establish how much of an impact websites running outdated versions of software has. What percentage of websites are running a CMS and what are the prevalent software used.

It is hard to find hard empirical evidence on the prevalence of use of CMSs on the Internet. In this section, we present the most credible sources and those that present hard empirical data.

8.1.1 BuiltWith CMS Usage Statistics

Founded in 2007, BuiltWith is a website profiler and usage analytics for the internet. BuiltWith technology tracking includes widgets, analytics, frameworks, content management systems, advertisers, content delivery networks, web standards and web servers to name some of the technology categories we cover.[16] BuiltWith provides weekly trends in internet web technology usage and global ecommerce sales trends.

The following table summarizes BuiltWith CMS statistics, for the week beginning January 16th, 2017[17]:

Rank	CMS	Number of Websites	Proportion of Websites (%)
1	**WordPress**	**17402952**	**79.3**
2	**Joomla!**	**2234202**	**10.2**
3	Blogger	766970	3.5
4	**Drupal**	**692855**	**3.2**
5	CPanel	537003	2.4
6	Google Search Appliance	181526	0.8
7	ExpressionEngine	49278	0.2
8	vBulletin	27570	0.1
9	Adobe CQ	19186	0.1
10	Liferay	13262	0.1
11	Sitecore CMS	10611	0.0
12	Adobe Experience Manager	5839	0.0
13	Adobe Scene7	3538	0.0
14	HP TeamSite	1604	0.0
15	WordPress VIP	1384	0.0
16	Thomson Reuters Corporate Solutions	1046	0.0
17	Salesforce Desk	776	0.0
18	Endeca	664	0.0
19	Lithium Technologies	290	0.0
20	MoovWeb	136	0.0

Table 1 BuiltWith CMS Statistics - Week beginning January 16th 2017

A caveat to take into account is that these statistics are generated based on what can be found on the homepage of a website. Therefore, some technologies may be under-represented if they use custom implementations or do not appear on the landing page of a website. CMS usage may therefore be under-represented.

No additional details are provided as to the established methodology. Also, while they provide the number of websites for which a CMS was detected, they do not provide the total number of websites analyzed, nor the versions of the detected CMSs.

8.1.2 W3Techs CMS Usage Statistics

W3Techs is a division of Q-Success Web-based Services. Its goal is to collect information about the usage of various types of technologies used for building and running websites, and to produce and publish surveys that give insights into that subject.[18]

W3Techs provides the following statistics[19] as to the percentages of websites using various content management systems:

Rank	CMS	Absolute Percentage (%)	Market Share (%)
1	**WordPress**	**27.2**	**58.5**
2	**Joomla**	**3.4**	**7.2**
3	**Drupal**	**2.2**	**4.8**
4	Magento	1.2	2.7
5	Blogger	1.1	2.4
6	TYPO3	0.7	1.5
7	Bitrix	0.7	1.4
8	Shopify	0.6	1.3
9	PrestaShop	0.6	1.3
10	Adobe Dreamweaver	0.6	1.2
11	Squarespace	0.5	1.1
12	OpenCart	0.4	0.9
13	FrontPage	0.4	0.8
14	DataLife Engine	0.3	0.7
15	vBulletin	0.3	0.6
16	Wix	0.3	0.6
17	DotNetNuke	0.2	0.5
18	ExpressionEngine	0.2	0.5
19	phpBB	0.2	0.4
20	Bigcommerce	0.2	0.4

Table 2 W3TechsCMS Market Share

It is important to note that no CMS was detected for 53.4% of the websites analyzed. The absolute percentage is the percentage amongst all analyzed websites, for which a given CMS was detected. The market share is the percentage amongst all the websites for which a CMS was detected, for which a given CMS was detected.

W3Techs does provide the methodology used to formulate these statistics[20].

- Technologies are identified using information provided by the site itself when downloading web pages. The web pages are fetched and analyzed. Publicly available information is also aggregated from sources such as Alexa, Google, Microsoft and ipinfo.io.
- The analysis phase searches for specific patterns in the web pages that identify the usage of technologies, similarly to the way a virus scanner searches for patterns in

a file to identify viruses. They use a combination of regular expressions and DOM traversal for this search. They have identified several thousand indicators for technology usage. These indicators have different priorities, and based on the presence or absence of specific combinations of indicators in a specific context, they come to our conclusions.

Some technicalities are important to take into account[21]:

- W3Techs investigates technologies of websites, not of individual web pages. If a technology is found on any of the pages, it is considered to be used by the website.
- W3Techs includes only the top 10 million websites in the statistics in order to limit the impact of domain spammers. They use website popularity rankings provided by Alexa (an Amazon.com company) using a 3 months average ranking.
- W3Techs does not consider subdomains to be separate websites. For instance, sub1.example.com and sub2.example.com are considered to belong to the same site as example.com. That means for example, that all the subdomains of blogger.com, wordpress.com and similar sites are counted only as one website.
- W3Techs does not include redirected domains. For example, sun.com redirects to oracle.com, and is therefore not counted.

More information about the methodology can be found on their website[20] [21].

8.1.3 Wappalyzer CMS Usage Statistics

Wappalyzer is a browser extension that uncovers the technologies used on websites. It detects content management systems, e-commerce platforms, web servers, JavaScript frameworks, analytics tools and many more.[22]

Using the data aggregated from users who have the Wappalyzer extension installed on their browser, they provide the following statistics[1]:

Rank	CMS	Number of Websites	Proportion of Websites (%)
1	**WordPress**	**4806653**	**77.52**
2	**Joomla**	**675591**	**10.9**
3	**Drupal**	**407077**	**6.57**
4	TYPO3 CMS	102359	1.65
5	DNN	42485	0.69
6	Contao	23557	0.38
7	Concrete5	23540	0.38
8	CMS Made Simple	18537	0.3
9	Liferay	18196	0.29
10	SPIP	15170	0.24
11	SilverStripe	11782	0.19
12	Umbraco	9453	0.15
13	MODx	9316	0.15
14	eZ Publish	9069	0.15
15	Plone	7234	0.12
16	Movable Type	7050	0.11
17	XOOPS	6096	0.1
18	Pligg	3064	0.05
19	Contenido	2505	0.04
20	Squiz Matrix	1844	0.03

Table 3 Wappalyzer CMS Market Share

While this provides the number of websites detected, it doesn't provide the number of websites analyzed. So the proportion of websites is that of fingerprinted websites, not total websites.

Wappalyzer uses an extensive list of regular expressions to evaluate web pages and detect web applications[23]. These regular expressions enable the analysis of the HTML content, server response headers, included scripts and more. For example, the following pattern[24] description is used to identify WordPress instances:

```
"WordPress": {
        "cats": [
                1,
                11
        ],
        "env": "^wp_username$",
        "html": [
                "<link rel=[\"']stylesheet[\"'] [^>]+wp-(?:content|includes)",
                "<link[^>]+s\\d+\\.wp\\.com"
        ],
        "icon": "WordPress.svg",
        "implies": "PHP",
        "meta": {
                "generator": "WordPress( [\\d.]+)?\\;version:\\1"
        },
        "script": "/wp-includes/",
        "website": "wordpress.org"
},
```

Figure 1 Wappalyzer WordPress pattern

8.2 CMS Vulnerability Statistics

Once we have identified the CMS landscape on the internet, the interesting question becomes how vulnerable are the major CMS software. This data is available through CVE Details, which provides an easy to use web interface to CVE vulnerability data.[34]

Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools. If a report from one of your security tools incorporates CVE Identifiers, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem.[33]

CVE is:

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Free for public download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and CVE-Compatible Products

The following figure aggregates all the CVEs attributed to the main CMSs [26] [27] [28] [29] [30] [31] [32] since 2002:

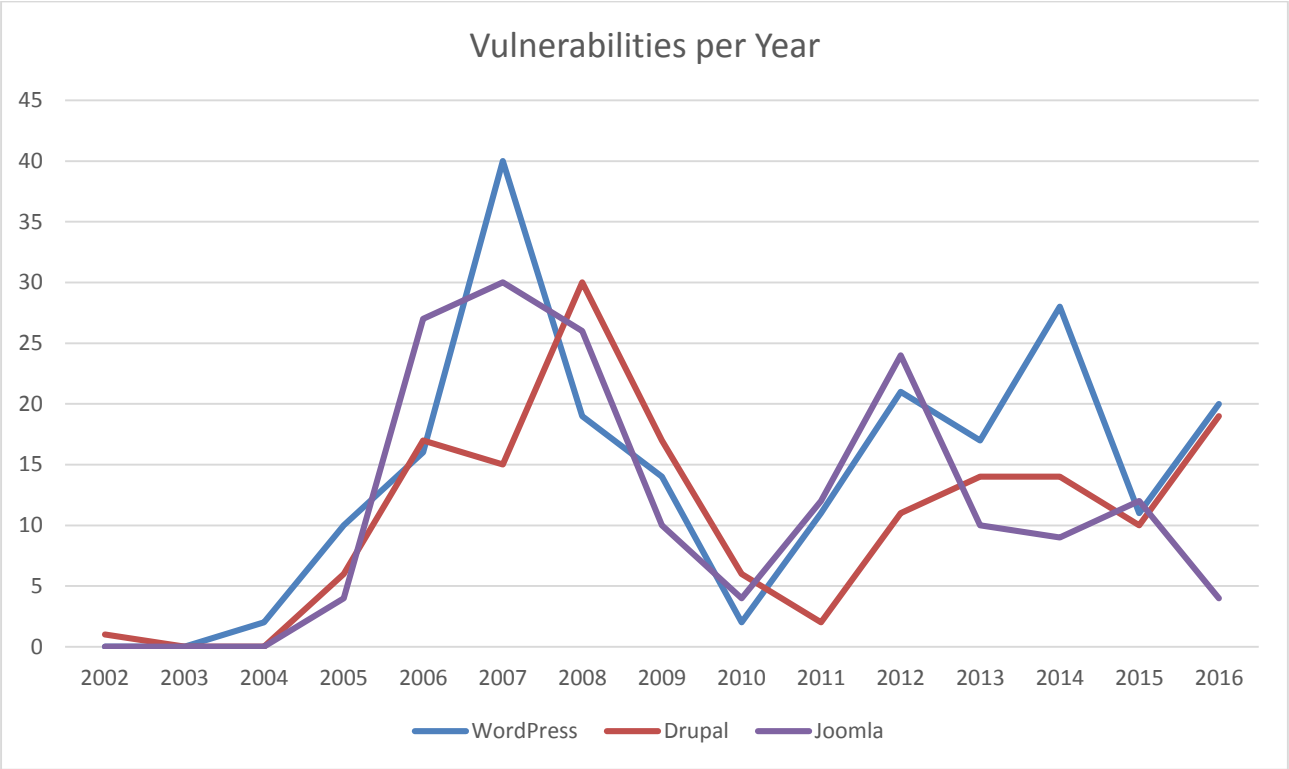

Figure 2 CVEs per year form WordPress, Drupal, Joomla

These vulnerabilities range through the whole scope of common web threats:

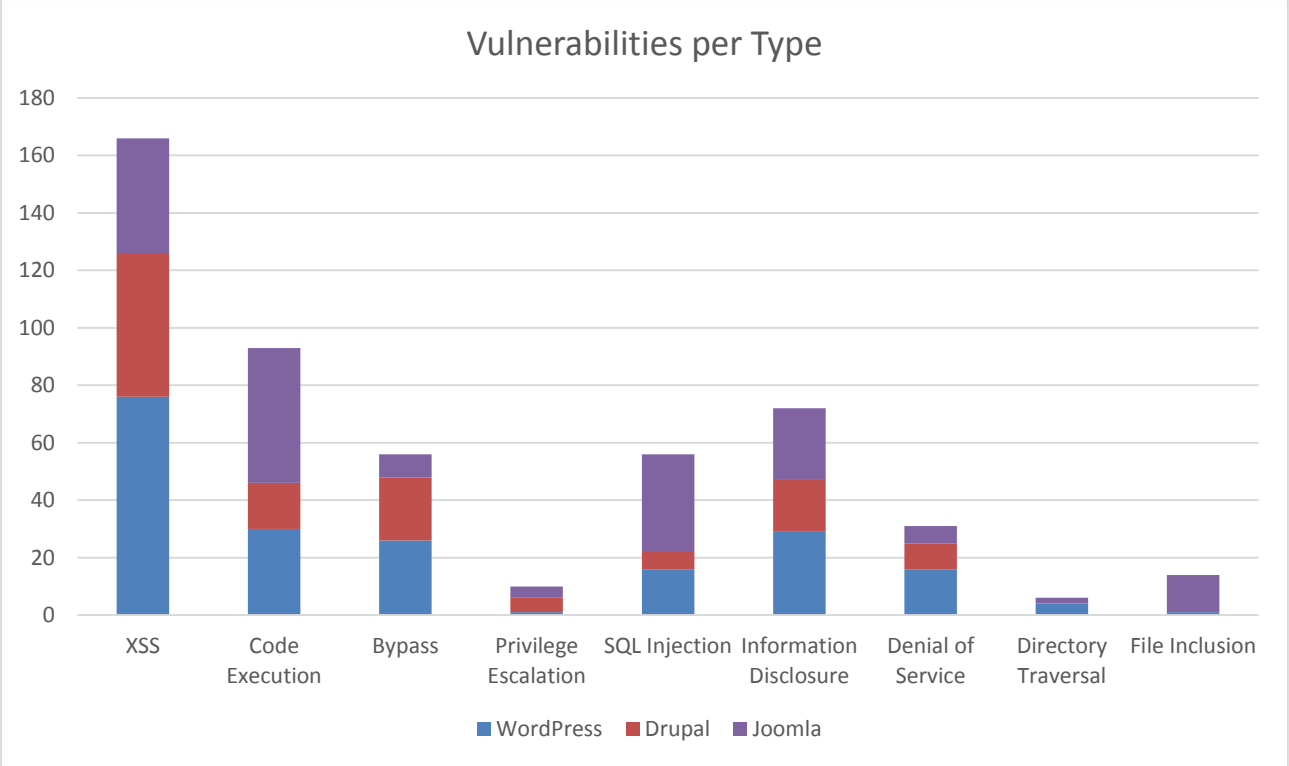

Figure 3 Vulnerabilities per type for WordPress, Drupal & Joomla

8.3 Similar Projects

After exhaustive research, no project was found to answer the questions analyses in this project. Empiric data on the versions of CMS instances on the Internet are non-existent, as are similar works on the “vulnerable web”.

The closest project is the Wappalyzer project, but this is proprietary data that is not accessible, and doesn’t provide data about versions. Therefore our project will be a significant contribution to the body of knowledge.

9 Hypothesis

It is hard to make predictions based off of the previously established knowledge. The main issue is that, while there is some hard data on the percentage of the Internet may be running on content management software, there is no data available data on what these versions are.

While we have data that enables us to determine what versions of CMSs have vulnerabilities, since we do not have data on CMS versions, there is little we can extrapolate. This said, it seems that there where peaks in the number of CVEs reported in the years 2006-2008 and 2012-2014. It is therefore reasonable to extrapolate that websites running versions released in these periods will have more vulnerabilities. It is also reasonable to say that the older the version is, it should be exponentially more vulnerable.

One think to take into account is that reported CVEs only account for known vulnerabilities. But considering that we are most interested in the three primary CMS software, we can consider that these have been extensively analyzed. Therefore, while it is not impossible that these versions have vulnerabilities that are not known, the amount of these would be statistically negligible.

In conclusion, it is not possible to hypothesize on the order of magnitude of how many websites will be found to run outdated and vulnerable CMSs.

10 Investigation Objectives

The primary investigation objective of this document is to present empiric data on CMS usage and mapping of the “vulnerable web”. To do so, we have established four tasks:

1. Define how to fingerprint CMSs and their versions.
   For this, we will re-use the regular expressions defined by the Wappalyzer[22] project (refer to section 8.1.3). These regular expressions analyze the content of the website (HTML body, HTTP response headers, etc.) to find known markers and defined indicators.
2. Develop a software that can fingerprint a sizeable amount of websites.
   To get the data, we must develop a system that gathers data from a significant amount of websites.
3. Analyze the known vulnerabilities in the major CMSs.
   We will establish metrics for what versions of said CMSs are considered “vulnerable”.
4. Compare fingerprinted websites to vulnerable versions, to conclude what proportion of the Internet is running on known-vulnerable software.

11 Methodology

This section outlines the technologies used to develop the software required to go through with the project, the architecture of the software built as well as the results obtained.

11.1 Technologies

The following technologies where leveraged to build the CMSpyder tool.

11.1.1 Python

Official website: https://www.python.org/

Python is a widely used high-level, general-purpose, interpreted, dynamic programming language. Its design philosophy emphasizes code readability, and its syntax allows programmers to express concepts in fewer lines of code than possible in languages such as C++ or Java. The language provides constructs intended to enable writing clear programs on both a small and large scale.[3]

The primary reasons for using Python for this project where:

- Python supports multiple programming paradigms, including object-oriented, imperative, functional programming, and procedural styles. It features a dynamic type system and automatic memory management and has a large and comprehensive standard library.[3]
- Python has a large standard library, commonly cited as one of Python's greatest strengths, providing tools suited for many tasks. This is deliberate and has been described as a "batteries included" Python philosophy. For Internet-facing applications, many standard formats and protocols (such as MIME and HTTP) are supported. Modules for creating graphical user interfaces, connecting to relational databases, pseudorandom number generators, arithmetic with arbitrary precision decimals, manipulating regular expressions, and doing unit testing are also included. [3]
- Python network programming capabilities: Python provides access to the same low-level socket APIs as in C. As the core of this project relates to network and Internet functionalities, the abilities to have a fine-grained control over functionalities and implementation where an important asset.

Python version 3.5 was used for this project.

11.1.2 Django

Official website: https://www.djangoproject.com/

Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of Web development, so you can focus on writing your app without needing to reinvent the wheel. It's free and open source.[10]

The primary reason for using Django for this project was how fast it is to develop complete applications in this framework, while leveraging all the functionalities provided by the Python programming language. The availability of third party applications was also a determining aspect.

Django version 1.10.3 was used for this project.

11.1.3 Python Libraries & Django Apps

In addition to the Python programming language and the Django framework, many third-party libraries and Django apps where used. The most relevant ones are:

- Requests
  Requests is an elegant and simple HTTP library for Python, built for human beings.
- Beautiful Soup
  Beautiful Soup is a Python library for pulling data out of HTML and XML files. It leverages a XML/HTML parser to provide idiomatic ways of navigating, searching, and modifying the parse tree.[5]
- lxml
  lxml is the most feature-rich and easy-to-use library for processing XML and HTML in the Python language.9 It is used by the beautifulsoup4 library to parse HTML content.[6]
- tldextract
  tldextract is a Python library that accurately separates the gTLD or ccTLD (generic or country code top-level domain) from the registered domain and subdomains of a URL. For example, say you want just the 'google' part of 'http://www.google.com'. tldextract on the other hand knows what all gTLDs and ccTLDs look like by looking up the currently living ones according to the Public Suffix List. So, given a URL, it knows its subdomain from its domain, and its domain from its country code.[7]
- fake-useragent

fake-useragent is a Python library to fake the user-agent of requests using a real world database.[8] This is used by CMSpyder to make sure each request uses a unique user-agent, to simulate that the global requests are made by different clients.

- Psycopg

  Psycopg is the most popular PostgreSQL adapter for the Python programming language. At its core it fully implements the Python DB API 2.0 specifications. Several extensions enable access to many of the features offered by PostgreSQL.[9]

11.1.4 Celery

Official website: http://www.celeryproject.org/

Celery is an asynchronous task queue/job queue based on distributed message passing. It is focused on real-time operation, but supports scheduling as well. The execution units, called tasks, are executed concurrently on a single or more worker servers. Tasks can execute asynchronously (in the background) or synchronously (wait until ready).[11]

The Eventlet library was used for execution pool implementation. Eventlet is a concurrent networking library for Python that implements highly scalable non-blocking I/O.[12] The rationale for using Eventlet is that the tasks handled by CMSpyder are essentially network-driven, meaning that the tool makes a large number of HTTP requests and analyses the responses independently of each other. Eventlet enables to efficiently spawn a large number of asynchronous, non-blocking threads.

11.1.5 PostgreSQL

Official website: https://www.postgresql.org/

PostgreSQL is a powerful, open source object-relational database system. It has more than 15 years of active development and a proven architecture that has earned it a strong reputation for reliability, data integrity, and correctness. It runs on all major operating systems. It is fully ACID compliant, has full support for foreign keys, joins, views, triggers, and stored procedures (in multiple languages). It includes most SQL:2008 data types, including INTEGER, NUMERIC, BOOLEAN, CHAR, VARCHAR, DATE, INTERVAL, and TIMESTAMP. It also supports storage of binary large objects, including pictures, sounds, or video. It has native programming interfaces for C/C++, Java, .Net, Perl, Python, Ruby, Tcl, ODBC, among others, and exceptional documentation.[13]

The primary reason for using PostgreSQL is it's out of the box support by Django. Django is a database-agnostic web framework, in which you define database models that are then translated by the framework in SQL operations. This allows for rapid prototyping and development. For this project, the database is used to store all the analyzed domains, as well as the results of the analysis.

11.1.6 RabbitMQ

Official website: https://www.rabbitmq.com/

RabbitMQ is open source message broker software (sometimes called message-oriented middleware) that implements the Advanced Message Queuing Protocol (AMQP). Client libraries to interface with the broker are available for all major programming languages.[14] RabbitMQ works as a messaging broker - an intermediary for messaging. It provides applications a common platform to send and receive messages, and messages a safe place to live until received.[15]

RabbitMQ is used by CMSpyder as a task queue, used to send asynchronous messages to the workers. These tasks contain the domains which must be analyzed by the workers. This message broker was used based on its flexibility and reliability.

11.2 Architecture

The following figure illustrates the architecture of the presented framework:

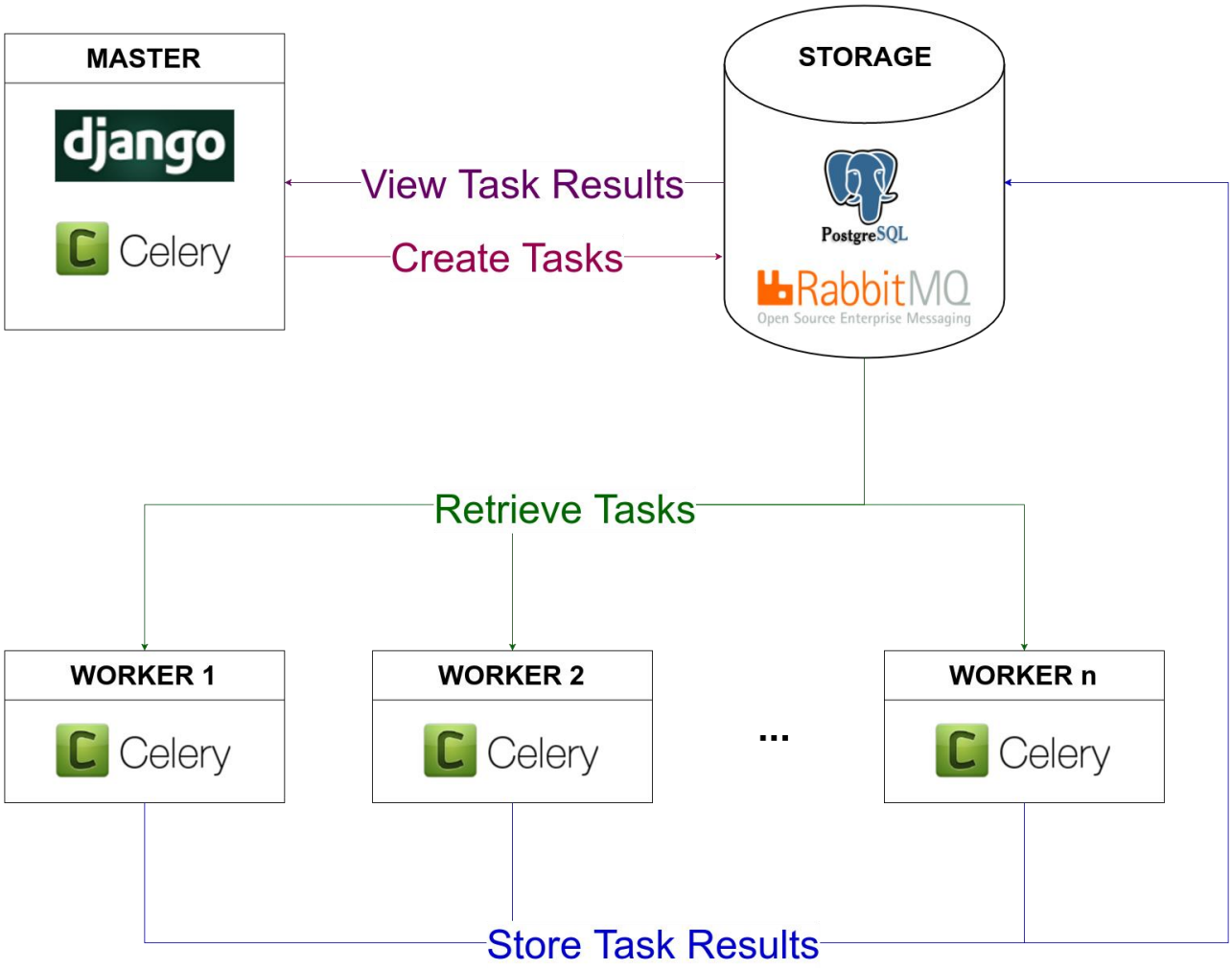

Figure 4 CMSpyder Architecture

This architecture relies on a centralized database and job queue. A number of independent workers pull jobs (i.e. websites that need to be analyzed) from the job queue, and return the results to the database. A master node fills the job queue, and enables analysis of results stored in the database, through a publicly accessible web interface.

11.3 Analysis Workflow

The process is as follows:

1. Master node retrieves a list of websites from the database.
    1) The selected websites are those that have not been analyzed yet, or have been analyzed the longest time ago.
2. Master node takes that list of websites and passes it to the task queue.
3. The workers retrieve tasks from the task queue.
    1) Each task is a website to analyze:
        i. The worker fetches the content.
        ii. The worker analyzes the content to fingerprint potential CMSs.
        iii. The worker analyzes the content to find new websites.
4. The worker stores the results in the database.
5. This process is automated and does not require any user interaction.

11.3.1 Workflow Illustration

While the process explained in the previous session designed to be is automated, it can also be done manually. This section explains these steps. The following figure illustrates the administration panel:

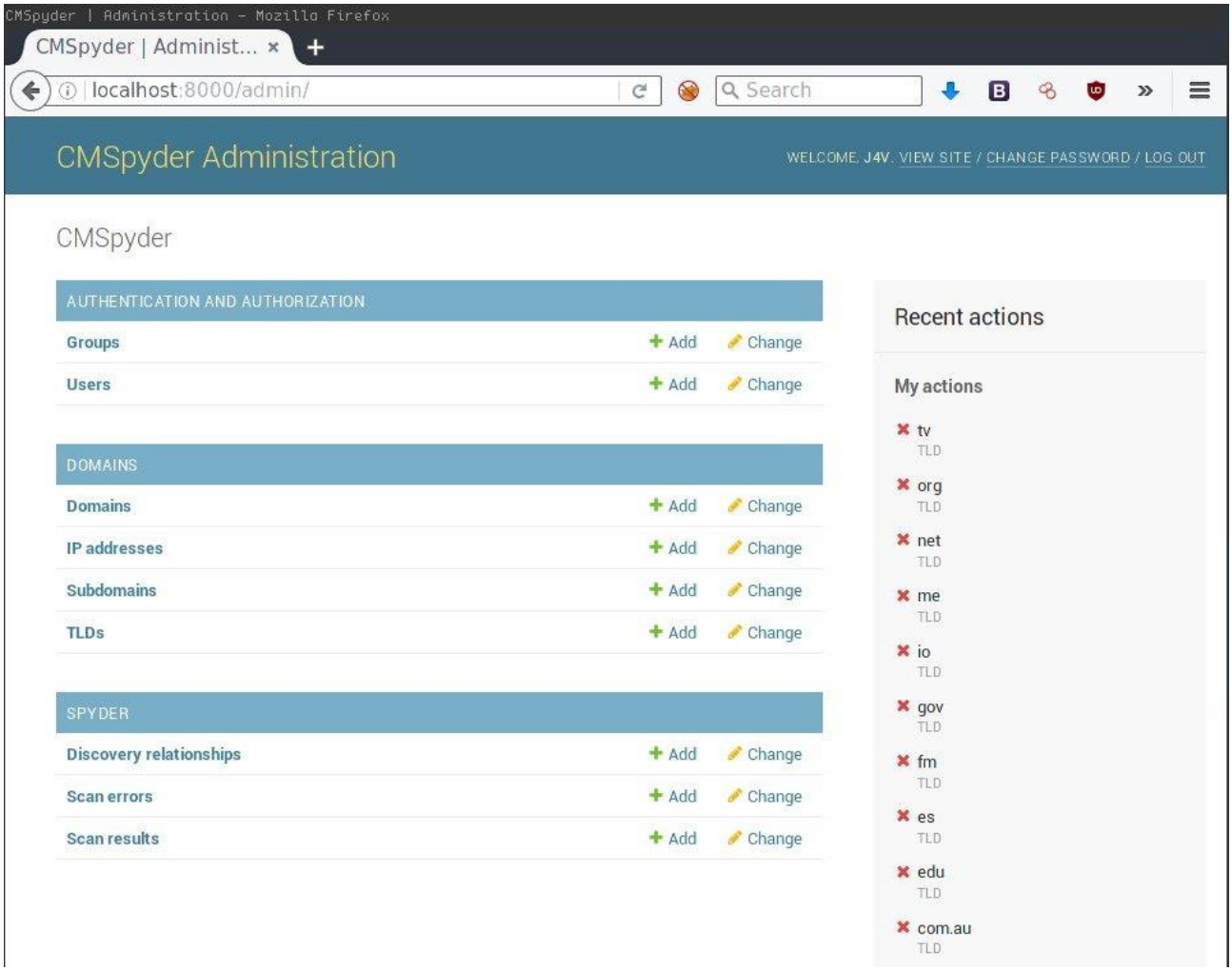

Figure 5 Administration Panel

The sections shown above are:

1. Authentication and Authorization
    i. Groups

    Groups can be created so as to assign different levels of authorization to different users. For example, a group could be created to enable members to access scan results, but not created new scan jobs.

    ii. Users

    Multiple users assigned to different groups can be created through the web interface.
2. Domains

    This encompasses how domain-related information is structured in the proposed too.

    i. Domains

    A domain (e.g. “google.com” or “unir.net”) to which multiple subdomains may belong to.

    ii. IP addresses

    An IP address (e.g. “127.0.0.1” or “192.168.0.1”) to which one or many subdomains may have been found to resolve.

    iii. Subdomains

    A unique subdomain (e.g. “translate.google.com” or campusingenieria.unir.net”).

    iv. TLDs

    A Top Level Domain (TLD, e.g. “.com” or “.net”) to which multiple domains and subdomains may belong to.
3. Spyder

    This encompasses how analysis-related information is structures in the proposed tool.

    i. Discovery relationships

    One of the steps of analyzing a website is uncovering new websites by parsing the HTML content. Discovery relationship enables us to keep track of what websites point us to new ones.

    ii. Scan errors

    Each time a scan job generates an error, a log entry is created. This enables improvement of the tool.

iii. Scan results

Results for every successful fingerprinting, including the fingerprinted CMS version, as well as the version, in the case it was possible to detect.

The following figure illustrates the initialization of the celery process:

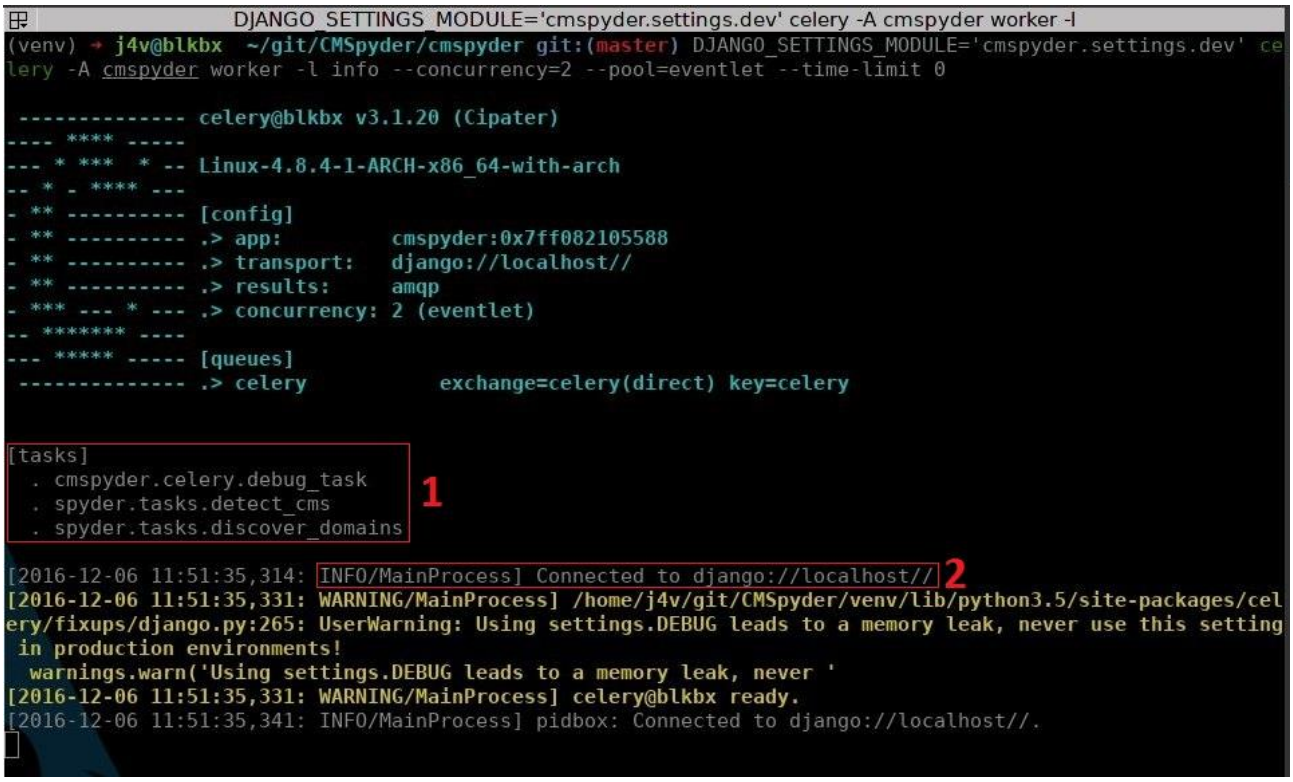

Figure 6 Celery Initialisation

The following are highlighted in the previous figure:

- Tasks

  The different tasks that a worker will process.

  - cmspyder.celery.debug_task

    Debugging task, to show errors and progress.

  - spyder.tasks.detect_cms

    Fingerprinting task, to discover a website's CMS and version.

  - spyder.tasks.discover_domains

    Domain discovery task, to find new subdomains to analyze.

- Connection to the job queue from which new jobs will be fetched.

At this point, all we have is an empty database. We will start by creating a new TLD (“org”), domain (“drupal.org”) and subdomain (“drupal.org”):

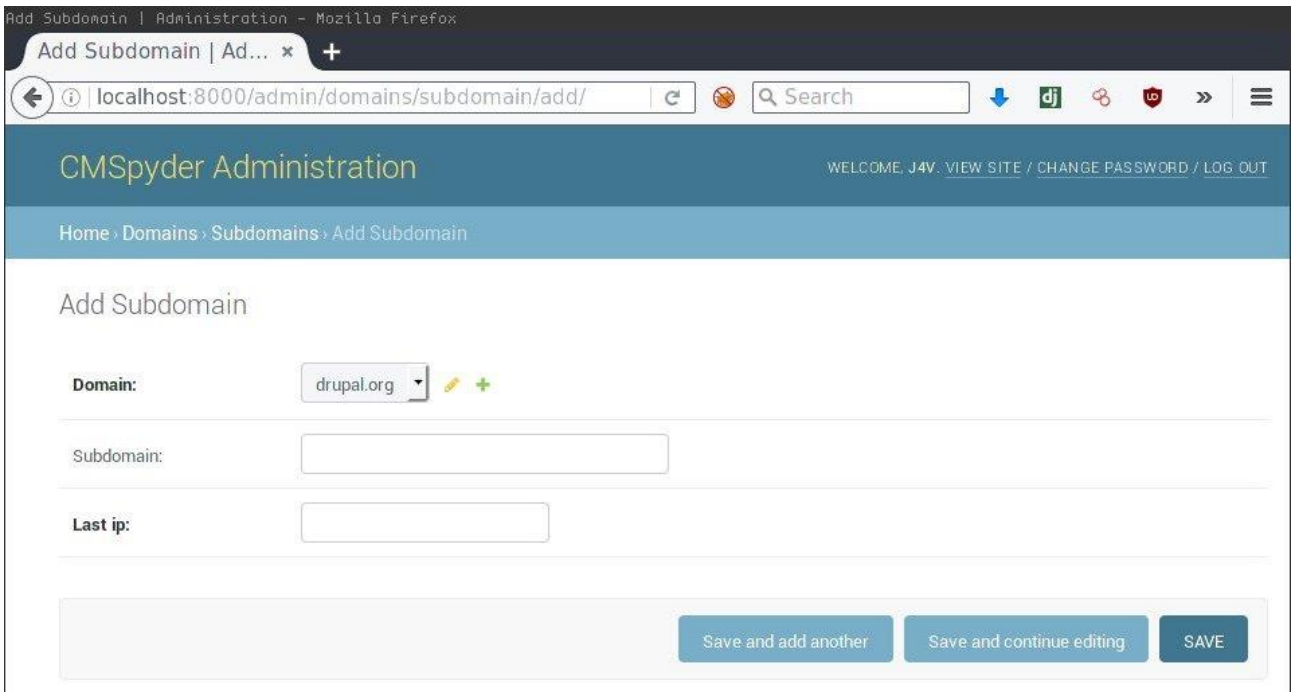

Figure 7 Addition of a new Domain and Subdomain

Once we “save”, the new subdomain appears in the panel:

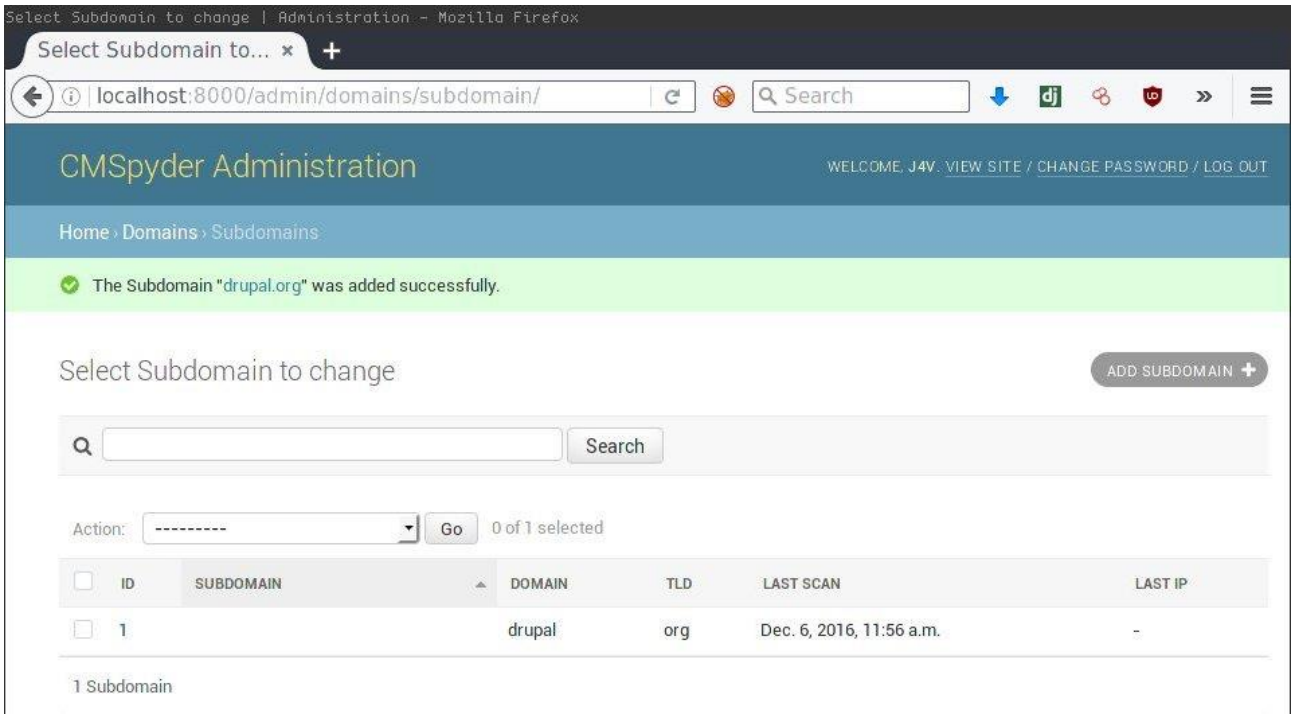

Figure 8 New Domain and Subdomain

To launch analysis jobs from the administration panel, we select the desired subdomains in the checkbox, and click on the “Detect CMS” action:

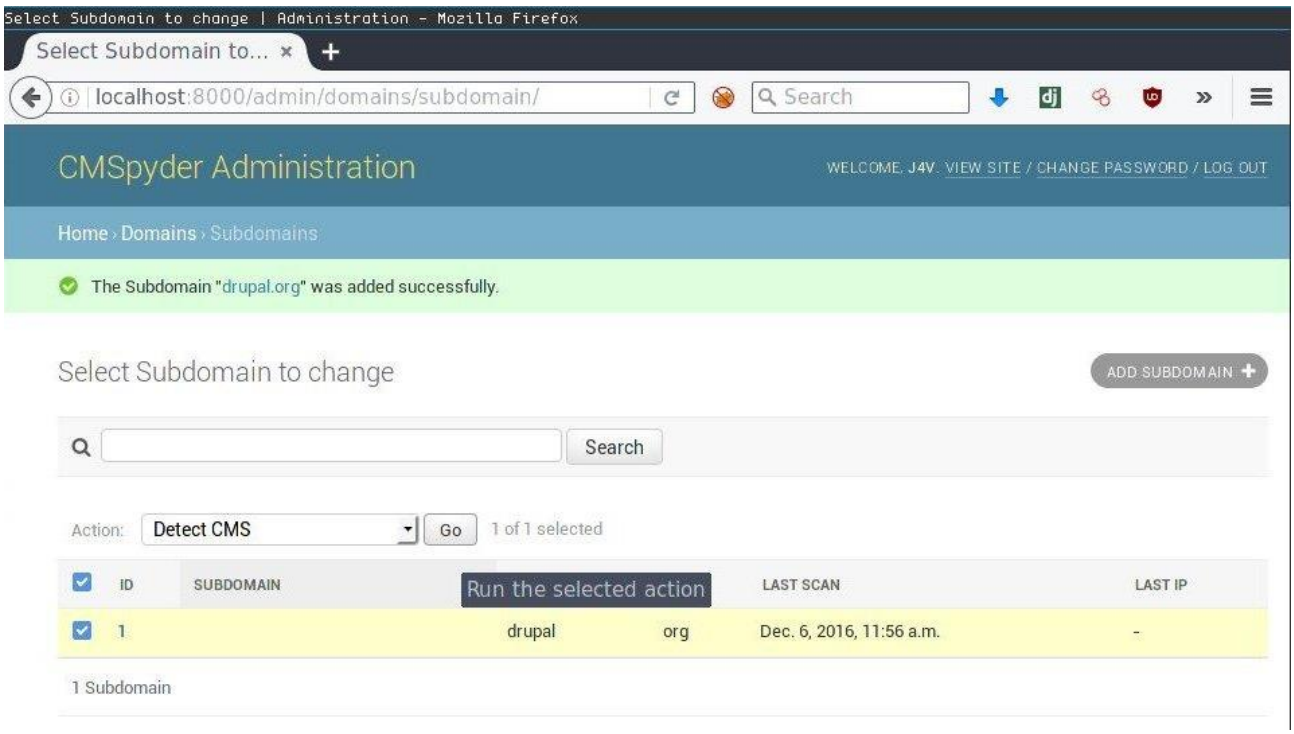

Figure 9 Running Analysis of Selected Subdomain

Once the tasks have been created, the celery process will pull them from the queue and start working:

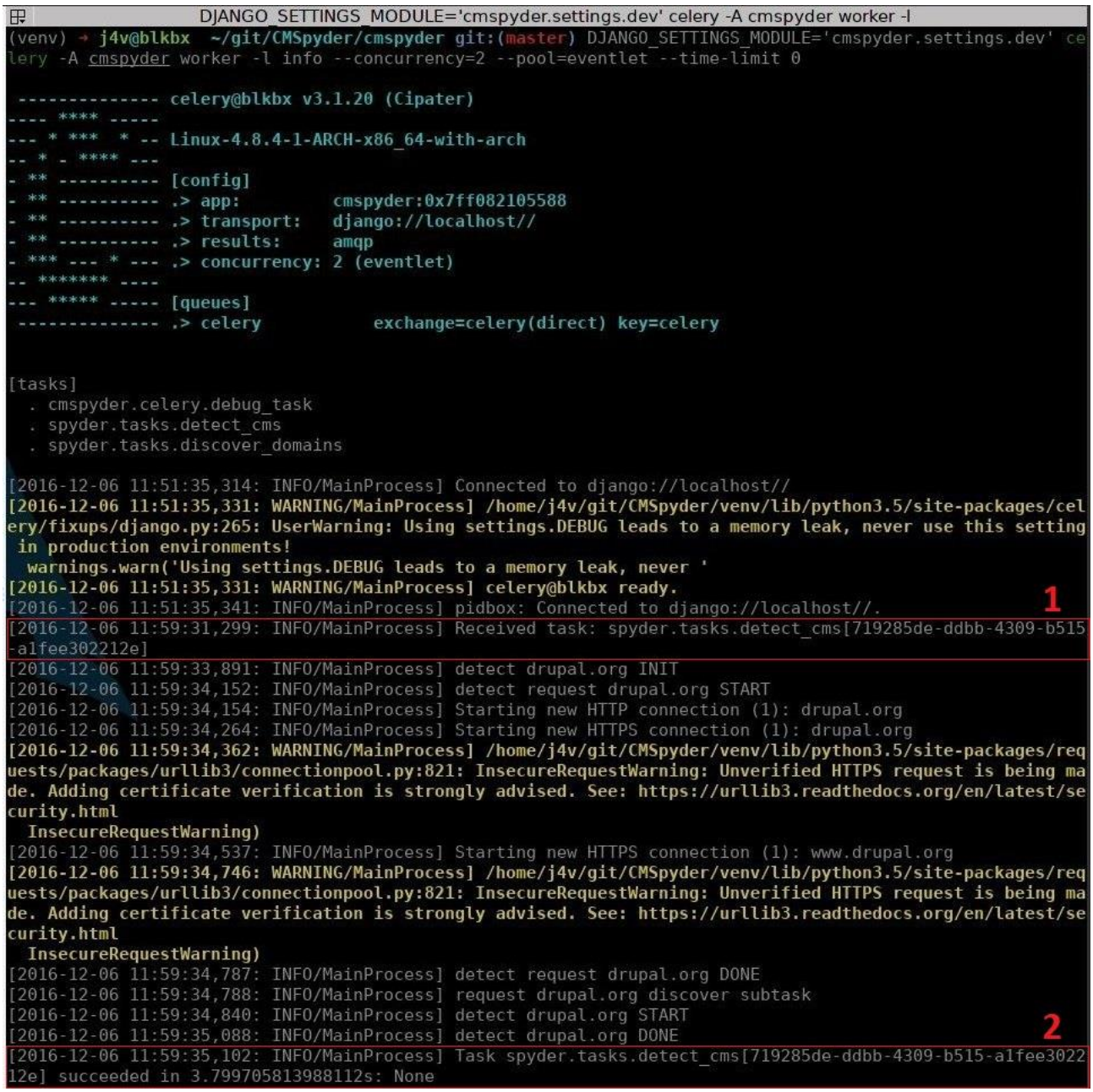

Figure 10 Celery Detection Task

In the previous figure, we can see the spyder.tasks.detect_cms task being executed.

Once the spyder.tasks.detect_cms task is completed, the spyder.tasks.discover_domains tasks starts, as shown in the following figure:

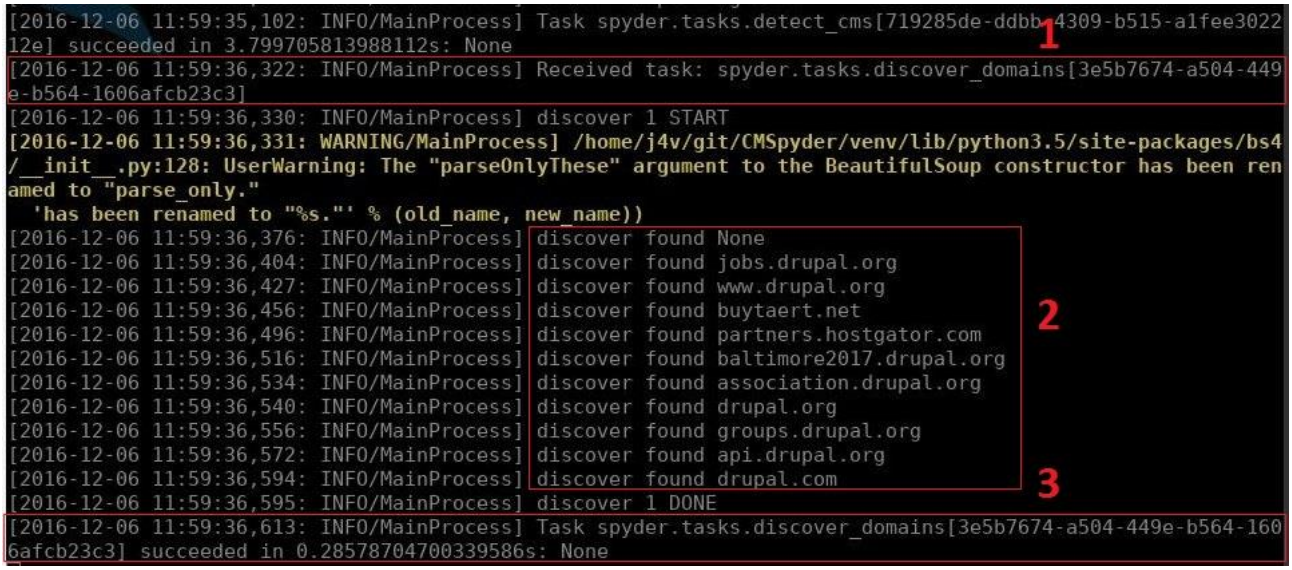

Figure 11 Celery Discovery Task

As the analyzed website was running Drupal, a new entry is created and visible in the administration panel:

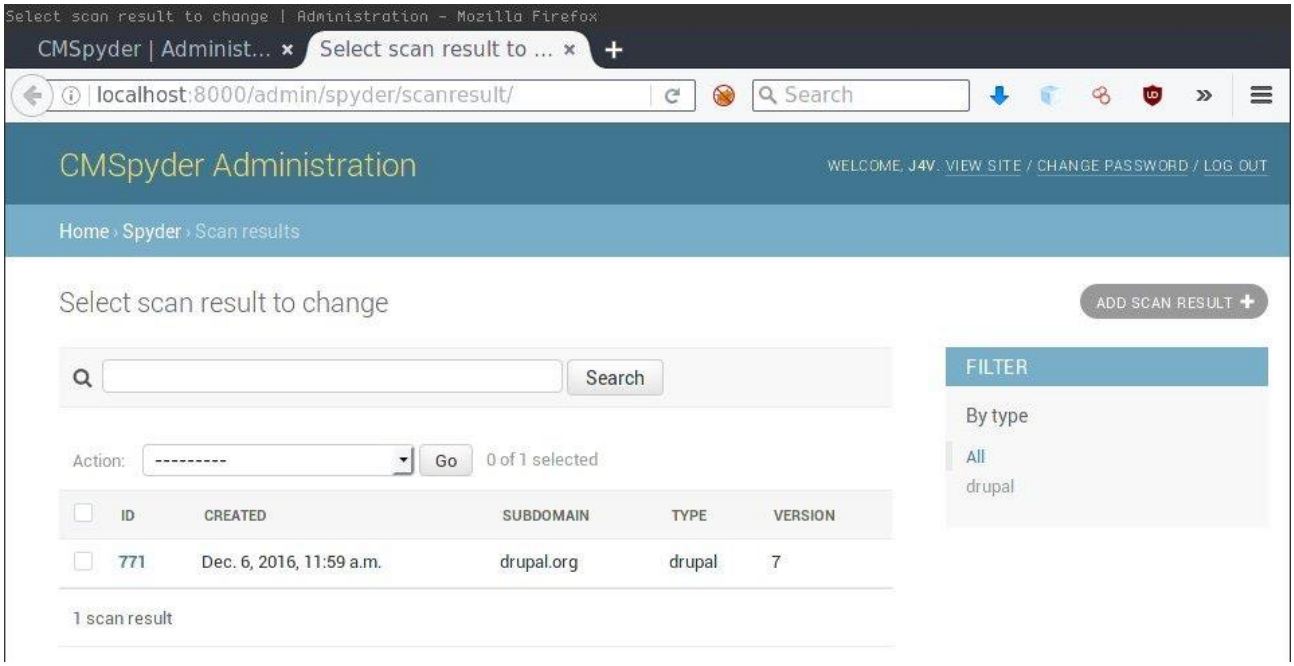

Figure 12 Detection Result

CMSpyder also detects that the version of Drupal running is version 7.

The discovery task also found many new websites on “drupal.org”. These are now visible in the subdomain page:

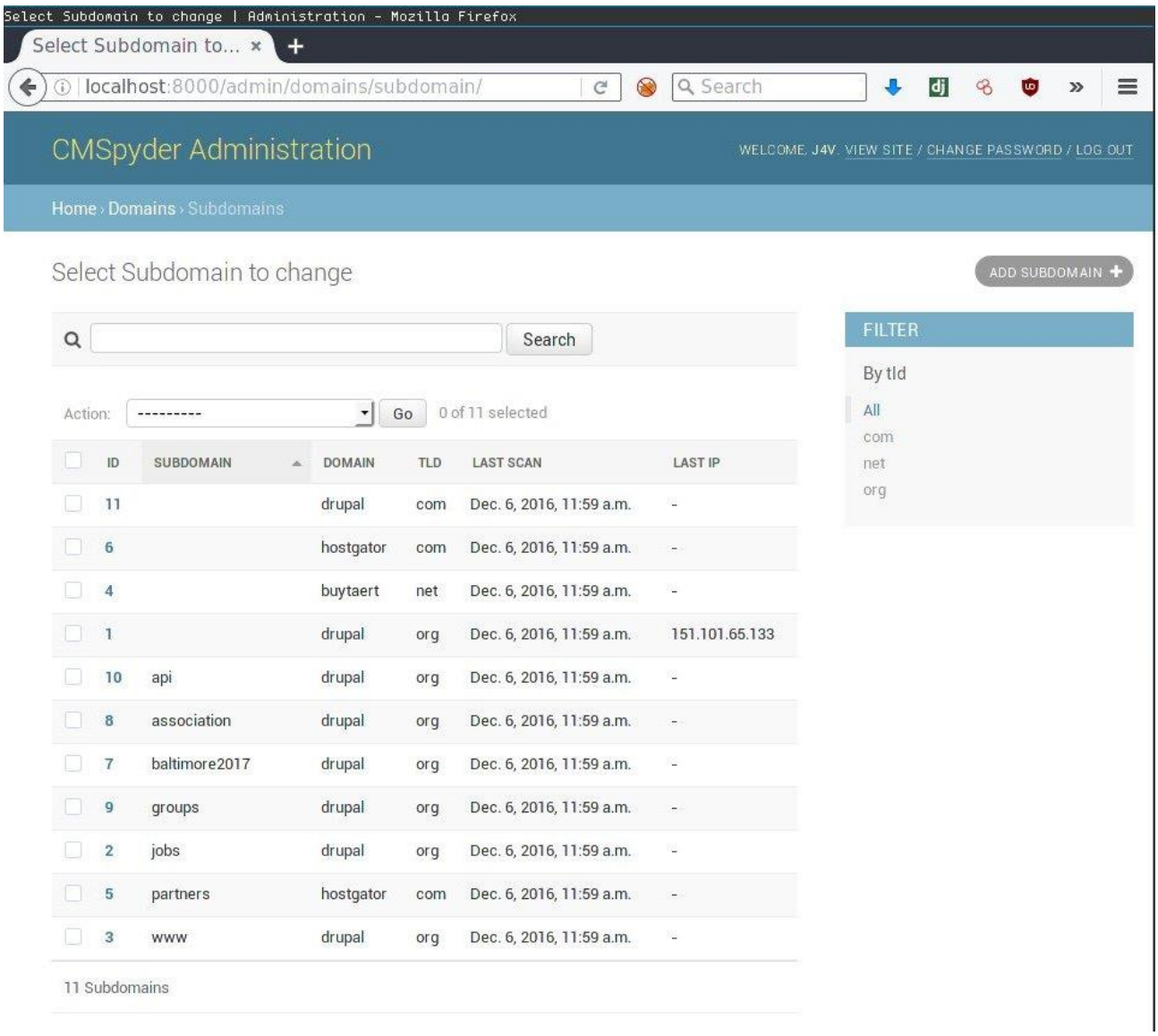

Figure 13 Discovery Result

The discovery relationship page keeps track of on what subdomain a given subdomain was first discovered. As shown on the following figure, all subdomains where discovered on “drupal.org”:

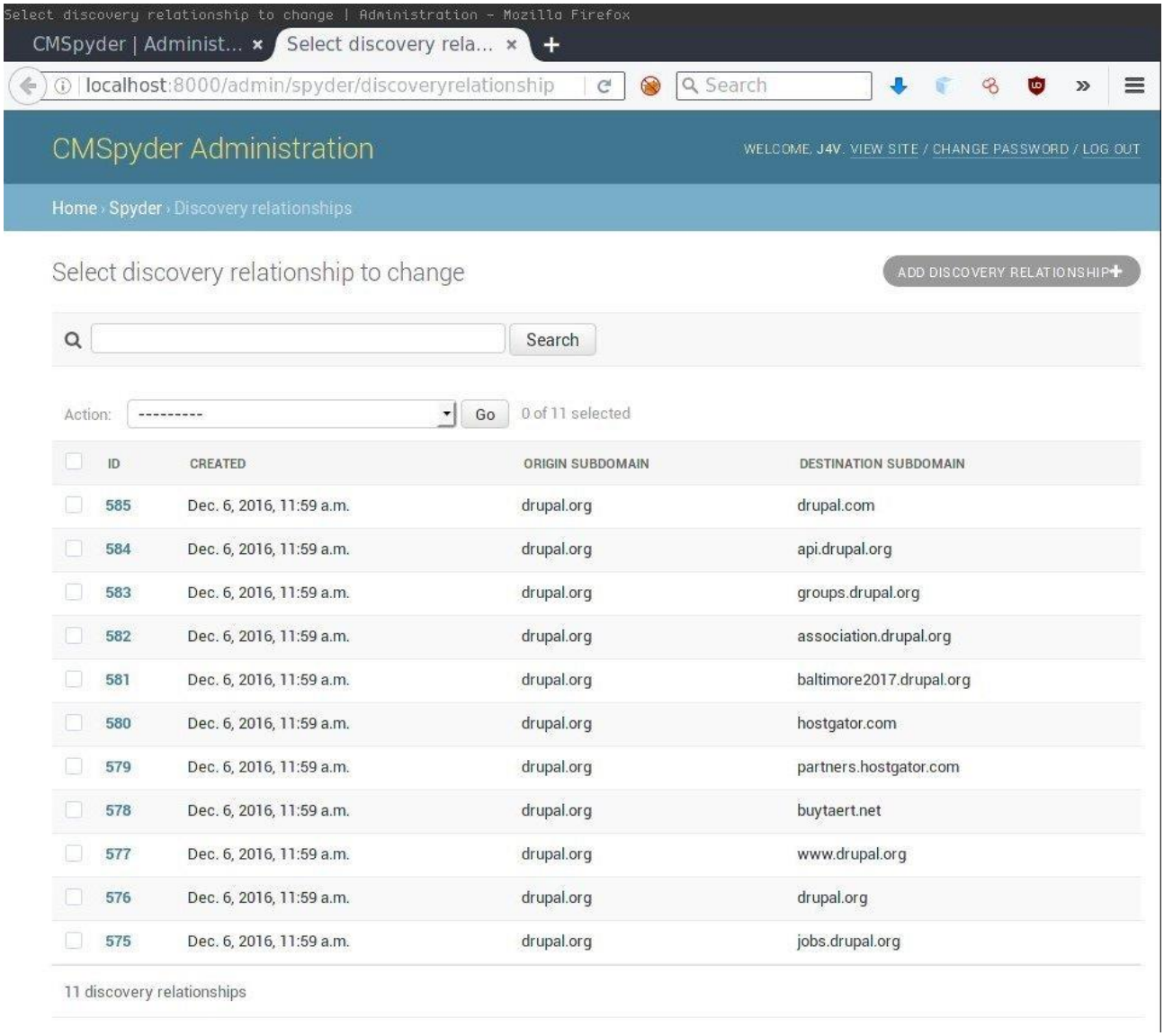

Figure 14 Subdomain Discovery Relationship

11.4 Experiment Resources

To run the developed tool, 8 machines where rented from a virtual private server. A virtual private server (VPS) is a virtual machine sold as a service by an Internet hosting service[36]. The VPS chosen is time4vps.eu, which is based in Lithuania and uses the OpenVZ operating system-level virtualization technology.

The virtual hardware is as follows:

- 1 Master node
    - 2 x 2.40 GHz CPU
    - 2048 MB RAM
    - 80 GB Storage
- 1 Storage node
    - 1 x 1.90 GHz CPU
    - 1024 MB RAM
    - 1024 GB Storage
- 6 Worker nodes
    - 1 x 2.40 GHz CPU
    - 1024 MB RAM
    - 40 GB Storage

These machines where run during a course of two weeks.

The initial seed used is the Alexa top million as seed[37]. Alexa Internet, Inc. is a California-based company that provides commercial web traffic data and analytics. Its toolbar collects data on browsing behavior and transmits them to the Alexa website, where they are stored and analyzed, forming the basis for the company's web traffic reporting. Alexa provides traffic data, global rankings and other information on 30 million websites[38].

11.5 Results

The tool was run non-stop during two weeks. While we started with a list of 1000000 websites, this list grew to 12003512, meaning that 11003512 new unique domains where identified. Of these new domains, 3765430 where analyzed, which accounts for 31% of all known domains. Of analyzed domains, 927417 where successfully fingerprinted, meaning that the presence of a CMS was established. This accounts for 24% of analyzed domains, and 7% of unique domains.

In this section, we will present the results of the analysis. We will then define the baseline for what versions of WordPress, Drupal and Joomla are considered vulnerable. By crossing both datasets, we will conclude what proportion of websites are considered to be vulnerable.

11.5.1 Results for WordPress

The following figure illustrates the version fingerprinting data for WordPress:

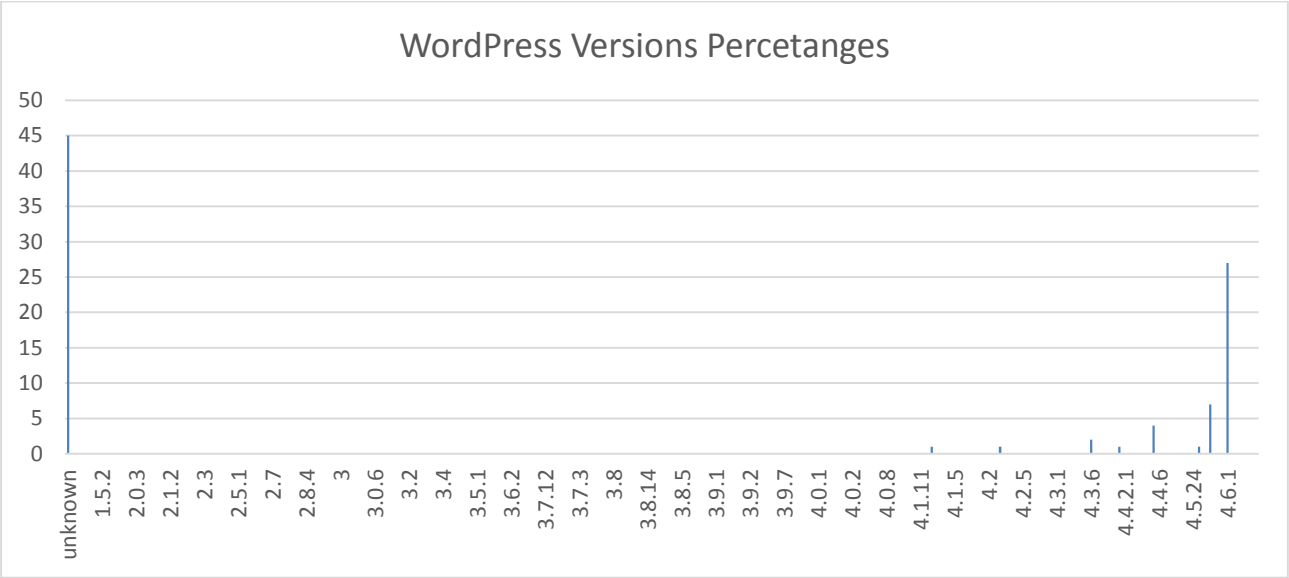

Figure 15 WordPress Versions Percentages

A total of 662813 instances where fingerprinted as WordPress, which represents 71% of fingerprinted domains. This is consistent with public reports (see review of literature section). Of these, it was impossible to establish the version running on 45% of websites known to be WordPress.

The following table summarizes the detected major versions and their release dates[35]:

Major Version	Release Date	Detection Count	Detection Percentage (%)
1	January 3, 2004	14	0.004
2	December 26, 2005	1730	0.434
3	June 17, 2010	29324	7.349
4	September 4, 2014	367957	92.214

Table 4 WordPress Major Versions Fingerprinted

While around 92% of fingerprinted WordPress installations are running on the major branch, there is a non-negligible percentage running on severely outdated versions.

Within the WordPress installations running on version 4, 50% where found to be running version 4.6.1 (367957 out of 185511). Version 4.6.1 was the latest stable version at the time of the scan. This probably represents the instances that have the “automatic update” functionality enables.

11.5.2 Results for Drupal

The following figure illustrates the version fingerprinting data for Drupal:

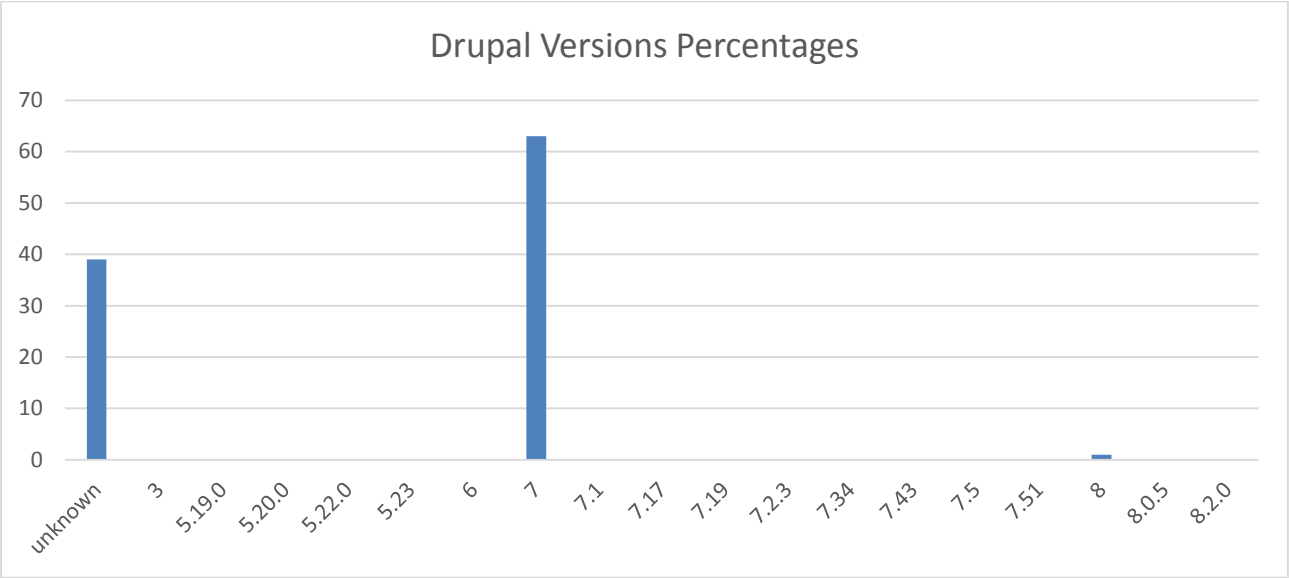

Figure 16 Drupal Versions Percentages

A total of 88389 instances where fingerprinted as Drupal, which represents 9% of fingerprinted domains. Of these, it was impossible to establish the version running on 62% of websites known to be Drupal.

The following table summarizes the detected minor versions and their release dates[40]:

Major Version	Release Date	Detection Count	Detection Percentage (%)
3	Unknown	2	0.0
4	March 8, 2005	0	0.0
5	January 15, 2007	8	0.0
6	February 13, 2008	8	0.0
7	January 5, 2011	55917	97.4
8	November 19, 2015	1482	2.6

Table 5 Drupal Major Versions Fingerprinted

While the detection count is trivial for versions 3 to 6, it would be surprising that the number of websites running on these versions is so low. A more likely explanation is that the detection capabilities for these versions is not as good as it is for versions 7 and 8. This would also explain why it was not possible to fingerprint versions for almost 40% of websites known to run on Drupal.

11.5.3 Results for Joomla

The following figure illustrates the version fingerprinting data for Joomla:

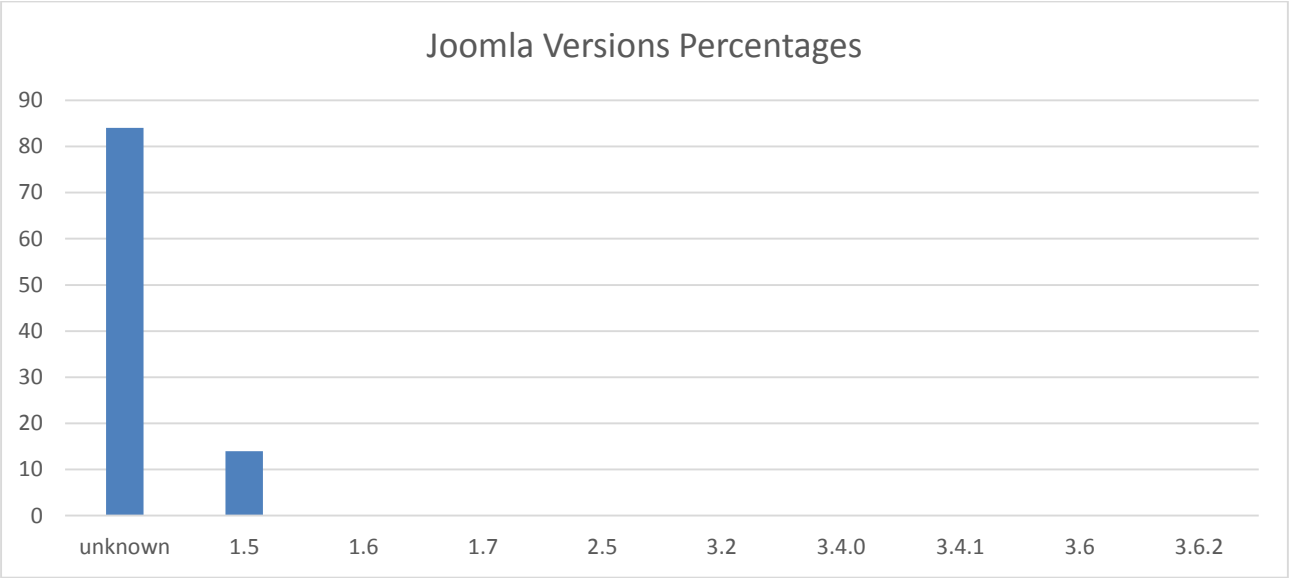

Figure 17 Joomla Versions Percentages

A total of 66144 instances where fingerprinted as Joomla, which represents 7% of fingerprinted domains. Unfortunately, very little versions where appropriately fingerprinted and account for 18% of fingerprinted Joomla instances. This is most likely due to the limitation of our version fingerprinting method, which may not apply well to the architecture of this CMS.

The following table summarizes the detected minor versions and their release dates[39]:

Minor Version	Release Date	Detection Count	Detection Percentage (%)
1.5	January 22, 2008	9537	93.23
1.6	January 10,2011	227	2.22
1.7	July 19, 2011	447	4.37
2.5	January 24, 2012	10	0.10
3.2	November 6, 2013	2	0.02
3.4	February 24, 2015	3	0.03
3.6	July 12, 2016	4	0.04

Table 6 Joomla Minor Versions Fingerprinted

It is interesting to observe that, contrary to WordPress and Drupal detections, for Joomla there is greater detection levels for older versions. This is likely due to an increased difficulty in version fingerprinting for the later versions of this CMS. Future works should improve detection methods, otherwise important data will not be acquired.

11.6 Result analysis

In this section, we identify the vulnerable versions of studied CMSs and determine metrics for what percentage is considered to be vulnerable.

11.6.1 CMS Vulnerabilities

The first step is to identify all reported CVEs for WordPress, Drupal and Joomla [26] [27] [28] [29] [30] [31] [32].

11.6.1.1 WordPress Vulnerabilities

The following high-criticality vulnerabilities have been reported:

CVE ID	Score	Description
CVE-2012-2400	10	Unspecified vulnerability in wp-includes/js/swfobject.js in WordPress **before 3.3.2** has unknown impact and attack vectors.
CVE-2011-3125	10	Unspecified vulnerability in WordPress **3.1 before 3.1.3 and 3.2 before Beta 2** has unknown impact and attack vectors related to "Various security hardening."
CVE-2011-3122	10	Unspecified vulnerability in WordPress **3.1 before 3.1.3 and 3.2 before Beta 2** has unknown impact and attack vectors related to "Media security."
CVE-2009-2853	10	Wordpress **before 2.8.3** allows remote attackers to gain privileges via a direct request to (1) admin-footer.php, (2) edit-category-form.php, (3) edit-form-advanced.php, (4) edit-form-comment.php, (5) edit-link-category-form.php, (6) edit-link-form.php, (7) edit-page-form.php, and (8) edit-tag-form.php in wp-admin/.
CVE-2008-6767	10	wp-admin/upgrade.php in WordPress, probably **2.6.x**, allows remote attackers to upgrade the application, and possibly cause a denial of service (application outage), via a direct request.
CVE-2006-4028	10	Multiple unspecified vulnerabilities in WordPress **before 2.0.4** have unknown impact and remote attack vectors. NOTE: due to lack of details, it is not clear how these issues are different from CVE-2006-3389 and CVE-2006-3390, although it is likely that 2.0.4 addresses an unspecified issue

		related to "Anyone can register" functionality (user registration for guests).
CVE-2011-3129	9,3	The file upload functionality in WordPress **3.1 before 3.1.3 and 3.2 before Beta 2**, when running "on hosts with dangerous security settings," has unknown impact and attack vectors, possibly related to dangerous filenames.
CVE-2008-4769	9,3	Directory traversal vulnerability in the get_category_template function in wp-includes/theme.php in WordPress **2.3.3 and earlier, and 2.5**, allows remote attackers to include and possibly execute arbitrary PHP files via the cat parameter in index.php. NOTE: some of these details are obtained from third party information.
CVE-2008-2392	9	Unrestricted file upload vulnerability in WordPress **2.5.1 and earlier** might allow remote authenticated administrators to upload and execute arbitrary PHP files via the Upload section in the Write Tabs area of the dashboard.

Table 7 High Vulneratibilities in WordPress

According to these reports, the following versions of WordPress are vulnerable[25]:

- Bellow 3.3.2
- Equal to 3.2 Beta 1
- From 3.1 to 3.1.2
- Bellow 2.8.3
- Equal to 2.6.x branch
- Bellow 2.5.1
- Equal to 2.5
- Bellow or equal to 2.3.3
- Bellow 2.0.4

We can therefore establish that any WordPress installation bellow version 3.3.2 is considered to be vulnerable.

11.6.1.2 Drupal Vulnerabilities

The following high-criticality vulnerabilities have been reported:

CVE ID	Score	Description
CVE-2008-6171	9,3	includes/bootstrap.inc in Drupal **5.x before 5.12** and **6.x before 6.6**, when the server is configured for "IP-based virtual hosts," allows remote attackers to include and execute arbitrary files via the HTTP Host header.

Table 8 High Vulneratibilities in Drupal

According to these reports, the following versions of Joomla are vulnerable[40]:

- From 5.0-beta1 to 5.11
- From 6.x-dev to 6.5

We can therefore establish that any Drupal installation within those versions is considered to be vulnerable.

11.6.1.3 Joomla Vulnerabilities

The following high-criticality vulnerabilities have been reported:

CVE ID	Score	Description
CVE-2008-3225	10	Joomla! **before 1.5.4** allows attackers to access administration functionality, which has unknown impact and attack vectors related to a missing "LDAP security fix."
CVE-2006-1047	10	Unspecified vulnerability in the "Remember Me login functionality" in Joomla! **1.0.7 and earlier** has unknown impact and attack vectors.
CVE-2006-0303	10	Multiple unspecified vulnerabilities in the (1) publishing component, (2) Contact Component, (3) TinyMCE Compressor, and (4) other components in Joomla! **1.0.5 and earlier** have unknown impact and attack vectors.
CVE-2005-3773	10	Unspecified vulnerability in Joomla! **before 1.0.4** has unknown impact and attack vectors, related to "Potential misuse of Media component file management functions."
CVE-2007-4188	9,3	Session fixation vulnerability in Joomla! **before 1.0.13** (aka Sunglow) allows remote attackers to hijack administrative web sessions via unspecified vectors.

Table 9 High Vulneratibilities in Joomla

According to these reports, the following versions of Joomla are vulnerable:

- Bellow 1.5.4
- Bellow 1.0.8
- Bellow 1.0.6
- Bellow 1.0.4
- Bellow 1.0.13

We can therefore establish that any Joomla installation bellow version 1.5.4 is considered to be vulnerable.

11.6.2 Vulnerable Websites

Taking into account the fingerprinted CMS versions and versions of these CMSs considered as vulnerable as per the preceding4 subsections, we draw the following conclusions.

In the case of WordPress, versions bellow 3.3.2 are considered as vulnerable. This represents 5667 unique fingerprinted instances, or 0.8% of all WordPress instances and 1.4% of all WordPress instances for which we know the version.

In the case of Drupal, the versions considered to be vulnerable are in branch 5 and 6. Only 6 Drupal websites where found to be in branch 6.x, which it marginal. It is therefore impossible to draw conclusions on the amount of vulnerable Drupal instances.

Finally, in the case of Joomla, versions in branch 1.5.x or bellow are considered vulnerable. This represents 9537 unique fingerprinted instances, or 14% of all Joomla instances and 94% of Joomla instances for which we know the version.

While these results are not groundbreaking, they are consistent with what we have seen all through this project. An important element is that not only where we unable to fingerprint versions for a large amount of analyzed websites, in most cases the analysis was concentrated in a limited scope of versions. While this may be due to the fact that most websites may be running on a few versions, it is also likely due to uneven fingerprinting capabilities between versions, because of changes in the code and architecture of CMSs.

We should underline that by concentrating our analysis to the core of CMSs (i.e. excluding configuration issues, plugins and third-party code), we limited the scope of what was considered vulnerable. This is also consistent with the conclusions of Sucuri's Q1 2016 "Website Hacked Trend Report", which concludes that, in most instances, the compromises analyzed had little, if anything, to do with the core of the CMS application itself, but more with improper deployment, configuration, and overall maintenance by the webmasters and their hosts.[43]

12 Contributions

The major contribution of this project is that it provided consistent empirical data with a defined methodology and reproducible results. This was done through the development of an expandable, modular and reusable framework.

While the results seem minor, this is likely attributable to the scope of the project and the established metrics. Indeed, by only analyzing the core of CMS projects, a lot is left behind. Had we expanded the methodology to plugins, we would likely have gotten better results. It is also important to underline that we only analyses the three major content management systems. While these are widely adopted, they are also under more scrutiny and likely that the core has less vulnerabilities. Also excluding plugins means that many websites that where considered to not be vulnerable may well be.

Fingerprinting method did not apply well to Joomla, which was shown by this work. This means that it is necessary to do further research in fingerprinting techniques. This should include active analysis of websites (e.g. searching for known files that would provide additional information), amongst other methods.

All the data is public and the code is re-usable, so that it can be picked up at any time by anyone who would like to continue development, re-run the tests or define different metrics.

13 Future Works

While this project has provided good results, it's most important contribution is that if provides a framework on which others can build. The most improvable aspects are fingerprinting capabilities and scalability.

The roadmap for future work contains:

- Distributed architecture
  While the current architecture is monolithic and centralized, a distributed architecture would provide better scalability.
- Version fingerprinting
  The version fingerprinting provided by the Wappalyzer project relies on a single web page. This passive approach could be improved by actively searching for files that could reveal the running version.
- Plugin detection
  It is widely known that third-party plugins are responsible for many vulnerabilities in content management system. Fingerprinting these plugins and their versions in the same way as we have done for the core would most likely provide significant results.
- Active analysis
  The analysis of the current framework is based on a single request made to the "/" or "index" of the website. An active approach targeting CMS-specific files would likely unable to fingerprint a greater proportion of websites.

13.1 Distributed architecture

The following figure illustrates the proposed architecture for the next version of the framework:

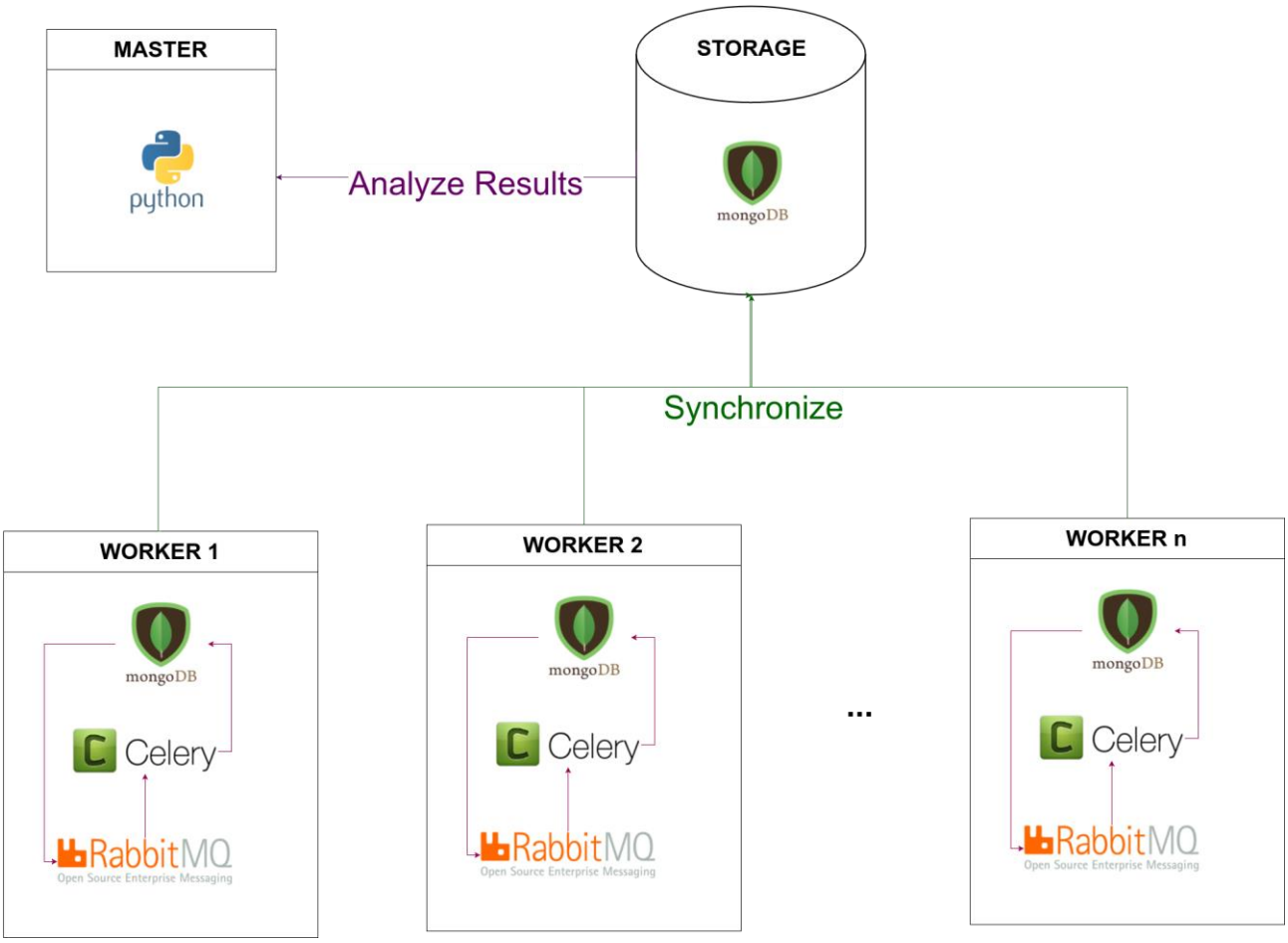

Figure 18 CMSpyder v2 Architecture

Instead of having a single relational database to keep all the data, each scanner instance will maintain a local non-relational database, as well as a job queue. A central database will maintain a copy of all the data, so that it can be queried to analyze global results. This architecture will minimize the network load as workers will not have to constantly request for jobs and send back results over the network.

13.2 Plugins Analysis

Checkmarx is a source code analysis solution that provides tools for identifying, tracking, and repairing technical and logical flaws in the source code, such as security vulnerabilities, compliance issues, and business logic problems.[41] In 2013, Checkmarx presented a report where they presented their findings of running multiple security scans against the source code of WordPress plugins.

These scans where performed on the top 50 most downloaded plugins on two separate occasions. During this survey, Checkmarx54 found 18 vulnerable plugins which amounted to 18.5 million downloads. Furthermore, they identified that more than 20% of the 50 most popular WordPress plugins are vulnerable to common Web attacks, such as SQL Injection. A concentrated research into e-commerce plugins revealed that 7 out of the 10 most popular e-commerce plugins contain vulnerabilities.[42]

14 Conclusions

This project aimed to analyze the prevalence of vulnerable content management systems on the Internet. To accomplish this goal, we developed a framework to analyze websites and fingerprint the code they were running, as well as the versions of known CMSs when possible. Comparing this data to known vulnerabilities, it was possible to establish what proportion of websites could be considered as trivially vulnerable.

While the results of this investigation are not groundbreaking, this project makes some very significant contributions to the state of knowledge. The most significant contribution is the creation of a reusable framework and reproducible methodology, as well as the presentation of hard empiric data – which was found to be critically lacking for this type of investigation.

While a small percentage of websites where found to be vulnerable, this is correlated with the high benchmark for considering a website vulnerable, i.e. running on a version of the CMS core that has at least one critical vulnerability.

Going forward, we present a clear roadmap for the next steps of the investigation. The framework must be improved to allow better scalability, so as to enable analysis of more websites. Improving the fingerprinting capabilities, by adding active analysis as well as by including CMS plugins in the scope of the analysis, will provide much more thorough results.

15 Glossary

Content Management System (CMS)

Computer application that supports the creation and modification of digital content. It is often used to support multiple users working in a collaborative environment. By their nature, content management systems support the separation of content and presentation[2].

Web Content Management System (WCM or WCMS)

CMS designed to support the management of the content of Web pages. Most popular CMSs are also WCMSs. Web content includes text and embedded graphics, photos, video, audio, maps, and code (e.g., for applications) that displays content or interacts with the user[2].

* In this document, we will refer to CMSs and WCMSs interchangeably.

16 References

1. Content Management System Market Share. (n.d.). Retrieved December 4, 2016, from https://wappalyzer.com/categories/cms

2. Content management system. (n.d.). Retrieved December 5, 2016, from https://en.wikipedia.org/wiki/Content_management_system

3. Python (programming language). (n.d.). Retrieved December 5, 2016, from https://en.wikipedia.org/wiki/Python_(programming_language)

4. Requests: HTTP for Humans. (n.d.). Retrieved December 8, 2016, from http://docs.python-requests.org/en/master/

5. Beautiful Soup Documentation. (n.d.). Retrieved December 8, 2016, from https://www.crummy.com/software/BeautifulSoup/bs4/doc/

6. Lxml - XML and HTML with Python. (n.d.). Retrieved December 14, 2016, from http://lxml.de/

7. Kurkowski, J. (2016, October 30). Tldextract - Python Module . Retrieved December 14, 2016, from https://github.com/john-kurkowski/tldextract

8. Kovtun, V. (n.d.). Fake-useragent 0.1.4 : Python Package Index. Retrieved December 14, 2016, from https://pypi.python.org/pypi/fake-useragent

9. Psycopg. (n.d.). Retrieved December 14, 2016, from http://initd.org/psycopg/

10. Django Project. (n.d.). Retrieved December 20, 2016, from https://www.djangoproject.com/

11. Celery Project. (n.d.). Retrieved December 20, 2016, from http://www.celeryproject.org/

12. Eventlet. (n.d.). Retrieved December 20, 2016, from http://eventlet.net/

13. About. (n.d.). Retrieved December 20, 2016, https://www.postgresql.org/about/

14. RabbitMQ. (n.d.). Retrieved December 20, 2016, https://en.wikipedia.org/wiki/RabbitMQ

15. Features. (n.d.). Retrieved December 20, 2016, https://www.rabbitmq.com/features.html

16. About Us. (n.d.). Retrieved January 2, 2017, from https://builtwith.com/about

17. CMS technologies Web Usage Statistics. (n.d.). Retrieved January 2, 2017, from https://trends.builtwith.com/cms

18. About Us. (n.d.). Retrieved January 2, 2017, from https://w3techs.com/about

19. Usage of content management systems for websites. (n.d.). Retrieved January 2, 2017, from https://w3techs.com/technologies/overview/content_management/all

20. Frequently Asked Questions. (n.d.). Retrieved January 2, 2017, from https://w3techs.com/faq

21. Technologies Overview. (n.d.). Retrieved January 2, 2017, from https://w3techs.com/technologies

22. Wappalyzer. (n.d.). Retrieved January 4, 2017, from https://www.wappalyzer.com/

23. AliasIO/Wappalyzer Specification. (n.d.). Retrieved January 4, 2017, from https://github.com/AliasIO/Wappalyzer/wiki/Specification

24. AliasIO/Wappalyzer Wappalyzer/src/apps.json. (n.d.). Retrieved January 4, 2017, from https://github.com/AliasIO/Wappalyzer/blob/master/src/apps.json

25. WordPress.org. (n.d.). Retrieved January 30, 2017, from https://wordpress.org/news/category/releases/

26. Drupal: Vulnerability Statistics. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/product/2387/Drupal-Drupal.html

27. WordPress : Vulnerability Statistics. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/product/4096/Wordpress-Wordpress.html

28. Magento : Vulnerability Statistics. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/vendor/15393/Magento.html

29. Magento Commerce: Vulnerability Statistics. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/vendor/9551/Magentocommerc.html

30. Magento Commerce: Vulnerability Statistics. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/vendor/12466/Magentocommerce.html

31. Joomla: Vulnerability Statistics. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/product/6129/Joomla-Joomla.html

32. Joomla: Vulnerability Statistics. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/product/16499/Joomla-Joomla-.html

33. Common Vulnerabilities and Exposures. (n.d.). Retrieved January 13, 2017, from https://cve.mitre.org/about/

34. Current CVSS Score Distribution For All Vulnerabilities. (n.d.). Retrieved January 13, 2017, from http://www.cvedetails.com/

35. WordPress.org. (n.d.). Retrieved January 30, 2017, from https://codex.wordpress.org/WordPress_Versions

36. Virtual private server. (n.d.). Retrieved January 30, 2017, from https://en.wikipedia.org/wiki/Virtual_private_server

37. Chilton, A. (2015, January 31). Getting the Alexa top 1 million sites directly from the server, unzipping it, parsing the csv and getting each line as an array. Retrieved January 30, 2017, from https://gist.github.com/chilts/7229605

38. Alexa Internet. (n.d.). Retrieved January 30, 2017, from https://en.wikipedia.org/wiki/Alexa_Internet

39. Joomla. (n.d.). Retrieved January 30, 2017, from https://en.wikipedia.org/wiki/Joomla

40. Releases for Drupal core. (n.d.). Retrieved January 30, 2017, from https://www.drupal.org/project/drupal/releases

41. Checkmarx CxSAST Overview - Checkmarx Knowledge Center -. (n.d.). Retrieved February 05, 2017, from https://checkmarx.atlassian.net/wiki/display/KC/Checkmarx CxSAST Overview

42. The Security State of WordPress' Top 50 Plugins. (n.d.). Retrieved February 5, 2017, from https://www.checkmarx.com/wp-content/uploads/2013/06/The-Security-State-of-WordPress-Top-50-Plugins.pdf

43. WEBSITE HACKED TREND REPORT 2016 - Q1. (2016, May 18). Retrieved February 5, 2017, from https://sucuri.net/website-security/Reports/Sucuri-Website-Hacked-Report-2016Q1.pdf

17 Annex

17.1 Annex 1 – CMS & Version Detection Results

17.1.1 1C-Bitrix

Total Count: 18025 (1% of CMS detections)

Version	Count	Percentage
unknown	18025	100

17.1.2 2z Project

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
0.9.7.1	2	100

17.1.3 3dCart

Total Count: 201 (0% of CMS detections)

Version	Count	Percentage
unknown	201	100

17.1.4 a-blog cms

Total Count: 157 (0% of CMS detections)

Version	Count	Percentage
unknown	157	100

17.1.5 Accessible Portal

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
unknown	2	100

17.1.6 Adobe Experience Manager

Total Count: 10003 (1% of CMS detections)

Version	Count	Percentage
unknown	10003	100

17.1.7 Ametys

Total Count: 75 (0% of CMS detections)

Version	Count	Percentage
unknown	75	100

17.1.8 Amiro.CMS

Total Count: 163 (0% of CMS detections)

Version	Count	Percentage
unknown	163	100

17.1.9 Anchor CMS

Total Count: 17 (0% of CMS detections)

Version	Count	Percentage
unknown	17	100

17.1.10 AsciiDoc

Total Count: 13 | 0% of CMS detections)

Version	Count	Percentage
7.1.2	1	7
8.6.6	1	7
8.6.9	11	84

17.1.11 Backdrop

Total Count: 5 (0% of CMS detections)

Version	Count	Percentage
1	5	100

17.1.12 BIGACE

Total Count: 3 (0% of CMS detections)

Version	Count	Percentage
unknown	2	66

2.7.7	1	33

17.1.13 Bolt

Total Count: 175 (0% of CMS detections)

Version	Count	Percentage
unknown	175	100

17.1.14 browseRCMS

Total Count: 55 (0% of CMS detections)

Version	Count	Percentage
3.0.6	1	1
3.1.2	5	9
3.1.3	4	7
3.1.5	2	3
3.3.1	1	1
3.3.3	1	1
3.3.4	2	3
3.4.1	1	1
3.4.2	2	3
3.5.2	3	5
3.5.3	3	5
3.5.4	10	18
3.5.6	4	7
3.5.7	6	10
3.5.7.2	2	3
4.0.0.	7	12
4.0.3	1	1

17.1.15 Business Catalyst

Total Count: 1232 (0% of CMS detections)

Version	Count	Percentage
unknown	1232	100

17.1.16 Cargo

Total Count: 293 (0% of CMS detections)

Version	Count	Percentage
unknown	293	100

17.1.17 Chameleon

Total Count: 7 (0% of CMS detections)

Version	Count	Percentage
unknown	7	100

17.1.18 CMS Made Simple

Total Count: 530 (0% of CMS detections)

Version	Count	Percentage
unknown	530	100

17.1.19 CMSimple

Total Count: 67 (0% of CMS detections)

Version	Count	Percentage
unknown	28	41
2.5	1	1
2.6	1	1
2.9	3	4
3.0	1	1
3.1	2	2
3.2	13	19
3.3	2	2
3.4	1	1
4.1.2	1	1
4.5	4	5
4.5.2	1	1
4.5.4	3	4
4.6.3	3	4
4.6.4	3	4

17.1.20 Concrete5

Total Count: 2533 (0% of CMS detections)

Version	Count	Percentage
unknown	394	15
1.2	1	0

5.3.1.1	1	0
5.3.2	12	0
5.3.3.1	3	0
5.4.0.5	7	0
5.4.1	3	0
5.4.1.1	29	1
5.4.1.1.1	2	0
5.4.2	2	0
5.4.2.1	4	0
5.4.2.2	25	0
5.5.1	15	0
5.5.2	11	0
5.5.2.1	95	3
5.6.0	2	0
5.6.0.1	3	0
5.6.0.2	61	2
5.6.1	25	0
5.6.1.1	7	0
5.6.1.2	207	8
5.6.1.3b2	7	0
5.6.2	12	0
5.6.2.1	213	8
5.6.3	22	0
5.6.3.1	264	10
5.6.3.2	127	5
5.6.3.3	292	11
5.6.3.4	198	7
5.6.3.5b1	3	0
5.6.3a3	3	0
5.7.1	1	0
5.7.2	1	0
5.7.2.1	4	0
5.7.3	1	0
5.7.3.1	25	0
5.7.4	2	0
5.7.4.1	8	0
5.7.4.2	47	1
5.7.5	3	0
5.7.5.1	26	1
5.7.5.10b1	1	0
5.7.5.2	77	3
5.7.5.3	24	0
5.7.5.4	5	0
5.7.5.4a1	2	0
5.7.5.5	2	0
5.7.5.6	87	3
5.7.5.7	23	0
5.7.5.7a1	1	0
5.7.5.8	74	2
5.7.5.9	72	2
8.0.0b6	2	0

17.1.21 Contao

Total Count: 1700 (0% of CMS detections)

Version	Count	Percentage
unknown	1700	100

17.1.22 Contenido

Total Count: 188 (0% of CMS detections)

Version	Count	Percentage
4.4.5	1	0
4.6.15	3	1
4.6.23	2	1
4.6.24	3	1
4.6.8	2	1
4.8	62	32
4.8.12	26	13
4.8.13	1	0
4.8.5	1	0
4.8.7	1	0
4.8.8	1	0
4.8.9	16	8
4.9	69	36

17.1.23 Contens

Total Count: 123 | 0% of CMS detections)

Version	Count	Percentage
4.0	1	0
6.0	1	0
7.1	2	1
7.2	2	1
8.0	1	0
8.1	21	17
8.2	33	26
8.3	61	49
9.0	2	1

17.1.24 ContentBox

Total Count: 8 (0% of CMS detections)

Version	Count	Percentage
unknown	8	100

17.1.25 Cotonti

Total Count: 47 (0% of CMS detections)

Version	Count	Percentage
unknown	47	100

17.1.26 CPG Dragonfly

Total Count: 23 (0% of CMS detections)

Version	Count	Percentage
unknown	23	100

17.1.27 Danneo CMS

Total Count: 10 (0% of CMS detections)

Version	Count	Percentage
0.5	3	30
0.5.2	7	70

17.1.28 DataLife Engine

Total Count: 4005 (0% of CMS detections)

Version	Count	Percentage
unknown	4005	100

17.1.29 DedeCMS

Total Count: 1740 (0% of CMS detections)

Version	Count	Percentage
unknown	1740	100

17.1.30 DM Polopoly

Total Count: 420 (0% of CMS detections)

Version	Count	Percentage
unknown	420	100

17.1.31 DNN

Total Count: 8722 (0% of CMS detections)

Version	Count	Percentage
unknown	8722	100

17.1.32 Drupal

Total Count: 88389 (9% of CMS detections)

Version	Count	Percentage
unknown	35180	39
3	2	0
5.19.0	2	0
5.20.0	2	0
5.22.0	2	0
5.23	2	0
6	8	0
7	55891	63
7.	1	0
7.1	8	0
7.17	1	0
7.19	2	0
7.2.3	2	0
7.34	3	0
7.43	3	0

7.5	3	0
7.51	4	0
8	1479	1
8.0.5	2	0
8.2.0	1	0
9	1	0

17.1.33 DTG

Total Count: 8 (0% of CMS detections)

Version	Count	Percentage
unknown	8	100

17.1.34 Dynamicweb

Total Count: 344 (0% of CMS detections)

Version	Count	Percentage
.	1	0
7	20	5
8	323	93

17.1.35 e107

Total Count: 247 (0% of CMS detections)

Version	Count	Percentage
unknown	247	100

17.1.36 Eleanor CMS

Total Count: 39 (0% of CMS detections)

Version	Count	Percentage
unknown	39	100

17.1.37 EPiServer

Total Count: 718 (0% of CMS detections)

Version	Count	Percentage
unknown	718	100

17.1.38 eSyndiCat

Total Count: 216 (0% of CMS detections)

Version	Count	Percentage
unknown	216	100

17.1.39 eZ Publish

Total Count: 1130 (0% of CMS detections)

Version	Count	Percentage
unknown	1130	100

17.1.40 FlexCMP

Total Count: 53 (0% of CMS detections)

Version	Count	Percentage
6.7.03	3	5
7.0.09	1	1
7.0.25	11	20
7.0.27	5	9
7.0.29	7	13
7.0.31	26	49

17.1.41 GetSimple CMS

Total Count: 101 (0% of CMS detections)

Version	Count	Percentage
unknown	101	100

17.1.42 Google Sites

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
unknown	2	100

17.1.43 Graffiti CMS

Total Count: 5 (0% of CMS detections)

Version	Count	Percentage
unknown	2	40
1.2	build 1.2.0.1451)	1
1.2	build 1.2.0.2308)	1
1.3 Beta	build 1.3.0.0)	1

17.1.44 Grav

Total Count: 88 (0% of CMS detections)

Version	Count	Percentage
unknown	85	96
0.9.40	1	1
0.9.43	1	1
1.0.0	1	1

17.1.45 Green Valley CMS

Total Count: 40 (0% of CMS detections)

Version	Count	Percentage
unknown	40	100

17.1.46 GX WebManager

Total Count: 49 (0% of CMS detections)

Version	Count	Percentage
unknown	41	83
9	8	16

17.1.47 Hippo

Total Count: 418 (0% of CMS detections)

Version	Count	Percentage
unknown	418	100

17.1.48 Hotaru CMS

Total Count: 8 (0% of CMS detections)

Version	Count	Percentage
unknown	8	100

17.1.49 Hugo

Total Count: 304 (0% of CMS detections)

Version	Count	Percentage
0.13	3	0
0.14	6	1
0.15	39	12
0.16	162	53
0.17	80	26
0.18	17	5

17.1.50 ibm WebspHERE portal

Total Count: 59 (0% of CMS detections)

Version	Count	Percentage
unknown	59	100

17.1.51 ImpressCMS

Total Count: 11 (0% of CMS detections)

Version	Count	Percentage
unknown	11	100

17.1.52 ImpressPages

Total Count: 42 (0% of CMS detections)

Version	Count	Percentage
unknown	41	97
1.0	1	2

17.1.53 IndExhibit

Total Count: 58 (0% of CMS detections)

Version	Count	Percentage
unknown	58	100

17.1.54 Indico

Total Count: 12 (0% of CMS detections)

Version	Count	Percentage
unknown	12	100

17.1.55 InProces

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
unknown	2	100

17.1.56 InstantCMS

Total Count: 202 (0% of CMS detections)

Version	Count	Percentage
unknown	202	100

17.1.57 Jalios

Total Count: 90 (0% of CMS detections)

Version	Count	Percentage
unknown	90	100

17.1.58 Jekyll

Total Count: 28 (0% of CMS detections)

Version	Count	Percentage
unknown	11	39
v2.4.0	1	3
v2.5.3	2	7
v3.0.0	2	7
v3.0.3	2	7
v3.1.6	1	3
v3.2.1	8	28
v3.3.0	1	3

17.1.59 Joomla

Total Count: 66144 (7% of CMS detections)

Version	Count	Percentage
unknown	56019	84
1.5	9537	14
1.5.	3	0
1.6	227	0
1.7	447	0
2.5	10	0
2.5.	1	0
3.2	2	0
3.4	1	0
3.4.0	1	0
3.4.1	1	0
3.6	3	0
3.6.2	1	0

17.1.60 Kentico CMS

Total Count: 95 (0% of CMS detections)

Version	Count	Percentage
4.0	build 4.0.3328)	4
4.0	build 4.0.3378)	2
4.1	build 4.1.3518)	6
4.1	build 4.1.3667)	2
5.0	build 5.0.3656)	1
5.0	build 5.0.3671)	1
5.0	build 5.0.3742)	2
5.0	build 5.0.3771)	2
5.5	build 5.5.3789)	18
5.5	build 5.5.3817)	1
5.5	build 5.5.3894)	1
5.5R2	build 5.5.3996)	3
5.5R2	build 5.5.4281)	3
6.0	build 6.0.4297)	3
6.0	build 6.0.4387)	1
6.0	build 6.0.4463)	1
6.0	build 6.0.4514)	1
6.0	build 6.0.4549)	1
6.0	build 6.0.4568)	2
6.0	build 6.0.4640)	2
6.0	build 6.0.4713)	1
7.0	build 7.0.4640)	5
7.0	build 7.0.4724)	3
7.0	build 7.0.4843)	3
7.0	build 7.0.4856)	1
7.0	build 7.0.4947)	3
7.0	build 7.0.5016)	3
7.0	build 7.0.5053)	2
7.0	build 7.0.5060)	1
7.0	build 7.0.5074)	2
7.0	build 7.0.5158)	1
7.0	build 7.0.5228)	1

7.0	build 7.0.5256)	1
7.0	build 7.0.5346)	2
7.0	build 7.0.5354)	9

17.1.61 Koala Framework

Total Count: 12 (0% of CMS detections)

Version	Count	Percentage
unknown	12	100

17.1.62 Koken

Total Count: 42 (0% of CMS detections)

Version	Count	Percentage
0.18.3	1	2
0.19.3	1	2
0.21.13	1	2
0.21.2	5	11
0.21.8	1	2
0.21.9	1	2
0.22.0	1	2
0.22.10	6	14
0.22.2	3	7
0.22.4	2	4
0.22.5	6	14
0.22.6	4	9
0.22.7	2	4
0.22.8	2	4
0.22.9	7	16

17.1.63 Komodo CMS

Total Count: 19 (0% of CMS detections)

Version	Count	Percentage
unknown	19	100

17.1.64 Koobi

Total Count: 3 (0% of CMS detections)

Version	Count	Percentage
unknown	1	33
kuvamist	1	33
muutumist	1	33

17.1.65 Kooboo CMS

Total Count: 70 (0% of CMS detections)

Version	Count	Percentage
unknown	70	100

17.1.66 Kotisivukone

Total Count: 68 (0% of CMS detections)

Version	Count	Percentage
unknown	68	100

17.1.67 LEPTON

Total Count: 1 (0% of CMS detections)

Version	Count	Percentage
unknown	1	100

17.1.68 Liferay

Total Count: 1 (0% of CMS detections)

Version	Count	Percentage
6.1.1	1	100

17.1.69 LightMon Engine

Total Count: 3 (0% of CMS detections)

Version	Count	Percentage
unknown	3	100

17.1.70 Lithium

Total Count: 3 (0% of CMS detections)

Version	Count	Percentage
unknown	3	100

17.1.71 Locomotive

Total Count: 132 (0% of CMS detections)

Version	Count	Percentage
unknown	132	100

17.1.72 Mambo

Total Count: 217 (0% of CMS detections)

Version	Count	Percentage
unknown	217	100

17.1.73 MaxSite CMS

Total Count: 123 (0% of CMS detections)

Version	Count	Percentage
unknown	123	100

17.1.74 Methode

Total Count: 248 (0% of CMS detections)

Version	Count	Percentage
unknown	248	100

17.1.75 Microsoft SharePoint

Total Count: 5717 (0% of CMS detections)

Version	Count	Percentage
unknown	5654	98
12.0.0.6554	1	0
14.0.0.6029	1	0
14.0.0.6106	2	0
14.0.0.6117	1	0
14.0.0.7006	12	0
14.0.0.7113	1	0
14.0.0.7128	5	0
14.0.0.7162	1	0
14.0.0.7166	12	0
15.0.0.4512	3	0
15.0.0.4569	13	0
15.0.0.4599	4	0
15.0.0.4649	2	0
15.0.0.4667	2	0
15.0.0.4727	1	0
15.0.0.4797	2	0

17.1.76 MODx

Total Count: 354 (0% of CMS detections)

Version	Count	Percentage
unknown	354	100

17.1.77 Moguta.CMS

Total Count: 89 (0% of CMS detections)

Version	Count	Percentage
unknown	89	100

17.1.78 Mono.net

Total Count: 43 (0% of CMS detections)

Version	Count	Percentage
unknown	43	100

17.1.79 MotoCMS

Total Count: 13 (0% of CMS detections)

Version	Count	Percentage
unknown	13	100

17.1.80 Movable Type

Total Count: 992 (0% of CMS detections)

Version	Count	Percentage
unknown	992	100

17.1.81 Mozard Suite

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
unknown	2	100

17.1.82 Mura CMS

Total Count: 404 (0% of CMS detections)

Version	Count	Percentage
5	101	25
6	295	73
7	8	1

17.1.83 Mynetcap

Total Count: 1 (0% of CMS detections)

Version	Count	Percentage
unknown	1	100

17.1.84 Odoo

Total Count: 132 (0% of CMS detections)

Version	Count	Percentage
unknown	132	100

17.1.85 OpenCms

Total Count: 369 (0% of CMS detections)

Version	Count	Percentage
unknown	369	100

17.1.86 OpenNemas

Total Count: 66 (0% of CMS detections)

Version	Count	Percentage
unknown	66	100

17.1.87 OpenText Web Solutions

Total Count: 309 (0% of CMS detections)

Version	Count	Percentage
unknown	309	100

17.1.88 Orchard CMS

Total Count: 947 (0% of CMS detections)

Version	Count	Percentage
unknown	947	100

17.1.89 Pagekit

Total Count: 18 (0% of CMS detections)

Version	Count	Percentage
unknown	18	100

17.1.90 papaya CMS

Total Count: 6 (0% of CMS detections)

Version	Count	Percentage
unknown	6	100

17.1.91 PencilBlue

Total Count: 27 (0% of CMS detections)

Version	Count	Percentage
unknown	27	100

17.1.92 Percussion

Total Count: 123 (0% of CMS detections)

Version	Count	Percentage
unknown	123	100

17.1.93 PHP-Fusion

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
unknown	2	100

17.1.94 PHPSQLitecms

Total Count: 3 (0% of CMS detections)

Version	Count	Percentage
1.0	2	66
3.2014.08.11.20.31	1	33

17.1.95 PHPwind

Total Count: 585 (0% of CMS detections)

Version	Count	Percentage
unknown	585	100

17.1.96 Pligg

Total Count: 936 (0% of CMS detections)

Version	Count	Percentage
unknown	936	100

17.1.97 Plone

Total Count: 1860 (0% of CMS detections)

Version	Count	Percentage
unknown	1860	100

17.1.98 Posterous

Total Count: 19 (0% of CMS detections)

Version	Count	Percentage
unknown	19	100

17.1.99 Quick.CMS

Total Count: 52 (0% of CMS detections)

Version	Count	Percentage
unknown	43	82
5.0	2	3
5.1	1	1
5.2	1	1
5.3	1	1
5.5	1	1
6.0	1	1
6.1	1	1
6.2	1	1

17.1.100 RBS Change

Total Count: 41 (0% of CMS detections)

Version	Count	Percentage
unknown	41	100

17.1.101 RCMS

Total Count: 22 (0% of CMS detections)

Version	Count	Percentage
unknown	22	100

17.1.102 Roadiz CMS

Total Count: 5 (0% of CMS detections)

Version	Count	Percentage
alpha 0.13.3	2	40
alpha 0.15.1	3	60

17.1.103 S.Builder

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
unknown	2	100

17.1.104 sarka-SPIP

Total Count: 56 (0% of CMS detections)

Version	Count	Percentage
unknown	1	1
3.0.0	1	1
3.0.2	1	1
3.0.4	1	1
3.0.5	1	1
3.0.7	5	8
3.2.16	1	1
3.2.24	1	1
3.2.28	1	1
3.2.34	1	1
3.2.36	9	16
3.3.37	1	1
3.3.45	1	1
3.4.3	1	1
3.4.5	3	5
3.4.6	14	25
4.5.3	1	1
4.5.7	12	21

17.1.105 SDL Tridion

Total Count: 720 (0% of CMS detections)

Version	Count	Percentage
unknown	720	100

17.1.106 Serendipity

Total Count: 51 (0% of CMS detections)

Version	Count	Percentage
unknown	18	35
0.8	1	1
1.1.4	1	1
1.3	1	1
1.4.1	1	1
1.5.1	4	7
1.5.2	2	3
1.5.3-2	1	1
1.5.4	2	3
1.5.5	4	7
1.6	1	1
1.6.2	1	1
1.7	2	3
1.7-rc3	1	1
1.7.2	1	1
1.7.5	1	1
1.7.8	2	3
2.0.2	1	1
2.0.3	5	9
2.1-beta2	1	1

17.1.107 SilverStripe

Total Count: 1538 (0% of CMS detections)

Version	Count	Percentage
unknown	1538	100

17.1.108 SIMsite

Total Count: 25 (0% of CMS detections)

Version	Count	Percentage
unknown	25	100

17.1.109 Sitecore

Total Count: 3265 (0% of CMS detections)

Version	Count	Percentage
unknown	3265	100

17.1.110 SiteEdit

Total Count: 175 (0% of CMS detections)

Version	Count	Percentage
unknown	175	100

17.1.111 Sitefinity

Total Count: 5245 (0% of CMS detections)

Version	Count	Percentage
3.0.1323.1	2	0
3.1.1483.2:1	2	0
3.2.1526.2:1	7	0
3.2.1616.2:1	4	0
3.2.1616.3	1	0
3.2.1616.4:0	1	0
3.5.1714.3	1	0
3.5.1747.1:0	2	0
3.5.1747.2:1	5	0
3.5.1747.2:11	1	0
3.5.1747.3	1	0
3.6.1870.220:2	2	0
3.6.1870.2:1	1	0
3.6.1870.2:2	2	0
3.6.1875.2:1	4	0
3.6.1936.220:1	2	0
3.6.1936.2:0	1	0
3.6.1936.2:1	7	0
3.7.1990.2:0	2	0
3.7.1990.2:1	5	0
3.7.1990.3	4	0

3.7.2022.2:1	10	0
3.7.2022.2:2	1	0
3.7.2022.2:3	1	0
3.7.2022.2:7	2	0
3.7.2022.3	1	0
3.7.2022.5	2	0
3.7.2057.120:0	1	0
3.7.2057.2:1	14	0
3.7.2057.2:2	1	0
3.7.2057.2:4	1	0
3.7.2057.3	2	0
3.7.2096.1:0	3	0
3.7.2096.220:1	1	0
3.7.2096.2:1	54	1
3.7.2096.2:2	7	0
3.7.2096.2:21	3	0
3.7.2096.2:8	4	0
3.7.2096.3	4	0
3.7.2096.4:0	8	0
3.7.2136.140:0	4	0
3.7.2136.1:0	4	0
3.7.2136.220:1	3	0
3.7.2136.220:8	2	0
3.7.2136.240:0	1	0
3.7.2136.240:1	1632	31
3.7.2136.240:2	5	0
3.7.2136.240:4	1	0
3.7.2136.2:1	47	0
3.7.2136.2:14	2	0
3.7.2136.2:2	9	0
3.7.2136.2:5	1	0
3.7.2136.2:7	1	0
3.7.2136.3	5	0
3.7.2136.340	3	0
3.7.2152.140:0	1	0
4.0.1098.0 SB	2	0
4.0.1210.0 SE	2	0
4.1.1395.0 SE	7	0
4.1.1501.0 PU	2	0
4.1.1574.0 SE	1	0
4.2.1650.0 PE	1	0
4.2.1650.0 SE	4	0
4.2.1733.0 SE	2	0
4.3.1885.0 PE	2	0
4.3.1885.0 SE	8	0
4.3.1885.0 SF4.0	2	0
4.4.2117.0 PE	2	0
4.4.2117.0 SB	3	0
4.4.2117.0 SE	34	0
5.0.2500.0 SE	7	0
5.0.2523.0 PE	1	0
5.0.2523.0 SE	11	0
5.0.2800.0 SE	5	0
5.0.2860.0 PE	5	0
5.0.2860.0 SE	15	0
5.1.3210.0 PE	1	0
5.1.3210.0 SB	6	0
5.1.3210.0 SE	6	0
5.1.3270.0 PE	5	0
5.1.3270.0 SE	15	0
5.1.3450.0 PE	4	0
5.1.3450.0 PU	1	0
5.1.3450.0 SB	1	0
5.1.3450.0 SE	20	0
5.1.3450.0 SF4.0	2	0
5.2.3700.0 SE	21	0
5.2.3700.0 SF4.0	1	0
5.2.3800.0 PE	4	0
5.2.3800.0 SE	8	0
5.3.3900.0 PE	5	0
5.3.3900.0 PU	2	0
5.3.3900.0 SB	2	0
5.3.3900.0 SE	9	0
5.3.3900.0 SF4.0	2	0
5.4.4000.0 PU	2	0
5.4.4000.0 SE	2	0

5.4.4010.0 PE	11	0
5.4.4010.0 PU	5	0
5.4.4010.0 SB	3	0
5.4.4010.0 SE	41	0
5.4.4020.0 SE	12	0
5.4.4040.0 PE	8	0
5.4.4040.0 SE	12	0
5.4.4042.0 SE	4	0
6.0.4100.0 PE	1	0
6.0.4100.0 PU	7	0
6.0.4100.0 SE	10	0
6.0.4100.0 SF4.0	2	0
6.0.4200.0 MS	1	0
6.0.4200.0 PE	3	0
6.0.4200.0 SE	9	0
6.0.4210.0 PE	3	0
6.0.4210.0 PU	3	0
6.0.4210.0 SB	1	0
6.0.4210.0 SE	28	0
6.1.4300.0 MS	2	0
6.1.4300.0 PE	5	0
6.1.4300.0 PU	3	0
6.1.4300.0 SE	24	0
6.1.4600.0 PE	12	0
6.1.4600.0 PU	5	0
6.1.4600.0 SB	3	0
6.1.4600.0 SE	17	0
6.1.4601.0 PE	6	0
6.1.4601.0 SE	4	0
6.1.4700.0	2	0
6.1.4700.0 PE	7	0
6.1.4700.0 PU	1	0
6.1.4700.0 SE	32	0
6.1.4700.0 SF4.0	1	0
6.2.4900.0 PE	4	0
6.2.4900.0 SE	3	0
6.2.4910.0 ISE	1	0
6.2.4910.0 PE	10	0
6.2.4910.0 PU	17	0
6.2.4910.0 SE	21	0
6.3.5000.0 PE	46	0
6.3.5000.0 PU	22	0
6.3.5000.0 SE	96	1
6.3.5000.0 SF4.0	1	0
6.3.5001.0 SE	2	0
6.3.5014.0 PE	2	0
6.3.5014.0 SE	2	0
6.3.5020.0 SE	8	0
6.3.5023.0 SE	2	0
6.3.5026.0 PE	1	0
6.3.5028.0 SE	1	0
6.3.5029.0 SE	2	0
7.0.5100.0 OME	7	0
7.0.5100.0 PE	40	0
7.0.5100.0 PU	33	0
7.0.5100.0 SE	69	1
7.0.5100.0 SF4.0	1	0
7.0.5101.0 PU	9	0
7.0.5101.0 SE	2	0
7.0.5101.0 SF4.0	2	0
7.0.5103.0 SE	2	0
7.0.5107.0 PE	3	0
7.0.5107.0 SE	1	0
7.0.5109.0 SE	1	0
7.0.5114.0 OME	3	0
7.0.5115.0 PU	29	0
7.0.5115.0 SE	1	0
7.1.5143.0 SF4.0	1	0
7.1.5200.0 PE	29	0
7.1.5200.0 PU	30	0
7.1.5200.0 SB	4	0
7.1.5200.0 SE	55	1
7.1.5201.0 PU	6	0
7.1.5201.0 SE	4	0
7.1.5202.0 PE	2	0
7.1.5203.0 PE	4	0

7.1.5205.0 PE	2	0
7.1.5205.0 SE	1	0
7.1.5207.0 PE	2	0
7.1.5207.0 SE	1	0
7.1.5208.0 SE	4	0
7.1.5210.0 PE	2	0
7.1.5213.0 PE	1	0
7.1.5213.0 SE	9	0
7.2.5300.0 PE	2	0
7.2.5300.0 PU	2	0
7.2.5300.0 SE	4	0
7.2.5310.0 OME	5	0
7.2.5310.0 PE	12	0
7.2.5310.0 PU	38	0
7.2.5310.0 SE	23	0
7.2.5310.0 SF4.0	1	0
7.2.5311.0 SE	2	0
7.2.5312.0 PU	1	0
7.2.5314.0 PE	2	0
7.2.5314.0 PU	3	0
7.2.5314.0 SE	1	0
7.2.5318.0 SE	1	0
7.2.5318.0 SF4.0	1	0
7.2.5320.0 MS	9	0
7.2.5320.0 OME	2	0
7.2.5320.0 PE	21	0
7.2.5320.0 PU	9	0
7.2.5320.0 SB	1	0
7.2.5320.0 SE	35	0
7.2.5321.0 PE	9	0
7.2.5321.0 SE	7	0
7.2.5324.0 PE	4	0
7.2.5324.0 PU	2	0
7.2.5324.0 SE	7	0
7.3.5600.0 PE	2	0
7.3.5600.0 PU	2	0
7.3.5600.0 SE	2	0
7.3.5610.0 OME	8	0
7.3.5610.0 PE	43	0
7.3.5610.0 PU	6	0
7.3.5610.0 SE	72	1
7.3.5611.0 PE	2	0
7.3.5614.0 PU	1	0
7.3.5615.0 SE	2	0
7.3.5616.0 PU	2	0
7.3.5617.0 PE	2	0
7.3.5619.0 PE	2	0
7.3.5619.0 PU	2	0
7.3.5621.0 PE	1	0
7.3.5621.0 SE	2	0
7.3.5630.0 OME	7	0
7.3.5630.0 PE	11	0
7.3.5630.0 PU	10	0
7.3.5630.0 SE	19	0
7.3.5636.0 SE	3	0
7.3.5650.0 PE	5	0
7.3.5650.0 PU	3	0
7.3.5650.0 SE	1	0
7.3.5651.0 OME	3	0
7.3.5651.0 PE	4	0
7.3.5651.0 SE	5	0
7.3.5653.0 PU	3	0
7.3.5654.0 PU	6	0
8.0.5700.0 CE	2	0
8.0.5700.0 OME	7	0
8.0.5700.0 PE	29	0
8.0.5700.0 PU	47	0
8.0.5700.0 SB	1	0
8.0.5700.0 SE	39	0
8.0.5700.0 SF4.0	1	0
8.0.5701.0 PE	1	0
8.0.5702.0 PU	4	0
8.0.5703.0 OME	1	0
8.0.5703.0 PU	1	0
8.0.5704.0 PU	1	0
8.0.5704.0 SE	2	0

8.0.5705.0 PU	2	0
8.0.5705.0 SE	2	0
8.0.5706.0 PE	5	0
8.0.5706.0 SE	4	0
8.0.5710.0 MS	3	0
8.0.5710.0 OME	6	0
8.0.5710.0 PE	40	0
8.0.5710.0 PU	4	0
8.0.5710.0 SB	2	0
8.0.5710.0 SE	82	1
8.0.5713.0 SE	1	0
8.0.5715.0 PE	2	0
8.0.5717.0 OME	19	0
8.0.5719.0 SE	3	0
8.0.5720.0 OME	2	0
8.0.5720.0 PE	3	0
8.0.5720.0 PU	1	0
8.0.5720.0 SE	9	0
8.0.5730.0 PE	10	0
8.0.5730.0 PU	2	0
8.0.5730.0 SE	1	0
8.0.5731.1 PU	1	0
8.0.5734.0 OME	18	0
8.1.5800.0 OME	9	0
8.1.5800.0 PE	33	0
8.1.5800.0 PU	9	0
8.1.5800.0 SE	50	0
8.1.5801.0 SE	6	0
8.1.5802.0 PE	3	0
8.1.5802.0 PU	3	0
8.1.5802.0 SB	2	0
8.1.5804.0 PU	5	0
8.1.5804.0 SE	2	0
8.1.5805.0 PE	4	0
8.1.5810.0 OME	2	0
8.1.5810.0 PE	8	0
8.1.5810.0 PU	24	0
8.1.5810.0 SE	4	0

8.1.5811.0 PE	1	0
8.1.5811.0 PU	2	0
8.1.5811.0 SE	3	0
8.1.5820.0 OME	10	0
8.1.5820.0 PE	37	0
8.1.5820.0 PU	30	0
8.1.5820.0 SB	1	0
8.1.5820.0 SE	35	0
8.1.5821.0 OME	1	0
8.1.5821.0 PE	5	0
8.1.5822.0 PU	2	0
8.1.5823.0 PE	1	0
8.1.5823.0 PU	4	0
8.1.5823.0 SE	2	0
8.1.5824.0 PE	16	0
8.1.5824.0 PU	9	0
8.1.5824.0 SE	7	0
8.1.5827.0 PU	2	0
8.1.5828.0 PU	1	0
8.2.5870.0 SE	3	0
8.2.5900.0 MS	11	0
8.2.5900.0 OME	36	0
8.2.5900.0 PE	104	1
8.2.5900.0 PU	84	1
8.2.5900.0 SE	133	2
8.2.5901.0 OME	2	0
8.2.5901.0 PE	6	0
8.2.5901.0 SE	1	0
8.2.5902.0 OME	2	0
8.2.5902.0 PE	4	0
8.2.5902.0 SE	4	0
8.2.5903.0 OME	2	0
8.2.5903.0 PU	3	0
8.2.5903.0 SE	2	0
8.2.5904.0 PE	2	0
8.2.5905.0 PE	30	0
8.2.5905.0 SE	2	0
8.2.5906.0 SE	11	0

8.2.5907.0 OME	1	0
8.2.5907.0 PE	3	0
8.2.5907.0 PU	1	0
8.2.5907.0 SE	2	0
8.2.5908.0 OME	6	0
8.2.5908.0 PE	7	0
8.2.5908.0 PU	12	0
8.2.5909.0 PU	2	0
8.2.5910.0 OME	3	0
8.2.5910.0 SE	3	0
8.2.5911.0 PE	4	0
8.2.5911.0 PU	6	0
8.2.5912.0 OME	6	0
8.2.5912.0 PE	7	0
8.2.5912.0 PU	2	0
8.2.5912.0 SE	1	0
8.2.5913.0 OME	18	0
8.2.5913.0 PE	4	0
8.2.5914.0 OME	9	0
8.2.5914.0 PE	11	0
8.2.5914.0 PU	13	0
8.2.5914.0 SE	1	0
9.0.6000.0 OME	1	0
9.0.6000.0 PE	2	0
9.0.6000.0 PU	13	0
9.0.6000.0 SB	1	0
9.0.6000.0 SE	11	0
9.0.6001.0 OME	2	0
9.0.6001.0 PU	4	0
9.0.6001.0 SE	1	0
9.0.6010.0 OME	7	0
9.0.6010.0 PE	21	0
9.0.6010.0 PU	11	0
9.0.6010.0 SE	12	0
9.0.6011.0 PE	2	0
9.0.6011.0 SE	2	0
9.0.6012.0 PE	1	0
9.0.6012.0 PU	5	0

9.0.6013.0 PE	3	0
9.0.6013.0 PU	3	0
9.0.6013.0 SE	5	0
9.0.6014.0 PE	3	0
9.0.6014.0 SE	2	0
9.0.6015.0 PU	2	0
9.1.6100.0 OME	9	0
9.1.6100.0 PE	8	0
9.1.6100.0 PU	32	0
9.1.6100.0 SE	20	0
9.1.6110.0 MS	8	0
9.1.6110.0 OME	22	0
9.1.6110.0 PE	52	0
9.1.6110.0 PU	70	1
9.1.6110.0 SB	4	0
9.1.6110.0 SE	63	1
9.1.6111.0 PE	1	0
9.1.6111.0 PU	2	0
9.1.6112.0 OME	2	0
9.1.6112.0 PU	3	0
9.1.6113.0 PE	2	0
9.1.6113.0 PU	3	0
9.1.6114.0 PE	2	0
9.1.6115.0 PU	8	0
9.1.6115.0 SE	2	0
9.1.6116.0 PE	2	0
9.1.6116.0 PU	17	0
9.1.6116.0 SE	2	0
9.1.6117.0 PE	2	0
9.1.6117.0 PU	5	0
9.1.6117.0 SE	2	0
9.1.6119.0 PE	3	0
9.1.6119.0 PU	8	0
9.1.6120.0 OME	13	0
9.1.6120.0 PE	4	0
9.1.6120.0 PU	2	0
9.1.6120.0 SE	3	0
9.2.6200.0 OME	5	0

9.2.6200.0 PE	3	0
9.2.6200.0 PU	32	0
9.2.6200.0 SE	11	0

17.1.112 Sivuviidakko

Total Count: 19 | 0% of CMS detections)

Version	Count	Percentage
unknown	19	100

17.1.113 SmartSite

Total Count: 15 (0% of CMS detections)

Version	Count	Percentage
unknown	15	100

17.1.114 sNews

Total Count: 30 (0% of CMS detections)

Version	Count	Percentage
unknown	30	100

17.1.115 Solodev

Total Count: 32 (0% of CMS detections)

Version	Count	Percentage
unknown	32	100

17.1.116 SPIP

Total Count: 1189 (0% of CMS detections)

Version	Count	Percentage
unknown	80	6
1.9.1	1	0
1.9.1 [7385]	1	0
1.9.1 [7502]	7	0
1.9.2	35	2
2	3	0
2.0	2	0
2.0.10	2	0
2.0.10 [14698]	10	0
2.0.12 [15876]	1	0
2.0.23 [20567]	2	0
2.0.24 [21143]	1	0
2.0.25	4	0
2.0.25 [21260]	1	0
2.0.26	1	0
2.0.6 [13835]	1	0
2.0.7 [13888]	3	0
2.0.8	1	0
2.0.8 [13982]	4	0
2.0.9 [14357]	2	0
2.0.9 [14398]	1	0
2.0.9 [14452]	1	0
2.1.0	2	0
2.1.0 [15608]	12	1
2.1.10	5	0
2.1.10 [17657]	20	1
2.1.11 [18566]	5	0
2.1.12	4	0
2.1.12 [11132]	1	0
2.1.12 [18732]	8	0
2.1.13	1	0
2.1.13 [19292]	1	0
2.1.14 [19381]	3	0
2.1.16 [19678]	1	0
2.1.17	1	0
2.1.17 [19782]	3	0
2.1.19	3	0
2.1.19 [19922]	2	0
2.1.2	1	0
2.1.2 [16017]	6	0
2.1.20	1	0
2.1.23 [20601]	10	0
2.1.25 [21141]	2	0
2.1.26	10	0
2.1.26 [21262]	34	2
2.1.26 [22915]	1	0
2.1.27	1	0

2.1.27 [22103]	1	0
2.1.28	3	0
2.1.28 [19782]	1	0
2.1.28 [19922]	1	0
2.1.28 [22259]	10	0
2.1.29	5	0
2.1.29 [22915]	28	2
2.1.5	1	0
2.1.8	1	0
2.1.8 [14357]	3	0
2.1.8 [16966]	11	0
2.1.9 [17500]	3	0
2.17	2	0
3.0.0 [19425]	1	0
3.0.10	5	0
3.0.10 [20600]	9	0
3.0.10 [22913]	2	0
3.0.11 [20757]	20	1
3.0.13 [20422]	1	0
3.0.13 [20956]	1	0
3.0.13 [20962]	9	0
3.0.14	2	0
3.0.14 [20573]	2	0
3.0.14 [20757]	1	0
3.0.14 [21141]	6	0
3.0.15	1	0
3.0.15 [21231]	4	0
3.0.16	4	0
3.0.16 [21266]	36	3
3.0.16 [22914]	1	0
3.0.17	14	1
3.0.17 [18732]	1	0
3.0.17 [19436]	1	0
3.0.17 [19905]	1	0
3.0.17 [21515]	61	5
3.0.18	1	0
3.0.19	3	0
3.0.19 [22089]	14	1

3.0.2	1	0
3.0.20	7	0
3.0.20 [14698]	2	0
3.0.20 [21515]	4	0
3.0.20 [22255]	23	1
3.0.21 [20962]	2	0
3.0.21 [22462]	44	3
3.0.22	17	1
3.0.22 [22089]	2	0
3.0.22 [22914]	53	4
3.0.23	27	2
3.0.23 [23171]	1	0
3.0.24	117	9
3.0.24 [21515]	1	0
3.0.24 [23212]	49	4
3.0.4 [19781]	2	0
3.0.5	4	0
3.0.5 [19905]	20	1
3.0.6 [20322]	2	0
3.0.7 [20352]	1	0
3.0.8	2	0
3.0.8 [11132]	2	0
3.0.8 [20422]	2	0
3.1.0	5	0
3.1.0 [21266]	1	0
3.1.0 [22707]	22	1
3.1.1	5	0
3.1.1 [20962]	1	0
3.1.1 [21515]	1	0
3.1.1 [22255]	1	0
3.1.1 [22462]	1	0
3.1.1 [22913]	80	6
3.1.1 [23214]	1	0
3.1.2 [23169]	8	0
3.1.3	34	2
3.1.3 [22913]	6	0
3.1.3 [23213]	4	0
3.1.3 [23214]	71	5

17.1.117 Squiz Matrix

Total Count: 664 (0% of CMS detections)

Version	Count	Percentage
unknown	664	100

17.1.118 Subrion

Total Count: 35 (0% of CMS detections)

Version	Count	Percentage
unknown	35	100

17.1.119 Sulu

Total Count: 14 (0% of CMS detections)

Version	Count	Percentage
1.2.1	1	7
1.2.6	3	21
1.2.7	2	14
1.2.7.8	1	7
1.3.1	4	28
dev-develop	3	21

17.1.120 Textpattern CMS

Total Count: 31 (0% of CMS detections)

Version	Count	Percentage
unknown	31	100

17.1.121 Thelia

Total Count: 39 (0% of CMS detections)

Version	Count	Percentage
unknown	39	100

17.1.122 Tiki Wiki CMS Groupware

Total Count: 98 (0% of CMS detections)

Version	Count	Percentage
unknown	98	100

17.1.123 TYPO3 CMS

Total Count: 22187 (2% of CMS detections)

Version	Count	Percentage
unknown	12746	57
3.6	2	0
3.7	4	0
3.8	16	0
4.0	63	0
4.1	152	0
4.2	414	1
4.3	192	0
4.4	347	1
4.5	4428	19
4.6	326	1
4.7	1381	6
6.0	150	0
6.1	723	3
6.2	1220	5
6.3	1	0
7.1	13	0
7.2	13	0
	5	0

17.1.124 uKnowva

Total Count: 1 (0% of CMS detections)

Version	Count	Percentage
unknown	1	100

17.1.125 Umbraco

Total Count: 40 (0% of CMS detections)

Version	Count	Percentage
unknown	37	92
4.7	3	7

17.1.126 Vignette

Total Count: 120 (0% of CMS detections)

Version	Count	Percentage
unknown	120	100

17.1.127 webEdition

Total Count: 1 (0% of CMS detections)

Version	Count	Percentage
unknown	1	100

17.1.128 WebGUI

Total Count: 183 (0% of CMS detections)

Version	Count	Percentage
6.7.7	1	0
7.0.6	1	0
7.10.23	2	1
7.10.28	11	6
7.10.29	4	2
7.10.30	13	7
7.4.15	2	1
7.4.20	1	0
7.4.22	1	0
7.4.35	1	0
7.4.40	1	0
7.5.24	3	1
7.5.40	5	2
7.6.18	1	0
7.6.35	5	2
7.8.18	2	1
7.8.24	2	1
7.9.22	2	1
7.9.30	101	55
7.9.33	10	5
7.9.34	14	7

17.1.129 WebsiteBaker

Total Count: 13 (0% of CMS detections)

Version	Count	Percentage
unknown	13	100

17.1.130 WebsPlanet

Total Count: 60 (0% of CMS detections)

Version	Count	Percentage
unknown	60	100

17.1.131 Weebly

Total Count: 5026 (0% of CMS detections)

Version	Count	Percentage
unknown	5026	100

17.1.132 Wolf CMS

Total Count: 2 (0% of CMS detections)

Version	Count	Percentage
unknown	2	100

17.1.133 WordPress

Total Count: 662813 (71% of CMS detections)

Version	Count	Percentage
unknown	301880	45
0.0.0	2	0
0815	1	0
1.0.3	1	0
1.2.2	1	0
1.3.3.7	1	0
1.5	5	0
1.5.1.3	1	0
1.5.2	5	0
1.9.2	1	0
10	4	0
10.1	1	0
103	1	0
104	2	0
114	1	0
12.34	2	0
130	1	0
14.8	1	0

144	1	0
147	1	0
1518	1	0
1542	1	0
156	1	0
158	1	0
159	1	0
1620	1	0
164	1	0
169	1	0
1730	1	0
1764	1	0
180.0.0	1	0
1813	1	0
1838	1	0
1856	1	0
187	1	0
2.0	5	0
2.0.1	5	0
2.0.11	1	0
2.0.2	8	0
2.0.3	6	0
2.0.4	17	0
2.0.5	9	0
2.0.6	2	0
2.0.7	1	0
2.1	10	0
2.1.2	6	0
2.1.3	7	0
2.2	9	0
2.2.1	11	0
2.2.2	10	0
2.2.3	11	0
2.3	6	0
2.3.1	11	0
2.3.2	17	0
2.3.3	22	0
2.3.4	2	0

2.5	27	0
2.5.1	57	0
2.6	29	0
2.6.1	18	0
2.6.2	20	0
2.6.3	113	0
2.6.5	30	0
2.7	58	0
2.7.1	147	0
2.8	38	0
2.8.1	11	0
2.8.2	20	0
2.8.3	8	0
2.8.4	187	0
2.8.5	65	0
2.8.6	192	0
2.9	29	0
2.9.1	144	0
2.9.2	361	0
20150320113940	2	0
2016.06	1	0
2016.42	9	0
2016.43	10	0
2016.44	4	0
2090	1	0
213	2	0
218	1	0
226	2	0
243	1	0
244	1	0
256	1	0
2608	1	0
2713	1	0
2715	1	0
273	1	0
279	1	0
281	1	0
2863	1	0

294	1	0
3.0	140	0
3.0.1	396	0
3.0.2	33	0
3.0.3	64	0
3.0.4	199	0
3.0.5	112	0
3.0.6	8	0
3.1	220	0
3.1.1	105	0
3.1.2	223	0
3.1.3	205	0
3.1.4	200	0
3.2	44	0
3.2.1	896	0
3.3	124	0
3.3.1	954	0
3.3.2	625	0
3.3.3	6	0
3.4	158	0
3.4.1	952	0
3.4.2	1467	0
3.4.3	2	0
3.4.4	1	0
3.5	641	0
3.5.1	3151	0
3.5.1.0	1	0
3.5.2	1070	0
3.5.3	4	0
3.6	1167	0
3.6.1	2060	0
3.6.2	3	0
3.6.6	1	0
3.7	38	0
3.7.1	418	0
3.7.10	10	0
3.7.11	15	0
3.7.12	7	0
3.7.13	11	0
3.7.14	8	0
3.7.15	22	0
3.7.16	707	0
3.7.2	12	0
3.7.3	31	0
3.7.4	24	0
3.7.5	31	0
3.7.6	2	0
3.7.7	2	0
3.7.8	6	0
3.8	381	0
3.8.1	989	0
3.8.10	40	0
3.8.11	69	0
3.8.12	18	0
3.8.13	73	0
3.8.14	29	0
3.8.15	170	0
3.8.16	2851	0
3.8.2	165	0
3.8.3	246	0
3.8.4	100	0
3.8.5	121	0
3.8.6	9	0
3.8.7	9	0
3.8.8	40	0
3.8.9	12	0
3.9	385	0
3.9.1	1374	0
3.9.10	32	0
3.9.11	92	0
3.9.12	36	0
3.9.13	116	0
3.9.14	3960	0
3.9.2	886	0
3.9.21	1	0
3.9.3	238	0

3.9.4	11	0
3.9.5	24	0
3.9.6	99	0
3.9.7	8	0
3.9.8	39	0
3.9.9	125	0
30135	1	0
302	1	0
311	1	0
329	1	0
33.1.6	1	0
345	1	0
3535	1	0
3563	1	0
3629	1	0
374	1	0
377	1	0
382	1	0
3830	1	0
386	1	0
388	1	0
4	15	0
4.	2	0
4.0	1860	0
4.0.020150116	1	0
4.0.1	1173	0
4.0.1.3	3	0
4.0.10	144	0
4.0.11	57	0
4.0.12	172	0
4.0.13	4235	0
4.0.2	17	0
4.0.3	11	0
4.0.4	17	0
4.0.5	91	0
4.0.6	9	0
4.0.7	37	0
4.0.8	93	0
4.0.9	45	0
4.1	1545	0
4.1.1	1841	0
4.1.1.3	2	0
4.1.10	156	0
4.1.11	86	0
4.1.12	183	0
4.1.13	7346	1
4.1.2	180	0
4.1.3	48	0
4.1.4	221	0
4.1.5	258	0
4.1.6	27	0
4.1.7	106	0
4.1.8	190	0
4.1.8.2	1	0
4.1.9	51	0
4.2	249	0
4.2.1	537	0
4.2.10	11360	1
4.2.2	3817	0
4.2.3	601	0
4.2.4	1281	0
4.2.5	394	0
4.2.6	133	0
4.2.7	301	0
4.2.8	149	0
4.2.9	342	0
4.3	1268	0
4.3.1	5630	0
4.3.1.0	2	0
4.3.2	256	0
4.3.3	549	0
4.3.4	250	0
4.3.5	460	0
4.3.6	15121	2
4.3.767	1	0
4.4	1639	0

4.4.0	2	0
4.4.1	2288	0
4.4.2	8562	1
4.4.2.1	9	0
4.4.2.1.1	1	0
4.4.3	634	0
4.4.4	1024	0
4.4.41	1	0
4.4.5	30681	4
4.4.6	4	0
4.5	1541	0
4.5.1	1212	0
4.5.17	2	0
4.5.2	5491	0
4.5.2.4	1	0
4.5.24	2	0
4.5.3	11869	1
4.5.3.1	2	0
4.5.4	49319	7
4.5.5.1	1	0
4.6	5014	0
4.6.1	185511	27
4.6.13	1	0
4.6.2	100	0
4.6.8	2	0
4.7	119	0
4.9.1	2	0
400	1	0
4046	1	0
42.5	1	0
4214	1	0
4326	1	0
435	2	0
4366	1	0
462	1	0
4757	1	0
476	1	0
4864	1	0

489	1	0
5.2.5	1	0
5.6	2	0
5049	1	0
5211	1	0
5226	1	0
5356	1	0
5417	1	0
5503	2	0
6.5.3	4	0
6.6.6	1	0
6180	1	0
6424	1	0
6554	1	0
6560	1	0
6625	1	0
6765	1	0
6826	1	0
6921	1	0
7.0	1	0
7.4.7	2	0
7.9	1	0
7.9.0	1	0
7050	1	0
728	1	0
765	1	0
7745	1	0
8.2.2	6	0
8096	1	0
8122	1	0
8230	1	0
8258	1	0
8386	1	0
84	1	0
8565	1	0
8765	1	0
8939	1	0
9.0	2	0

9.8.1	1	0
9.9.9	3	0
9059	1	0
9139	1	0
923	1	0
9301	1	0
9779	1	0

17.1.134 XOOPS

Total Count: 510 (0% of CMS detections)

Version	Count	Percentage
unknown	510	100

17.1.135 XpressEngine

Total Count: 881 (0% of CMS detections)

Version	Count	Percentage
unknown	881	100