Marin Kaluža[1]
Bernard Vukelić[2]
Tamara Rojko[3]

Preliminary communication
UDC 004.056.57

CONTENT MANAGEMENT SYSTEM SECURITY[4]

ABSTRACT

Content Management Systems (CMS) are often used for website development. Websites are targets of various malicious attackers, and therefore it is necessary to be familiar with the security level of websites.The paper describes some basic features of the well-known open source CMS platforms: WordPress, Joomla and Drupal. It also explains the ten most common web vulnerabilities. Web vulnerability testing has been carried out by means of various software tools. The basic installations of the CMS systems have been tested. After having tested each web vulnerability, a possible additional web security measurement for each CMS is indicated. The web vulnerabilities which cannot be directly affected by the CMS security settings have been explained. It has been shown that the basic installations of the CMSs fail to ensure safety requirements due to irresistance to some threats. Necessary software tools for the tested CMSs have been specified in order to ensure the resistance to threats which have not been provided in the basic installation of the tested CMSs. A questionnaire has been developed for the purpose of examining the security level on the websites of business entities in Croatia, and a survey has been conducted in Croatian business entities engaged in computer science, accounting and industry.

Key words: *CMS, security, web vulnerability, attack, protection*

1. INTRODUCTION

Content Management System (CMS) is a computer program used to create, edit, manage and publish content in a consistently organized manner. CMS is often used for handling specific documentation such as news, technical manuals, guides and brochures. Content management may include image media, audio and video files, electronic documents and other web content (CARNet, 2008). Today, many companies use CMSs for the development and maintenance of various websites. CMSs present a type of software solution with the function of content management on websites. Since such a software solution is used by means of a web browser, it is affected by various security threats in the same way other software solutions (web applications) are.

In general, it refers to each solution which provides for classification, organization, networking and any other form of content editing. Although the term may be used for manual processes of content management, today it is primarily used for various software solutions that enable advanced

[1] PhD, Senior Lecturer, Polytechnic of Rijeka, Vukovarska 58, Rijeka,Croatia. E-mail: mkaluza@veleri.hr

[2] MSc, Senior Lecturer, Polytechnic of Rijeka, Vukovarska 58, Rijeka,Croatia. E-mail: bvukelic@veleri.hr

[3] Student, Polytechnic of Rijeka, Vukovarska 58, Rijeka,Croatia. E-mail: rojko.tamara@gmail.com

[4] Received:15. 1. 2016.; Accepted: 1. 4. 2016.

management of a large amount of information. CMSs are used to sync data from multiple sources, execute collaborative projects, organize work in corporate settings, etc. (CARNet, 2008).

In order to prepare, publish and display content, a web browser is sufficient, and there is no need for additional softwares on a user's computer. A CMS usually interprets a large number of file formats (e.g. XML[5], PDF[6], JPEG[7], AVI[8], MP3[9], etc.), which may be stored in the CMS repository. After creating the structure of documents and the design of content elements (*container*), the standardized templates allow modification of the existing and adding a new content, while the appearance and the structure of web pages remain unchanged.

The aim of this paper is to examine the extent to which companies engaged in computer and related activities carry out security techniques to protect the CMS system used and whether they are resistant to threats. We believe that the resistance of CMSs to critical web application threats can be achieved by installing frequently used CMSs, the necessary safety add-ons and application server settings. Since some threats to web applications may be avoided regardless of the CMS used, because they refer to the application server settings, the resistance to threats depends on the knowledge of the CMS administrator. Are the administrators familiar with the threats to the system security?

We believe that the CMS administrators fail to use and fail to set the mechanisms necessary to protect the system from threats to web applications, which makes CMS implementations open to malicious attacks. In order to verify the above mentioned, a research, which will examine the types of CMS implementations, the presence of security mechanisms to threats to web applications, as well as techniques and procedures for verifying the existence of errors (holes, backdoors) in the system protection, will be conducted with the aim to maximize the CMS security level.

2. RELATED WORK

The research conducted in December 2014 by the company Sungard Availability Services (Florentine, 2015) demonstrated three main features that presented the greatest concern to IT (Information Technology) managers: security threats, delays in accessing and processing data, finding talented employees. Threats to IT systems in companies have become increasingly sophisticated. More than half of the respondents believe that when it comes to the security of systems, the companies should not be thrifty. Although IT managers are mostly concerned about external threats, a very common cause of safety errors is the lack of attention of the employees within a company. For example, 62% of the questionnaire respondents have answered that they

[5] XML (*EXtensible Markup Language*) – data marking language - URL: http://www.w3.org/XML/

[6] PDF (*Portable Document Format*) – document file format. It is used for storing two-dimensional document regardless of device and printing resolution - URL: https://acrobat.adobe.com/us/en/products/about-adobe-pdf.html

[7] PDF (*Portable Document Format*) – document file format. It is used for storing two-dimensional document regardless of device and printing resolution - URL: https://acrobat.adobe.com/us/en/products/about-adobe-pdf.html

[8] AVI (*Audio Video Interleave*) multimedia resource (file) which enables syncronized reproduction of sound and video - URL: https://en.wikipedia.org/wiki/Audio_Video_Interleave

[9] MP3 (*MPEG Layer III Audio Encoding*) standardized technology and format for compression of sound into file - URL: https://en.wikipedia.org/wiki/MP3

leave their mobile phone turned on and their laptop open in the place where they can be accessed by an unauthorized person. According to the Eurobarometer[10] survey (EU, 2015), European citizens are concerned about their online safety. A total of 89% of the users avoid disclosing their personal information online, while 85% believe that the risk of cybercrime is increasing. Almost half of the respondents have detected malicious software on their device, almost one third say to have received a malicious email, phone call or, in fewer cases, another type of cybercrime, such as online frauds or identity thefts. If they experienced some type of cybercrime, the majority of the respondents would contact the police.

One out of two companies in Germany is affected by cyber-attacks. The Bitkom association conducted a research in which more than 1,000 companies (Kempf, 2015) participated. As a part of the research, more than 5,000 companies were contacted, and 1,074 provided answers. The results of the phone surveys conducted in January and February basically confirmed the already known diagnosis. Companies of all sizes are at huge risk of digital attacks. More than half of the companies surveyed (51%) have been affected by cyber-attacks in the last two years. Another 28% believe to have been the victims of virtual attacks, although they have no evidence for that. When analyzing individual industries, the automobile industry is the favorite target for cyber "terrorists". This is because it is "a very innovative industry" (Kempf, 2015). The same applies to chemical and pharmaceutical industries (66%). Financial and insurance branches, in which identity theft plays an important role, are slightly less affected (60%) (Kempf, 2015).

3. WEB APPLICATION VULNERABILITIES

Web applications represent software solutions which provide accessibility to the user interface through a web browser, and are performed on a remote server by means of interpreter programming languages. Accordingly, and as explained in the previous chapter, CMSs represent the kind of web application that performs the function of content management.

There are many organizations which deal with the security issues of computer systems and web applications. Some of them are: SANS Institute[11], Web Application Security Consortium[12], Computer Emergency Response Team (CERT)[13], The Open Web Application Security Project (OWASP)[14], SecurityFocus[15]. In this paper, the recommendations of the OWASP organization are used. The representatives of the OWASP organization have created a document in which

[10] Eurobarometar (EB) is a specific research project of international, comparative and social research conducted for the needs of the European Commission – URL: http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/General/index

[11] SANS Institute is a private American company specialized in information security and cybersecurity training - URL: https://www.sans.org/.

[12] WASC is an international group of experts and organizational representatives who create open source safety standards for World Wide Web - URL: http://www.webappsec.org/.

[13] CERT is a group of experts who work on security incidents on computers - URL: http://www.cert.org/.

[14] OWASP is a non-profit voluntary organization directed towards the improvement of software security - URL: https://www.owasp.org.

[15] SecurityFocus is an online portal which provides information related to computer security to users - URL: http://www.securityfocus.com/.

the ten most critical vulnerabilities of web applications are listed and explained (OWASP, 2013). The same organization has recommended certain tools for testing critical vulnerability of web applications. A list of vulnerabilities and tools for testing individual vulnerability is shown in Table 1.

Table 1. Tools for detecting Web application vulnerabilities

No.	WEB VULNERABILITY	TESTING TOOLS
1.	*Injection flaws*	SQL Inject Me and Zed Attack Proxy (ZAP)
2.	*Broken Authentication and Session Management*	ZAP
3.	*Cross Site Scripting* – XSS	ZAP
4.	*Insecure Direct Object References*	HTTP Directory Traversal Scanner, Burp Suite and ZAP
5.	*Security Misconfiguration*	OpenVAS and WATOBO
6.	*Sensitive Data Exposure*	Qualys SSL Server Test
7.	*Missing Function Level Access Control*	OpenVAS
8.	*Cross Site Request Forgery* – CSRF	Tamper Data (Samurai WTF), WebScarab or ZAP
9.	*Using Known Vulnerable Components*	OpenVAS
10.	*Unvalidated Redirects and Forwards*	ZAP

Source: http://resources.infosecinstitute.com/owasp-top-ten-testing-and-tools-for-2013/

Injection flaws threat occurs when an application sends untrusted data to an interpreter. These shortcomings are particularly common in legacy systems[16], and are often found in SQL[17], LDAP[18] and XPath[19] queries, operating system (OS) commands, program arguments and similar. Injection flaws occur when a user's data are used for creating queries and commands without checking whether they contain special characters that could be used for malicious purposes. A malicious code can change the content and meaning of the query (command), and therefore the server can perform the user's customized commands. Injection flaws could be detected with almost every vulnerability detection tool (scanner).

Authentication and session management represent a basic and crucial security mechanism which protect web applications against attackers. Vulnerabilities of these mechanisms usually result in complete compromisation of a web application. By taking advantage of these vulnerabilities, the attacker can completely bypass authentication and gain an unauthorized

[16] legacy system – a system built using old or obsolete technologies, important for the environment in which it is used because it performs important functions.

[17] SQL (*Structured Query Language*) is the most popular query language used for the management (development, updating and research) of data in relational databases.

[18] LDAP (*Lightweight Directory Access Protocol*) is an application protocol used for directory reading and writing using IP protocol.

[19] XPath (*XML Path Language*) is a query language used for addressing different parts of XML documents and searching for values in an XML document.

access to the web application content or may come into possession of usernames and passwords, session IDs or other sensitive data (OWASP, 2007). Broken Authentication refers to the incorrect implementation of mechanisms for authentication while Session Management relates to the associated functions such as logging off, session expiry, secret questions, password reset, etc. If the authentication mechanisms have not been properly implemented, it is possible to take advantage of this weakness in order to gain more rights over the application. Some examples of poor implementation of authentication process are: different return error for a failed authentication, improper process for providing forgotten password, no existing protection against excessive number of attempts, reminders along with authentication questions (OWASP, 2007). Users are mostly authorized with the help of a session key which is usually stored in the session ID, and therefore session keys are the attackers' targets. If the algorithm for creating session key is bad, the attacker can guess or calculate the value of the other existing session key and can access the target application on behalf of the user of the found session key. The attack is known as Credential/Session Prediction (OWASP, 2011).

Cross-site scripting - XSS is an attack technique which forces the web application to forward an attacking script to a user, and the script is later injected into the user's web browser and executed. The attacking script is usually written with JavaScript[20] language, but also in other programming languages supported by the user's web browser: VBScript[21], ActiveX[22], Java[23] and Flash[24]. Taking advantage of XSS vulnerability allows the attacker execution of arbitrary code within the user's web browser which may result in: hijacking the user session ID, execution of phishing attack[25], redirecting of web browser to any location, installation of malicious softwares, etc.

Insecure Direct Object References is a vulnerability which allows the attacker to approach a variety of objects, such as files, folders or data in a database. URL addresses, parameters in forms or session IDs are often used in applications as a reference to access various objects. If the access control of a web application object has not been achieved or has been achieved improperly, an attacker can achieve an unauthorized access to other web application objects. The web application objects are often various files, folders, records in a database, various parts and functionalities of a web application (OWASP, 2010).

Security Misconfiguration may occur at any application level, including platforms, application server, original source and custom program code. Developers and network administrators need to collaborate in order to achieve the correct configuration of all components of the application system. Automated scanners are useful for detecting defects, incorrect settings, the way of using user accounts, unnecessary services (OWASP, 2010).

[20] JavaScript is a script programming language, executed on the user's Web browser.

[21] Visual Basic Scripting Edition is an active script language developed by the Microsoft on the basis of Visual Basic.

[22] ActiveX is a software framework developed by Microsoft which adapts Component Object Model (COM) and Object Linking and Embedding (OLE) technologies for the content downloaded from network, especially in the context of World Wide Web.

[23] Java is an object-oriented programming language.

[24] Flash is a tool for creating vector graphic, animation, presentation, complex application and other content which enable multimedia interaction with users.

[25] Phishing attacks are activities by which unauthorized users try to force users to reveal their confidential information via false emails and false Web sites.

Sensitive Data Exposure distorts integrity and confidentiality of data. Many web applications fail to protect sensitive data (e.g. credit card information or authentication information) in a proper way, with the appropriate encryption. For transferring secure data, web applications can use the secure version of HTTP protocol - HTTPS (*Hypertext Transfer Protocol Secure*) protocol which uses SSL (*Secure Sockets Layer*) for the protection of messages transmitted via network. Secure Data should be written in an encrypted form with the help of web application, and they should also remain in that form during transmission via network in order to ensure their integrity and confidentiality (OWASP, 2013).

Access level must be defined for each user. It is necessary to determine for each user what s/he may and/or may not access. A web application must undergo access control to determine whether a certain user has the right to access the requested part of the web application. It is necessary to ensure the navigation through the user interface by allowing only authorized functions.

Cross-site Request Forgery - CSRF is a vulnerability which undermines confidence between a web application and a user's web browser. All sites which rely only on automatically sent authentication information are vulnerable. Automatically sent authentication information are *cookies*, authentication header (HTTP[26] basic), IP address, client SSL[27] certificates, authentication to domain (CARNet, 2010). Measures for achieving resistance against CSRF vulnerability are the following: requiring a secret user-specific token for each request towards a web application, client's data sending for authentication in each HTTP request towards operations in a web application, limitation of session cookies duration (OWASP, 2013).

Insufficient systematization and application of engineering methods in developing a web application and the use of other components in a web application may contribute to increase the web application security flaws. **Using Known Vulnerable Components** is insecure because it jeopardizes security of a web application. One option to avoid this vulnerability is to use only the original, copyright components, which actually present an unexpected phenomenon due to the fact that the efficiency of a web application is questionable. In order to prevent using known vulnerable components, the following is required: identifying all components and versions being used (including add-ons); monitoring the safety of these components in public databases and similar, and updating them; establishing safety policies (good practice, software development, security tests, acceptable licenses); setting up security wrappers (envelopes) around components; collecting information on the current use of components; identifying vulnerabilities in applications and repositories (OWASP, 2013).

Applications often redirect users to other sites and use redirections of parameters. **Unvalidated Redirects and Forwards** allow the attacker to select (change) the target site and/or sent parameters. Due to insufficient validation, the attacker may redirect the victims to phishing or malware sites or use redirects unauthorized access to sites (OWASP, 2013).

[26] HTTP - HyperText Transfer Protocol - a communication protocol which is used on the application layer for the comunication between a server and a client

[27] SSL - Secure Sockets Layer - a cryptographic protocol designed to provide communications security over a computer network

4. TESTING CMS VULNERABILITIES

There are a number of CMSs on the market, commercial as well as free (shareware, opensource). According to the analysis of various forums, blogs and other sources, the most widely used free CMSs are: WordPress, Drupal and Joomla (Tripp, 2016), (Chapman, 2011), (Beale, 2014), (Sponaugle, 2013).

All three mentioned CMSs have been tested according to the tools from Table 1 (Rojko, 2015.)

Table 2. Existence of security mechanisms according to web vulnerabilities for tested CMSs

No	WEB VULNERABILITY	WordPress	Joomla	Drupal
1	Injection flaws	Yes	Yes	Yes
2	Broken Authentication and Session Management	Yes+	Yes+	Yes+
3	Cross Site Scripting	Yes	Yes	Yes
4	Insecure Direct Object References	Yes Server	Yes Server	Yes Server
5	Security Misconfiguration	Yes Server	Yes Server	Yes Server
6	Sensitive Data Exposure	Yes Server	Yes Server	Yes Server
7	Missing Function Level Access Control	Yes+	Yes+	Yes
8	Cross Site Request Forgery	Yes	Yes	Yes
9	Using Known Vulnerable Components	Yes	Yes	Yes
10	Unvalidated Redirects and Forwards	Yes+	Yes	Yes+

Source: Author

Table 2 shows (non)implementation of protective mechanisms for vulnerabilities explained in Chapter 3 for all tested CMSs. “Yes” indicates the existence of protection mechanisms in the basic version of the tested CMS. “Yes+” indicates the existence of protective mechanisms after the plug-ins, extensions or modules have been installed. “Yes Server” indicates the existence of protection mechanisms against vulnerability, which are set on the application server, and not as application elements of the CMS.

Broken Authentication and Session Management threat usually carried out by Brute-force attack can be avoided by installing plug-ins (add-ons) on all systems tested. For Wordpress, it is necessary to install the *Brute Force Login Protection* plug-in which limits the number of allowed login attempts, provides blocking/unblocking of a certain IP address, informs users on the number of login attempts left, and notifies the administrator via an e-mail about the failed attempt to login from a particular IP address. For Joomla, it is necessary to install *Brute Force Stop plugin* which stores the number of logins failed, provides setting for the number of logins failed and blocking of IP address. For Drupal, it is necessary to install the *Flood control* module which allows limiting the number of invalid logins in the system before blocking the account, disallows access for a particular IP address (temporary or permanently). Session Management problem can be solved in WordPress by installing the *User Session Control* plug-in which shows all active sessions of the user, sorts sessions by user, roles, creation date, expiration date or an IP address, and allows for a session to be destroyed quickly and easily. For Joomla, it is necessary to install the *Session Keeper plugin* which allows limiting the session duration according to a user. For Drupal, the *Session Limit* module should be installed which provides logout for the oldest session without asking, prevents logging from a different place, informs the user about the disconnection, provides configuration of the maximum number of sessions, limits the exclusion of a session per privilege, and provides implementation of a *trigger*[28].

Insecure Direct Object References threat that is manifested in the so-called *Directory browsing* attack, and the Security Misconfiguration threat do not refer to web application settings and functionalities, and they may be protected against by proper web server settings (e.g. the use of a firewall, setting up security settings of the Apache web server such as *RequestReadTimeout, TimeOut, MaxRequestWorkers, ServerSignature, ServerTokens*, and other).

Sensitive Data Exposure threat in addition to the application settings for storing confidential data in encrypted form, includes encryption of messages transmitted between a client (a user's web browser) and a server (a web application) during which SSL can be used through HTTPS[29] protocol. This threat also cannot be prevented by application setting, but it can be prevented by application server settings (e.g. Apache HTTP Server[30]).

Missing Function Level Access Control threat in Drupal has been covered in the basic installation. This threat is not covered in the basic installation of WordPress, but it can be covered by installing Advanced Access Manager plug-in. In Joomla, this threat can also be covered by installing the ACL *Manager (Access Control List)* extension.

Invalidated Redirects and Forwards threat has been covered in a Joomla test version. For ensuring against this threat in WordPress it is required to install the Redirection plugin, while in Drupal it is necessary to install Page manager redirect module.

Using known Vulnerable Components threat represents a vulnerability of CMSs which may occur after the installation of add-ons (modules, extensions, plug-ins) and which should be checked and tested by means of appropriate scanners (e.g. Acunetix[31], Defensecode Web Security Scanner[32], Webscanner[33], Netsparker[34]).

Other uncommented threats have been covered and tools for testing the threats (scanners) have not registered any failure in the tested CMSs.

[28] Trigger – a mechanism on a database used for preserving integrity of data

[29] HTTPS - HyperText Transfer Protocol Secure - a communication protocol used on the application network layer, it enriches

[30] HTTP protocol with security functionalities

[31] Acunetix - URL: http://www.acunetix.com/

[32] Defensecode Web Security Scanner - URL: https://www.defensecode.com/

[33] Webscanner –URL: http://webscanner.sourceforge.net/

[34] Netsparker - URL: https://www.netsparker.com/web-vulnerability-scanner/

Given the fact that the tested CMSs can cover all the threats by using various mechanisms and add-ons, it can be said that all tested CMSs are resistant to the ten critical threats to web applications. However, some threats cannot be covered by application mechanism and add-ons, but rather by application server settings (e.g. Apache HTTP Server). For the purpose of checking the protection against threats to web applications, a research has been carried out on whether the administrators of CMSs are in charge of the threats by setting the security settings on the application server.

5. RESEARCH METHODOLOGY

The objective of this paper has been to determine which security techniques are used by companies in their operations to protect the CMS. The analysis includes the following variables: the size of the company, the type of ownership, business activity, the use of CMS in business, the type of CMS, the name of CMS used, the frequency of CMS backups execution, the frequency of using web scanners, the type of web scanner used while testing CMS, the person in charge for CMS administration, the frequency of checking log files, the use of SSL protocol, the type of SSL protocol, the mode of using SSL protocol, the use of additional network protocols which provide additional security to the application layer, the use of security tools for detecting web vulnerability, a way of checking for software updates for providing security, following novelties related to web vulnerability.

The variables have been selected on the basis of the issues presented in the previous chapters. The research was conducted in the period between 7 August 2015 and 10 September 2015 on the sample of 54 respondents. The data were collected by means of a questionnaire created in the open source code tool SurveyMonkey[35]. The questionnaire contained 18 questions, out of which three were related to the company structure, and the remaining 15 referred to the issues related to testing the security techniques for protection of the CMS system used. The questionnaire was sent to 400 email addresses. The information on email addresses was taken from a business search website Tvrtke.com[36] under the following categories: information science, accounting, industry, and other. A request to fill out a questionnaire was sent to the respondents via email, and the questionnaire was accessed through the link sent. The survey was carried out anonymously. The research results were presented in a clear manner; they were described textually and presented graphically.

6. RESEARCH RESULTS

6.1 The analysis of the structure of companies which participated in the research

Of the total number of the companies which participated in the research, 74.03% of them had up to **10 employees**, 24.08% had up to **50 employees**, 1.90% up to **200 employees and** 0.00% companies had **more than 200 employees**.

The type of ownership of the companies which participated in the research was **private** for all the respondents who answered the questionnaire (100.00%), while 0% were state-owned or in the

[35] SurveyMonkey is a free online scanner for creating surveys. Home page: https://www.surveymonkey.com/.

[36] Tvrtke.com business search website - URL: http://www.tvrtke.com/

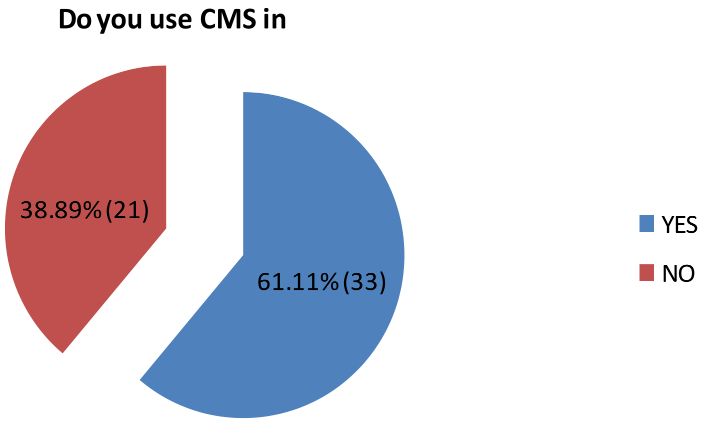
form of mixed ownership (the form of cooperation between two or more entrepreneurs seated in different countries).

The companies which participated in the research were primarily engaged in computer and related industries (75.93%), manufacturing (3.70%), trade and catering (3.70%), telecommunications and postal services (0.00%), health (0.00%), finances (0,00%), and education (1.85%), but 14.81% of the companies selected the option 'other activity'. The 'other activities' were construction and court expertise.

6.2 The analysis of questions related to security techniques for CMS protection

When the companies were asked whether they used CMSs, 61.11% of them answered "**Yes**" and 38.89% answered "**No**". Further analysis is based on the companies which provided a positive answer.

Chart 1. Using CMS



Source: Author

When asked about the type of CMSs they used, 48.48% of the respondents answered **free**, 6.06% answered **commercial**, 18.18% answered **custom** CMS and 27.27% of the respondents **failed to provide** an answer.

The respondents were asked to enter the name of the CMS they used, and a list of twenty-one name appeared. They are the following: Wordpress,Trac; Joomla; Drupal; Wikimedia; SharePoint; Luaus ISWAP; self-owned CMS; Marker CMS; CakePHP; Django CMS; DotNetNuke; VTiger.

Prior to any change of the content, 9.09% of the respondents performed backup of the CMS, 21.21% **prior to any change of the CMS structure**, 6.06% **failed to perform backup**, 36.36% chose the option **other** (**please specify**) and 27.27% **failed to provide an answer**. Under the option **other (please specify)**, 12 answers were provided, and they were daily and weekly. Since these were IT companies, the surprising fact was that 6.06% of them failed to perform backup, which was one of the basic activities that administrators had to do.

After every change of the content, 6.06% of the respondents checked their CMS by using web scanners, 21.21% checked their CMS after each change of the CMS structure, 27.27% failed to check the security of CMS by using web scanners, 18.18% chose option **other (please specify)** and 27.27% failed to provide an answer.

Under option **other (please specify)**, six answers were provided which were the following:

- Weekly,
- Daily,
- Occasionally,
- CMS is located on a private network,
- Very rarely, the security settings are set during the setting up of the CMS and the administration is performed via SSH,
- Web scanner is not the primary mechanism for CMS security check, it is performed when necessary.

When asked about the kind of web scanner used for testing CMSs 36.36% answered **free**, 6.06% answered commercial, 9.09% answered **custom**, 21.21% answered **other (please specify)** and 27.27% **failed to provide an answer**.

When asked about the person in charge of the administration of the CMS, 51.52% answered it was **the administrator**, 18.18% answered that **several people** were in charge, 3.03% answered it was **anyone** in the company, 0.00% stated **"other" (please specify)** and 27.27% **failed to provide an answer**. These answers were in line with the expectations given the fact that these were IT companies which employed an employee as a system administrator.

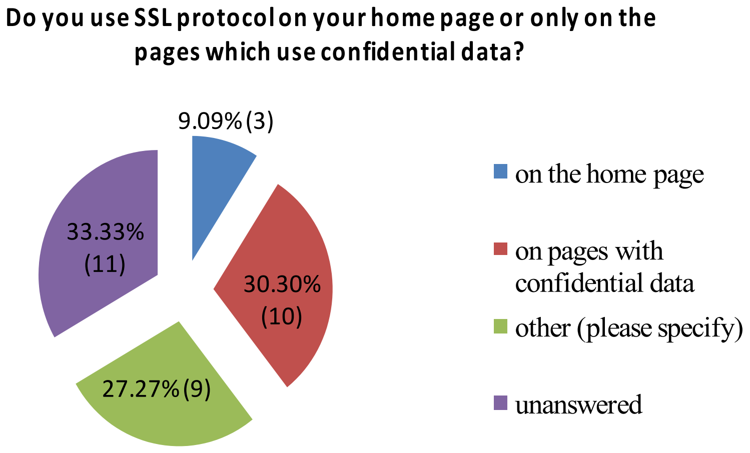
Log files were checked on **daily basis** by 12.12% of the respondents, **weekly** by 12.12%, **monthly** by 24.24%, 15.15% **failed to check** the log files, and 9.09% selected the **option other (please specify)**, and 27.27% **failed to answer**. Under the option **other (please specify)**, the answers were: when necessary, we used plugins as warnings.

When asked whether they used SSL protocol, 36.36% answered positively and 30.30% negatively, while 33.33% of the respondents failed to answer the question.

A **purchased certificate** for SSL protocol was used by 18.18% of the users, **free version** was used by 30.30%, 18.18% selected the option **other (please specify) and** 33.33% of the users **failed to provide an answer**. Under the option **other (please specify)**, six identical answers were given, that they did not use SSL protocol.

On their **home page** 9.09% of the users use SSL protocol, 30.30% used on the **sites that contained confidential data,** the option **other (please specify**) was selected by 27.27% and 33.33% of the respondents **failed to provide an answer**. Under the option other (please specify) the answers were: on each one, we did not use it.

Chart 2. The use of SSL protocol on certain sites



Source: Author

When asked about the use of additional network protocols related to security, the **Diameter** protocol, which provided additional security for the application layer related to logging into the system, was used by 15.15%, the **LDAP** protocol was used by 12.12%, the **RADIUS** protocol by 6.06%, the **SIP** protocol by 0.00%, the option **other (please specify)** was selected by 24.24% and 42.42% of the respondents **failed to provide an answer**. Under the option **other (please specify)** the following answers were given: our own protocol, we did not use a protocol, and SSH protocol.

The respondents provided the following answers when asked about the name of the security tool they used: the **ZAP** tool was used by 12.12%, **OpenVAS** by 6.06%, **WebScarab** by 3.03%, **Wapiti** by 0.00%, the option "**I don't use**" was selected by 36.36%, the option **other (please specify)** was selected by 6.06% and 36.36% of the respondents **failed to provide an answer.** Under the option **other (please specify)** the following answers were given: our own tools and tests, and DefenseCode Web Security Scanner.

New information and components, software versions or new add-ons were checked by 30.30% **by Internet searching**, 9.09% heard from their **colleagues**, 30.30% by **following project sites**, the option **"I never check**" was selected by 3.03%, the option **other (please specify)** was selected by 15.15%, and 12.12% of the respondents **failed to provide** an answer. Under the option **other (please specify)** the following answers were provided:

- Automatically,
- Package managers,
- A partner company is responsible for web server maintenance and it performs regular upgrades and active monitoring of servers, while the CMS is upgraded by security upgrades immediately after their appearance (mailing list).

News related to web vulnerabilities were followed by means of various organizations by 30.30% of the users, 36.36% never followed and 33.33% of the users **failed to answer** the question.

7. DISCUSSION

Of the total number of the companies surveyed (54), the majority are companies with up to 10 employees (40). It may be noticed that it is mainly about micro companies (<10 employees), followed by small companies (<50 employees). This kind of result was expected given the fact that the primary activity of the above mentioned companies is information science where the ability to adapt to constant changes is of huge importance, and where it is certainly easier to achieve that in companies with fewer employees.

All companies surveyed are privately owned. This is probably due to a relatively small sample (N=54) considering the fact that the questionnaire was sent to 400 addresses of the companies all across the Republic of Croatia, randomly chosen from a previously mentioned source (Chapter 5).

The companies' activities are mainly computer and related activities, which is of no surprise given the fact that the CMS is used for managing the content on the Internet and is increasingly used for developing websites. Most of the companies surveyed use CMSs in their business; however, the number (33) is not much bigger than the one for those who do not use it (21). The companies that use CMSs mostly use a free version, while a very small number of companies use a commercial version, although a good portion of the respondents failed to answer the question. Most of the companies have stated that they use WordPress which is in line with global trends. This CMS is exceptionally popular among free CMSs due to its ease of use and a great number of modules which are provided and may be relatively easily adapted to the needs of users.

The companies perform backup mostly on daily basis and thus provide additional security measure to their work, while a small percentage (6.06%) of the users never perform backup. A large number of companies do not use web scanners as an additional tool for checking security, although a number of companies check for possible security flaws after every change in the CMS structure. Part of the companies which use web scanners, use the free version of the tool. In most companies, the administration of the CMS is the responsibility of the administrator whose task is to set the maximum security level of work, which is also something expected given the fact that the companies are mainly engaged in computer technology.

Log files are usually checked monthly, although a large number of respondents did not answer this question. Such a small number of daily and weekly checks is surprising given the presence of malicious attacks on the system via the Internet. The reasons for this may be of different character, or they have positive experiences with the security techniques they have used so far or they have not experienced any serious threats and attacks so far.

A large number of the respondents (33.33 %) failed to answer the question about whether they used an SSL protocol. Only 36.36 % of the companies surveyed used an SSL protocol in their business, while 30.30 % never used it. The companies surveyed which used an SSL protocol generally used a free version mainly set up on sites with confidential data. The companies mostly used the Diameter and LDAP protocol as an additional security to the application layer during logging into the system, although most of the companies failed to answer the question.

For detecting web vulnerabilities, majority of the companies (36.36 %) did not use safety tools recommended by organizations engaged in security of computer systems and web application. Most of the companies (60.60 %) checked whether a component, a software version or a new add-on had been updated by searching the Internet or following the project sites. Most of the companies (36.36 %) did not follow the news related to web vulnerabilities with the help of various organizations such as the SANS Institute, OWASP organization, Web Application Security Consortium, Computer Emergency Response Team. A somewhat disturbing fact is that 36.36 % of them did not follow the news, as well as the fact that more than 30 % failed to answer the question, although they were mostly IT companies.

8. CONCLUSION

Today many companies use CMSs for developing and maintaining various web pages and sites. Some companies develop their own CMSs, some use the commercial ones, and some use free CMSs.

In this paper, some basic features of three CMSs have been presented: WordPress, Joomla and Drupal. Critical web vulnerabilities against web applications have been explained. Each vulnerability has been tested on the basic installation of all the tested CMSs (Wordpress, Joomla, Drupal) and possible security measures have been listed. The test results of the CMS systems have been presented as well as the list of threats against which the tested CMS systems were resistant in their basic installations. A list of software add-ons for each tested CMS has been presented which has helped CMSs become resistant to some threats. A list has been presented which contains the threats that may not be solved by the CMS setting, but only by the settings of the web server and network resources. Free CMSs with basic installation fail to provide the necessary security level (resistance to threats). The resistance of the tested CMSs to each of the ten analyzed critical threats against web applications may be achieved by installing add-ons (plugin, extension) and the web server and network resource settings.

A questionnaire was developed and a survey was conducted in 400 Croatian companies engaged in: computer science, accounting, industry and other. The tested sample of the questionnaire was relatively small (N=54).

It has been established that the majority of the companies surveyed use a CMS and they use a free version. It has also been found that the majority of the companies, in case they use any tools for testing or protocols for additional security, use free versions. A larger number of companies perform backup on daily basis, and thus, they provide a higher security level to their business. The companies pay most attention to sites with confidential data, and there they provide communication through SSL, although there is a great number of the companies surveyed that fail to do that in any place. Based on the survey results it could be concluded that the number of companies trying to fully maximize the security level is not considerable. A future research should cover all companies registered for the computer industry and the register of the Croatian Chamber of Economy can be used for that purpose.

REFERENCES

Beale, S. (2014) "Top Content Management Systems for Designers", *HOW,* 13. 5. 2014., http://www.howdesign.com/web-design-resources-technology/top-content-management-systems-designers/ (18. 1. 2016.)

CARNet (2008) "CMS sustavi i sigurnost - CCERT-PUBDOC-2008-12-249", *CARNet,* 2008, http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-12-249.pdf (2. 1. 2016.)

Chapman, C. (2011) "TOP 10 CONTENT MANAGEMENT SYSTEMS", 31. 10. 2011., http://www.webdesignerdepot.com/2011/10/top-10-content-management-systems/ (18. 1. 2016.)

EU (2015) "Special Eurobarometer 423 - Cyber Security", *European Comission*, 2015, http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2019 (7. 1. 2016.)

Florentine, S. (2015) "CIOs Reveal Their Worst Nightmares", 24. 2. 2015., http://www.cio.com/article/2888037/leadership-management/cios-reveal-their-worst-nightmares.html (7. 1. 2016.)

Kempf, D. (2015) "Digitale Wirtschaftsspionage, Sabotage und Datendiebstahl", *BITKOM*, 16. 4. 2015., https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/04-April/Digitale-Angriffe-auf-jedes-zweite-Unternehmen/BITKOM-Charts-PK-Digitaler-Wirtschaftsschutz-16-04-2015-final.pdf (6. 3. 2016.)

Kumar, A.(2014) "12 Best Free CMS (Content Management Systems) for Website Building", 8. 11. 2014., http://hubpages.com/technology/Top-12-Best-Content-Management-Systems-You-Can-Freely-Use-For-Website-Building (16. 1. 2016.)

Mikoluk. K. (2013) "Drupal vs Joomla vs WordPress: CMS Showdown", *Udemy Blog*, 18. 6. 2013., https://www.udemy.com/blog/drupal-vs-joomla-vs-wordpress/ (2. 1. 2016.)

OWASP (2007) "OWASP Top 10: THE TEN MOST CRITICAL WEB APPLICATION SECURITY VULNERABILITIES", *OWASP Foundation*, https://www.owasp.org/images/e/e8/OWASP_Top_10_2007.pdf (17. 1. 2016.)

OWASP (2010) "OWASP Top 10 - 2010: The Ten Most Critical Web Application Security Risks", *OWASP Foundation*, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjpltrblLHKAhXGOhQKHT2oB4YQFggZMAA&url=https%3A%2F%2Fowasptop10.googlecode.com%2Ffiles%2FOWASP%2520Top%252010%2520-%25202010.pdf&usg=AFQjCNFuwObQQvvWV4f3EcrVKcRFhN9JUg&bvm=bv.112064104,d.ZWU (17. 1. 2016.)

OWASP (2011) "Attacks, Session Prediction", 6. 12. 2011, *OWASP Foundation*, https://www.owasp.org/index.php/Session_Prediction (25. 1. 2016.)

OWASP (2013) "OWASP Top 10 - 2013: The Ten Most Critical Web Application Security Risks", *OWASP Foundation*, https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CDUQFjACahUKEwix_OnnidPHAhWKESwKHdc2Cbw&url=https%3A%2F%2Fowasptop10.googlecode.com%2Ffiles%2FOWASP%2520Top%252010%2520-%25202013.pdf&ei=lSfkVfHdBIqjsAHX7aTgCw&usg=AFQjCNGNt-a-lvsOz2in9Dy4HOLc19NQPw (17. 1. 2016.)

Rojko, T. (2015) *Sigurnost CMS sustava*, Veleučilište u Rijeci

Sponaugle, B. (2013) "Best CMS: A Short Guide to the Best Content Management Systems Available to You", *Udemy Blog*, 26. 11. 2013., https://blog.udemy.com/best-cms/ (18. 1. 2016.)

Tripp, N. (2016) "Content Management System Software Review", *TopTenReviews*, 2016, http://cms-software-review.toptenreviews.com/ (18. 1. 2016.)

Vlahović V. (2004) "Sustavi za upravljanje sadržajem (CMS)", *Fakultet elektronike i računarstva*, 7. 2004., http://web.zpr.fer.hr/ergonomija/2004/vlahovic/index.html (6. 3. 2016.)

Marin Kaluža[1]
Bernard Vukelić[2]
Tamara Rojko[3]

Prethodno priopćenje
UDK 004.056.57

SIGURNOST CMS-A[4]

SAŽETAK

Za razvoj web-*sjedišta danas se često koriste CMS-ovi.* Web-*sjedišta meta su raznim malicioznim napadačima, stoga je potrebno poznavati razinu sigurnosti* web-*sjedišta i postaviti maksimalnu moguću razinu sigurnosti. U radu su prikazane osnovne značajke poznatijih CMS-ova u otvorenom pristupu Wordpress, Joomla i Drupal. Objašnjeno je deset najčešćih* web-*ranjivosti. Izvršeno je testiranje* web-*ranjivosti pomoću različitih programskih alata. Testirane su osnovne instalacije CMS-ova. Nakon testiranja svake* web-*ranjivosti za svaki CMS navedena je moguća dodatna mjera sigurnosti. Objašnjene su* web-*ranjivosti na koje sigurnosne postavke CMS-ova ne mogu direktno utjecati. Pokazano je da osnovne instalacije CMS-ova ne zadovoljavaju sigurnosne zahtjeve jer nisu otporne na neke prijetnje. Specificirani su potrebni programski dodaci na testirane CMS-ove kako bi se osigurala otpornost na prijetnje koje osnovne instalacije testiranih CMS-ova nisu osigurale. Za potrebe provjere stanja sigurnosti na* web-*sjedištima poslovnih subjekata u Hrvatskoj izrađen je anketni upitnik i provedena je anketa nad poslovnim subjektima u Hrvatskoj za djelatnosti informatika, računovodstvo, industrija.*

Ključne riječi: *CMS, sigurnost,* web-*ranjivosti, napadi, zaštita*

[1] Dr. sc., viši predavač, Veleučilište u Rijeci, Vukovarska 58, Rijeka, Hrvatska. *E-mail:* mkaluza@veleri.hr

[2] Mr. sc., viši predavač, Veleučilište u Rijeci, Vukovarska 58, Rijeka, Hrvatska. *E-mail:* bvukelic@veleri.hr

[3] Studentica, Veleučilište u Rijeci, Vukovarska 58, Rijeka, Hrvatska. *E-mail:* rojko.tamara@gmail.com

[4] Datum primitka rada: 15. 1. 2016.; datum prihvaćanja rada: 1. 4. 2016.