https://doi.org/10.53656/math2022-5-2-sec

*Educational Matters*
*Научно-методически статии*

# SECURITY ANALYSIS ON CONTENT MANAGEMENT SYSTEMS

**[1] Dr. Lilyana Petkova, [2] Dr. Vasilisa Pavlova, Assist. Prof.**
*[1] "LiLuzeNet" Ltd (Bulgaria)*
*[2] South-West University "Neofit Rilski" (Bulgaria)*

**Abstract.** This paper is dedicated to the challenges of the use of the most popular content management systems (CMS) in software development. Fundamental information about the selected CMS platforms and vulnerability analysis are introduced. The review is made on CMS like Umbraco, Sitecore, WordPress and Drupal categorized in two groups defined by the technology used for development. And as the IT world changes a lot these brings one constant battle against threats. Therefore, this article will add some vulnerabilities analysis of the selected systems since 2014. Results were grouped by common vulnerabilities of the selected platforms and such specific ones.

*Keywords:* CMS; web application; security; vulnerability

## 1. Introduction

Content Management System (CMS) is a web-based application that helps multiple users with different permission levels to build and manage content online even without web programing knowledge. But on the other hand, they can be even used in education as the visual presentation of objects as part of the Object-Oriented Programming (OOP)[1)] module in Informatics. Every page created by the CMS can be accepted as a complex object which is composed of different sub objects. This by its definition is what the OOP is for – simplification by breaking it down into its simpler parts.

The market share provides us with different options which technically reviewed have their advantages and disadvantages. That can be visible from the description of the use of each of the reviewed systems.

This article is meant to provide an analysis of several CMS over the years and their vulnerability level according to international insights. The selected CMS are chosen according to personal opinion and to international insights!

In preparation of the article, the reports begin with a market share of the use of various content management systems among more than 10000 web applications. Part of personal experience, the analyses are structured in two categories based on the used technology for building the application: Microsoft technology – Umbraco and Sitecore, and PHP[2)] – WordPress and Drupal, which as part of the research defines them as the most popular among the selected technology.

As the IT world changes a lot these brings one constant battle against threats. Therefore, this article will add a vulnerabilities' report of the selected systems prepared as a comparison of the number and the common vulnerability for the selected CMS per year for the period of 2014 up until 2022. The data is collected through reports from the most popular worldwide insights like CVE and CVSS (Tal 2019).

**2. Relevance of the problem**

As CMSs become so popular, people would not pay attention to security, they only focus on having the best website to present to people with great design, pictures, and simple functionality. Hackers will find it easier to hack a simple website where there are no simple security functions to protect the website. Website owners always think that hackers have no interest in their websites since they are not considered as a large corporation as other websites, so they don't implement any security measures because it will cost more to implement in a website. However, hackers might not target the user website specifically, but it can be targeted from an automated system run by the hackers to hack many websites (Vasek, Wadleigh & Moore 2016).

Up until 2022, approximately 800 million web applications use a CMS, which is around 69% of all applications (Walsh 2022). And by 2026, the CMS market will reach more than 120 billion (Galov 2022). It is easy to think that CMSs are used by hobby bloggers, but those numbers prove the opposite. The CMS provides relatively easy development and maintain, which makes them quite popular choice in quickly providing the best solution to the client.

As software development is evolving with each new year providing new platforms and languages for development, for each programming language there are various content management systems.

Even though over the past decade the number of CMSs evolves, the analysis shows that since 2003, the year WordPress CMS was launched (WordPress 2015), it still dominates the CMS market share (see Figure 1). Another open-source CMS which holds around 10% of the CMS market share, is Drupal, which even though was created a couple of years before WordPress is still way down with those numbers. But according to the analysis those are the most popular content management systems using the PHP as programming basis.

Another concurrent programming option in the development industry is Microsoft technology. CMSs using that technology are also part of the market share (see Figure 1). According to it, the numbers are significantly lower than the PHP ones, but the practice shows that Microsoft technology usage grows, and its advantages are better than the popular PHP. According to the market share, two of the most popular CMS using Microsoft are Umbraco and Sitecore. The first one is open-source and the other is paid software property of Sitecore Corporation (initially called Pentia A/S).

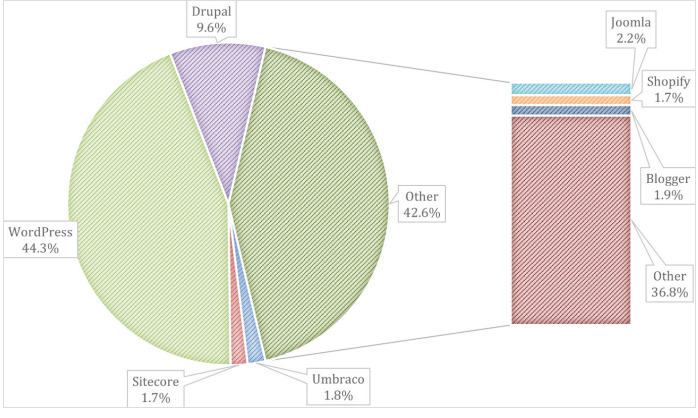
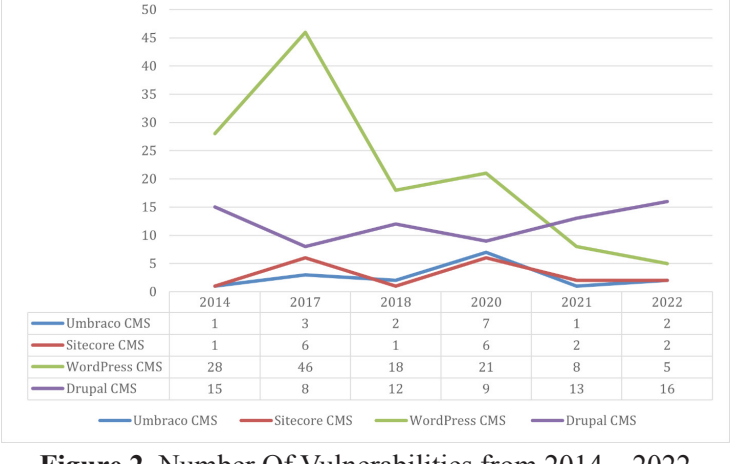



**Figure 1.** CMS Market Share among the Top 10000 Web Application

But the never stop innovating IT industry requires the development to be constantly aware of the new "trends" in cybersecurity, which makes us wander of the vulnerabilities level of the CMS technology (Schryen 2009).

From Figure 2 we can view the number of vulnerabilities for the period from 2014 until 2022 for the selected CMSs. On a first view, it is clear that one of the systems (the most popular as shown at Figure 1) becomes less vulnerable through the years, while the other three have a constant turnover. But analyzing the numbers, the CMS with decreased number is still in the list of vulnerability due to its popularity. This still makes it the most vulnerable.




| | 2014 | 2017 | 2018 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|---|
| Umbraco CMS | 1 | 3 | 2 | 7 | 1 | 2 |
| Sitecore CMS | 1 | 6 | 1 | 6 | 2 | 2 |
| WordPress CMS | 28 | 46 | 18 | 21 | 8 | 5 |
| Drupal CMS | 15 | 8 | 12 | 9 | 13 | 16 |

**Figure 2.** Number Of Vulnerabilities from 2014 – 2022

**3. Microsoft CMS**

Microsoft CMS included in this category are the kind of CMS that use Microsoft .NET platform in implementing the necessary functionality. With the help of the report from Figure 1, in the Microsoft CMS we have chosen: Umbraco and Sitecore.

*3.1. Umbraco CMS*

Umbraco is an open-source CMS built on Microsoft's .NET framework using ASP.NET and is written in C#. It was born in 1999 but version 1.0 was announced in 2003 by Niels Hartvig. And on February 16th, 2005, with Umbraco 2.0 it became fully open-source CMS. The latest major version, Umbraco 9, was launched on September 28th, 2021. Umbraco 9 saw a transition from ASP.NET to the .NET Core framework (Umbraco community, n.d.).

In 2005, Umbraco started hosting Codegarden – the official annual Umbraco developer conference. It evolved from 23 developers to more than 2000 attendees from all around the world.

In 2009, Umbraco launched a dedicated Umbraco Community site, called Our Umbraco. It serves as a platform for the online developer community to find technical documentation about Umbraco products, exchange knowledge, or ask other developers about Umbraco-related questions (Umbraco community, n.d.).

In 2013, the Umbraco source code became available on GitHub, making Umbraco more open-source-friendly and making it easier for the global community of developers to create issues and to make pull requests.

Besides the free CMS, Umbraco's offer of products expanded in 2015 to include Umbraco Cloud, a product providing secure and updated hosting through Microsoft Azure. Umbraco Heartcore, the headless CMS solution released in 2019, is running on Umbraco Cloud (Wahlberg & Sterling 2011).

Umbraco CMS can be used for complex solutions. It provides third-party integration, powerful audit trail, rollback and scheduling functionality. Its use is not bound by any templating which makes it flexible in design and functionality but on the other hand it means longer effort in development and in-depth planning.

This CMS has a powerful built-in search engine and user management. Another positive point is the availability of page preview in different devices which makes the content management more mobile. Umbraco also supports multi-sites and multilingual.

According to the market share (see Figure 1), 1.8% of the web applications are using Umbraco CMS, but the developer community is very supportive and active and with each year passed it expands very fast. Also, from a security point of view it is less vulnerable than the other open-source CMS selected in the article.

According to CVE reports from 2014 to 2022 (see Figure 2), Umbraco shows minimal quality of vulnerabilities (CVE details n.d.). The biggest number in that period was from year 2020 which in our personal opinion can be because of the

massive digital activities due to Covid-19 crisis and because of the major changes from that year in the Umbraco organization – the appearance of the new Umbraco CMS version and all additional features.

To sum up the flaws as visible on Figure 3, 36% of the vulnerabilities are from gaps in the executed code and another 36% from deficiency in protection against cross site scripting (XSS)[2] attacks. The other damages can be done from gaining information (9%), directory tranversal[4] (9%) and what is called a cross-site request forgery (CSRF)[5].

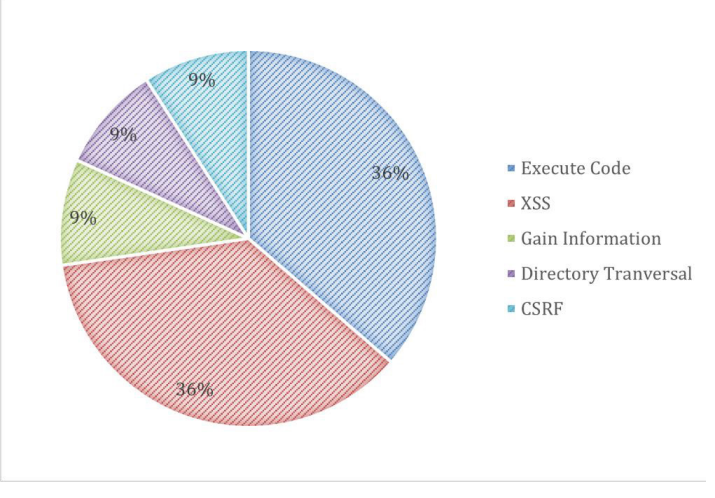



**Figure 3**.Umbraco CMS Vulnerabilities

Some of the international companies using Umbraco CMS are: Veterans Crisis Line, Marie Curie Library, International Tennis Federation, and Johnnie Walker.

As part of main work experience, Umbraco CMS will be further reviewed in future researches.

*3.2. Sitecore CMS*

Sitecore is a customer experience management company that provides web content management, and multichannel marketing automation software founded in the 1990s in Denmark. By 2001 it had evolved into the Sitecore CMS. Today, it is one of the world's most notable digital experience platforms (DXP) (Roberti 2007).

Sitecore differentiates the following products (Sitecore Manual - A guide to using the college CMS 2020):

– Sitecore Experience Manager (XM) – a content management system that powers omnichannel content delivery.

– Sitecore Experience Platform (XP) – a marketing automation solution that creates personalized customer experiences.

– Sitecore Experience Commerce (XC) – an e-commerce platform that leverages marketing automation to create a shopping experience.

Sitecore CMS can be used for very complex solutions. It provides third-party integration, powerful audit trail, rollback and scheduling functionality. Its use is also not bound to any templating but on it requires longer effort in development and in-depth planning (even longer than Umbraco CMS).

The CMS has also powerful built-in search engine and user management and also supports multi-sites and multilingual.

According to the market share (see Figure 1), 1.7% of the web applications are using Sitecore CMS which is less than the use of Umbraco CMS. One of the reasons might be the cost of the CMS as it is not an open-source platform.

From security perspective seen in Figure 2, Sitecore CMS shows minimal number of vulnerabilities. And again, the year 2020 shows higher number of flaws. From all those flaws as visible on Figure 4, the vulnerabilities are due to the executed code and 35% from lack of protection against XSS attacks. The other damages are from directory traversal (15%) and CSRF (10%), or by bypassing something from the application.

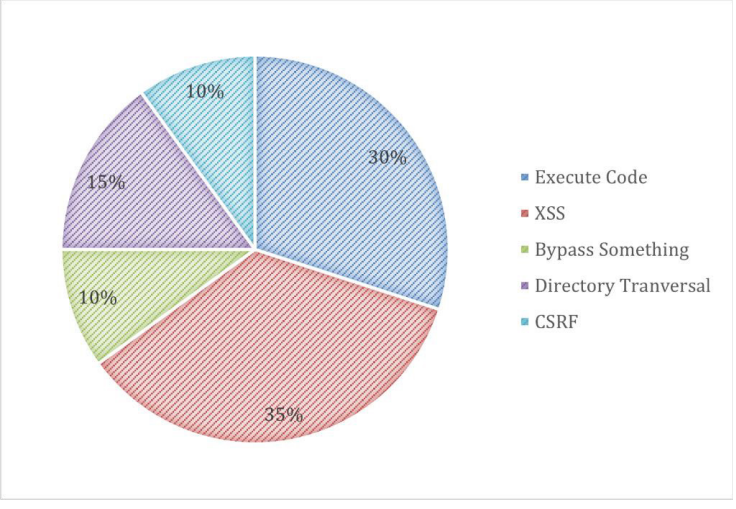



**Figure 4.** Sitecore CMS Vulnerabilities

Some of the international companies using Sitecore CMS are:

- L'Oreal
- Puma
- United Airlines
- Microsoft

**4. PHP CMS**

PHP CMS group includes CMS which uses PHP language in its functionality. PHP CMS selected in this analysis are the most popular ones according to *Figure 1. CMS Market Share Among the top 10000 web application*: WordPress and Drupal.

*4.1. WordPress CMS*

WordPress is an open source CMS, which allows the users to build dynamic websites and blogs. WordPress is the most popular blogging system on the web and allows updating, customizing and managing the website from its back-end CMS and components (WordPress 2015).

WordPress CMS provides more affordable solutions on a low-cost basis. It is easy to learn and use without of the box functionality. Due to its popularity, the developer community is bigger than all the others CMS' communities. WordPress has over 5000 themes and over 50000 plugins. And as part of the Google suits of products, the SEO perspective is very powerful. As part of the provided functionality, this CMS has a good audit trail and scheduling features (Zamościński & Kozieł 2020).

But as the coin has two sides, the disadvantages are more than the advantages. It over relies on third-party plugins and uses a huge number of resources which makes the design very restricted, and the performance is overweighted. Any customization comes at extra cost. For multilanguage sites, this CMS is not an option as it does not provide multi-sites solutions.

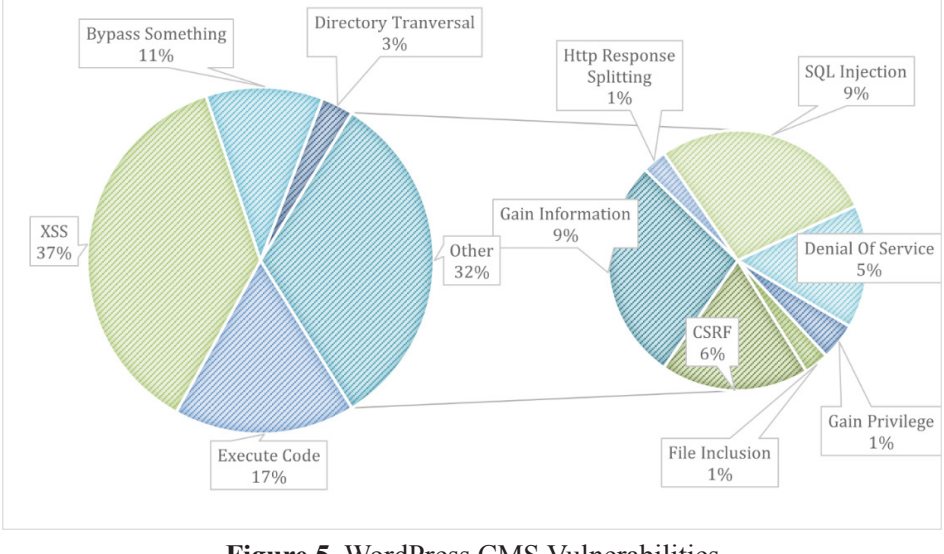



**Figure 5.** WordPress CMS Vulnerabilities

One of the biggest disadvantages of WordPress CMS is its vulnerability. Its popularity helps in finding solutions in the community of users and developers, but the security level is very low. According to CVE reports from 2014 to 2022 (see Figure 2), WordPress is the CMS that shows most flaws in its software which provides hackers an opportunity to gain access to a system or network, even though through the years the number of vulnerabilities decreases (CVE details n.d.).

According to the CVE report visible on Figure 5, the common vulnerabilities so far are as follows: executed code (17%), XSS attacks (37%), bypassing something (11%), directory traversal (3%). But there are a lot more to be aware of. Such as SQL injections[6] (9%), gaining information (9%), CSRF (6%), denial of service (5%), file inclusion (1%), gain privilege (1%) and HTTP response splitting (1%). (Zamościński & Kozieł 2020)

According to the market share, more than 33% among 10000 application used WordPress CMS which placed it the most popular among the selected CMS in this research (see Figure 1). But based on the vulnerability report, this makes us wonder how much the content used in applications with WordPress is secured and how much it is exposed of being harmed.

Some of the internationals companies using WordPress CMS are: The Walt Disney Company, Sony Music, BBC America, The New York Times Company, Mercedes-Benz, TechCrunch, The White House, University of Washington, and PlayStation Blog.

*4.2. Drupal CMS*

Drupal is a flexible CMS based on the LAMP stack, with a modular design allowing features to be added and removed by installing and uninstalling modules, and allowing the entire look and feel of the website to be changed by installing and uninstalling themes. The base Drupal download, known as Drupal Core, contains the PHP scripts needed to run the basic CMS functionality, several optional modules and themes, and many JavaScript, CSS, and image assets. Many additional modules and themes can be downloaded from the Drupal.org website (Hodgdon 2015 – 2017).

According to the market share, 9.6% of the word-wide application used Drupal CMS which placed it the second most popular among the selected CMS in this research (see Figure 1).

This CMS provides solutions to complex problems with more than 2500 themes and 46 000 modules to use in development like newsletters, podcasting components, etc. But in comparison to WordPress, it is harder to learn and use and needs more time to develop an application using Drupal CMS (Alghofaili 2018).

Drupal developers maintain their own security team responsible for evaluating security warning, searching for vulnerabilities, etc. The CMS has a section from where the users can be informed for the current security state (Meike, Sametinger

& Wiesauer 2009). Drupal CMS is considered more secure than WordPress, but proportionally less due to the difference in their popularity.

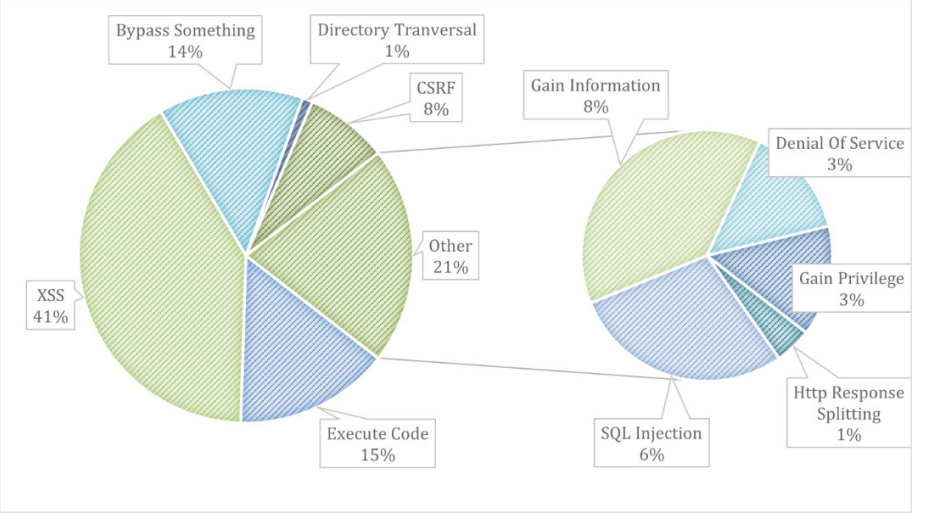



**Figure 6.** Drupal CMS Vulnerabilities

From Figure 2 it is visible than in the period from 2014 – 2022 the numberof vulnerabilities in applications using Drupal CMS increases. From Figure6 the common vulnerabilities can be seen too: executed code (15%), XSS attacks (41%), bypassing something (14%), directory traversal (1%), CSRF(8%). But again, we can see some additional ones: SQL injections (6%), gaining information (8%), denial of service (3%), gain privilege (3%) and HTTP response splitting (1%).

Some of the international companies using Drupal CMS are: Nasdaq; The University of Colorado; The Principal Financial Group; Tesla; NPR; NBC; Pfizer; The Grammy.

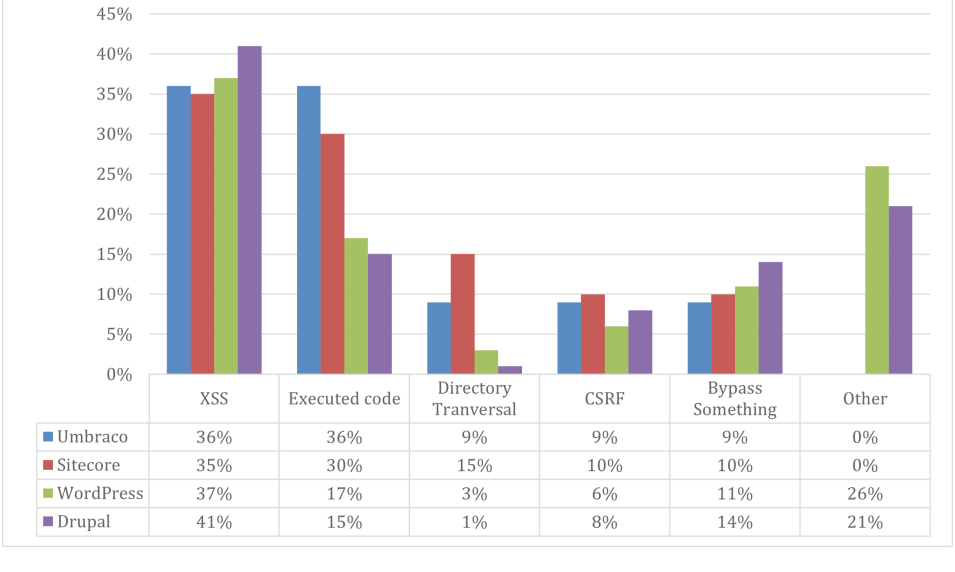
## 5. Conclusions

Choosing the right technology is always hiding a big risk. But all depends on the selected building technology and the necessary requirements. Not always the paid one is the best, nor the most popular. In this article, we analyzed two groups of systems separated by the technology used in the development. But with the analyses we are hoping of giving more clearness on the best system to work with or even educate in school or university.

Regarding the purpose of the research, we can conclude that Microsoft CMS provides more secure and flexible solutions (*as part of the advantages*

*and disadvantages description for each system*) for developing a web application which is even visible from the beginning of the present research on Figure 2. And as demonstrated on Figure 7, .NET platforms have a constant of only 5 common vulnerabilities compared to the PHP systems which have not only those 5 but also some other threats which go over 20% of the whole.

And among the selected systems in current review, we can conclude that the most preferable according to description and the vulnerability's report is Umbraco CMS, and the most vulnerable and less mobile (*as presented in the description of the system*) is WordPress CMS. That is also visible on *Figure 7. CMS common vulnerabilities report* – 26% of the threats on WordPress are from another group of flaws compared to the 0% on Umbraco CMS.




| | XSS | Executed code | Directory Tranversal | CSRF | Bypass Something | Other |
|---|---|---|---|---|---|---|
| Umbraco | 36% | 36% | 9% | 9% | 9% | 0% |
| Sitecore | 35% | 30% | 15% | 10% | 10% | 0% |
| WordPress | 37% | 17% | 3% | 6% | 11% | 26% |
| Drupal | 41% | 15% | 1% | 8% | 14% | 21% |

**Figure 7.** CMS common Vulnerabilities Report

Even though the technologies are constantly innovating, the better one is the one which is constantly up-to-date to every new technology in the IT industry. In further research we are going to present the use of such system in the education process as a method for converting the complex programming in something easy and simple.

## NOTES

1. Object-Oriented Programming (OOP) – a programming approach of decomposition of a problem into a number of entities called objects and builds data and functions around their objects (Ericson 2009).
2. PHP: Hypertext Preprocessor is a general-purpose scripting language for web development (PHP 2017 – 2022).
3. Cross Site Scripting (XSS) attack is a type a script injection into trusted web applications. Usually, the malicious script is sent through forms and can harm in different ways the end user – by manipulating the page content, accessing cookies, sensitive information, etc. (Singh 2018; OWASP, Cross-site scripting n.d.).
4. Directory traversal flaw aims to access files and directories (*configuration or system files or source code*) stored outside the web root folder (OWASP, Path Traversal n.d.).
5. Cross-Site Request Forgery (CSRF) is an attack which forces authenticated users to submit a request to the application against which they are authenticated. This kind of attacks can compromise the entire web application (OWASP, Cross Site Request Forgery 2022).
6. SQL injection exploit can manipulate the database data by executing SQLInsert/Update/Delete queries, shutting down database server, and in some cases commanding the operating system. (OWASP, SQL Injection n.d.).

## REFERENCES

ALGHOFAILI, R. A., 2018. *Security Analysis Of Open Source Content Management Systems Wordpress, Joomla, And Drupal*. Pomona: California State Polytechnic University.

CVE DETAILS., (n.d.). Retrieved from https://www.cvedetails.com/

ERICKSON, C., 2009. *Object Oriented Programming*. Retrieved from https://atomicobject.com/uploads/archive/files/ObjectOriented Programming.pdf

GALOV, N., 2022, March 7. *33 Mind-Blowing CMS Market Statistics You Need to Know in 2022*. Retrieved from https://review42.com/resources/cms-market-statistics/

HODGDON, J., 2015 – 2017. *Drupal 8 User Guide.* Drupal Org.

MEIKE, M., SAMETINGER, J., & WIESAUER, A., 2009. Security in Open Source Web Content Management Systems. *IEEE Security & Privacy*, 44 – 51. doi:http://dx.doi.org/10.1109/MSP.2009.104

OWASP, (n.d.). *Cross Site Request Forgery (CSRF)*. Retrieved from https://owasp.org/www-community/attacks/csrf

OWASP, (n.d.). *Path Traversal*. Retrieved from https://owasp.org/www-community/attacks/Path_Traversal

OWASP. (n.d.). *Cross-site scripting (XXX)*. Retrieved from https://owasp.org/www-community/attacks/xss/

OWASP, (n.d.). *SQL Injection*. Retrieved from https://owasp.org/www-community/attacks/SQL_Injection

PHP, 2017 – 2022. Retrieved from https://www.php.net/

ROBERTI, D., 2007. *Understanding Sitecore Fundamentals.* Sitecore Corporation.

SCHRYEN, G., 2009. Security of open source and closed source software: An empirical comparison of published vulnerabilities. *Proceedings of the 15th Americas Conference on Information Systems.* San Francisco, California.

SINGH, S., 2022, July. *5 Practical Scenarios for XSS Attacks. Sitecore Manual – A guide to using the college CMS.* Community College of Baltimore County.

TAL, L., 2019. Scoring security vulnerabilities 101: Introducing CVSS for CVEs Snyk.

VASEK, M., WADLEIGH, J., & MOORE, T., 2016, April 1. Hacking Is Not Random: A Case-Control Study of Webserver-Compromise Risk. *IEEE Transactions on Dependable and Secure Computing,* **13,** 206 – 219. doi:10.1109/TDSC.2015.2427847.

UMBRACO COMMUNITY, (n.d.). Retrieved from https://our.umbraco.com/

WAHLBERG, N., & STERLING, P., 2011. *Umbraco User's Guide.*

WALSH, S., 2022, June 29. CMS Market Share Trends: Top Content Management Systems In 2022. *Search Engine Journal*. Retrieved from https://www.searchenginejournal.com/cms-market-share/

WORDPRESS, 2015. Tutorials Point (I) Pvt. Ltd.

ZAMOŚCIŃSKI, P., & KOZIEŁ, G., 2020. Analysis of security CMS platforms by vulnerability scanners. *Journal of Computer Sciences Institute*, 261 – 268. doi:https://doi.org/10.35784/jcsi.2020

✉ **Dr. Lilyana Petkova, .NET Developer**
ORCID iD: 0000-0002-2859-8302
Web of Science Researcher ID: AEE-3308-2022
Scopus Author ID: 57435516700
CEO&.NET Developer at "LiLuzeNet Ltd"
2700 Blagoevgrad, Bulgaria
E-mail: lilyanapetkova92@gmail.com

✉ **Dr. Vasilisa Pavlova, Assist. Prof.**
ORCID iD: 0000-0003-3094-155X
Web of Science Researcher ID: H-4596-2015
South-West University "Neofit Rilski" (SWU)
Technical Faculty
66, Ivan Mihaylov Blvd.
2700 Blagoevgrad, Bulgaria
E-mail: vasypavv@gmail.com