Security Analysis Issues and Usability for Web Content Management Systems

Maraga Alex*
(Student MSC-Information Systems)
Kisii University
Nairobi - Kenya

James Ogallo (PhD)
(Lecturer – Computing Department)
Kisii University
Nairobi - Kenya

Abstract:- Web Content Management System (WCMS) massages workflow in elaborative status ranging from publishing, editing, modifying and maintenance of content from a central interface. The cutting-edge in every discussion of WCMS, it is absolutely necessary to make your opinion depending on your experience, and converse the advantages and disadvantages serenely and objectively. The greater number give their subjective opinions very first simply because they could be only well known with either Word Press, Drupal or Joomla. Many users of (WMCS) are not mindful of the security controls and concerns in them. Vulnerabilities in these systems provide appealing targets for potential attackers. Users of WCMS may be exposed to threats beyond their imagination which they might not be aware of. This study will review the security analysis awareness of the users of these susceptibilities and to what extent Drupal, Joomla and Word Press are secure and their possible ex-poser to the attackers.

Keywords:- *Web Content Management Systems; Vulnerabilities Joomla; Word Press; Drupal.*

I. INTRODUCTION

Security analysis for any component in all information systems has proved to be very important. Since technology is growing and on the other side vulnerabilities are increasing. It is in this regard this paper seeks to review the security analysis for web content management system(WCMS).A WCMS is a computer based package program that enables developers to publish, edit and modify content as well as maintain them from a central interface.

According to [1] approves that this systems of content management enables one to procedurally manage flow of information or data in a dynamic way also in a collaborative environment. These procedures can be physical manual steps or an electronically automated flow of information or data. Also he confirms that this WCMS have been in existence since 1990s and are mostly used to run websites customized in i.e blogs, news etc.

That is why [4] give us the background problem of the WCMS as security is concerned.He says that there are various types of attacks on website using WCMS.He numbers them such as SQL injections, link hacks, denial of services and many more. In this ideal structure system finds these type of attacks quickly and easily hence challenging to stop them from spreading. When taking into consideration of all this different issues in play it becomes evident why hackers and attackers deem CMSs to be attractive targets to them. Some of them may assume so easly since WordPress, Joomla, and Drupal are such common names, which needs to be provided with some form of protection.

Also [6] says that WCMS are vulnerable. He confirms that this is true because WCMSs are built on open source frameworks and platforms. Such mult-shared development community and environments bids several benefits but also they share many defects of which arise form a lack of accountability.

[7] While comparing the usability of the three WCMS, WordPress leads the park followed by Joomla and Drupal. But on security Drupal is preferred most compared to the two, further in scrutiny of Joomla and WordPress, Joomla is preferred to be secure even if is being the lesser CMS overall. Usability of WordPress has been friendly hence being preferred by majority. Due to many user, it’s vulnerability is high hence it receives poor support in terms of security concerns.

In support [2] says that Drupal wins this round. WordPress’ many plugins can have vulnerabilities and be easily hacked, particularly if the website owner doesn’t update to the latest version or the plugin gets old. Or simply, hackers target WordPress because it is so popular.

Despite all this above confirmations [18] saw need for organizations to have knowledge on how to evaluate these open source systems and this paper draws attention to how an evaluation technique in terms of security may be used in an organization to assess a short list of possible WMCS systems. This article focuses on security awareness on side of web admins and developers in WCMS and as well as point out the solutions towards choosing the most secure WCMs.

II. SECURITY ANALYSIS

- *Drupal*

This one of the open source WCMS which many users in union to customize and in addition of the content to a website, without much having the need to pass through or aquire knowledge of a webmaster expert. But however, the Drupal as a WCMS, it has been proven of it’s extensive use. In addition Drupal frameworks has been also extensively used to create website applications and software's as well.

Majority of websites hosted currently online are developed by Drupal. [10].

Backed by the world-wide Drupal community, the Drupal Security Team resolves security issues found in code hosted on drupal.org, including Drupal core and thousands of community-contributed modules and themes. The published Security Advisories uncover vulnerabilities and weaknesses in core and contributed code, separately, and provide mitigation solutions. Erroneous use of core application programming interfaces (APIs) and individual site misconfiguration is the origin of most vulnerabilities and weaknesses. Organizations should stand firm on developer training and employ security testing before moving code and configuration to production. As a process, a secure approach and method must be used during the entire software development life cycle and for all layers of the site and its related infrastructure[15]

[22] further asserts that Drupal has a low number of vulnerabilities compared to Joomla, and the condition to exploit Drupal, in almost all cases, requires permissions typically granted to trusted users. Joomla, on the other hand, is at high risk not only because of the sheer number of exploits, but the extremety, and the capability to trigger the exploit as an anonymous (unauthenticated) user. The Drupal manages its security using it's support community which is very consequential in it and and also they have a team which takes care and supports security concerns.

In this regard, Drupal is much more secure than other content management systems. The enterprise level security makes Drupal websites safe from hackers that's why the big enterprises and government websites are built up with Drupal. With Drupal you can build sites that are very large, require a lot of customization, are very secure, and can handle many users at once. With Drupal you can also build a small blog site that requires little flexibility or customization but needs to go live quickly [2].

In terms of securing sites, Drupal is definitely the best PHP CMS among WordPress, Joomla, and Drupal. And this is also one of the reasons why Drupal can be the first option of CMS for enterprise websites with a big volume of traffic. (The other four are: Scalability, Flexibility, User Management, and Accessibility, according to a professional post [7].

Internet Security Drupal developers have their own security team that's in-charge for accepting and evaluating security-related warnings, searching for vulnerabilities in the core application, and supporting module developers in fulfilling security requirements. In recognition of security's importance, the Drupal Web site has a dedicated section to inform users about current vulnerabilities and appropriate patches [22].

Market-wise Drupal has been termed and voted to the most secure WCMS since even White House uses it. In comparison of Joomla and WordPress, Joomla is preferred but remember it only not popular as WordPress hence many users using WordPress [7].

- *Joomla*

This one of the open source WCMS used by website developer. It is estimated to have been used by roughly four million user to build websites internationally. This type of WCMS its relatively easy to use. Hence one doesn't need really technical skills so that he or she can be able use it. In addition, this CMS provides many website such as forums and chat rooms, calendars, and blogging platforms [22].

Joomla is a class of Open Source CMSs written in PHP scripting language and uses MySQL database for the back-end. Compared to Drupal, Joomla is fairly new and is gaining popularity among users because of many aspects, including ease of usability and extensibility. There are around 4500 extensions and modules available to enhance the functionality of the core Joomla package. Joomla can be installed and run on Linux, Windows or Macintosh OS. It is distributed under GPL and is free to use[29].

Joomla developers estimate that there are more than 140,000 active registered users on the Official Joomla community forum. The Joomla forum comprises a security section in which users discuss security issues and submit possible vulnerabilities. This section also contains guidelines, tutorials, and hints for increasing security and mitigating risks. Security issues are categorized according to level (low, medium, or high) and are fixed in minor releases or by patches. [22].

Joomla as WCMS is termed to be more secure due to the way they handle security issues from their user. They have online platforms where security issues are posted and their solution discussed. In this forum, guidelines are provided, tutorials shared and tips of mitigating the increasing security risks[23].

The main outline of the scenario is, Joomla is much secure at its core. The things which should be considered most includes its extensions (components) [24].

- *WordPress*

Having WordPress supporting very high percentage of users, security susceptibilities are expected because among all this user not all are aware of this vulnerabilities, or even not aware of security concerns facing their websites. Among this larger percentage, an hacker can be able to manage one which is more vulnerable and unable to counter attack the hacker. They do this by scanning through maybe updated WCMS and the patches to hack them [32].

The WordPress Core code is actively maintained, and the contributing developers are very hip to the latest security threats. However, the biggest threat to your WordPress security is user error — namely, mishandling of plugins and software updates [17].

WordPress' many plugins can have vulnerabilities and be easily hacked, particularly if the website owner doesn't update to the latest version or the plugin gets old [14].

This sequence came to a close with the Thanksgiving 2009 release of 2.8.6. Though the long-term effect of tightening up overall WordPress security was incredibly positive, many in the community will remember it as a dark time for the platform, when it seemed like an upgrade was required every other week. [20].

Also more information is recorded here that WordPress has majority in record that it's vulnerable than Joomla. Furthermore, majority users use exclusive and locally made themes and plugins which are easily hackable and quickly infected. Market-wise Drupal has been termed and voted to the most secure WCMS since even White House uses it. In comparison of Joomla and WordPress, Joomla is preferred but remember it only not popular as WordPress hence many users using WordPress [7].

III. RELATIONSHIP BETWEEN SECURITY VULNERABILITY AND USABILITY OF WCMS.

According to [11] is comparing the widely used WCMS. This three are;WordPress, Drupal and Joomla. They popular because of their wide range of use statistically. The three are open source WCMS and they have different levels of exposure vulnarabilitie as security analysis is concerned. Aso in usability they have different flexibilities , hence one may be preferred by many than the other. That why their review of security is very much important, hence when one chooses one for usability he or she can also consider the security aspect.

- *WordPress*

This a a widely preferred WCMS in globally. It is widely known by its easy to use and to customize it to blogs and websites. Its attractive themes is an added advantage for attractiveness and easy customization. However, this widely use exposes it to more vulnerabilities than the drupal and joomla. [33].

Having a thought this way.If you are a attacker and you want to attack as wcms websites as possible, you could try to find a security hole in the individual software that runs on each website, or you could find a security loop-hole in the most popular software used by websites and attack them all. If a attacker can find a security loop-hole in WordPress itself, or a popular theme or plugin used by WordPress, it allows them to very quickly infect many websites using programmed attacks [30].

- *Joomla*

This one of the open source WCMS used by website developer. It is estimated to have been used by roughly four million user to build websites internationally. This type of WCMS its relatively easy to use. Hence one doesn't need really technical skills so that he or she can be able use it. In addition, this CMS provides many website such as forums and chat rooms, calendars, and blogging platforms.This means it is widely used from private entities to public ones [19].

The user interface is very friendly with extensive use of images. Creating a new page is easy and it can be published by assigning it to the appropriate section and category. The updates on security are released on joomla.org and these updates occur frequently. Joomla has had only one major upgrade and it doesn't support the legacy version with security updates and fixed bugs [29].

In Joomla is also known for its easy to share information pertains to vulnerabilities, each identified and accepted vulnerability is identified uniquely. Based on this, one can get data related to the vulnerability, including its explanation, the product concerned, the version of the product, the date of vulnerability records formation and some explanations. [3].

- *Drupal*

Drupal was ranked second in the aforementioned "Open Source CMS Award" in 2006. Like Joomla!, Drupal provides huge amount of additional modules, like newsletters, podcasting components, etc. Drupal developers maintain their own security team. This team is responsible for accepting and evaluating security related warnings, searching for vulnerabilities in the core application and for supporting developers of additional modules to fulfill security requirements. The Drupal website contains a section where users get informed about current vulnerabilities and appropriate patches. This demonstrates the fact that Drupal developers have identify the importance of providing a high level of security [20].

IV. CONCLUSION

It's very clear from the above that there exists security issues of different levels in WCMS. Due to these different levels of security issues on the side of web admins and developers, more susceptible WCMS is preferred because of ease of use. That is why more survey is required and security consciousness done on this affected groups .Hence through this knowledge we are able to choose a more secure content management system,by balancing the security vulnerability of the candidate WCMS against their perceived usability features both from the developers and the administrators.

RECOMMENDATION

The study therefore recommends the following based on the findings and reviews;

- The choice of WCMS should be based on holistic consideration that is, its security and the usability features.
- A detailed document needs to be provided to a sustain each of the WCMs application strength and weakness.

REFERENCES

[1]. Baldaniya & Baldaniya. (2014). Web Development Using Content Management System. *International Journal of Emerging Research in Management &Technology*, 166.

[2]. Barron, B. (2015, April 7). *WordPress vs. Drupal: Choosing Between Two Platforms*. Retrieved November 2, 2016, from Elegant themes Blog:

https://www.elegantthemes.com/blog/resources/wordpress-vs-drupal

[3]. Bissyand´, T. F. (2014). Vulnerabilities of Government Websites in a DevelopingCountry – The Case of Burkina Faso. *achives*, 4.

[4]. Brunswick, N. (2010, MAY 10). *PRIVACY AND TERMS*. Retrieved JANUARY 2, 2017 , from New Brunswick website: http://www.tourismnewbrunswick.ca/Help/Privacy.aspx

[5]. Canavan, T. (2008). *Joomla! Web Security*. United States: PACKT PUBLISHING.

[6]. Cassetto, O. (2014, 11 11). *security access control*. Retrieved 5 3, 2017, from inacapsula: https://www.incapsula.com/blog/cms-security-tips.html

[7]. Devious. (2011, July 12). *Tech Blog Articles WordPress Vs Joomla Vs Drupal Which One is Best and Why?* Retrieved January 12, 2017, from Techlila: https://www.techlila.com

[8]. Ekinović, S. (2011, SEPTEMBER 12). *Trends in the Development of Machinery and Associated Technology*. Retrieved JANUARY 5, 2017, from TMT: http://www.tmt.unze.ba/proceedings2011.php

[9]. Ghorecha & Bhatt. (2013). A guide for Selecting Content Management System. International Journal of Advance Research in Computer Science and Management Studies, 13.

[10]. Holton, D. (2009). Blended Learning with Drupal. *MERLOT Journal of Online Learning and Teaching*, 348.

[11]. IJARSE. (2015, April). *International Journal of Advance Research in Science and Engeneering*. Retrieved January Monday, 2017, from www.ijarse.com: www.ijarse.com

[12]. Ivanova, A. (2015). Multiple SQL injection vulnerabilities in Joomla. *referaadid*, 2.

[13]. J Jeavons,G Knaddison. (2014). Drupal Security. *white paper*, 2.

[14]. Jain, A. (2016, November). *wordpress-themes*. Retrieved January 12, 2017, from Built with: http://trends.builtwith.com

[15]. Jeavons & Knaddison. (2014). Drupal Security. *white paper*, 2.

[16]. Lemes, S. (2011). INFORMATION SECURITY MANAGEMENT. 4.

[17]. Leslie, A. (2016, December 14). *Joomla vs. WordPress vs. Drupal - (Security, SEO, eCommerce, Speed)*. Retrieved January 13, 2017, from Hosting Advice.com: http://www.hostingadvice.com/how-to/joomla-vs-wordpress-vs-drupal/

[18]. Mautone, S. (2009). Security in Dynamic Web Content Management Systems Applications. *Communications of the ACM*, 121-125.

[19]. Meike & Sametinger & Wiesauer. (2009). Security in Open Web Content Management System. *cse*.

[20]. Meike & Sametinger & Wiesauer. (2009). Security in Open Web Content Management System. *cse*.

[21]. Meo & Rocchetto & Luca. (2016). Formal Analysis of Vulnerabilities of WebFormal Analysis of Vulnerabilities of Web. *arxiv*, 4.

[22]. Michael. (2010). Internal Security. *International white papers publishers*.

[23]. Michael M, Johannes S,Andreas W. (2009). Security in Open Source Web Content Management Systems. *Security of PHP-based Open Source Web Content Management Systems*, 44-51.

[24]. Mittal, S. (2016). Guidelines forPen-testing a Joomla Based Site. *exploit*, 14.

[25]. Schaferhoff, N. (2010, January 2). WORDPRESS VS. JOOMLA WHICH IS THE RIGHT CMS FOR YOU. *WPENGINE*, 5.

[26]. Spolan, S. (2016, october 1). *Which CMS is More Secure: Drupal vs. WordPress*. Retrieved January 4, 2017, from Zivtech: https://www.zivtech.com/blog/which-cms-more-secure-drupal-vs-wordpress

[27]. Stockley, M. (2013, September 27). *How to avoid being one of the "73%" of WordPress sites vulnerable to attack*. Retrieved March 6, 2017, from necked security: https://nakedsecurity.sophos.com/2013/09/27/how-to-avoid-being-one-of-the-73-of-wordpress-sites-vulnerable-to-attack/

[28]. Vedpathak, Y. (2014). Research Paper on Content Management System. *NCI2TM*, 31.

[29]. Wakod & Chaudhari. (2007). STUDY OF CONTENT MANAGEMENT SYSTEMS JOOMLA AND DRUPAL. *IJRET*, 569.

[30]. wordfence. (2017, January 4). *How to Protect Yourself from WordPress Security Issues & Threats*. Retrieved March 6, 2017, from wordfence: https://www.wordfence.com/learn/how-to-protect-yourself-from-wordpress-security-issues/

[31]. wordpress. (2015). *About Us*. Retrieved March 9, 2017, from wordpress.com: https://wordpress.com/about/

[32]. Wright, K. (2017, January 16). *Common WordPress Security Issues*. Retrieved January 17, 2017, from ithemes: https://ithemes.com

[33]. Yang & Kim & Yangwon & Lim. (2016). A Comparison of Open-Source CMS and Analysis of Security Vulnerability. *INTERNATIONAL JOURNAL OF COMPUTERS*, 82.