DOI: https://doi.org/10.30837/csitic52021232202

Ways of protecting the CMS WordPress-based sites

Maksym Akshentsev[1]

Gennady Khalimov[2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine, maksym.akshentsev@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine, hennadii.khalimov@nure.ua*

Abstract. *WordPress is the most popular software for websites or blogs as millions of users use it today. It allows customizing the site to one's own tastes and needs without spending money and regardless of the technical skills of the user. Yet, incorrect configuration and/or usage of untested external software (e.g. plugins and graphical environments) may lead the site to compromisation. The paper has reviewing of ways to increase the security of a WordPress-based web resource as its goal.*

Keywords: *WordPress, plugin, website, security.*

I. Introduction

Thanks to providing a quick and easy way for users unfamiliar with the technical ins and outs of the Internet to publish information, blogging as a phenomenon has spread around the world in a short time. Nowadays the whole world considers blogging common, because regular Internet users, as well as large corporations, news organizations and educational institutions are running blogs [1]. A popular aphorism states that if there is no website of the organization then [for users] there is no organization itself, which in particular is relevant for blogs [2].

Today it is possible to choose one of several software platforms for managing blogs in particular and sites in general. One of most leading platforms is WordPress as in addition to functions for actual management; it is a full-featured content management system (hereinafter: CMS) that lets creating a web site without a lot of technical knowledge [1]. Nevertheless, even using the most advanced CMS will not guarantee the security of the Internet resource without proper configuration.

The purpose of the report is to review existing practices for ensuring the security of WordPress-based web resources. It will be shown that both quite expected causes such as computer viruses and less trivial aspects can be critical for the site – the latter include third-party graphical environments for the website (hereinafter: themes).

The report will focus on ways to set up a website the way it is close to impossible to get it hacked. Among other things, it will be shown that despite the ability to extend the functionality of WordPress with additional plug-in software (hereinafter: plugins), not every such plugin shall be worth of trusting.

1. The CMS version's recentness.

The following is relevant for most software but speaking of WordPress, installing the CMS updates is among the fastest ways to ensure security. On average, developers publish a new version of the CMS every 120 days [1]. The problem, which arises because of the aforementioned fact, is that releasing a newer version signifies ceasing supporting the older ones, rendering them deprecated and vulnerable to malicious attacks. A large fraction of hacks and security failures of WordPress-based sites occur due to usage of not-so-recent-anymore version with them. What is more, due to the popularity of the content management system, many programs have been developed that automate such hacking ergo the attacker does not have to possess professional technical skills to achieve their goals [3]. Therefore, it is a good idea to update the CMS as soon as the system control panel prompts one to perform the update to reduce the likelihood and damage of site attacks. While enabling automatic updates in the WordPress configuration file to eliminate the human factor is even better idea.

2. Regular audit of themes and plugins.

Plugins and themes can become deprecated or filled with vulnerabilities that undermine the security of a WordPress-based web resource, even with the latest version of the content management system installed. However, there exist factors [4] that determine the degree of possible trust in these software applications:

1) The number of existing software users, which is usually directly proportional to its security degree as the product owner usually cares about the reputation of the software and of his own;
2) The number of reviews from users in general with the positive ones in particular is also directly proportional to the software application's security;
3) The frequency of software updates made by developers may be either positive or warning sign on how quickly vulnerabilities are fixed and whether are they fixed at all so this one has the same interrelation with the trust in an application the previous two factors have;
4) Availability and the degree of detail of legal agreements such as terms of use and privacy policy. If the developer had specified his contact information in the terms of service, it is an additional sign of trustworthiness. On the other hand, though, their existence implies the need to be acquainted with them, as the texts of agreements may contain unsatisfactory requirements for the end user, which happens especially often after the transfer of software rights to another owner.

Although the first two factors are rather related to plugins and themes that have not yet been installed by the user but are to be established, the impact of the last two may change at any time. This is especially applicable to the fourth factor because the aforementioned transfer may happen without the former owner notifying users at all.

Thus, accounting the combination of the above factors before and after the application's installation as well as periodically auditing the recentness of the applications versions used it is possible to prevent many potential hacks into the website.

3. Choosing a reliable hosting.

Given that the website must be located in a certain place, as well as maintained, it is worth noting that, firstly, there are organizations that provide resources for this purpose also known as hosting. And, secondly, hosting companies work accordingly to four different models, the choice of which (i.e.

the choice both from companies and models) also is likely to affect the security of the website [3,4]. The models do include:

1) Shared hosting means storing a number of websites on the same one server which is cheaper than the models specified below, but usually has a negative impact on both the speed of data processing and resource security so this is not recommended to select this option;
2) Virtual private server is a modification of the first model which additionally isolates web resources from each other through the use of virtual machines, thus providing an increased security and control over the resource but it does not increase neither the speed nor readiness to supercritical loads;
3) Managed hosting environment dictates the company to provide the pre-configured remote software and hardware complex for hosting a web resource which is characterized by ease of use but not the configuration flexibility;
4) Dedicated server, which in contrast to the third model, provides the hardware resources only, however, grants close-to-absolute control up to rights to replace the operating system or configure the firmware of the motherboard. Accordingly, this model requires sufficient technical skills from the user, but provided the system has been set up correctly, it will have the highest degree of safety and resistance to abnormally high operational loads.

In general (provided, of course, that the hosting company support WordPress-based sites), a managed hosting environment model is worth its money for beginners, whereas for professionals and corporations with such experts as their staff virtual private or dedicated servers are the best existing choice. In addition, it is necessary to question the company representatives what measures the hosting company will take to protect the website (separately from their server) and what actions will it take in case of its hacking.

4. Proper configuration.

WordPress-specific configuration requirements include the need to move the configuration file to any location other than the standard one. It is also an often demand to change the standard encryption keys which here are also known as salt because if the cryptanalyst finds them it will have access to user accounts and all associated data. The leak or disclosure of the new keys is also a serious reason for their immediate change. It should be noted that the developers of CMS have published an online service for instant generation of cryptographic salt, which reduces the number of actions required to the single copy-pasting into the configuration file (for resource owners) and re-logging into the account (for users).

It will also not be superfluous for the owner to restrict access to the administrative panel to anyone but himself (or herself) and in one’s own person looking for ways to solve problems with the resource and doing that without assistance [1]. Finally, it is noteworthy recommendation to attach a robust security plugin to the WordPress-based website, which users often call an antivirus as an allusion to the computer anti-virus software.

Other recommendations are equally effective for sites that do not use CMS WordPress - for instance:

1) Set a non-standard login and complex password (opposed to the far-too-common “admin-admin” credentials”) for the administrative panel with letters in different registers, numbers and symbols that do not belong to those two groups;
2) Set a limit on attempts to gain access to the control panel to prevent brute force attacks;
3) Set access rights for directories and files that will reduce the range of potentially destructive actions affecting the web resource (and most likely its owner, too) in case of its hacking;
4) Follow the rules of protection against computer viruses and install an antivirus for personal computer in addition to the antivirus for CMS.

II. Conclusion

For the most part, the security of a website, whether it is a simple blog, a full-fledged online program, or a game, depends solely on the owner of the website. Nevertheless, using the trustworthy software coupled with constantly updating it negates the possibility of hacking as well as the loss or the disclosure of sensitive data (provided there is such data). Due to the popularity of the WordPress content management system, sites based on it are a desirable target for attackers, but developers are actively working on it, periodically publishing updates to improve security and functionality, as well as encouraging others to create plugins for both purposes. It is an actual plan for the paper’s author to create own plugin to protect sites based on CMS WordPress, but this is beyond the scope of this paper.

REFERENCES

[1] WordPress: all in one for teapots / [L. Sabin-Wilson, K. Miller, K. Palmer, etc.]. - Indianapolis: Wiley, 2011. - 916 p.-(Dummies). - (For Dummies).

[2] "If it is not on the Internet, it does not exist ": Electronic information resources - myth and reality [Electronic resource] // Astronomical Society of the Pacific Ocean. - 1998. - Mode of access to the resource: https: //www.stsci .edu / stsci / meetings / lisa3 / stevens-rayburns.html.

[3] Burovinsky E. Security WordPress [Electronic resource] / Eugene Burovinsky-Mode of access to the resource: https://ru.hostings.info/schools/bezopasnost-wordpress-saytov.html.

[4] WordPress security: how to secure and protect WordPress [Electronic resource]//Sucuri.-2020.-Resource access mode: https://sucuri.net/guides/wordpress-security/.