



Hardening WordPress

(WordPress වෙබ් අඩවියක ආරක්ෂාව තර කිරීම)

By LK Domain Incident Response Team

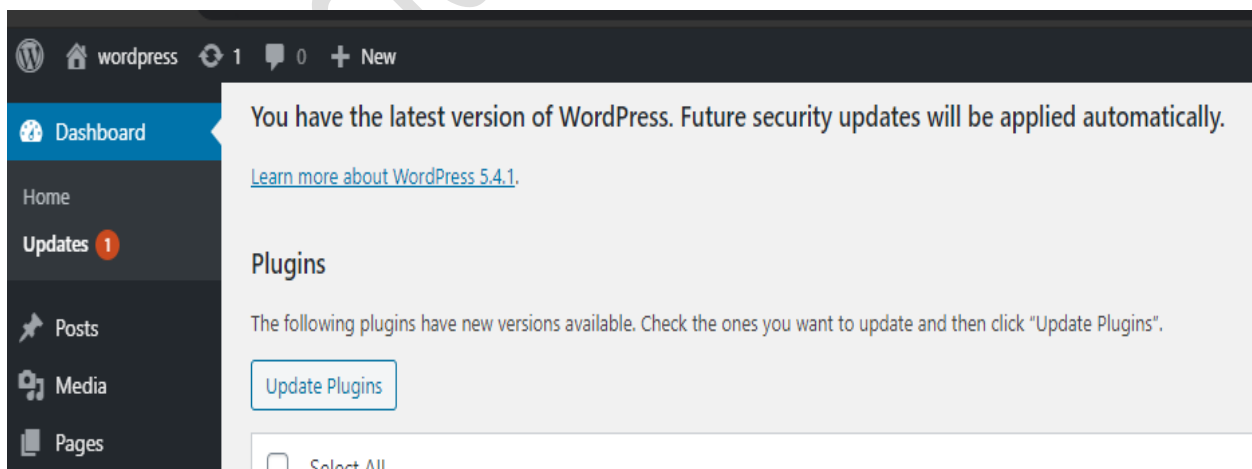
WordPress වෙබ් අඩවියක ආරක්ෂාව තර කිරීම

1. WordPress යාවත්කාලීන කිරීම.
2. තේමා සහ plugins සකස් කර ගැනීම.
3. ශක්තිමත් සහ ආවේනික වූ මුරපද භාවිතය.
4. wp-admin සහ wp-includes සුරක්ෂිතකරණය.
5. wp-config.php සුරක්ෂිතකරණය.
6. wordpress admin හි ලිපිගොනු වෙනස් කිරීම වැලැක්වීම.
7. අන්තර්ජාල මෘදුකාංග firewall එකක් (web application firewall (WAF)) භාවිතය.
8. අපැහැදිලි බව තුලින් ආරක්ෂාව
9. දත්ත උපස්ථය හෙවත් Backup කිරීම
10. Username හරහා වන අනවසර ඇතුළුවීම් අවහිර කිරීම
11. functions.php හරහා Rest API අක්‍රිය කිරීම.
12. .htaccess ගොනුව හරහා WordPress හි XML-RPC අක්‍රිය කිරීම

1. WordPress යාවත්කාලීන කිරීම.

නවතම WordPress සංස්කරණය <https://wordpress.org> හරහා Wordpress ප්‍රධාන වෙබ් අඩවියෙන් ලබාගත් හැක.

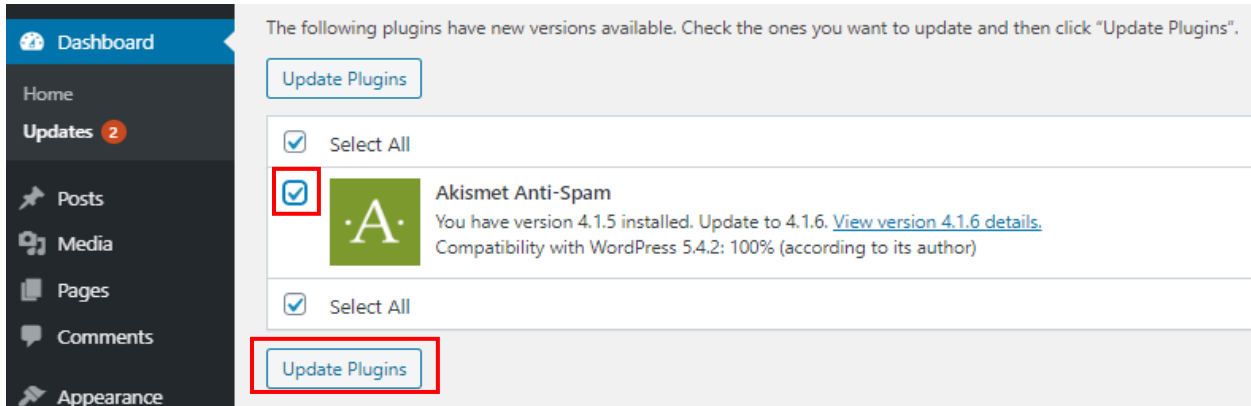
3.7 සංස්කරණයේ සිට, WordPress විසින් ස්වයංක්‍රීය යාවත්කාලීන වීම් ලබා දේ, නවතම සංස්කරණය භාවිතය සඳහා WordPress යාවත්කාලීන කර තබා ගැනීමට මෙම පහසුකම භාවිත කරන්න.



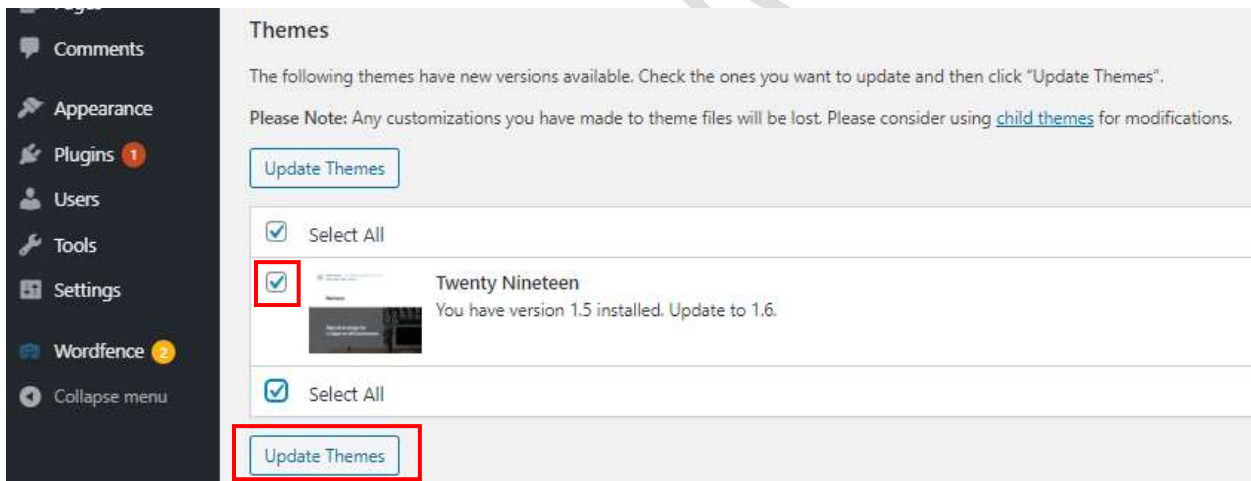
2. තේමා සහ plugins යාවත්කාලීන කිරීම.

WordPress මූල වැඩසටහන යාවත්කාලීන කරන විට, ඔබේ තේමා සහ plugins ද යාවත්කාලීන කිරීමට අමතක නොකරන්න. පැරණි තේමාවල හඳුනාගත් විවිධ ආරක්ෂණ අඩුපාඩු දන්නා හැකර්වරුන් ඒවාට ප්‍රියතාවක් දක්වයි.

Plugins යාවත්කාලීන කිරීම.



තේමා යාවත්කලීන කිරීම.



Plugins තෝරාගන්නා විට, මේ පිළිබඳව පරීක්ෂා කල යුතුය;

- Plugin පිළිබඳ විවාර.
- එම plugin එක කොපමණ දෙනෙකු භාවිත කර ඇතිද යන්න
- එහි හඳුනාගත් අවදානම් තත්ත්වයන්.

contact form plugin, WAF, backup plugin සහ security plugin යන plugins භාවිත කිරීම සුදුසු වේ.

- ❖ WAF – wordfence plugin
- ❖ Contact form plugin – wp forms
- ❖ Backup plugin – updraft

කාලයත් සමඟ මෙම අනුමත කිරීම් වෙනස් විය හැක.

ඔබ plugin එකක් භාවිත කරන විට, ඔබට <https://wpsvulndb.com/> හරහා එහි කලින් හඳුනාගත් අවදානම් තත්වයන් ගැන සොයා බැලිය හැක.

The screenshot shows the WPScan Vulnerability Database website. At the top, there is a navigation bar with links for WordPress, Plugins, Themes, API, Submit, Login, and Register. A search bar contains the text 'updraft' and a 'SEARCH' button. Below the navigation bar, the main heading is 'WPScan Vulnerability Database' with a subtitle 'Cataloging 21621 WordPress-Core Vulnerabilities, Plugin Vulnerabilities and Theme vulnerabilities.' There are three buttons: 'Email Alerts', 'Submit a Vulnerability', and 'Try our API'. Below these buttons is a search bar with 'updraft' entered. A table of results is displayed below the search bar, with columns for ID, Added, and Title.

ID	Added	Title
9843	2019-08-28	Updraftplus < 1.13.5 - XSS
9840	2019-08-28	Updraftplus < 1.9.64 - XSS
7918	2015-04-20	UpdraftPlus Backup & Restoration <= 1.9.6.3 - Cross-Site Scripting (XSS)
7781	2015-02-03	UpdraftPlus <= 1.9.50 - Privilege Escalation via Nonce Leakage

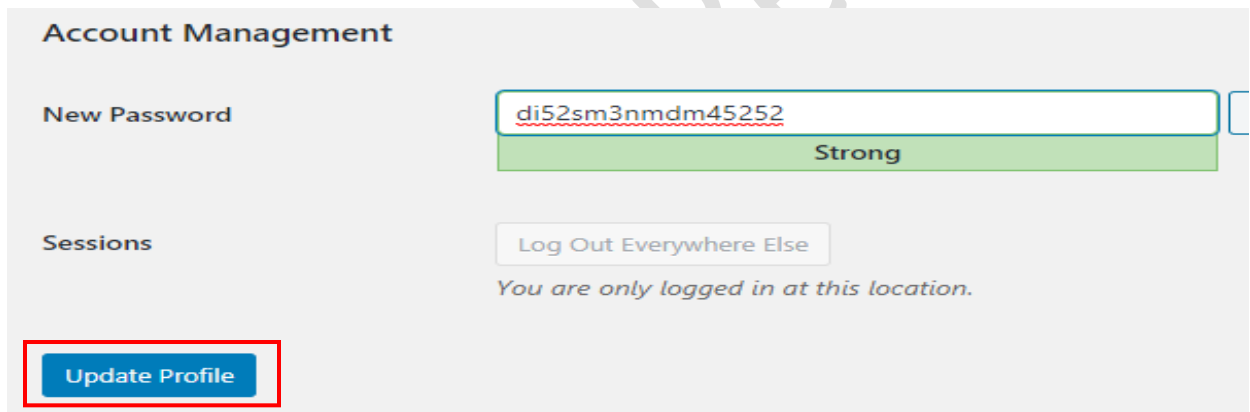
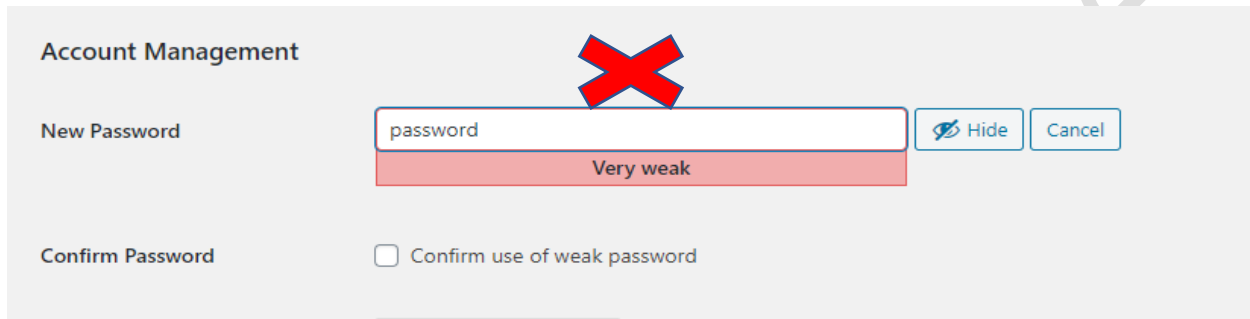
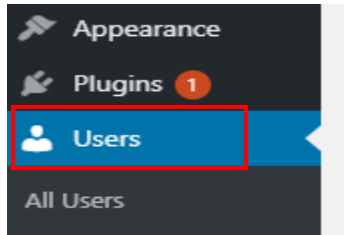
3. ආවේනික සහ ශක්තිමත් මුරපද භාවිත කරන්න.

හොඳ ආරක්ෂක උපක්‍රම අනුගමනය තුළින් ඇතිවිය හැකි බොහෝ අවදානම් තත්වයන් මඟ හරවාගත හැක. මෙහිදී ශක්තිමත් මුරපදයක් භාවිතය අත්‍යවශ්‍ය වේ.

මුරපදයක් තෝරාගැනීමේදී වැලකී සිටිය යුතු යුතු කරුණු:

- ඔබේ නමෙහි, පරිශීලක ගිණුම් නාමයෙහි, ආයතන නාමයෙහි, ඔබේ වෙබ් අඩවියේ නාමයෙහි අකුරු අඩංගු වන ලෙස සුළු වෙනස් කිරීම් සිදු කල වචන භාවිතය.
- ශබ්දකෝෂයකින් හෝ යම්කිසි භාෂාවකින් උපුටාගත් වචනයක් භාවිතය.
- ඉතා කෙටි මුරපදයක් තෝරාගැනීම.
- ඉලක්කම් පමණක් හෝ අකුරු පමණක් අඩංගු වන මුර පදයක් තෝරාගැනීම(එම ආකාර දෙකම කලවමේ භාවිත කිරීම ඉතා යෝග්‍ය වේ).

How to change password in a WordPress account.



4. wp-admin සහ wp-includes සුරක්ෂිතකරණය.

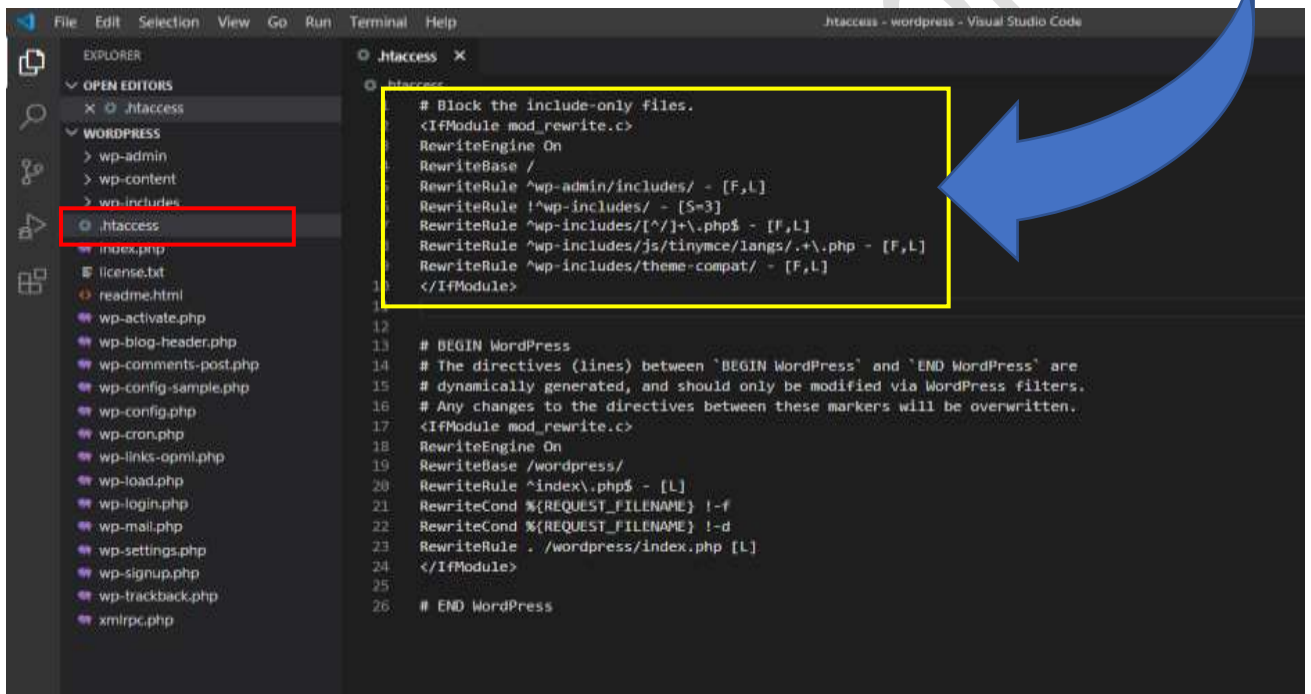
/wp-admin/ වෙතට සර්වර් ආශ්‍රිතව මුරපදයක් ඇතුළත් කිරීමෙන් ඔබේ බ්ලොග් අඩවියේ admin කොටසට, ඇතුළුවීමේ Login තිරයට සහ ඔබේ ගොනු වලට දෙවෙනි මට්ටමක ආරක්ෂාවක් ලැබේ. එමඟින් අනවසර හැකර්වරයෙකුට හෝ හැකර් මෘදුකාංගයකට ඔබේ admin කොටසට ඇතුළුවීමට උත්සාහ ගැනීමේදී තවත් ආරක්ෂක ස්ථරයක් බිඳ දැමීමට සිදුවේ.

ක්‍රමලේඛයන් වෙතට වෙනත් පරිශීලකයෙකුට ඇතුළුවීමට අවස්ථාව ලබා නොදීමට අවශ්‍ය අවස්ත්‍රාවලදී දෙවෙනි ස්ථරයේ ආරක්ෂාවක් ලබාදීම කල හැකිය.

.htaccess file හි අඩංගු mod_rewrite හරහා එම ක්‍රමලේඛ අවහිර කිරීම මෙය කල හැකි එක් ආකාරයකි.

```
# Block the include-only files.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^\.]+\.\php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.\php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
</IfModule>
```

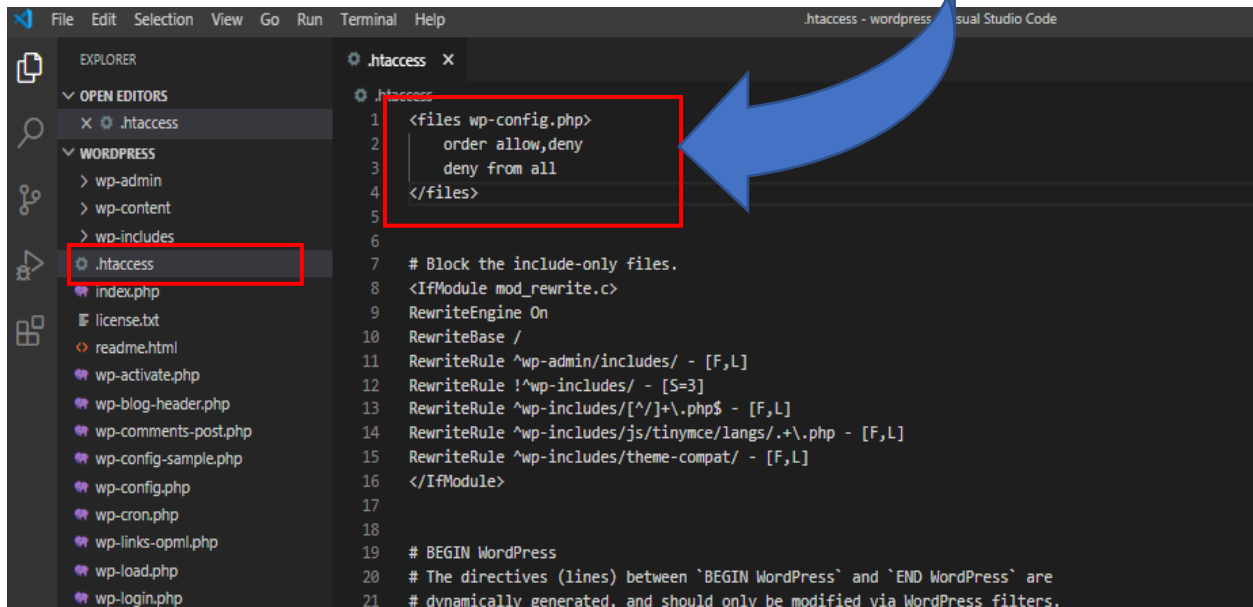
BEGIN WordPress යන්නට ඉහලින් මෙය තැබිය යුතුයි.



5. wp-config.php සුරක්ෂිතකරණය

ඔබ භාවිතා කරන සර්වර් එක .htaccess සහිත නම්, මෙයට ඇතුළු වීමට උත්සාහ දරන්නන් අවහිර කිරීමට මෙය එම ගොනුව තුළට(ඉහලින්ම) ඇතුළත් කළ යුතුය.

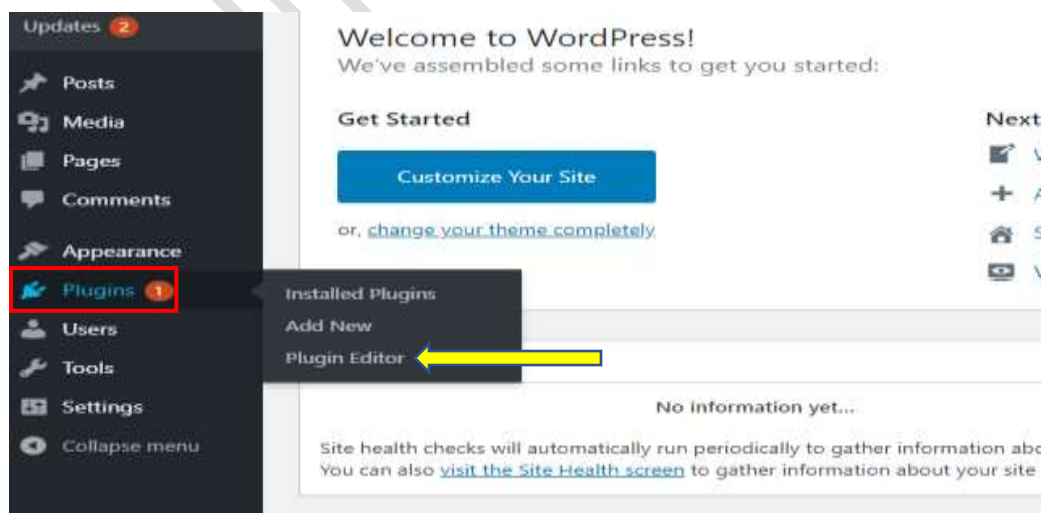
```
<files wp-config.php>
order allow,deny
deny from all
</files>
```



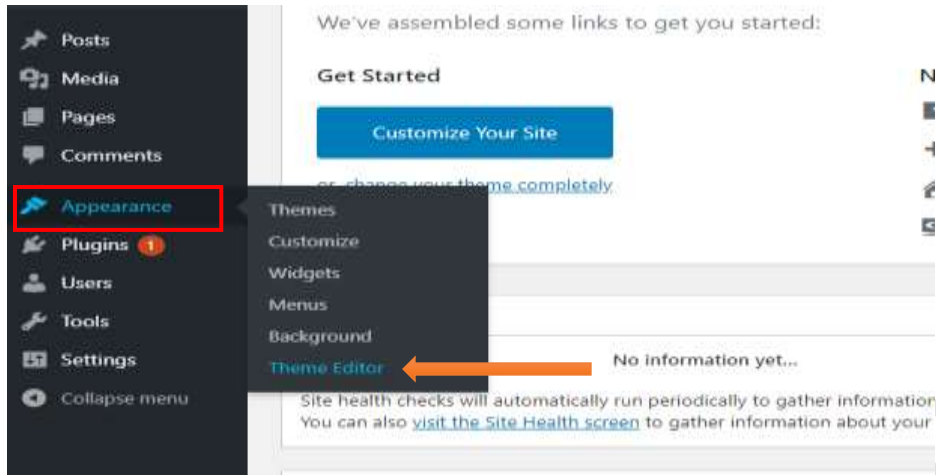
6. WordPress admin හි ගොනු වෙනස් කිරීම අවහිර කිරීම.

WordPress dashboard එක මගින් ආරම්භයේදීම administrator වෙත plugins හා තේමා වැනි php ගොනු වෙනස් කිරීමට අවස්ථාව ලබා දේ.

Plugins → Plugin Editor



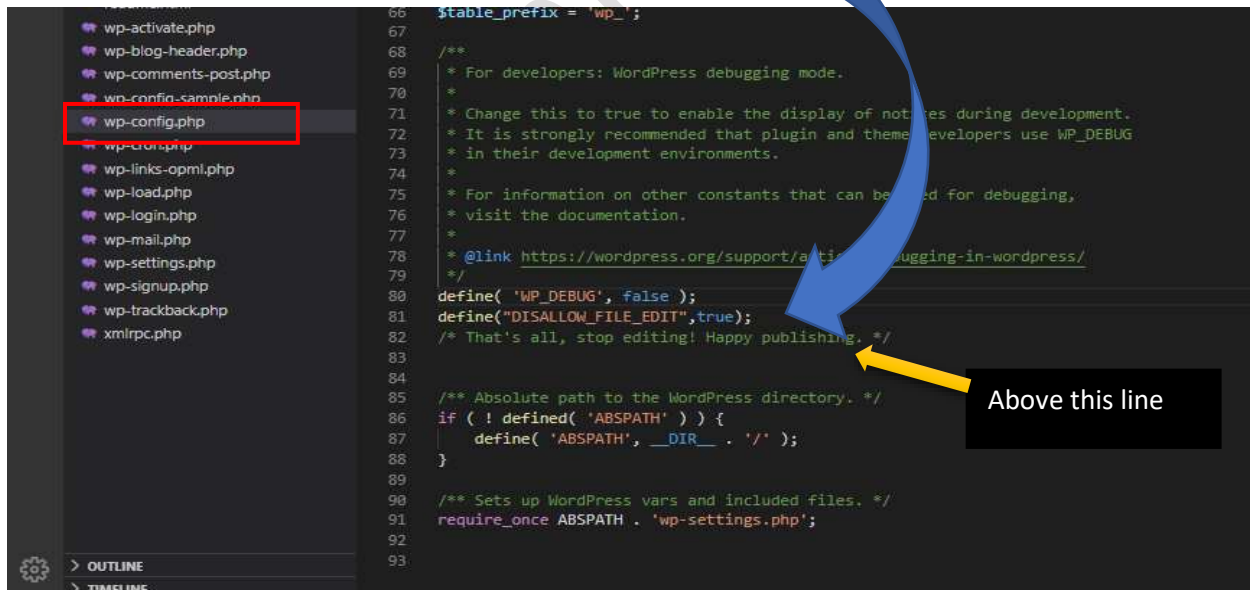
Appearance → Theme Editor



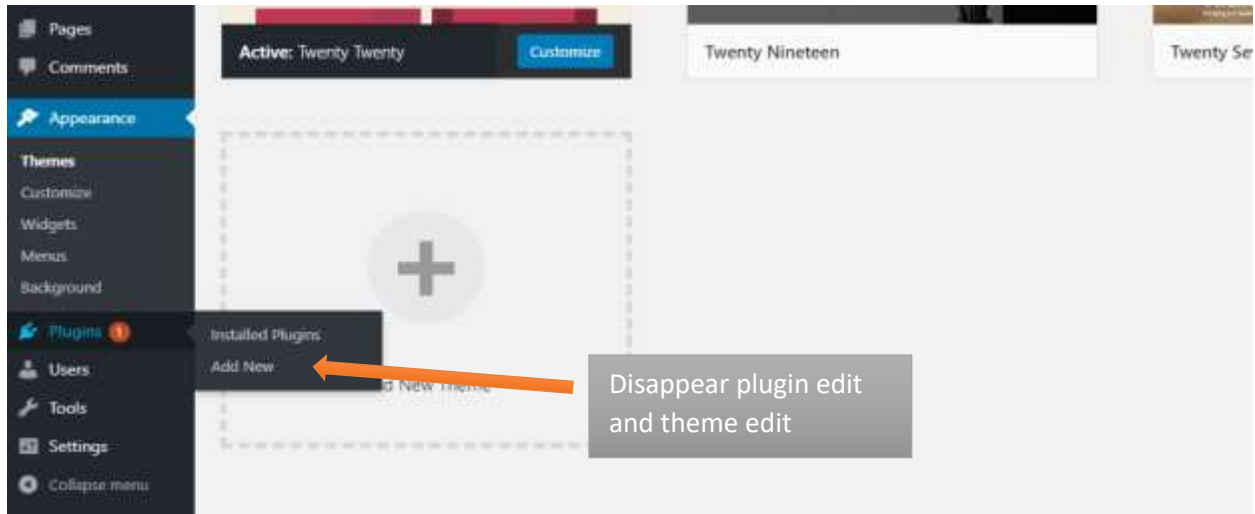
මේ හරහා ක්‍රමලේඛ ක්‍රියාත්මක කරවීමට හැකි වන නිසා හැකර්වරයෙකුට login form එක හරහා ඇතුළුවීමට ලැබෙන අවස්ථාවකදී පහර දෙන පළමු tool එක මෙය වේ.

WordPress හි ගොනු වෙනස් කිරීම අවහිර කරන ආකාරය.

```
define ("DISALLOW_FILE_EDIT",true);
```



එම කේතය ලබාදීමෙන් පසුව:



මෙය යම් ප්‍රහාරකයෙකුට ඔබේ වෙබ් අඩවියට මැල්වේයාර් ගොනු ඇතුළු කිරීම වළක්වනවා මෙන්ම වෙනත් ආකාරයේ සයිබර් ප්‍රහාරද වලක්වයි.

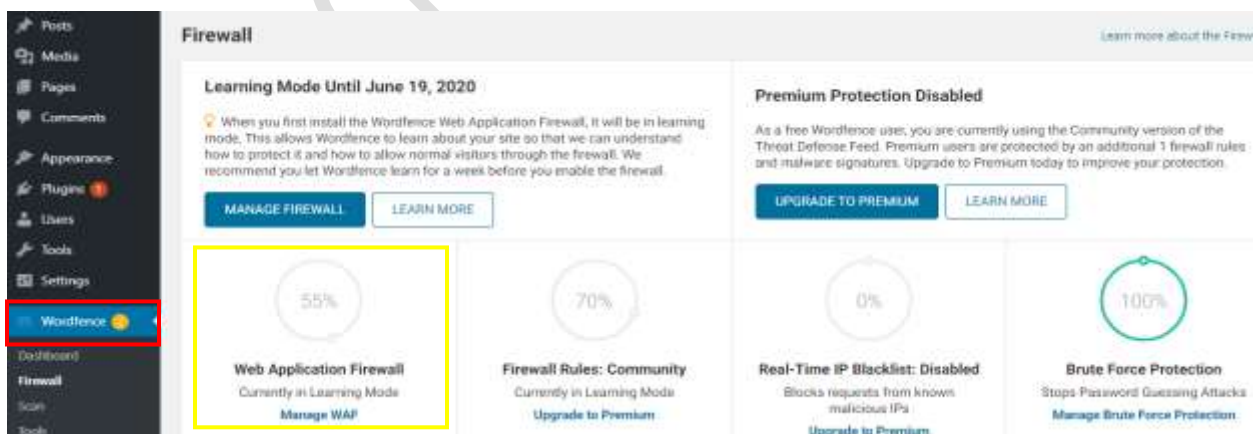
7. web application firewall (WAF) එකක් භාවිත කිරීම.

ඔබේ වෙබ් අඩවියට Firewall එකක් ලෙස ක්‍රියාකළ හැකි සේවාවන් සහ plugins රාශියක් ඇත.

අනෙක් ඒවායේ යම් ආරක්ෂණ දෝෂ පැවතිය හැකි නිසා අප විසින් wordfence plugin එක අනුමත කර සිටිමු.

[Wordfence plugin එක ස්ථාපනය\(install\) කරගන්නා ආකාරය.](#)

Install කිරීමෙන් පසු ඔබට පහත තිරය දිස්වේ;



ඔබ WAF plugin එකක් තෝරාගන්නා විට පහත දැ පිලිබඳ සැලකිලිමත් වන්න:

- ලබාදෙන පහසුකම්.
- නිරන්තර යාවත්කාලීනවීම් සිදුවේද යන්න.

විශේෂයෙන් සැලකිලිමත් විය යුතු කරුණු,

- Blacklist (ලබා දෙන IP range එක).
- Whitelist (ලබාදෙන ip range එක).
- Dynamic blacklist.
- වෙබ් අඩවියේ සිදුවන ක්‍රියාකාරකම් Admin හට පරීක්ෂා කිරීමට අවස්ථාව ලැබේද යන්න.
- Strict mode පිලිබඳ දැනුම් දීම්.
- ගොනුවල අඛණ්ඩතාවය හෙවත් ගොනු හානි වීම්වලට ලක්ව තිබේදැයි පරීක්ෂාව.
- හානිදායක යෙදවුම් හෙවත් මැල්වෙයාර් පරීක්ෂා කිරීම.

8. අපැහැදිලි බව තුළින් ආරක්ෂාව.

Administrative ගිණුමෙහි නම වෙනස් කරන්න.

Administrative account එකක් සෑදීමේදී, admin හෝ webmaster වැනි පහසුවෙන් අනුමාන කල හැකි පරිශීලක ගිණුම් නාමයන් භාවිත නොකළ යුතුයි. එවැනි නම් සහිත ගිණුම් වලට ප්‍රහාරකයින් පහරදීමේ අවස්ථාව වැඩිය.

The screenshot shows the phpMyAdmin interface. On the left, the database structure is listed, with 'wordpress' and 'wp_users' highlighted in red boxes. A yellow box labeled 'Your WordPress Database' has an arrow pointing to the 'wordpress' database. The main area shows the 'wp_users' table with one row: 'admin' with a long password. Below the table, there are options for 'Query results operations' and 'Bookmark this SQL query'.

The screenshot shows the SQL query editor. The query is: `UPDATE wp_users SET user_login = 'newuser' WHERE user_login = 'admin';`. The query is highlighted with a yellow box. A blue arrow points from the text 'New Username' below to the 'newuser' string in the query.

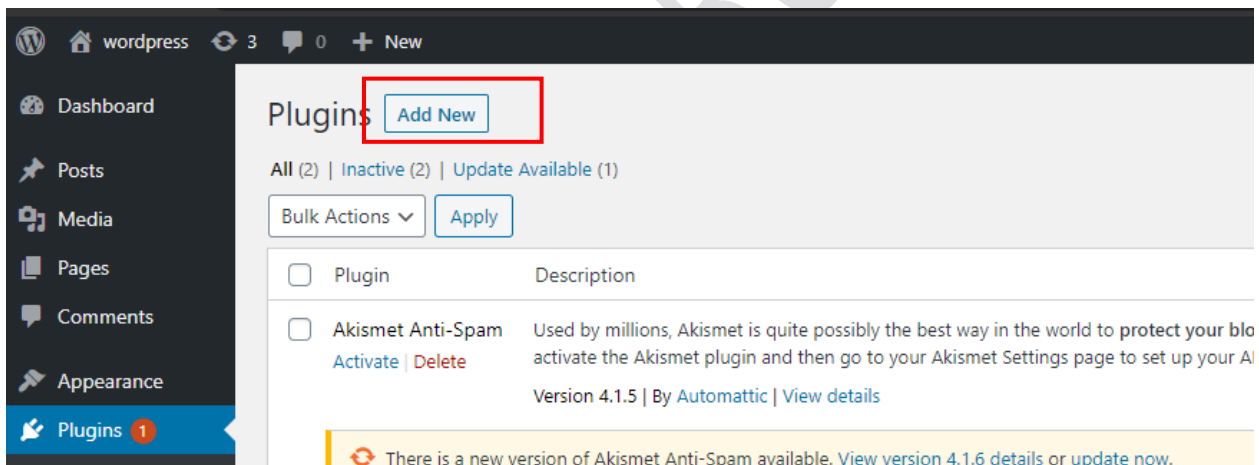
+ Options		ID	user_login	user_pass
<input type="checkbox"/>	Edit Copy Delete	1	newuser	\$P\$Bjml1.qRn2kxcy7sbxzddZ72Q/9M
Check all		With selected: Edit Copy Delete Export		

9. දත්ත උපස්ථය හෙවත් backup කිරීම

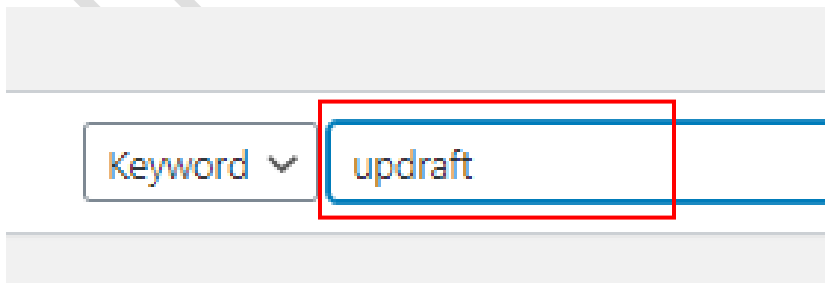
ඔබේ WordPress වෙබ් අඩවියේ විශාලත්වය කෙතරම් වුවත් යාවත්කාලීන වීම් ඇනහිටීම්, හැකර් ප්‍රහාර, පරිශීලකයන්ගේ වැරදීම් සහ හදිසි බිඳවැටීම් වලදී ඔබේ දත්ත වලට හානි වීම වලින් වලක්වා ගැනීම අත්‍යවශ්‍ය වැදගත් වේ.

WordPress වෙබ් අඩවියක් පහසු සහ නොමිලේ ලබාදෙන backup plugin එකක් හරහා backup කරගන්නා ආකාරය බලමු. මේ සඳහා UpdraftPlus plugin එක වඩා සුදුසුය.

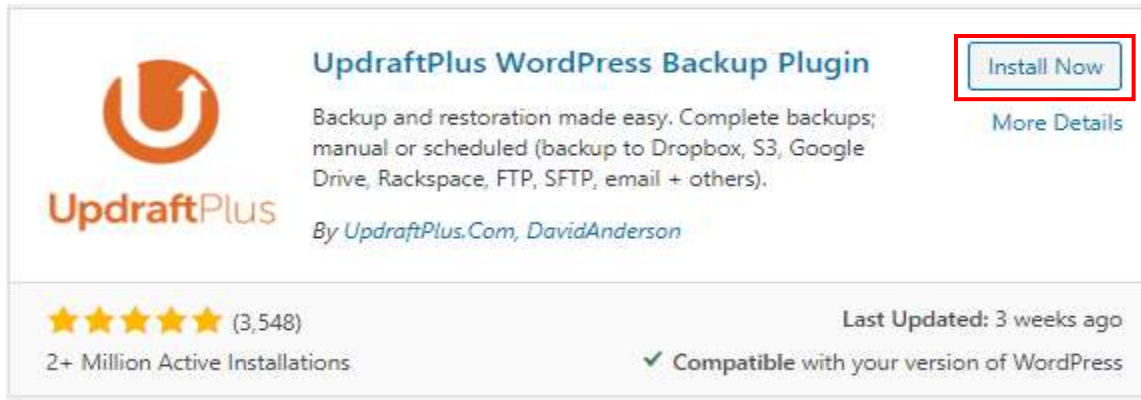
පියවර 1



පියවර 2



පියවර 3



UpdraftPlus WordPress Backup Plugin [Install Now](#)
[More Details](#)

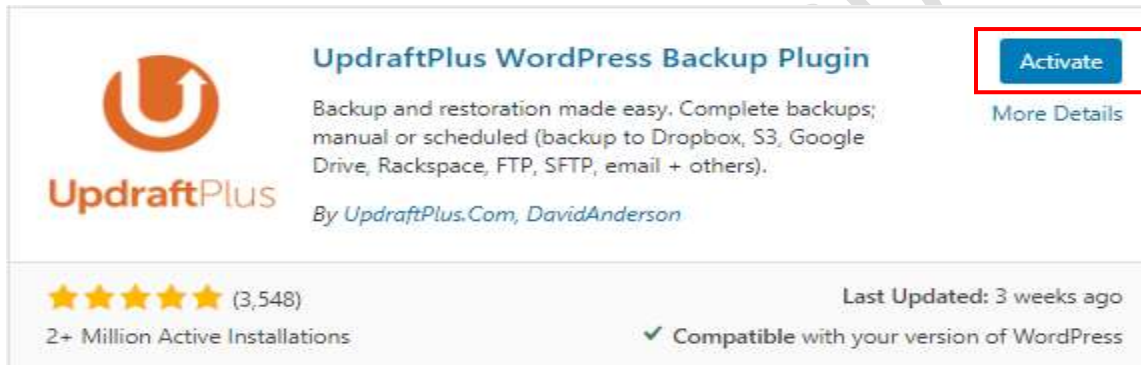
Backup and restoration made easy. Complete backups; manual or scheduled (backup to Dropbox, S3, Google Drive, Rackspace, FTP, SFTP, email + others).

By *UpdraftPlus.Com, DavidAnderson*

★★★★★ (3,548)
2+ Million Active Installations

Last Updated: 3 weeks ago
✓ Compatible with your version of WordPress

පියවර 4



UpdraftPlus WordPress Backup Plugin [Activate](#)
[More Details](#)

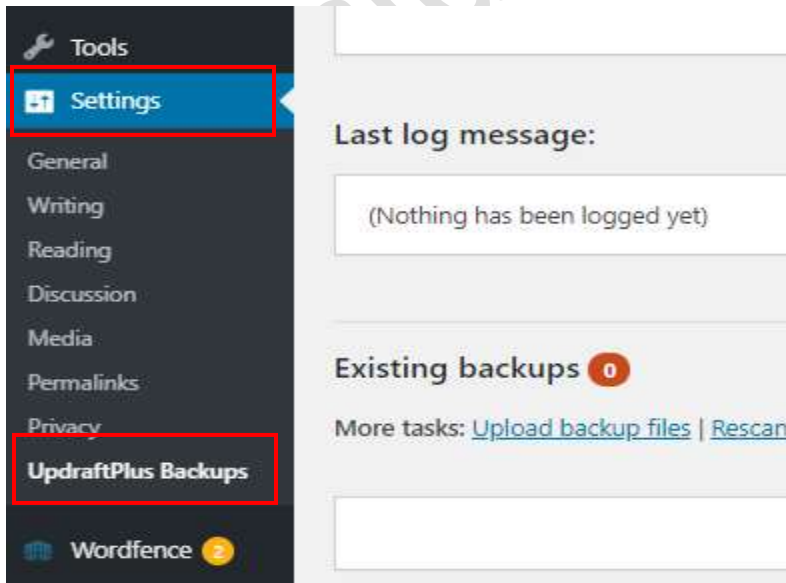
Backup and restoration made easy. Complete backups; manual or scheduled (backup to Dropbox, S3, Google Drive, Rackspace, FTP, SFTP, email + others).

By *UpdraftPlus.Com, DavidAnderson*

★★★★★ (3,548)
2+ Million Active Installations

Last Updated: 3 weeks ago
✓ Compatible with your version of WordPress

පියවර 5



Tools

Settings

General

Writing

Reading

Discussion

Media

Permalinks

Privacy

UpdraftPlus Backups

Wordfence 2

Last log message:

(Nothing has been logged yet)

Existing backups 0

More tasks: [Upload backup files](#) | [Rescan](#)

Step 6

[UpdraftPlus.Com](#) | [Premium](#) | [News](#) | [Twitter](#) | [Support](#) | [Newsletter sign-up](#) | [Lead developer's homepage](#) | [FAQs](#) | [More plugins](#) - Version: 1.16.25

Backup / Restore | Migrate / Clone | **Settings** | Advanced Tools | Premium / Extensions

Files backup schedule: and retain this many scheduled backups:

Database backup schedule: and retain this many scheduled backups:

To fix the time at which a backup should take place, (e.g. if your server is busy at day and you want to run overnight), to take incremental backups, or to configure more complex schedules, [use UpdraftPlus Premium](#)

පියවර 7

ඔබ Remote storage ලෙස Google Drive ලබා දෙන්නේ නම් (අනෙක් පහසුකම්ද ලබා දිය හැක.);

Choose your remote storage (tap on an icon to select or unselect):

	UpdraftPlus Vault		FTP		S3-Compatible (Generic)
	Dropbox		Microsoft Azure		OpenStack (Swift)
	Amazon S3		SFTP / SCP		DreamObjects
	Rackspace Cloud Files		Google Cloud		Email
	Google Drive		Backblaze		
	Microsoft OneDrive		WebDAV		

Choose remote storage

[You can send a backup to more than one destination with an add-on.](#)

Google Drive

පියවර 8

Expert settings: [Show expert settings](#) - open this unless you have a problem or are curious.

Like UpdraftPlus Please help UpdraftPlus by giving a positive review at wordpress.org. [Review UpdraftPlus](#)

Save Changes

Saving...

පියවර 9

Google Drive

Please read [this privacy policy](#) for use of our Google Drive authorization app (none of your backup data is sent to us).

Google Drive Folder:
To be able to set a custom folder name, use UpdraftPlus Premium.

Authenticate with Google: [After you have saved your settings \(by clicking 'Save Changes' below\), then come back here once and follow this link to complete authentication with Google Drive.](#)





පියවර 10

Sign in with Google

Choose an account
to continue to **UpdraftPlus**

පියවර 11

This will allow **UpdraftPlus** to:

-  See and download all your Google Drive files 
-  View and manage Google Drive files and folders that you have opened or created with this app 

Make sure you trust UpdraftPlus

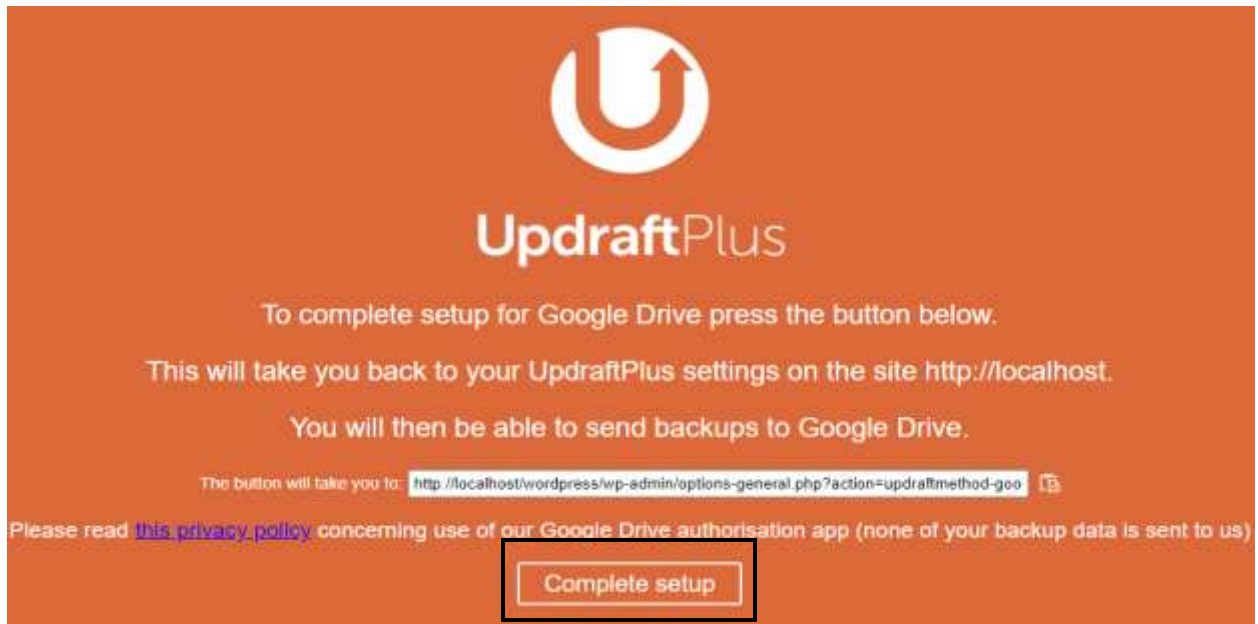
You may be sharing sensitive info with this site or app. Learn about how UpdraftPlus will handle your data by reviewing its [privacy policies](#). You can always see or remove access in your [Google Account](#).

[Learn about the risks](#)

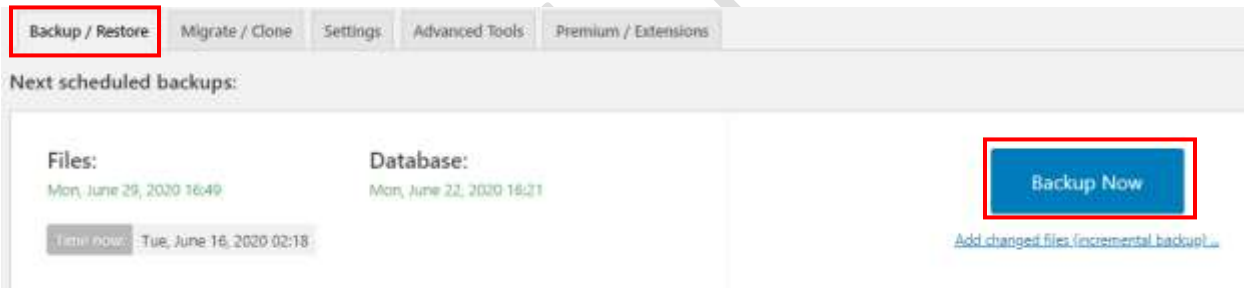
Cancel

Allow

ଛେପର 12



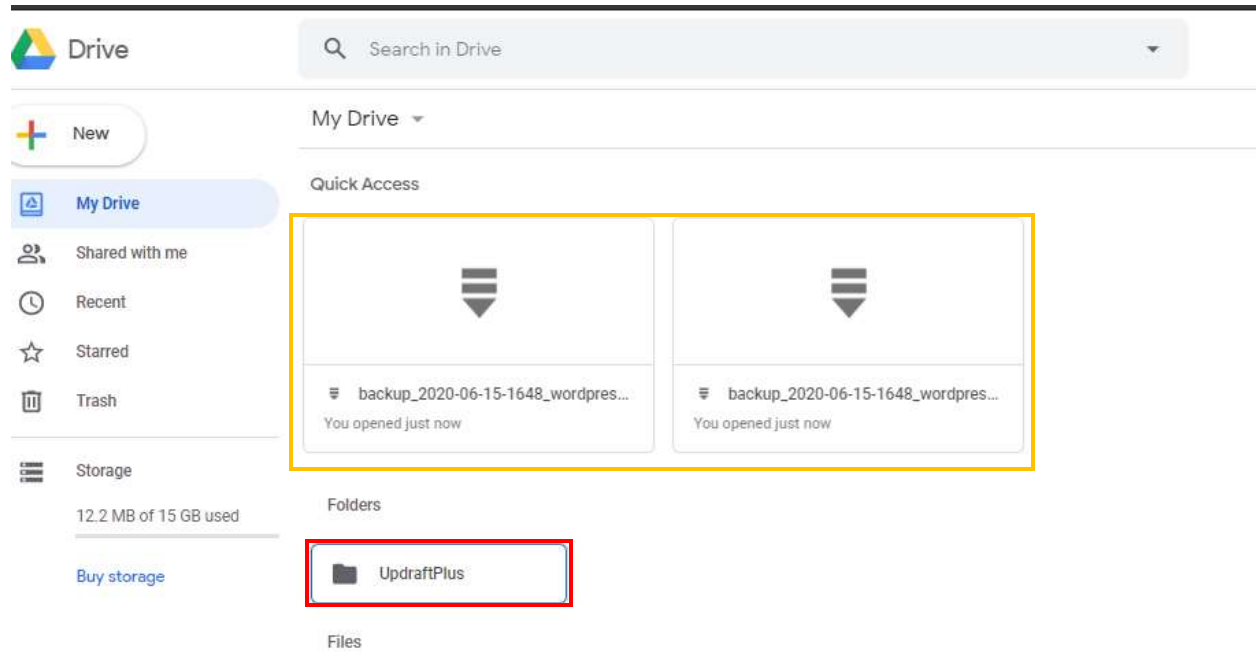
ଛେପର 13



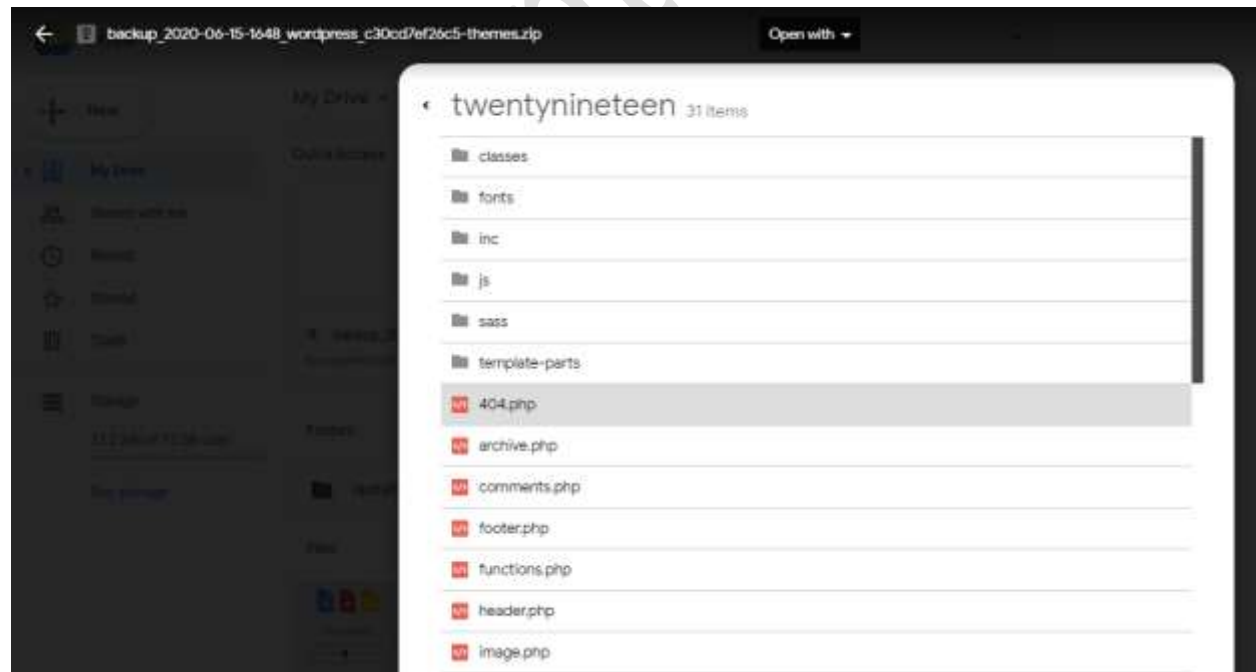
ଛେପର 14



පියවර 15

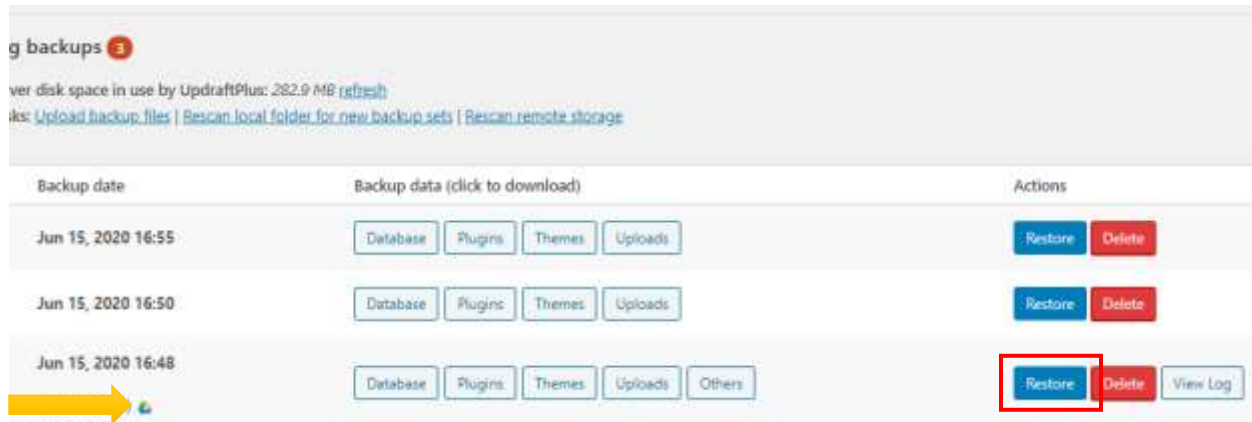


පියවර 16

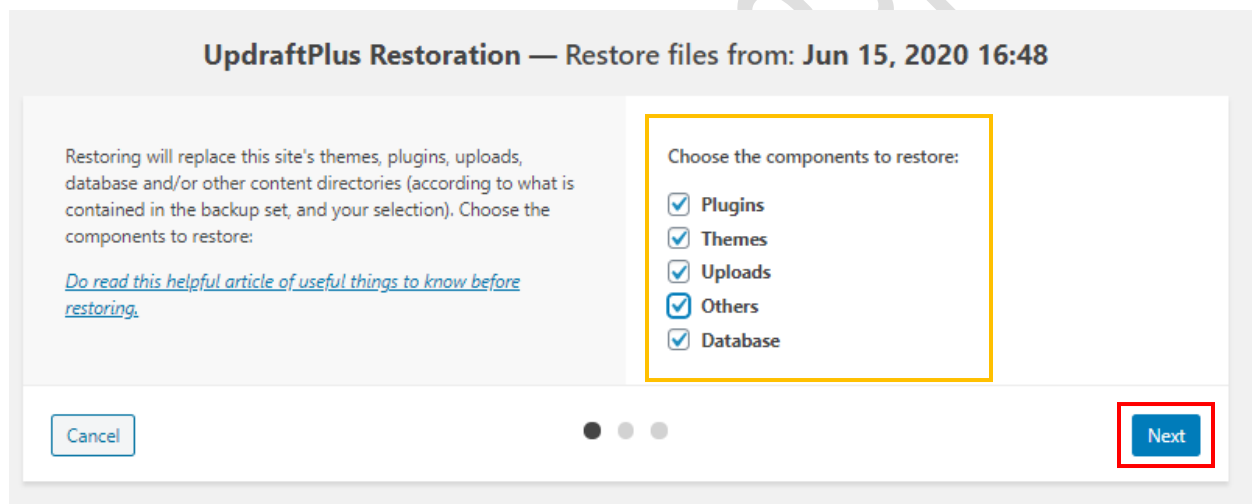


ඔබේ WordPress වෙබ් අඩවිය backup කිරීමකින් පසුව නැවත ලබාගන්නා ආකාරය

පියවර 1



පියවර 2



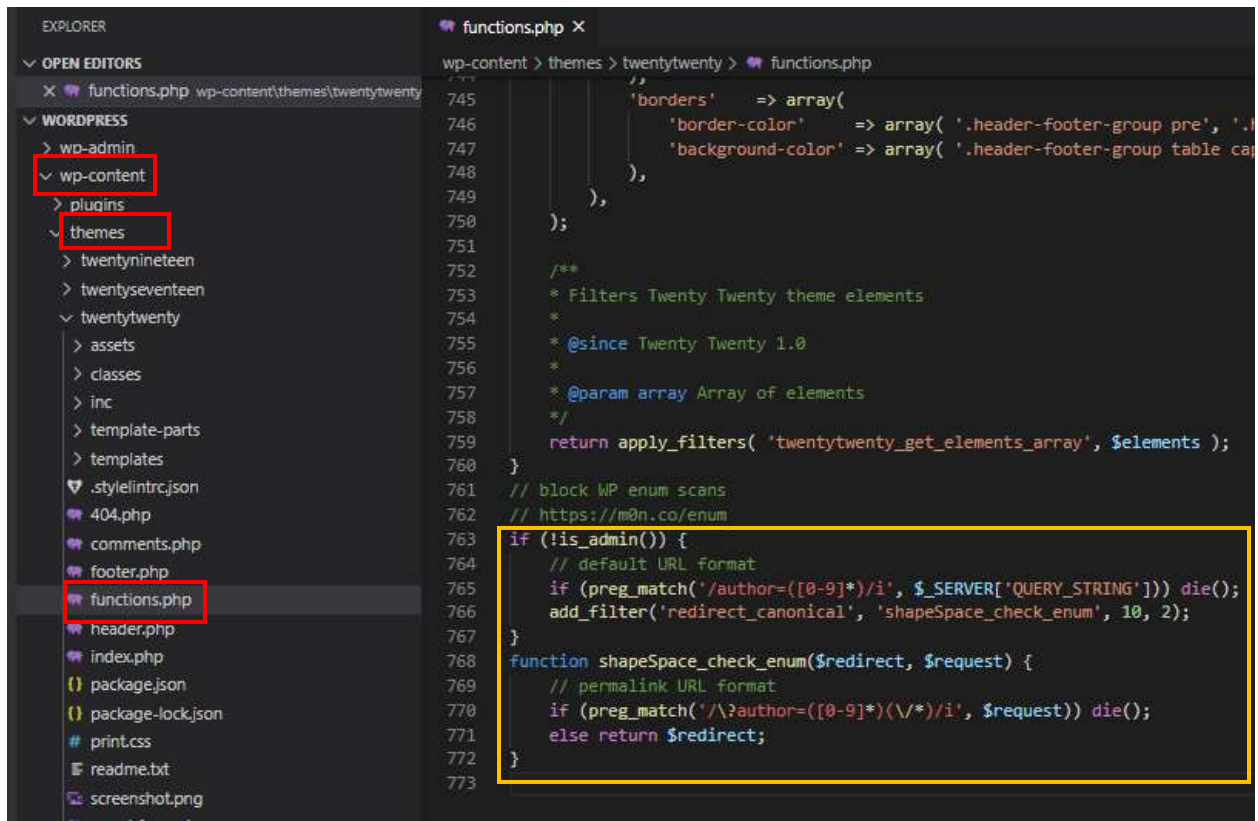
10. User name එකක් හරහා සිදු කරන අනවසර ඇතුළුවීම් අවහිර කිරීම.

- functions.php හරහා

ඔබේ නේමාවට අදාළ functions ගොනුවට මෙම කේතය ඇතුළත් කරන්න:

```
// block WP enum scans
// https://m0n.co/enum
if (!is_admin()) {
    // default URL format
    if (preg_match('/author=([0-9]*)/i', $_SERVER['QUERY_STRING'])) die();
    add_filter('redirect_canonical', 'shapeSpace_check_enum', 10, 2);
}
function shapeSpace_check_enum($redirect, $request) {
    // permalink URL format
    if (preg_match('/\?author=([0-9]*) (\/*)/i', $request)) die();
}
```

```
    else return $redirect;
}
```



```
wp-content > themes > twentytwenty > functions.php
745     'borders' => array(
746         'border-color' => array( '.header-footer-group pre', '.f
747         'background-color' => array( '.header-footer-group table cap
748     ),
749 ),
750 );
751
752 /**
753  * Filters Twenty Twenty theme elements
754  *
755  * @since Twenty Twenty 1.0
756  *
757  * @param array Array of elements
758  */
759 return apply_filters( 'twentytwenty_get_elements_array', $elements );
760 }
761 // block WP enum scans
762 // https://m0n.co/enum
763 if (!is_admin()) {
764     // default URL format
765     if (preg_match('/author=([0-9]*)/i', $_SERVER['QUERY_STRING'])) die();
766     add_filter('redirect_canonical', 'shapeSpace_check_enum', 10, 2);
767 }
768 function shapeSpace_check_enum($redirect, $request) {
769     // permalink URL format
770     if (preg_match('/\?author=([0-9]*)(&V*)/i', $request)) die();
771     else return $redirect;
772 }
773 }
```

- .htaccess භරහා

වෙබ් අඩවියේ root .htaccess ගොනුවට පහත කේතය ඇතුළත් කරන්න.

```
# Block User ID Phishing Requests
```

```
<IfModule mod_rewrite.c>
    RewriteCond %{QUERY_STRING} ^author=([0-9]*)
    RewriteRule .* http://example.com/? [L,R=302]
</IfModule>
```

```

38 <IfModule mod_php7.c>
39     php_value auto_prepend_file 'C:\New folder\htdocs\
40 </IfModule>
41 <Files ".user.ini">
42 <IfModule mod_authz_core.c>
43     Require all denied
44 </IfModule>
45 <IfModule !mod_authz_core.c>
46     Order deny,allow
47     Deny from all
48 </IfModule>
49 </Files>
50
51 # END Wordfence WAF
52 # Block User ID Phishing Requests
53 <IfModule mod_rewrite.c>
54     RewriteCond %{QUERY_STRING} ^author=([0-9]*)
55     RewriteRule .* http://example.com/? [L,R=302]
56 </IfModule>
57

```

11.functions.php හරහා Rest Api අක්‍රිය කිරීම

ඔබේ තේමාවේ functions file (Wp-content/ themes/ functions.php) එකට පහත කේතය ඇතුළු කරන්න:

```

add_filter( 'rest_authentication_errors', function( $result ) {
    // If a previous authentication check was applied,
    // pass that result along without modification.
    if ( true === $result || is_wp_error( $result ) ) {
        return $result;
    }

    // No authentication has been performed yet.
    // Return an error if user is not logged in.
    if ( ! is_user_logged_in() ) {
        return new WP_Error(
            'rest_not_logged_in',
            __( 'You are not currently logged in.' ),
            array( 'status' => 401 )
        );
    }

    // Our custom authentication check should have no effect // on logged-
    in requests
    return $result;
});

```

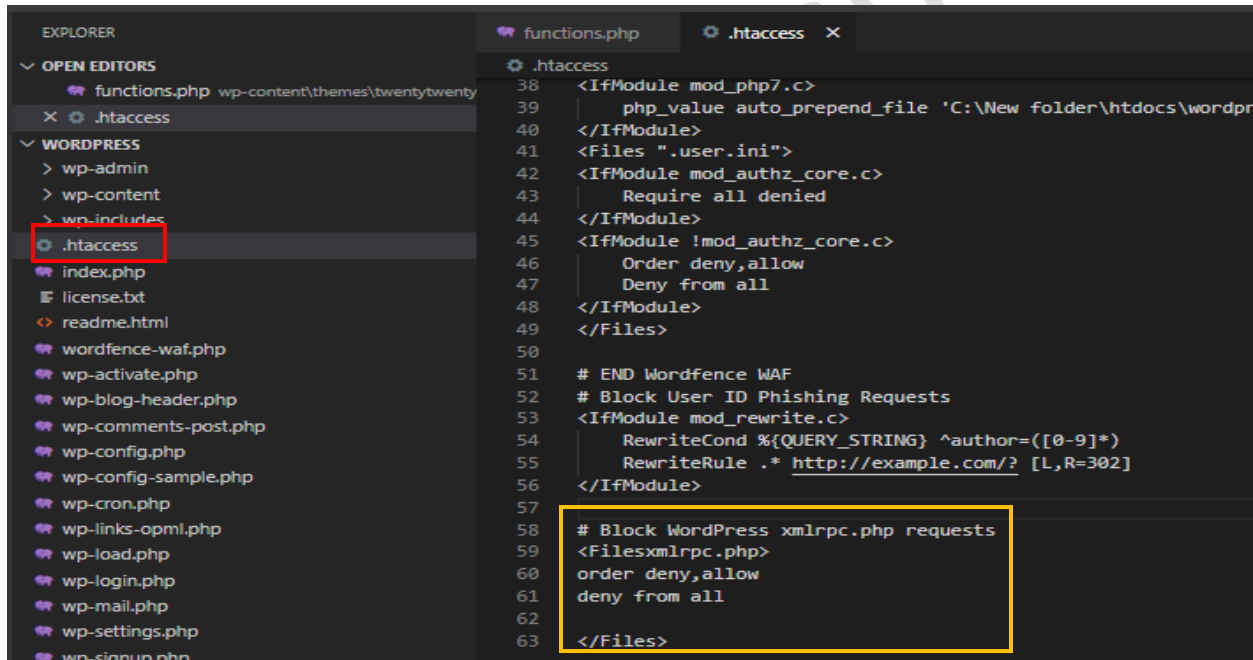
12. .htaccess file භාවිත කර WordPress හි XML-RPC අක්‍රිය කිරීම

පහත කේතය වෙබ් අඩවියේ root .htaccess ගොනුවට ඇතුළු කරන්න.

```
# Block WordPress xmlrpc.php requests
<Filesxmlrpc.php>

order deny,allow
deny from all

</Files>
```



```
EXPLORER
└─ OPEN EDITORS
  └─ functions.php wp-content\themes\twentytwenty
  └─ .htaccess
  └─ WORDPRESS
    ├── wp-admin
    ├── wp-content
    ├── wp-includes
    │ └─ .htaccess
    ├── index.php
    ├── license.txt
    ├── readme.html
    ├── wordfence-waf.php
    ├── wp-activate.php
    ├── wp-blog-header.php
    ├── wp-comments-post.php
    ├── wp-config.php
    ├── wp-config-sample.php
    ├── wp-cron.php
    ├── wp-links-opml.php
    ├── wp-load.php
    ├── wp-login.php
    ├── wp-mail.php
    ├── wp-settings.php
    └─ wp-signup.php

functions.php
.htaccess
  38 <IfModule mod_php7.c>
  39 |   php_value auto_prepend_file 'C:\New folder\htdocs\wordpr
  40 </IfModule>
  41 <Files ".user.ini">
  42 <IfModule mod_authz_core.c>
  43 |   Require all denied
  44 </IfModule>
  45 <IfModule !mod_authz_core.c>
  46 |   Order deny,allow
  47 |   Deny from all
  48 </IfModule>
  49 </Files>
  50
  51 # END Wordfence WAF
  52 # Block User ID Phishing Requests
  53 <IfModule mod_rewrite.c>
  54 |   RewriteCond %{QUERY_STRING} ^author=([0-9]*)
  55 |   RewriteRule .* http://example.com/? [L,R=302]
  56 </IfModule>
  57
  58 # Block WordPress xmlrpc.php requests
  59 <Filesxmlrpc.php>
  60 |   order deny,allow
  61 |   deny from all
  62 </Files>
  63
```