Everything about Wordpress Website- Plugins,Security,SEO,Copyright Protection

Prof. M.A. Dhotay
Department of Computer Engineering
MIT Polytechnic, Pune, Kothrud
Megha.dhotay@mitwpu.edu.in

Mayur Solankar
Department of Computer Engineering
MIT Polytechnic, Pune, Kothrud
Mayursolankar3@gmail.com

Shubh Tank
Department of Computer Engineering
MIT Polytechnic, Pune, Kothrud
shubhrajeshtank@gmail.com

Harshal Sukale
Department of Computer Engineering
MIT Polytechnic, Pune, Kothrud
Harshalsukale12@gmail.com

Atharva Salve
Department of Computer Engineering
MIT Polytechnic, Pune, Kothrud
Atharvasalve1912@gmail.com

ABSTRACT

This essay focuses on the vital task of protecting web operations, particularly for businesses that use Wordpress as their content management system. Our essay emphasises the importance of protecting Wordpress against potential hazards and threats. We also examine the security of Wordpress backup plugins, looking closely at the dangers of data leaks, frequent vulnerabilities, causes of vulnerabilities, and mistakes committed during development. We also evaluate the effects of these vulnerabilities and their potential to have serious negative effects. This essay also examines copyright protection and search engine optimization (SEO). This paper's statistical data representation of WordPress website growth over time is included.

Keywords: Wordpress, Plugins, Security, Wordpress site, SEO, Copyright defence.

Introduction

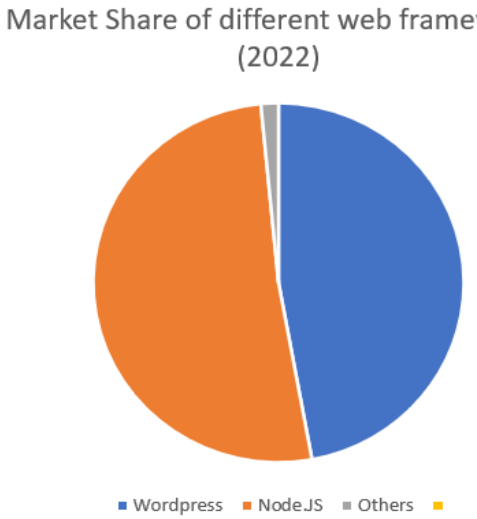
This study focuses on Web applications, such as content management systems like Wordpress, because they have seen recent significant growth and are frequently targeted by cybercriminals looking for weaknesses and sensitive data. Due to its extensive usage and the possible weaknesses in its plugins and themes, Wordpress is especially alluring to attackers. Nonetheless, in order to offer useful enhancements as soon as possible, even experienced developers could neglect security risks. For instance, Wordpress backup plugins may save private information on the same server as the web application, making it available to anyone who knows the name of the backup file. This study focuses on vulnerabilities associated with sensitive data leaking via Wordpress backup plugins and offers a fix to validate the issues. For companies looking to improve their online presence and draw in more customers, website design and SEO are as crucial factors to take into account as web application security.

SEO strategies can help websites become more discoverable by search engine algorithms by enhancing their structure, code, and content. This can facilitate the discovery of pertinent web pages by search engines and improve the website's organic ranking in search results. Internet payment gateways are also a crucial feature of the digital economy, especially in light of India's demonetization. The sensitivity of client information, however, and the function of payment gateways in enabling financial transactions our top priority. Standardized security procedures are essential to thwart future attacks and guarantee the security of payment gateways because past security breaches have cost businesses money and damaged their reputations. The article continues by highlighting the significance of addressing backup plugin security flaws and safeguarding web applications, building websites with SEO in mind, and outlining the significance of copyright protection and how to add copyright to material.

LITERATURE REVIEW

1. Wordpress Statistics

43.2% of websites on the internet are powered by the widely used content management system WordPress, which has been the fastest-growing CMS for 12 years running. 36.28% of the top 1 million websites and 65.2% of websites using CMSs use it. The official WordPress directories offer more than 9,000 free themes and close to 60,000 free plugins. The most popular plugin among the top 1 million websites is Yoast SEO, while the two most popular themes are Divi and Astra. A premium WordPress theme costs, on average, $77.57. Unfortunately, WordPress websites are equally subject to security attacks, as illustrated by the 18.5 billion password attack requests stopped by Wordfence in the first half of 2021. In addition, 90% of WordPress vulnerabilities are caused by plugins, 6% by themes, and 4% by the core programme.



2. Wordpress Plugins

[1] The main objective of this article is to assess the efficiency of accessible and affordable security technologies in locating vulnerabilities in WordPress websites. The report emphasises the fact that third-party plugins are a significant source of vulnerabilities in websites running on the WordPress platform. The capacity of security scanner plugins to identify vulnerable feature-rich plugins is therefore explicitly examined by the researchers. In order to rephrase the statement, the article analyses the efficacy of free and simple security tools in locating vulnerabilities in WordPress websites. The study highlights the significance of third-

party plugins as a frequent source of vulnerabilities in websites running on the WordPress platform. The researchers evaluate security scanner plugins' capacity to find flaws in feature-rich plugins in particular.

2.1 Plugins in wordpress

All-in-one-wp-migration

[1] The All-in-one-wp-migration plugin has over 1 million active installations on WordPress and stores backups in the "/wp-content/ai1wm-backups/" directory. The backup filename contains the website name, date and time with precision to seconds, and a random number between 100 and 999, with a ".wpress" extension. The frequency of backups depends on the website's backup settings. To start a brute-force attack to locate a backup file that may contain sensitive information, one could obtain the creation date of the "ai1wm-backups" directory by making a GET request to "/wp-content/ai1wm-backups/web.config". The "Last-Modified" parameter in the response header provides the last modified date of the file "web.config" with precision to seconds, which can be used as a starting point for the brute-force attack. If successful, the attacker may be able to access the website's database and stored files from WordPress.

BackWPup plugin

With over 600,000 active installs, the BackWPup plugin saves backups in a directory called /wp-content/uploads/backwpup-[hash]-backups, where [hash] is a random string. The whole path to the file backwpup.php is done twice to the md5 algorithm, and then 6 bytes are taken out of the middle to form the hash. The whole path to that file must be known in order to determine the directory, which is typically an easy estimate. Using the value of the Last-Modified argument from the HTTP request sent to /wp-content/uploads/backwpup-[hash]-backups/.donotbackup once the hash has been retrieved, the first backup log may be viewed. The backup log file of the initial backup, which contains the backup file name that is unpredictable, can be located using the date. All directories contain an.htaccess file with deny from allaccess rights, although this preventative measure is not always successful.

BackitUP plugin

The BackitUP plugin saves backups in the /wp-content/wpbackitup backups/ directory with a.htaccess file that restricts access, however as shown in section IV, this is not an adequate security protection. By utilising an HTTP request to find the index.html file's creation date and a brute-force search for the log file, which has the name logs [timestamp].zip, it is possible to find the name of the backup file. The log file includes details about database backups and the website.

BulletProof Security plugin

[1] With over 70,000 current installations, the BulletProof Security plugin creates an illegible backup file name using cryptographic techniques. This offers details about the backup, such as the backup file's entire path and name.

The contents of the backup can be retrieved from the internet using this information.

Astra Widgets

With the help of the robust Astra Widget plugin, you can quickly design unique widgets for your website, such as social profile widgets, address widgets, and list icons that can be placed in the header, sidebar, footer, and other places. Due to the best coding practises and performance optimization, one of the main advantages of Astra is its blazing-fast performance. Astra also provides a large number of customization options, all of which are simple to control with the customizer. Furthermore, Astra is completely compatible with all popular page builders, such as Beaver Builder, Elementor, and Gutenberg. For those who wish to save time and streamline the design process, Astra offers a big collection of free, pixel-perfect website demonstrations that can be quickly imported and changed to match your needs. Moreover, WooCommerce, LifterLMS, and LearnDash's deep connections with Astra make it simple to build beautiful online shops and course websites in a matter of minutes. Last but not least, Astra offers pre-built website designs for Elementor, Beaver Builder, Brizy, and Gutenberg that can be imported and adjusted to launch your website quickly. It is obvious why Astra is regarded as one of the best WordPress themes available right now given all of these features and advantages.

Wp sec-

UpdraftPlus created the security plugin All-In-One Security particularly for WordPress. It provides a number of tools to strengthen your website's security and guard it against various attacks. Login Security Tools, which shield your website from brute force assaults and stop bots from attacking it, are one of the plugin's key features. The Web Application Firewall monitors website traffic and stops malicious requests to provide automatic defence against security threats. In order to protect the content of your website, All-In-One Security additionally offers Content Protection Features. With the help of technologies like iFrame blocking and copywriter protection, it gets rid of comment spam and stops other websites from stealing your content. Consumers like how simple All-In-One Security is to use and how many of its features are free. It's crucial to keep in mind that no security plugin can offer 100 percent security, therefore you must take additional precautions to protect your website.

Firewall And file protection

The Web Application Firewall (WAF) from All-In-One Security guards your website automatically by keeping track of traffic and thwarting nefarious requests. You may adapt your protection to your needs with its gradually activated firewall settings, which range from basic to advanced.

Further features of the plugin include the 6G blacklist, which filters known malicious URL requests, bots, spam referrers, and other assaults, as well as other capabilities to defend

your website from specific threats. Also, it guards against phoney Google bots that can steal your material and leave spam comments on your website. The plugin also provides a number of security features, including the ability to block users by IP address or IP range, defend against DDOS assaults, and prevent attacks and illegal access. To stop attackers from inserting harmful scripts onto your website, it also incorporates Cross-site scripting (XSS) security.[2] File change detection is another feature of All-In-One Security, which also notifies you of any unusual modifications to your WordPress system. To safeguard your code, you can prevent PHP file editing. You can also get permission setting notifications to know which files or directories have insecure permission settings. The plugin also offers access prevention for the readme.html, license.txt, and wp-config-sample.php files. Experienced users can implement custom rules to prohibit access to particular URLs on their site. The Firewall and File Protection features of All-In-One Security provide thorough defence for your WordPress website against a range of security risks.

Content protection

All-In-One Security includes many content protection tools to defend your website's content and maintain your search engine results. Spam comments can damage your brand, the user experience, and your SEO. [2] Comment SPAM prevention is a crucial function that gets rid of them. The IP addresses of spammers are indefinitely blocked by All-In-One Security, which also bans comments coming from other domains. Moreover, website owners can utilise Google reCAPTCHA or Cloudflare Turnstile to stop malicious users and lessen comment spam.

By preventing other websites from using your material in a "iFrame," iFrame protection protects both your intellectual property and your visitors. Copywriting protection disables the right-click, select, and copy text feature to prevent users from copying your work. The capability to turn off RSS and Atom Feeds is another crucial function provided by All-In-One Security. Bots can scrape the material from your website and display it as their own using RSS and Atom feeds. This can be avoided by disabling RSS and Atom Feeds on your website, improving website security.

3. Payment gateway

Several government initiatives aimed at boosting digital transactions and attaining a cashless economy in India have been prompted by the growing importance of online payment gateways, especially in the wake of demonetization. Security is a major issue due to the sensitivity of the client data and the function that payment gateways play in facilitating financial transactions. Payment gateway vulnerabilities and weak points must be found because security breaches in the past have cost businesses money and reputational damage. [3] The goal is to determine future weaknesses and attack spots by studying prior breaches in order to improve and secure digital transactions through payment gateways. By doing this, we

can provide a standardised set of security precautions that will shield payment gateways against assaults in the future.

3.1 Ways to secure payment gateway

We were able to find weaknesses and missing security procedures that may have stopped these assaults after completing an investigation of prior breaches at the payment gateway level. Based on our research, we suggest putting into practise a few common security postures to improve the security of payment gateway systems going forward. First and foremost, two-factor authentication needs to be used to increase the security of digital payments. [3] This entails employing two different factors, such as tokens, RFID tags, or smartphone applications, to access a platform. With this technique, transaction security is improved and unauthorised users are prevented from making purchases. Second, sensitive credit card information should be changed to a special electronic identifier, or token, using tokenization. This guarantees the preservation of all important information without compromising the confidentiality of personal information. As tokens are generated at random, it is extremely improbable that they may be compromised or turned back. To create encrypted messages that only authorised users may decode, data encryption and masking should be used. This shields private user information from intrusion and assault. In order to avoid the disclosure of user information even in the event of a security breach, data held in payment processor repositories should also be encrypted. Last but not least, secure socket layer (SSL) certificates should be used to validate the legitimacy of a website and establish a secure connection for processing financial data. SSL certificates make sure that all digital payments made on the website are authorised and secured while also maintaining the privacy of client information. Also increasing consumer trust, conversion rates, and revenue is the adoption of SSL certificates.

4. Copyright Protection

It is possible to effectively conserve picture file resources and significantly lower the cost of picture file storage by building photography picture websites based on the network environment. [4] Digital watermarking is a useful technique for copyright protection of multimedia data. These data-embedded watermarks may take the form of numbers, serial numbers, text, or images. protecting copyright, ensuring communication security, identifying data files, and labeling products. Visible and invisible watermarks are the two main types of watermarks, depending on whether the watermark signal is visible or not. Visible watermarks are commonly used to declare copyright and are embedded in previewed pictures on most websites. The most widely used electronic watermark method for securing network photos involves adding a copyright tag to a particular region of the image that will be posted. This tag merges with the original data to form an integral part. But, before images are uploaded, a time-consuming process called applying watermarks to declare copyright

must be completed. We tried with various applications to test the effectiveness of the procedure because the number of photographs to be uploaded can be considerable.

5.SEO

Search engines have become indispensable tools for individuals to navigate and discover what they need as the internet has grown into a vast ocean of knowledge in the current digital age. Unfortunately, the majority of visitors frequently ignore lower-ranked pages in favour of merely paying attention to the top search results. This demonstrates how crucial search engine optimization (SEO) is for raising website rankings and boosting traffic. In order to make websites, webpages, and material more discoverable and understandable to search engine algorithms, SEO approaches entail optimising website structure, webpage code, and content. SEO may make websites more search engine-friendly by understanding how search engines index web pages and determine ranks for particular keywords. In turn, this can make it easier for search engine spiders to identify pertinent web pages and raise the website's organic rating in search results. In the end, SEO is a potent instrument that helps organizations connect with their target market and expand their marketing and revenue potential. Understanding how search engines index web pages and assign rankings for specific keywords can help SEO make websites more search engine friendly. This can improve the website's organic rating in search results by making it simpler for search engine spiders to find relevant web pages. Finally, SEO is a powerful tool that enables businesses to reach their target audience and increase their marketing and income potential. [5] The three main functions of full-text search engines are page collecting, page analysis, and page sorting. The search engine gathers information from the internet and stores it in its own database as part of page collection. [5] A spider programme is used by the search engine to find the webpage using its URL and then retrieve its information. Page analysis entails the search engine processing the gathered webpage using a variety of approaches, including label filtration, webpage text information extraction, text parsing, and creating an index between keywords and webpages. By doing this, the website is made user-searchable. Finally, when users submit keywords, a ranking programme calls the index database data to determine relevancy. The search result page is then produced by the search engine in a certain format. To properly optimize a website for search engine exposure and traffic, it is essential to understand some fundamental principles of search engine operation.

Keyword optimization

In order to improve a website's visibility in search engine results, one of the most important components of search engine optimization (SEO) is keyword optimization. When looking for websites, users frequently employ keywords, and search engines do the same. [5] Keywords are one of the main criteria used to retrieve websites.

Finding the core keywords that best describe the content and goal of a website is the first step in optimising its keyword strategy. Then, related keyword phrases and terms that users are likely to look for should be generated using these core keywords. Once the keywords and associated terms have been determined, they should be naturally and appropriately included into the website's content. This entails utilising the keywords consistently throughout the material, including in titles, headers, meta descriptions, and body copy.

Good keyword optimization increases the likelihood that a website will show up at the top of search results pages by assisting search engines in understanding the content of the website and its relevance to user queries.

Link optimization

A crucial component of search engine optimization (SEO) is link optimization, which entails carefully controlling the links on a website in order to raise its position in search engine results pages (SERPs). [5] The three link kinds that website owners should pay attention to are internal links, external links, and inbound links. In conclusion, in order to raise their website's rating in search engine results pages, website owners should strive to have high-quality incoming links, pertinent outgoing links, and comprehensive internal links. Also, it's critical to periodically check and manage these links to make sure they are not broken or go to unreliable websites that could harm the website's ranking.

REFERENCES

[1] Daniel T. Murphy ,Minhaz F. Zibran ,Farjana Z. Eishita, Plugins to Detect Vulnerable Plugins: An Empirical Assessment of the Security ScannerPlugins for WordPress , ©2021 IEEE SERA 2021, June 20-22, 2021, Kanazawa, Japan.

[2] , Ionut Cernica, Nirvana Popescu, Bogdan Tiganoaia ,Security Evaluation of WordPress Backup Plugins, Department of Computer Science, Faculty of Automatic Control and Computer Science University Politehnica of Bucharest Bucharest, Romania.

[3] Abhishek Nagre, Anshuman Sen ,Study Of Security Postures In Payment Gateways Using a Case Study Approach,– Symbiosis Institute of Digital and Telecom Management, constituent of Symbiosis International-Deemed University, Pune.

[4] XUE Feng, SHI Xue-fei, The Copyright protection about digital images based on web, Educational Technology College, Shenyang Normal University Shenyang, Liaoning, China, 2013 International Conference on Communication Systems and Network Technologies.

[5] Zhou Hui1, Qin Shigang2, Liu Jinhua3, Chen Jianli4 ,Study on Website Search Engine Optimization, Hunan electrical college of technology Xiang Tan, Hunan, P.R. China, 2012 International Conference on Computer Science and Service System.