LKDR

Incident Response Team

Hardening WordPress

(WordPress වෙබ් අඩවියක ආරක්ෂාව තර කිරීම)

By LK Domain Incident Response Team

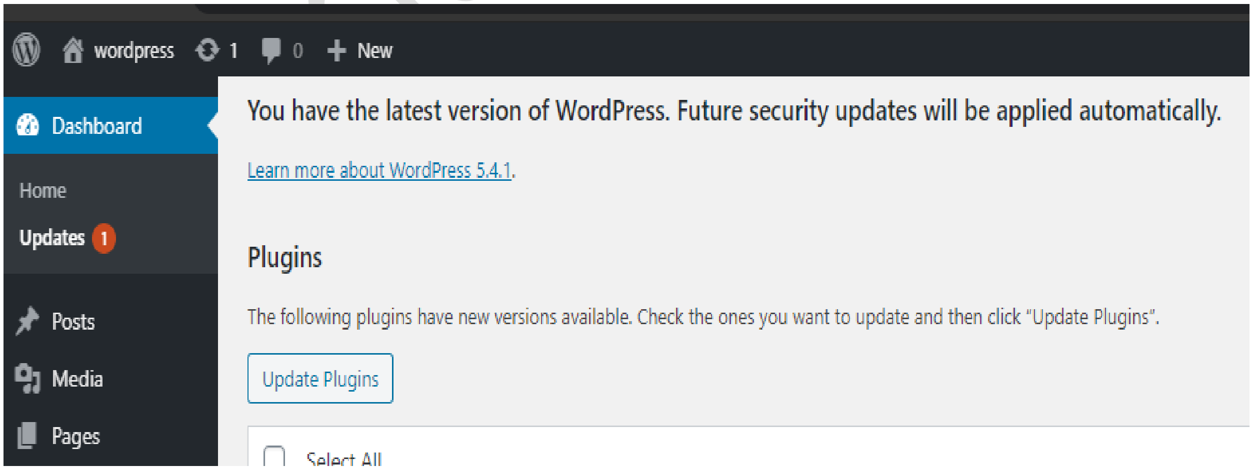
WordPress වෙබ් අඩවියක ආරක්ෂාව තර කිරීම

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.

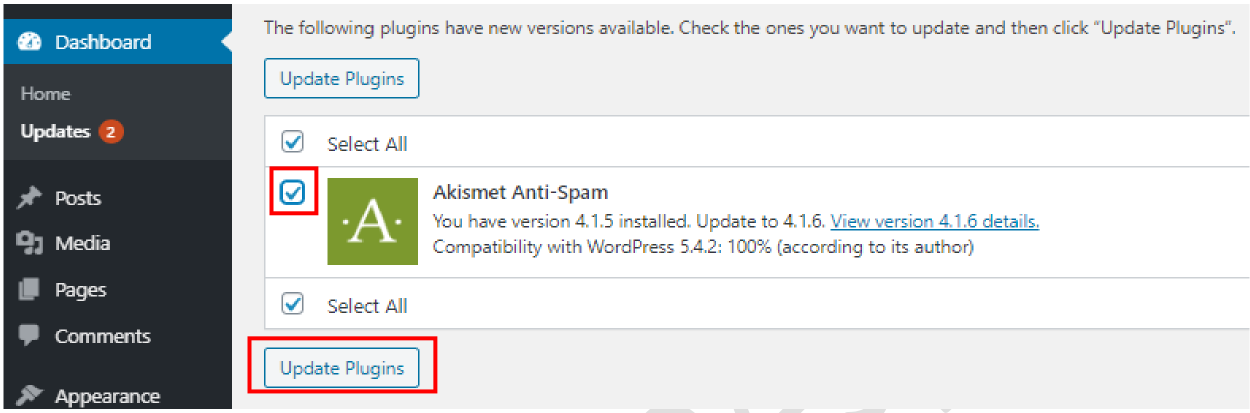
3.7 සංස්කරණයේ සිට, WordPress විසින් ස්වයංක්‍රිය යාවත්කාලීන වීම් ලබා දේ, නවතම සංස්කරණය භාවිතය සඳහා Wordpress යාවත්කාලීන කර තබා ගැනීමට මෙම පහසුකම භාවිත කරන්න.



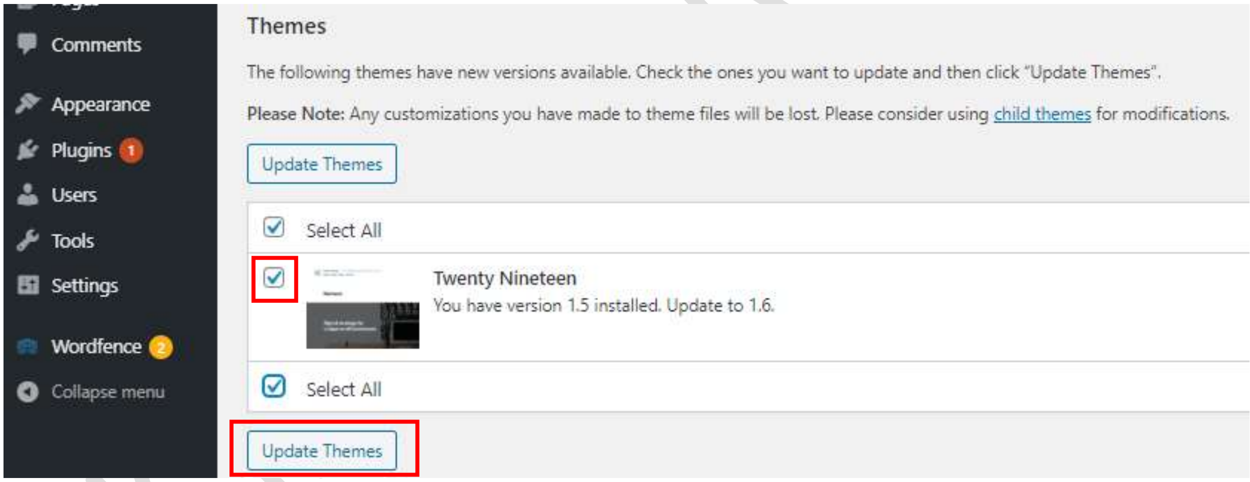
2. තේමා සහ plugins යාවත්කාලීන කිරීම.

WordPress මූල වැඩසටහ 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 පරික්ෂා කල යුතුය;

- Plugin පිළිබඳ විචාර.
- 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 සමග මෙම අනුමත කිරීම් වෙනස් විය හැක.

ඔබ plugin එකක් භාවිත කරන විට, ඔබට https://wpvulndb.com/ හරහා එහි කලින් හඳුනාගත් අවදානම් තත්ත්වයන් ගැන සොයා බැලිය හැක.

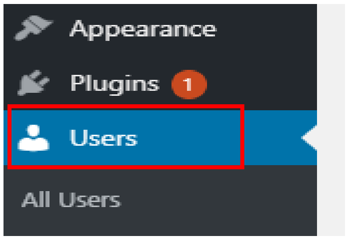
3. ආවේනික සහ ශක්තිමත් මුරපද භාවිත කරන්න.

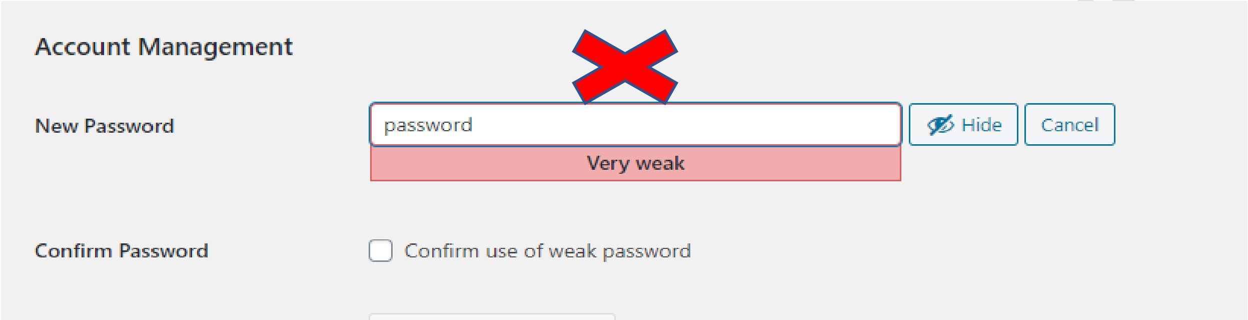
හොඳ ආරක්ෂක උපක්‍රම අනුගමනය තුලින් ඇතිවිය හැකි බොහෝ අවදානම් තත්වයන් මග හරවාගත හැක. මෙහිදී ශක්තිමත් මුරපදයක් භාවිතය අත්‍යවශ්‍ය වේ.

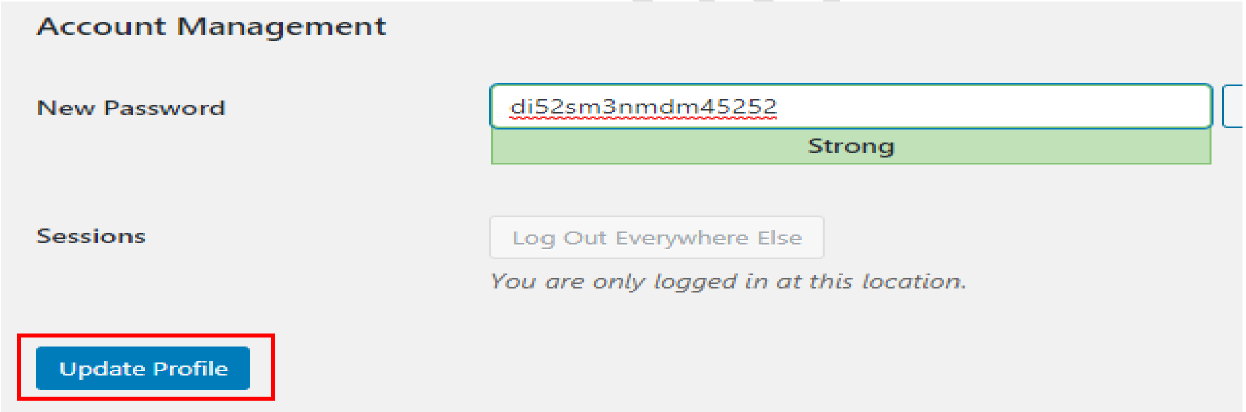
මුරපදයක් තෝරාගැනීමේදී වැලකී සිටිය යුතු යුතු කරුණු:

- 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.

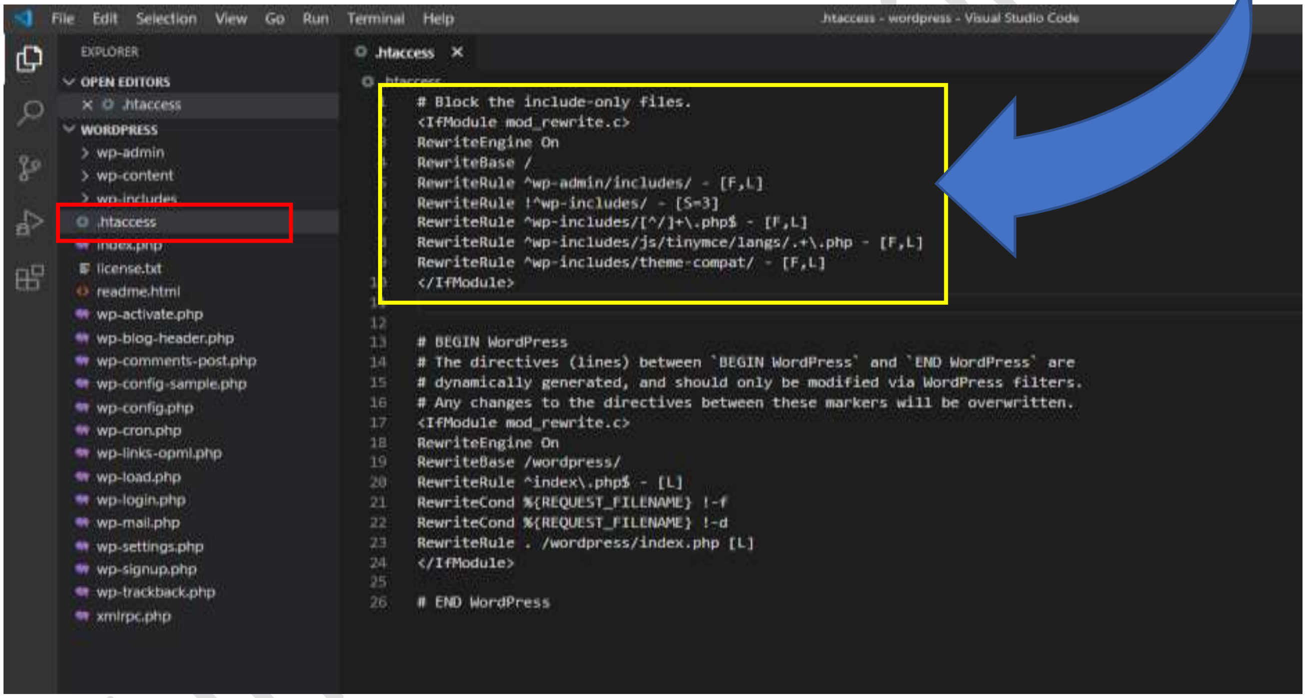
/wp-admin/ වෙතට සර්වර් ආශ්‍රිතව මුරපදයක් ඇතුළත් කිරීමෙන් ඔබේ බ්ලොග් අඩවියේ admin කොටසට, ඇතුළුවීමේ Login තිරයට සහ ඔබේ ගොනු වලට දෙවෙනි මට්ටමක ආරක්ෂාවක් ලැබේ. එමඟින් අනවසර හැකර්වරයෙකුට හෝ හැකර් මෘදුකාංගයකට ඔබේ admin කොටසට ඇතුළුවීමට උත්සාහ ගැනීමේදී තවත් ආරක්ෂක ස්ථරයක් බිඳ දැමීමට සිදුවේ.

ක්‍රමලේඛයන් වෙතට වෙනත් පරිශීලකයෙකුට ඇතුළුවීමට අවස්ථාව ලබා නොදීමට අවශ්‍ය අවස්ත්ථාවලදී 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>
```

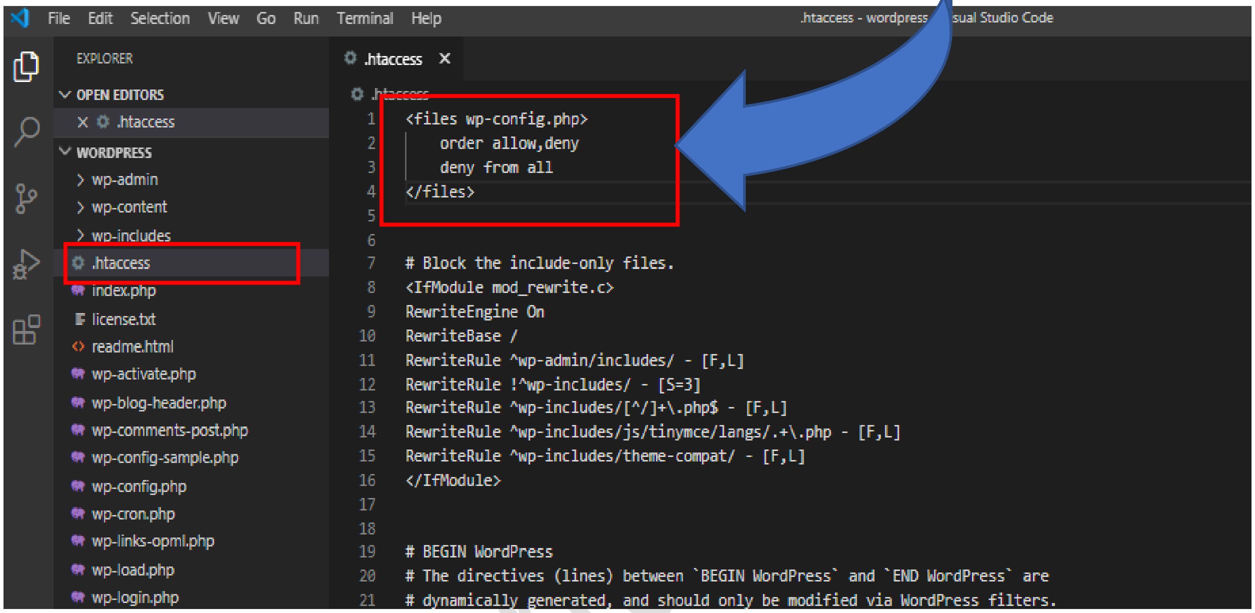
BEGIN WordPress යන්නට ඉහලින් මෙය තැබිය යුතුයි.



5. wp-config.php සුරක්ෂිතකරණය

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

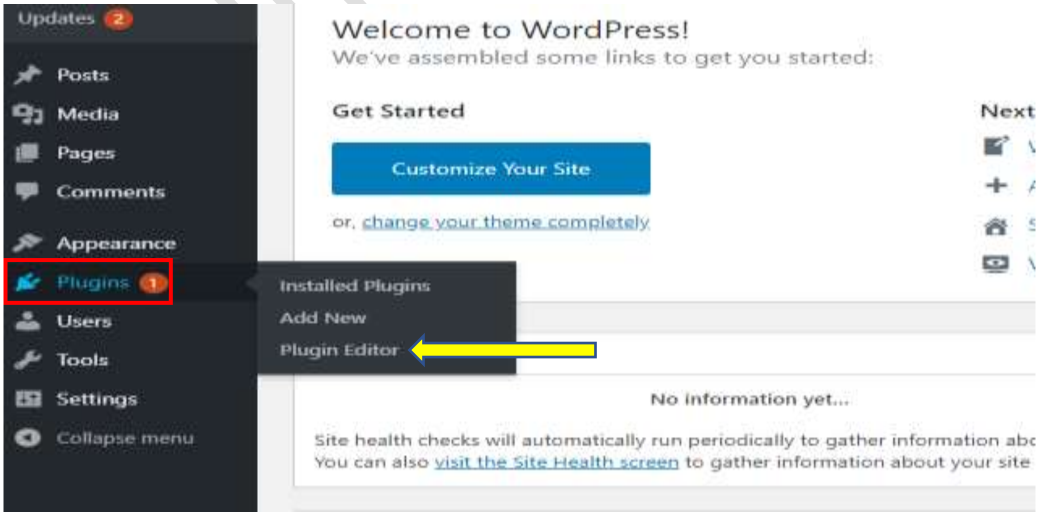
```
<files wp-config.php>
order allow,deny
deny from all
</files>
```



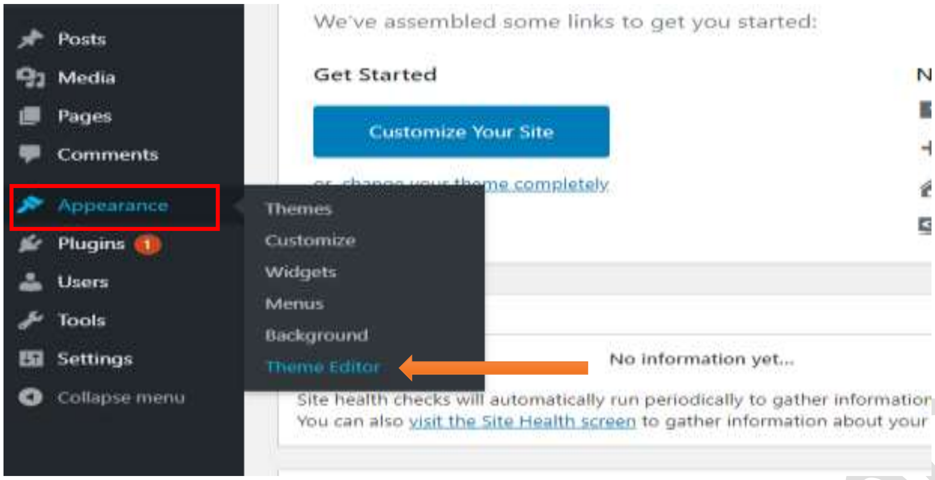
6. WordPress admin හි ගොනු වෙනස් කිරීම අවහිර කිරීම.

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

Plugins → Plugin Editor



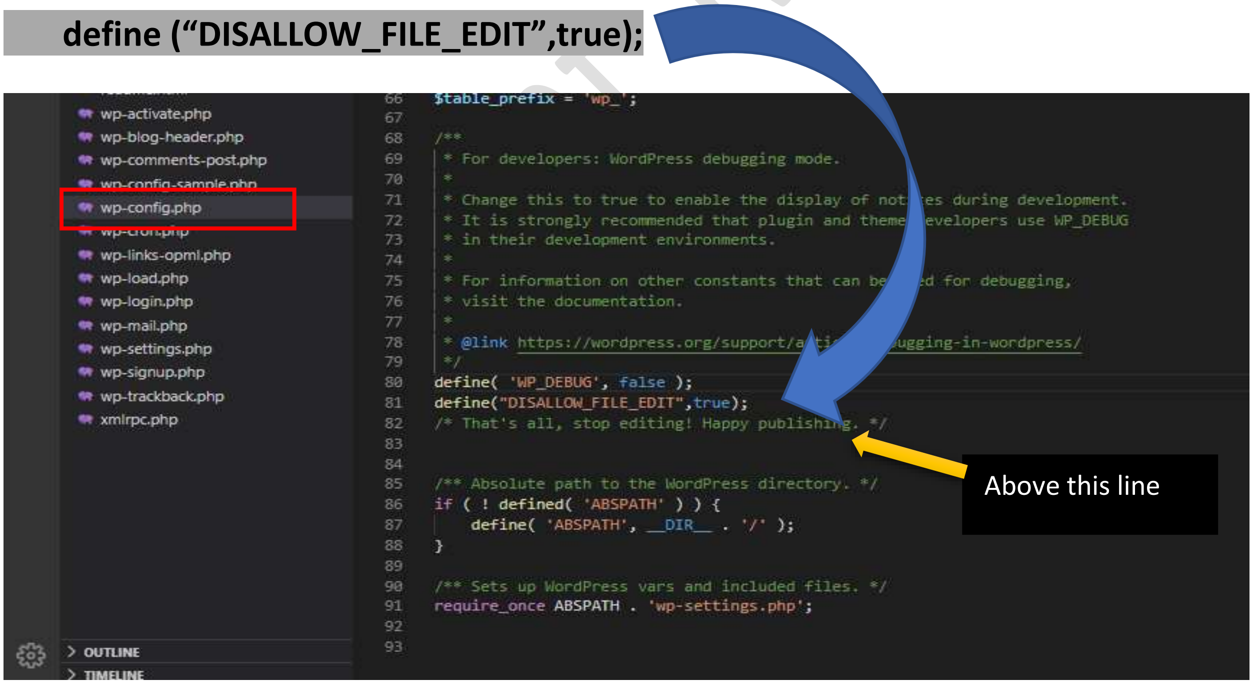
Appearance → Theme Editor



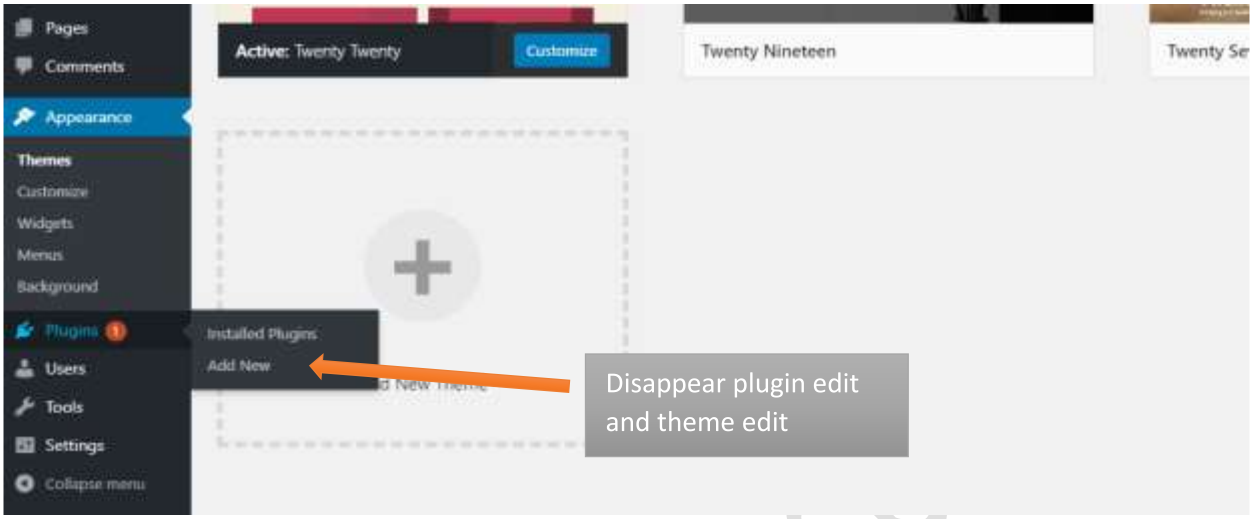
මේ හරහා ක්‍රමලේඛ ක්‍රියාත්මක කරවීමට හැකි වන නිසා හැකර්වරයෙකුට login form එක හරහා ඇතුළුවීමට ලැබෙන අවස්ථාවකදී පහර දෙන පළමු tool එක මෙය වේ.

WordPress හි ගොනු වෙනස් කිරීම අවහිර කරන ආකාරය.

define (“DISALLOW_FILE_EDIT”,true);



එම කේතය ලබාදීමෙන් පසුව:



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

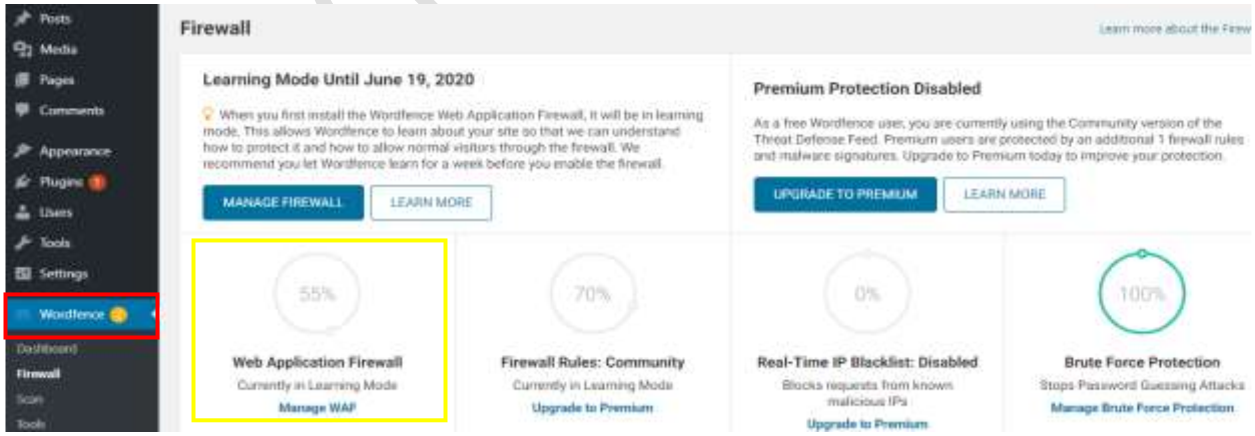
7. web application firewall (WAF) එකක් භාවිත කිරීම.

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 කිරිමෙන් පසු ඔබට පහත තිරය දිස්වේ;



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

- ලබාදෙන පහසුකම්.
- නිරන්තර යාවත්කාලිනවීම් සිදුවේද යන්න.

  විශේෂයෙන් සැලකිලිමත් විය යුතු කරුණු,

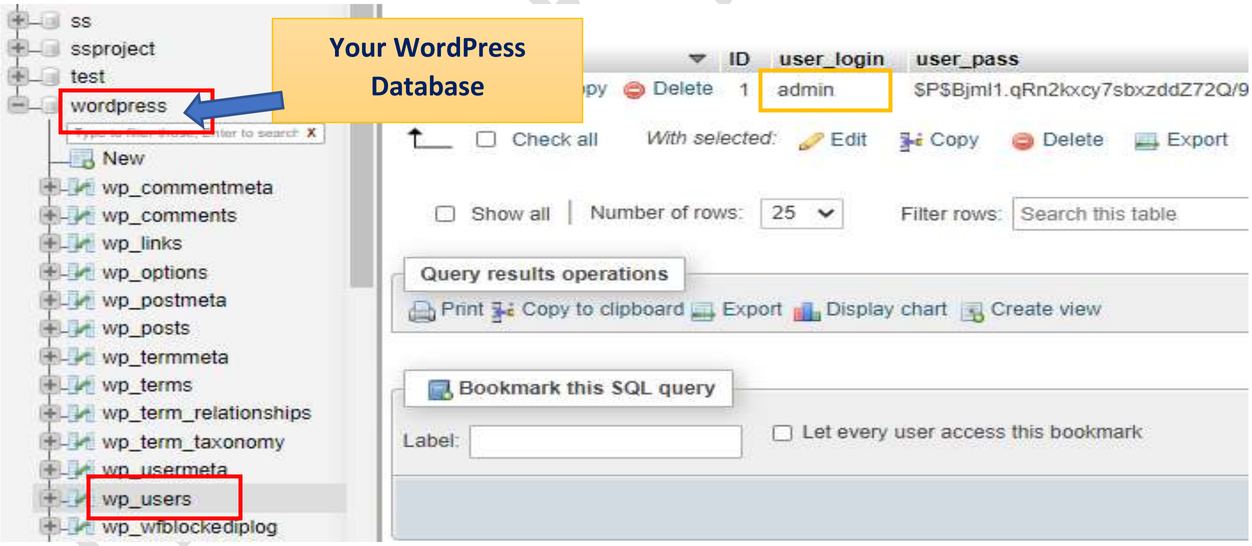
  - Blacklist (ලබා දෙන IP range එක).
  - Whitelist (ලබාදෙන ip range එක).
- Dynamic blacklist.
- වෙබ් අඩවියේ සිදුවන ක්‍රියාකාරකම් Admin හට පරික්ෂා කිරීමට අවස්ථාව ලැබේද යන්න.
- Strict mode පිලිබඳ දැනුම් දීම.
- ගොනුවල අඛණ්ඩතාවය හෙවත් ගොනු හානි වීම්වලට ලක්ව තිබේදැයි පරික්ෂාව.
- හානිදායක යෙදවුම් හෙවත් මැල්වෙයාර්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

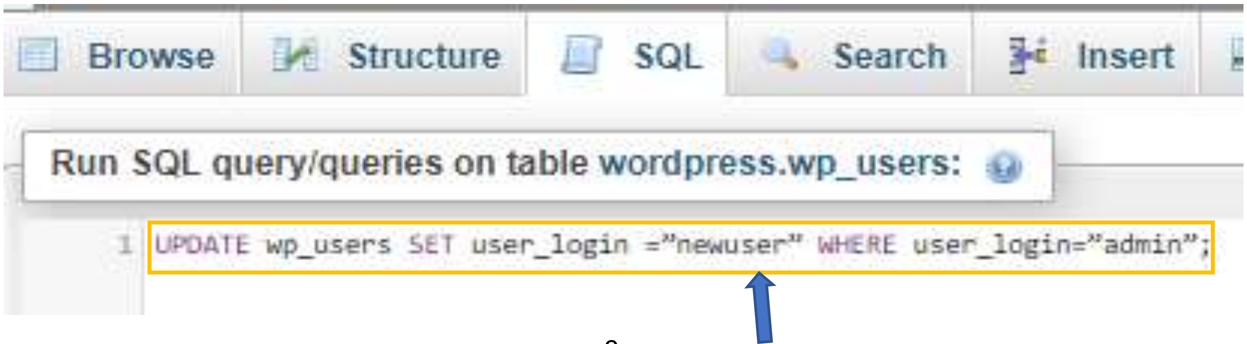
8. අපැහැදිලි බව තුලින් ආරක්ෂාව.

Administrative ගිණුමෙහි නම වෙනස් කරන්න.

Aadministrative 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.

Response





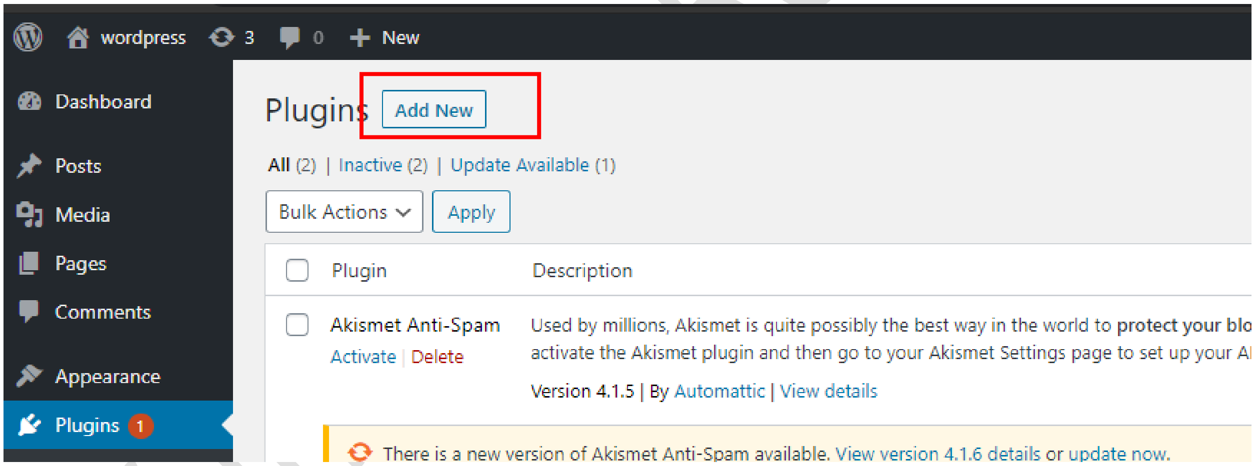
New Username

9. දත්ත උපස්ථය හෙවත් backup කිරීම

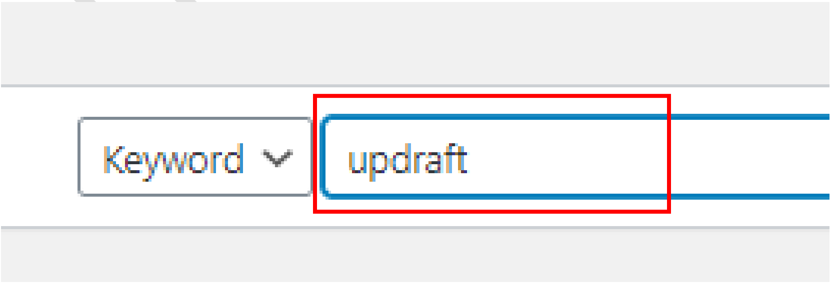
ඔබේ WordPress වෙබ් අඩවියේ විශාලත්වය කෙතරම් වුවත් යාවත්කාලීන වීම් ඇනහිටීම, හැකර් ප්‍රහාර, පරිශීලකයන්ගේ වැරදීම් සහ හදිසි බිඳවැටීම් වලදී ඔබේ දත්ත වලට හානි වීම් වලින් වලක්වා ගැනීම අතිශය වැදගත් වේ.

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

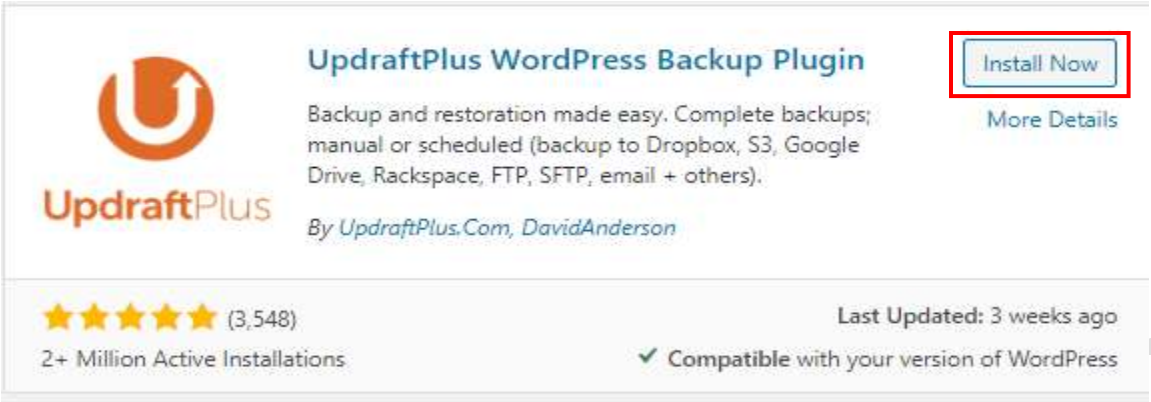
පියවර 1



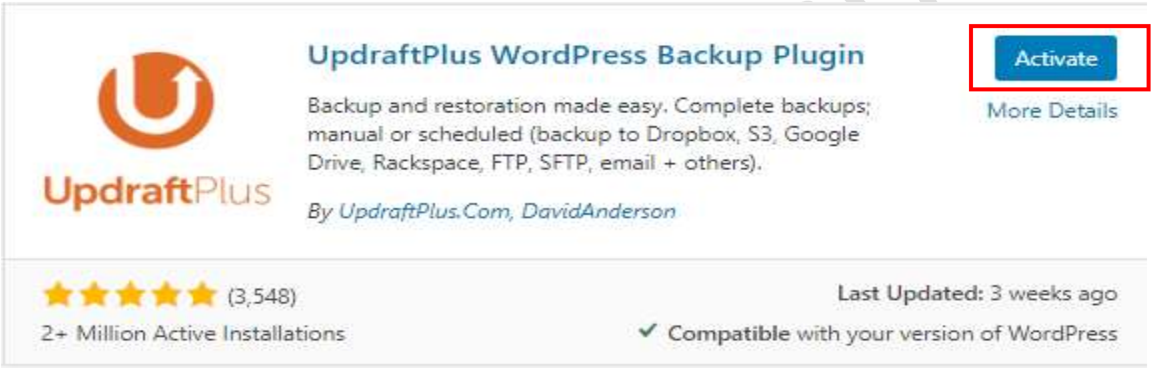
පියවර 2



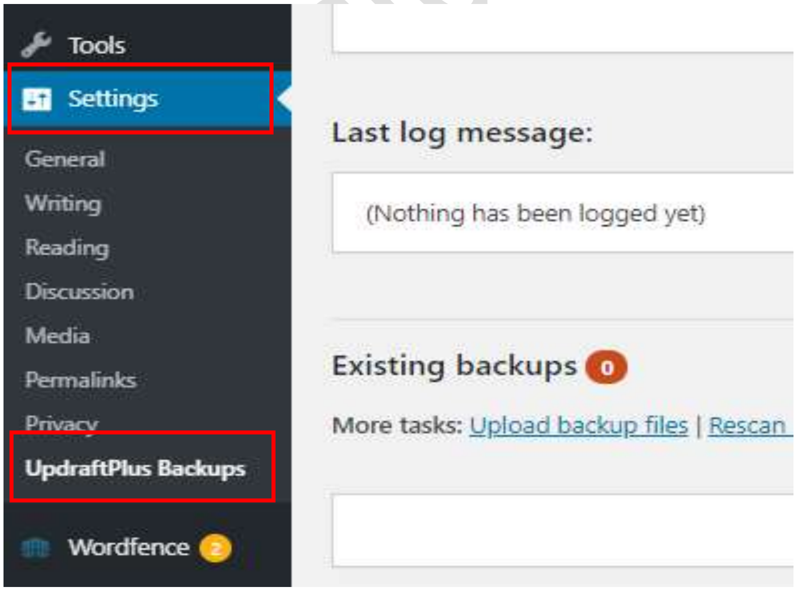
පියවර 3



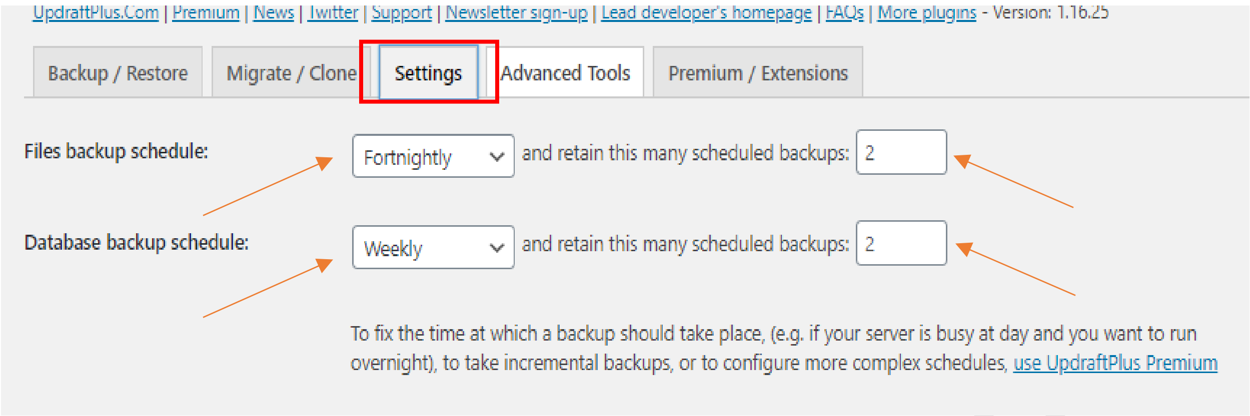
පියවර 4



පියවර 5

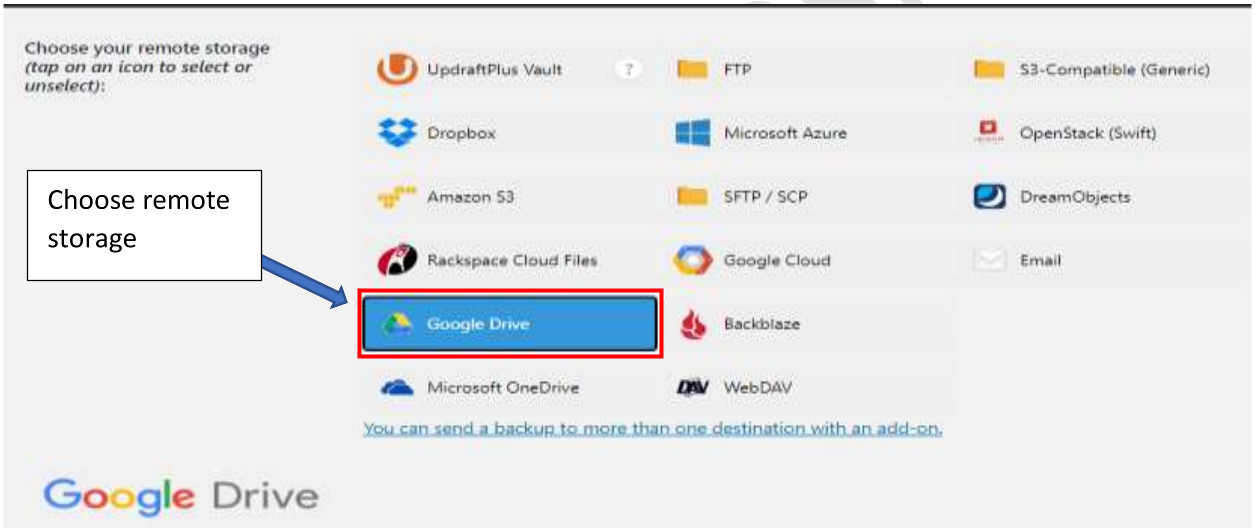


Step 6

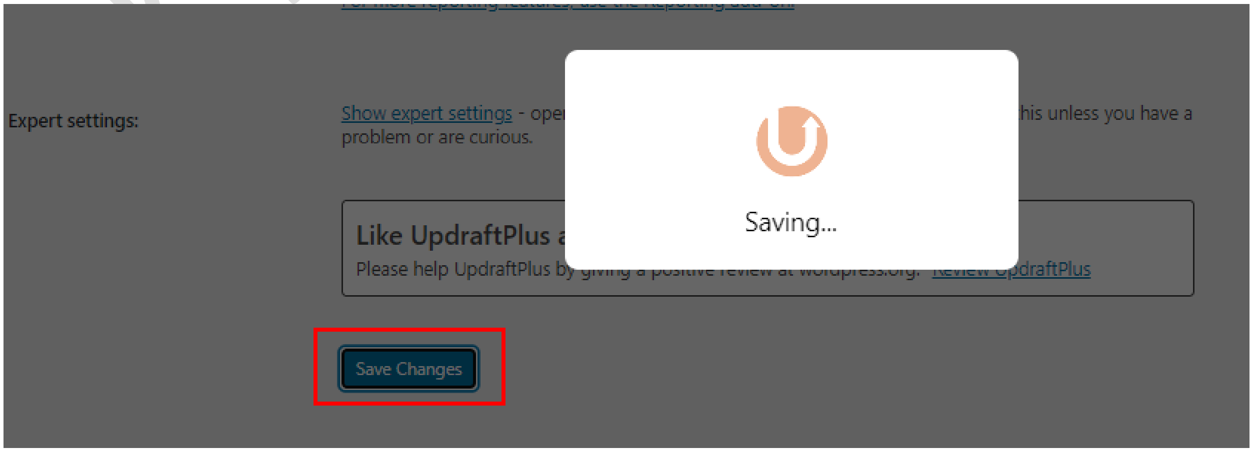


පියවර 7

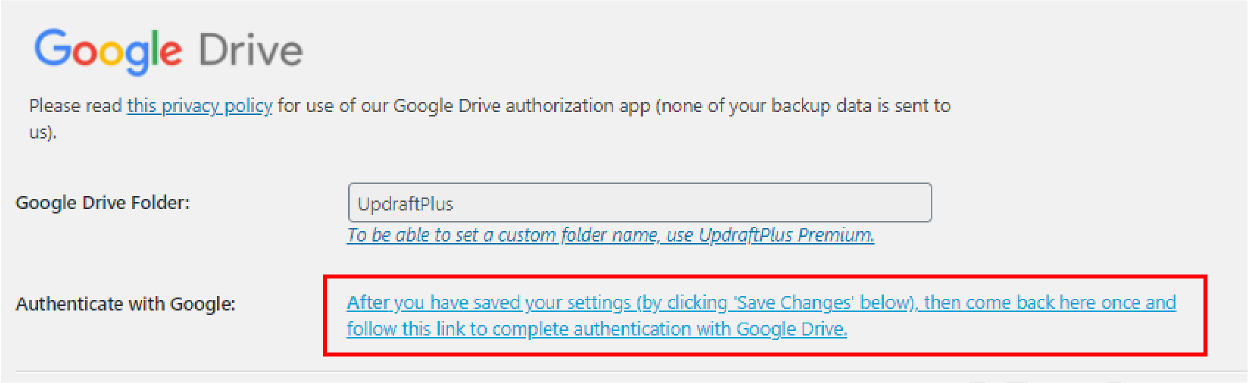
ඔබ Remote storage ලෙස Google Drive ලබා දෙන්නේ නම් (අනෙක් පහසුකම්ද ලබා දිය හැක.);



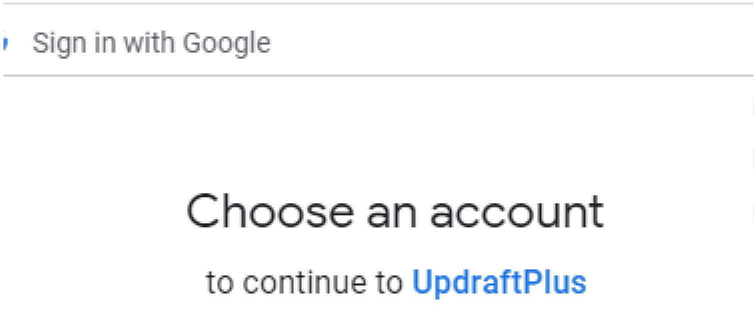
පියවර 8



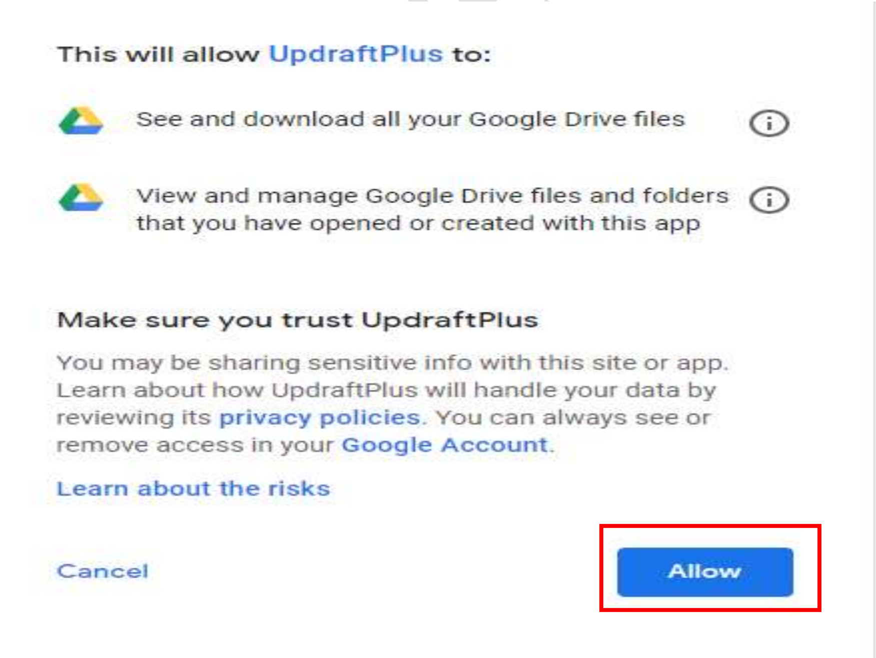
පියවර 9



පියවර 10

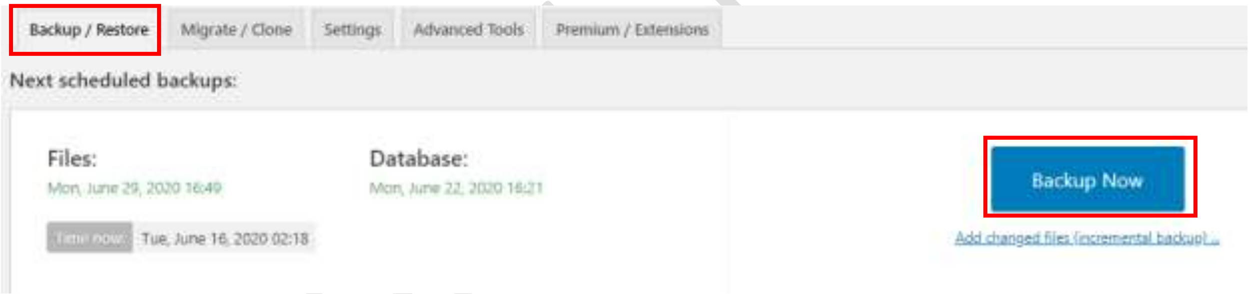


පියවර 11



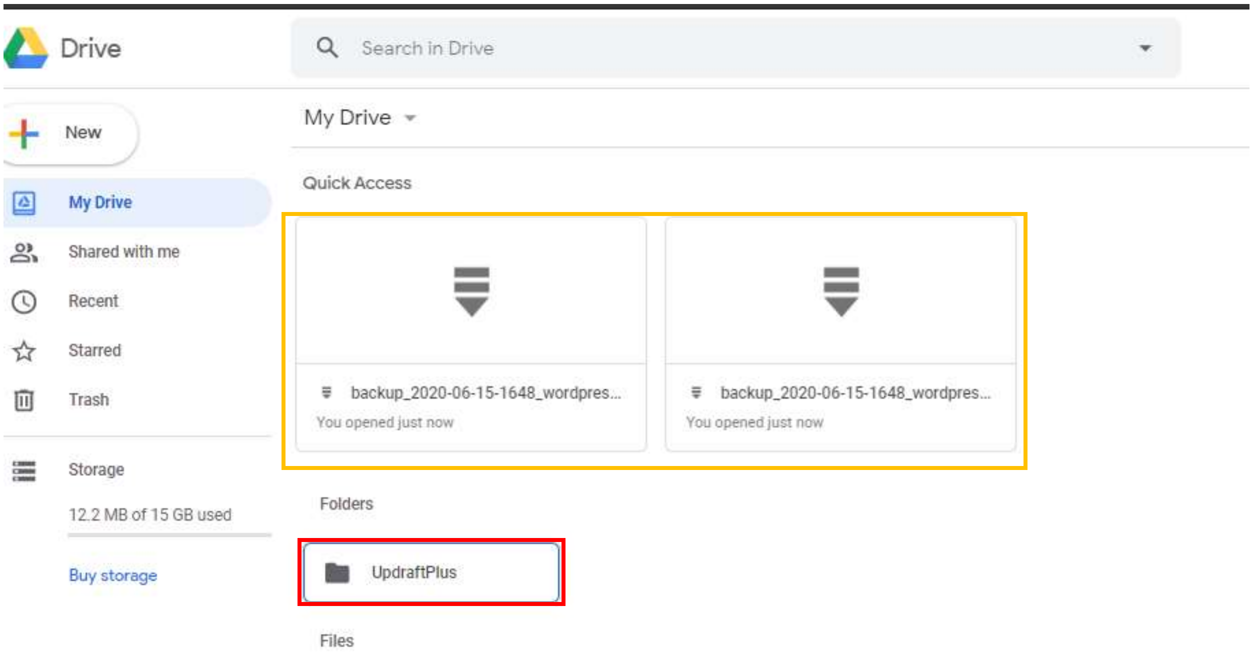
පියවර 12

පියවර 13

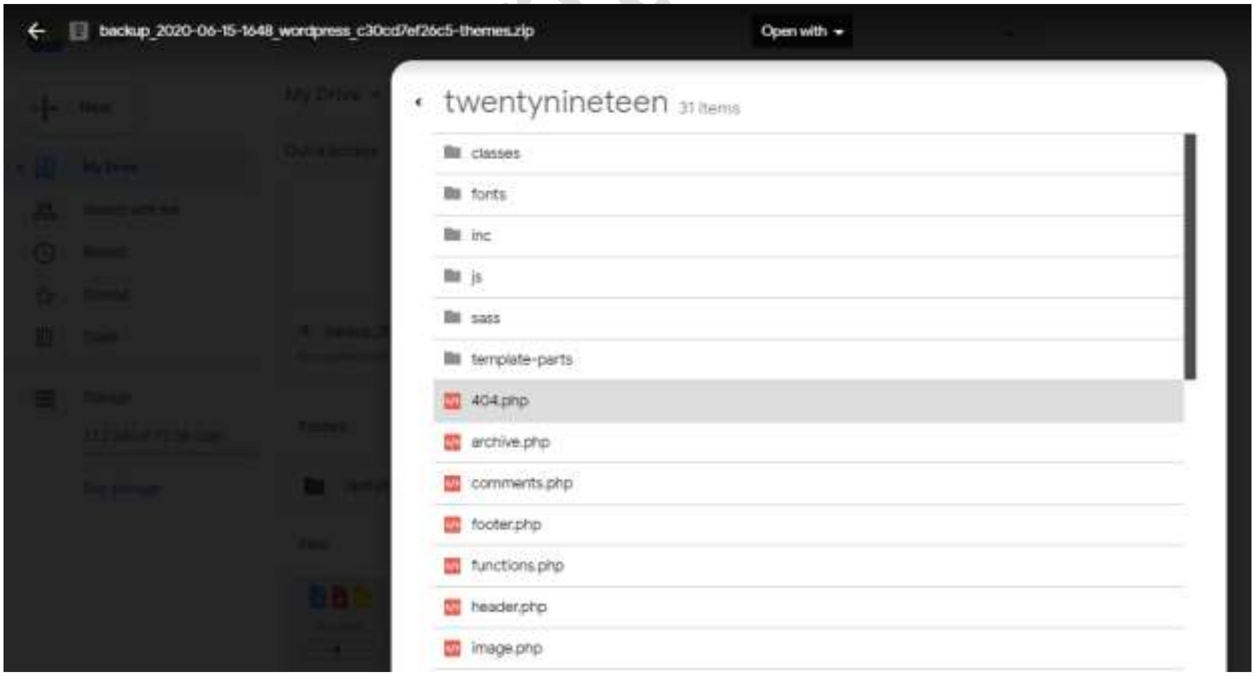


පියවර 14

පියවර 15



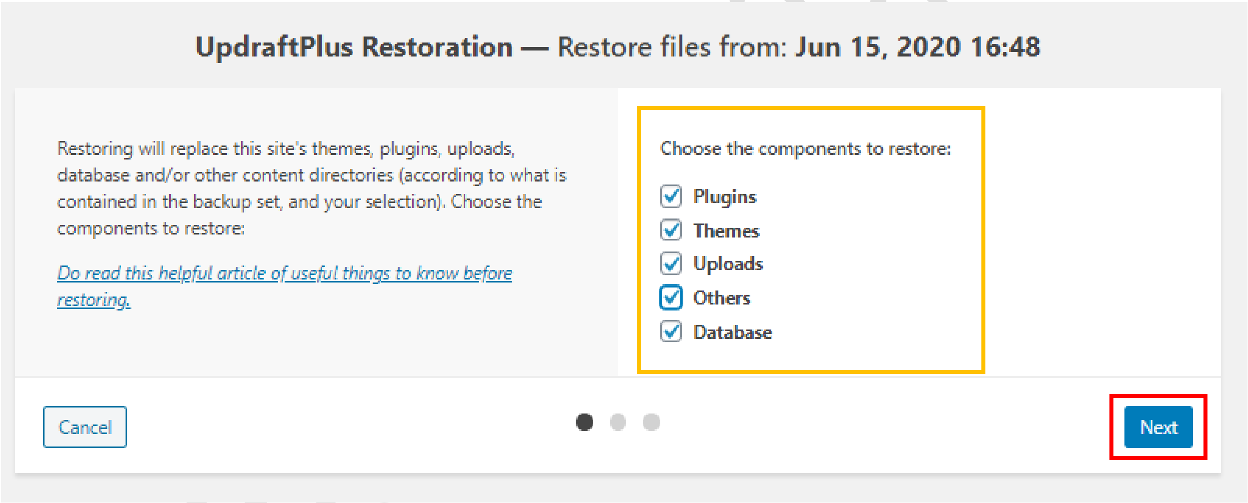
පියවර 16



ඔබේ WordPress වෙබ් අඩවිය backup කිරීමකින් පසුව නැවත ලබාගන්නා ආකාරය

පියවර 1

පියවර 2



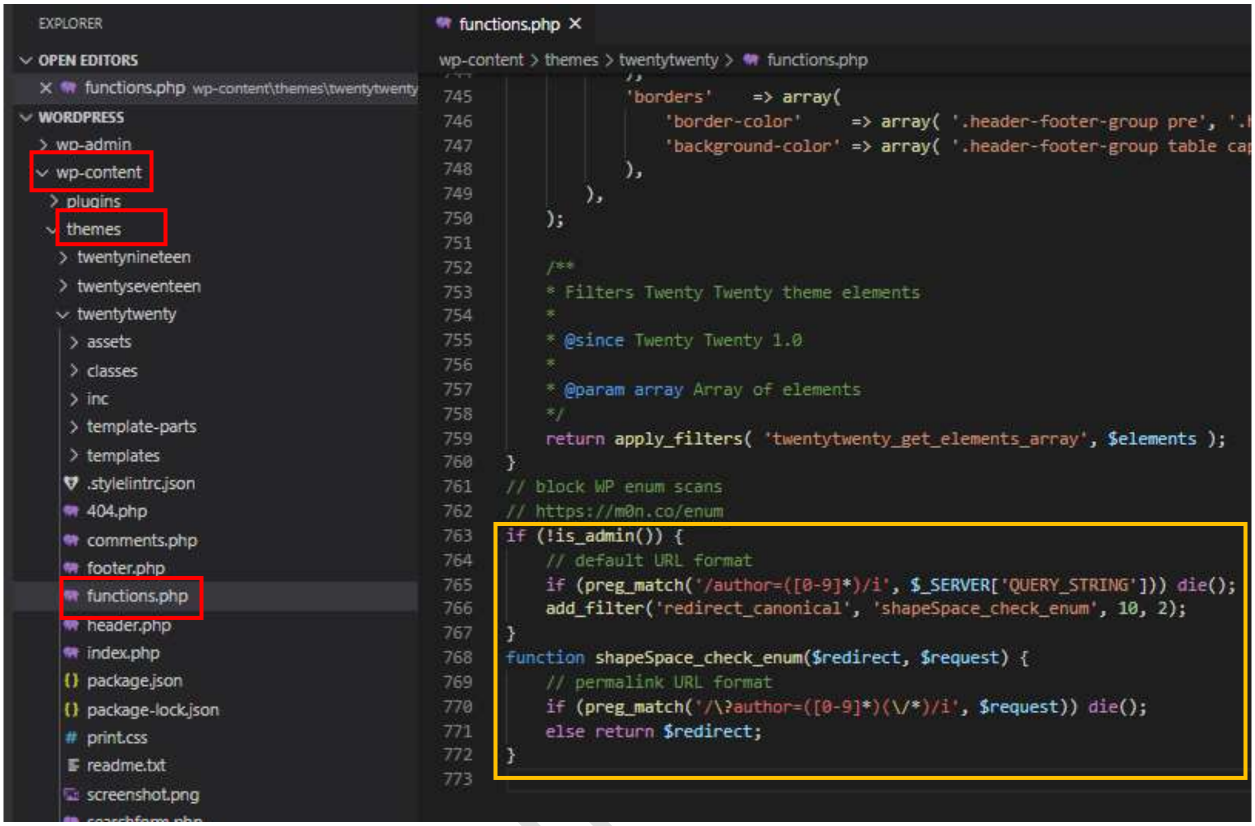
10.User name එකක් හරහා සිදු කරන අනවසර ඇතුළුවීම් අවහිර කිරීම.

- functions.php හරහා

ඔබේ තේමාවට අදාළ functions ගොනුවට මෙම කේතය ඇතුලත් 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;
}
```

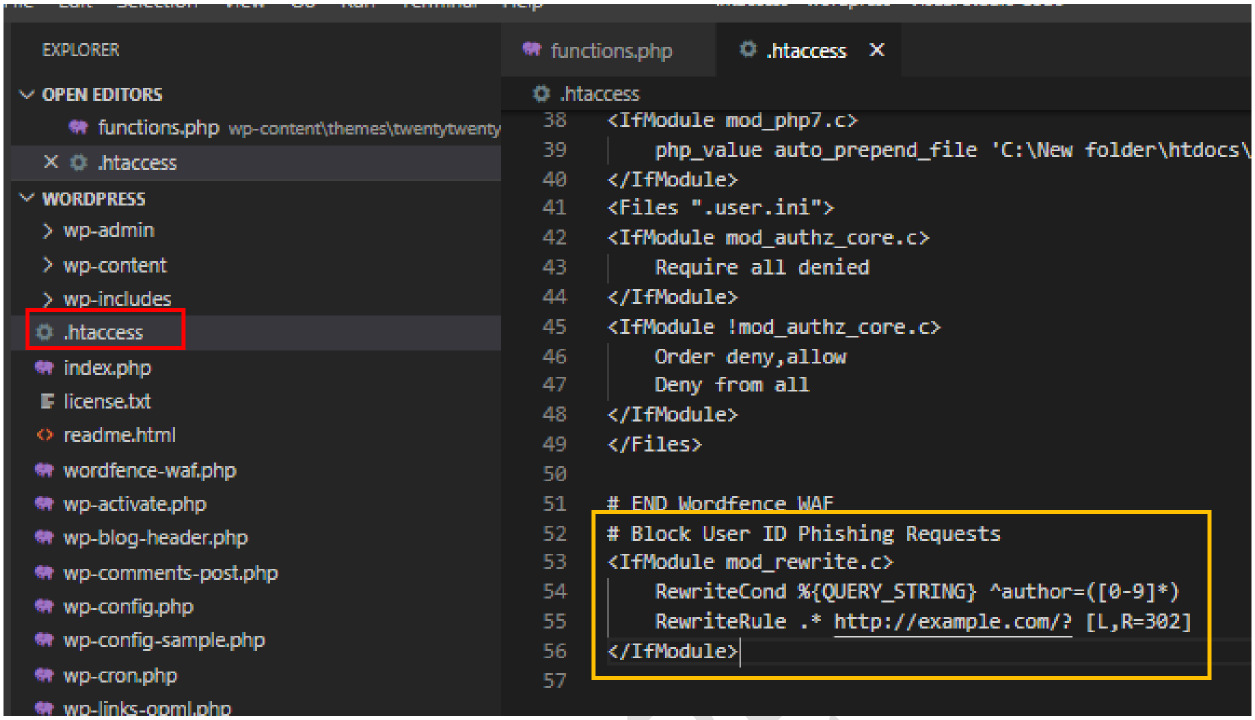


- .htaccess හරහා

වෙබ් අඩවියේ root .htaccess ගොනුවට පහත කේතය ඇතුලත් කරන්න.

```
# Block User ID Phishing Requests

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



11.functions.php හරහා Rest Api අක්‍රිය කිරීම

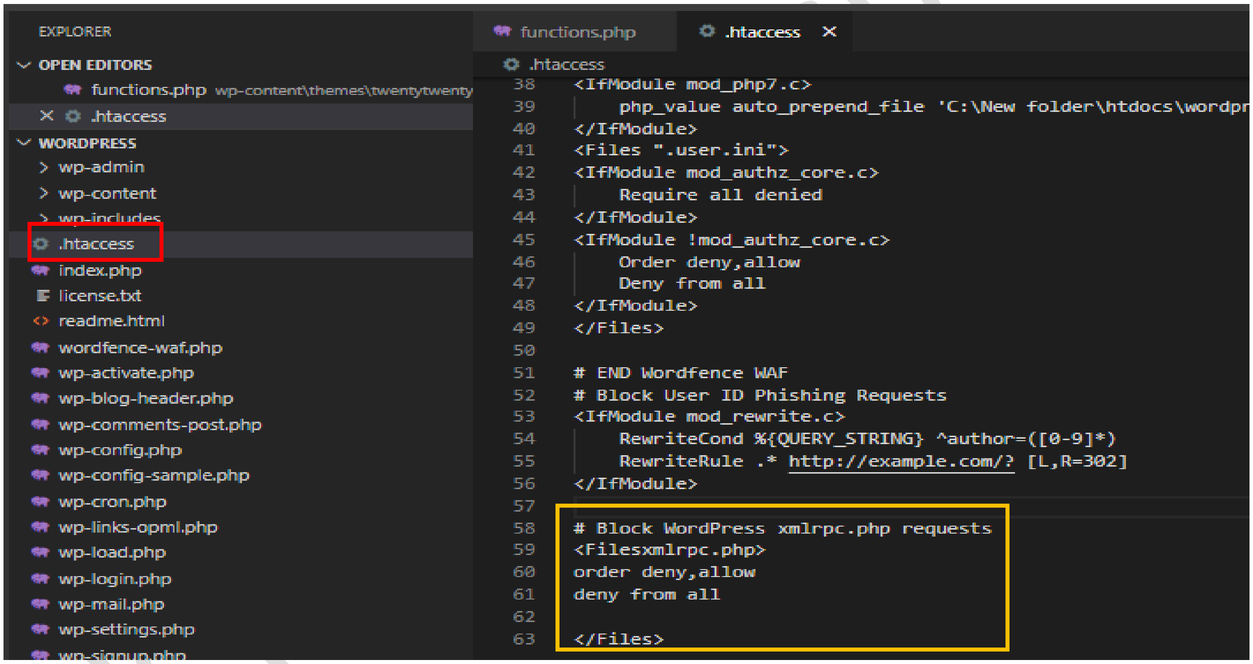
ඔබේ තේමාවේ functions file (Wp-content/ themes/ functions.php) එකට පහත කේතය ඇතුළු කරන්න:

```
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>
```