NATIONAL DATA
MANAGEMENT AUTHORITY

WordPress Security Hardening Guidelines

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This guide outline best practices to harden the security of any WordPress website.
2. This is a living document which will be updated annually or as required.
3. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

The purpose of these guidelines is to outline security best practices that should be implemented to harden the security of any WordPress website.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this guideline. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

These guidelines encompass all websites being managed and maintained by the Government of Guyana.

4.0 Information Statement

According to the security magazine website, there is a cyber-attack every thirty-nine (39) seconds[1]. It has never been easier for script kiddies and expert hackers to access information online, which is why good website security is more important than ever. Implementing the proper website security controls is essential to maintaining any website's confidentiality, Integrity, and Availability (CIA).

Many government websites are developed using WordPress. It is the most popular CMS (Content Management System) software in the world, and it powers approximately 43% of all websites on the web[2]. However, due to its popularity, it is the most targeted by hackers. Several articles have highlighted that WordPress is the most targeted content management system[3][4][5][6]. Therefore, Government agencies and ministries must implement the necessary security controls on their WordPress websites to keep nefarious individuals from accessing sensitive information.

The primary goal of Government websites is to facilitate information sharing among Government to Government (G2G), Government to Business (G2B), Government to Employees (G2E), and Government to Citizens (G2C) across the length and breadth of Guyana and globally. Thus, if the website of any Government agency or ministry in Guyana is compromised, it can affect citizens' trust in the Government of Guyana's ability to provide secure online services.

[1] https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
[2] https://www.wpbeginner.com/showcase/best-cms-platforms-compared/#:~:text=WordPress.org%20is%20our%20number,all%20websites%20on%20the%20internet.
[3] https://patchstack.com/articles/why-wordpress-sites-get-hacked/
[4] https://www.zdnet.com/article/wordpress-accounted-for-90-percent-of-all-hacked-cms-sites-in-2018/
[5] https://www.securityweek.com/wordpress-most-attacked-cms-report
[6] https://blog.hubspot.com/website/is-wordpress-secure

As new and more effective website security features and functions emerge for WordPress, hackers are continuously sharpening their skills to bypass these security features and attack vulnerable websites. Therefore, Government agencies and ministries must ensure that their websites are properly secure. This document outlines a list of security best practices that should be implemented to harden the security of any WordPress website.

5.0 Guideline

5.1 Security Best Practices for Hardening WordPress

The table below outlines a list of security best practices that should be implemented to harden the security of a WordPress website.

Recommendation	Benefit	Implementation Stage
Install and configure a paid security plugin	A security plugin protects a website from malware, brute-force attacks, and hacking attempts. Security plugins are designed to protect a website from attacks and to generate detailed security reports. These plugins also assist in cleaning WordPress sites infected with malware and hardening WordPress security. The following are some of the best WordPress security: • Sucuri • Malcare • Astra • Wordfence	***Development /Coding***
Implement and configure 2-factor authentication(2FA)	One of the most common ways nefarious individuals break into websites is through the login page. They use brute-force attacks to guess a website's login credentials. To further strengthen the security posture of a WordPress website, it is recommended that two-factor authentication (2FA) be implemented for every user, regardless of their role: Super Admin, Administrator, Editor, Author, Contributor, or Subscriber.	***Development /Coding***
Limit the number of failed login attempts *Note: The application's nature should determine the total number of failed login attempts allowed.*	Limiting the number of failed login attempts aids in eliminating brute-force attacks. WordPress, by default, allows an unlimited number of login attempts. Enabling limited failed login attempts on a WordPress website improves security by preventing hackers from trying thousands of username and password combinations to gain unauthorized access.	***Development /Coding***
Automatically logout inactive users	Idle users pose a security risk to a WordPress website. Suppose someone leaves their laptop unattended. In that case, a stranger may be able to see sensitive information, change their password, or gain unauthorized access to their account. Automatically	***Development /Coding***

Recommendation	Benefit	Implementation Stage
Period of Inactivity for Critical Application: 15 minutes ***Period of Inactivity for Non-Critical Application:*** 30 minutes	logging out users after a period of inactivity protect accounts from any unauthorized.	
Require the use of strong passwords	Passwords provide the first line of defense against unauthorized access to a website. The stronger a password is, the more protected a website will be from nefarious individuals. It is essential that website users maintain a strong password and change it regularly. WordPress, by default, will issue an alert if a user chooses a weak password. However, the user can choose to override it by checking 'confirm the use of a weak password.' Thus, this feature must be disabled, and the website should only allow users to create strong passwords.	***Development /Coding***
Disable the file editor	If nefarious individuals access a WordPress Administrator account, they gain complete control of the website. Through the "Editor" option on the dashboard, they can modify the code of the website theme and plugins. Additionally, they can upload malicious scripts to deface the website or create backdoors. Therefore, it is recommended that the website's editor be disabled before deployment.	***Deployment***
Change security keys from time to time ***Critical Application*:** This should be done every three (3) months ***Non-Critical Application:*** This should be done every six (6) months ***Breached Application:*** This should be done whenever an application is breached.	WordPress security keys are encryption tools that protect login information by making it harder to decode. These keys function like real keys, locking and unlocking encrypted data such as passwords and keeping a WordPress site secure. If nefarious individuals get their hands on the security keys and salts, they can decipher encrypted data and hack into user accounts. Thus, it is recommended that the old keys and salts be updated regularly.	***Deployment***
Secure wp-config.php file	Nefarious individuals love to go after the wp-config.php file because it is one of the most important files on a WordPress website. Wp-config is what	***Deployment***

Commented [A1]: It would be useful to suggest a timeframe for both critical and non critical applications

Recommendation	Benefit	Implementation Stage
	makes a WordPress site work and is also where the database login information for a WordPress site is kept. Because the configuration is vulnerable to attacks, it must be secured. One way of doing it is by changing its location so that hackers can't find it in its default location. Also, file permissions should be restricted as an additional security measure. Set the file permissions to 600 so that the wp-config file can only be edited by the owners. Finally, it is recommended that access to this file be set to deny to protect it. This can be accomplished by modifying the .htaccess file.	
Secure WP-Admin	One way to improve the admin login security is by forcing logins to be transmitted over SSL (Secure Sockets Layer). This can be done by adding this piece code "define ('FORCE_SSL_ADMIN,' true);" to the wp-config.php file. Ensure that an SSL certificate is installed on the website and that any mixed content issues are resolved.	***Development /Coding***
Change Database Prefix	WordPress databases hold all the website's data. They may be vulnerable to attacks if they are named with the platform's default prefix. Changing this to a unique prefix can help to hide table names and improve the website's overall security posture.	***Development /Coding***
Obfuscate the Admin portal	By default, the URL (Uniform Resource Locator) for logging into all WordPress websites is the website's main URL followed by wp-login.php or wp-admin - for example, testapp.com/wp-login.php. Cybercriminals are aware of this; if you can change this URL, you will make it more difficult for them to access the website's login page. Thus, it is recommended that the admin portal's URL be obfuscated to make it less predictable.	***Development /Coding***
Implement a CAPTCHA in the login page	Implementing a CAPTCHA on the login page can reduce hacking attempts by preventing automated scripts from attempting brute-force or other attacks on the login page without first solving the CAPTCHA's challenge.	***Development /Coding***

6.0 Compliance

These guidelines shall take effect upon publication. Compliance is expected with all organisational guidelines, policies, and standards. Failure to comply with the guidelines may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources

of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

7.0 Exceptions

Requests for exceptions to this guideline shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

8.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this guideline.

9.0 Definitions of Key Terms

Term	Definition
CAPTCHA[7]	Completely Automated Public Turing test to tell Computer and Humans Apart
Hardening[8]	A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.

10.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[7] *Retrieved from NIST* NIST Information Technology Laboratory Computer Security Resource Center *https://csrc.nist.gov/glossary/term/captcha*
[8] *Retrieved from NIST* NIST Information Technology Laboratory Computer Security Resource Center *https://csrc.nist.gov/glossary/term/hardening*