

# Hardening WordPress

By LK Domain Incident Response Team

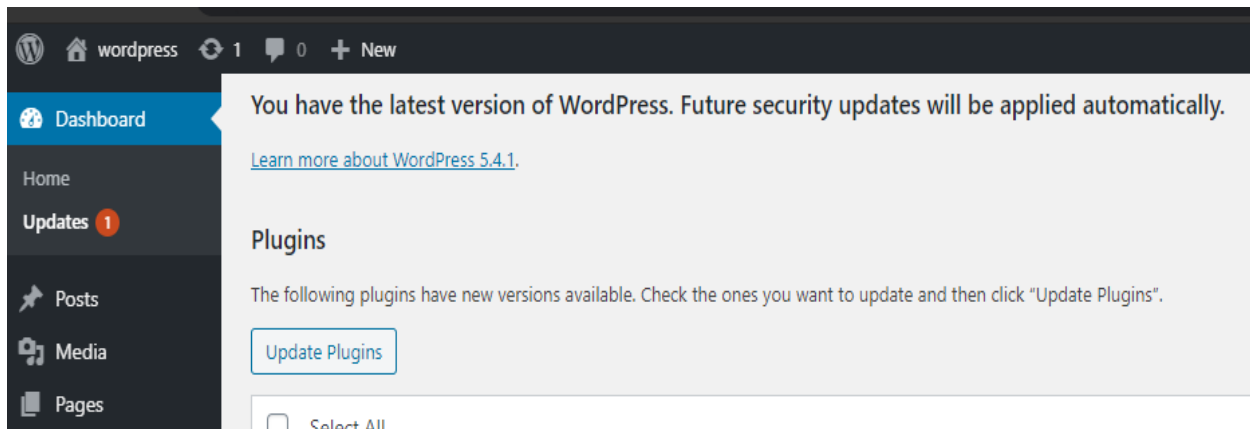
# Hardening WordPress

1. Update WordPress
2. Update themes and plugins
3. Use unique and strong passwords
4. Securing wp-admin & wp-includes
5. Securing wp-config.php
6. Disable file editing in wordpress admin
7. Use a web application firewall (WAF)
8. Security through obscurity
9. Data backup
10. Block user-enumeration
11. Rest Api disabled via functions.php
12. Disable XML-RPC in WordPress using .htaccess file

## 1. Update WordPress

The latest version of WordPress is always available from the main WordPress website at <https://wordpress.org>.

Since version 3.7, WordPress has featured automatic updates. Use this functionality to ease the process of keeping up to date.




## 2. Update themes and plugins

While updating the WordPress core, don't forget to update your themes and plugins too. Hackers are particularly fond of old themes and plugins with known security holes.

## Update plugins

The following plugins have new versions available. Check the ones you want to update and then click "Update Plugins".

Select All

 Akismet Anti-Spam  
You have version 4.1.5 installed. Update to 4.1.6. [View version 4.1.6 details.](#)  
Compatibility with WordPress 5.4.2: 100% (according to its author)

Select All


## Update theme

Themes

The following themes have new versions available. Check the ones you want to update and then click "Update Themes".

Please Note: Any customizations you have made to theme files will be lost. Please consider using [child themes](#) for modifications.

Select All

 Twenty Nineteen  
You have version 1.5 installed. Update to 1.6.

Select All

When we select plugins, normally we should check;

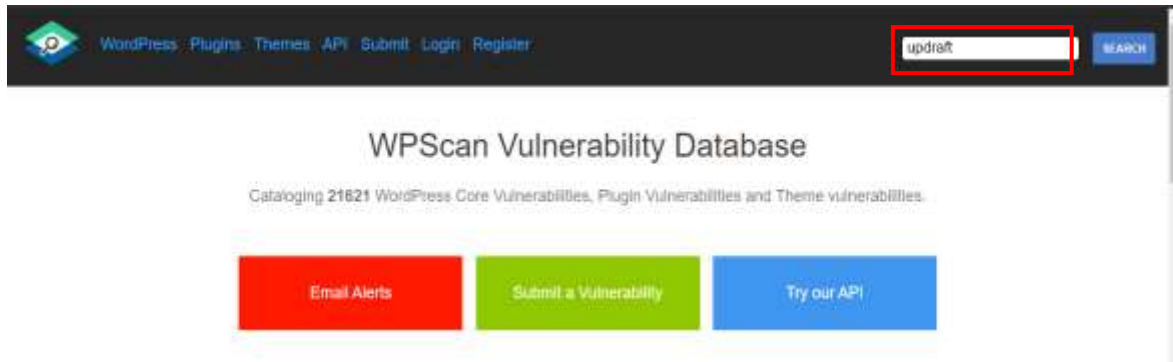
- Plugin reviews
- How many users used that plugin
- Previous vulnerabilities

We can recommend contact form plugin, WAF, backup plugin and security plugin for use.

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

These recommendations can change with the time.

When we use a plugin, we should go to <https://wpvulndb.com/> and search for checking their vulnerabilities.



updraft

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

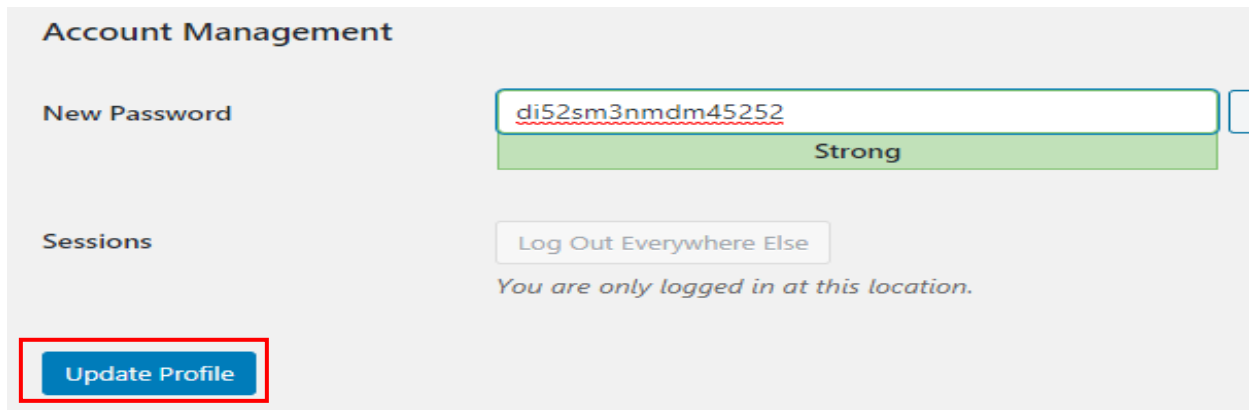
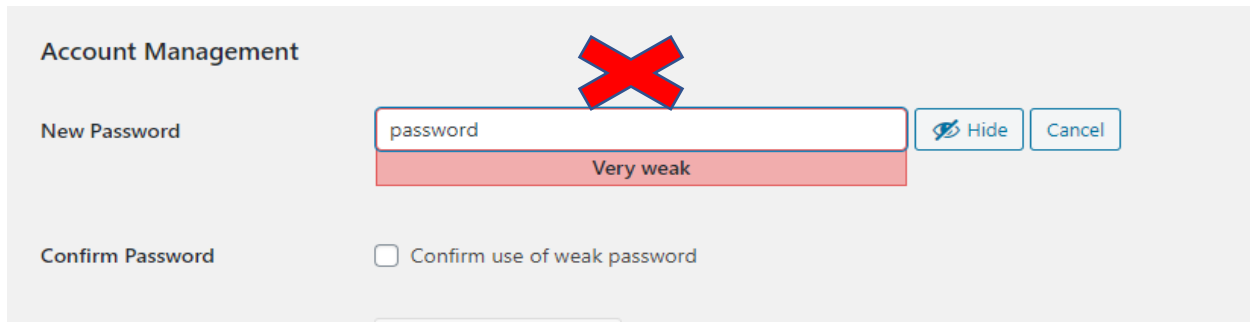
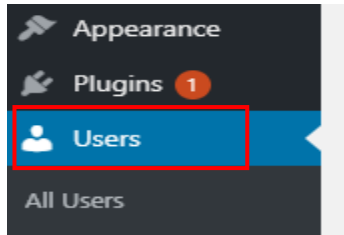
### 3. Use unique & strong passwords

Many potential vulnerabilities can be avoided with good security habits. A strong password is an important aspect of this.

Things to avoid when choosing a password:

- Any permutation of your own real name, username, company name, or name of your website.
- A word from a dictionary, in any language.
- A short password.
- Any numeric-only or alphabetic-only password (a mixture of both is best).

How to change password in a WordPress account.



#### 4. Securing wp-admin and wp-includes

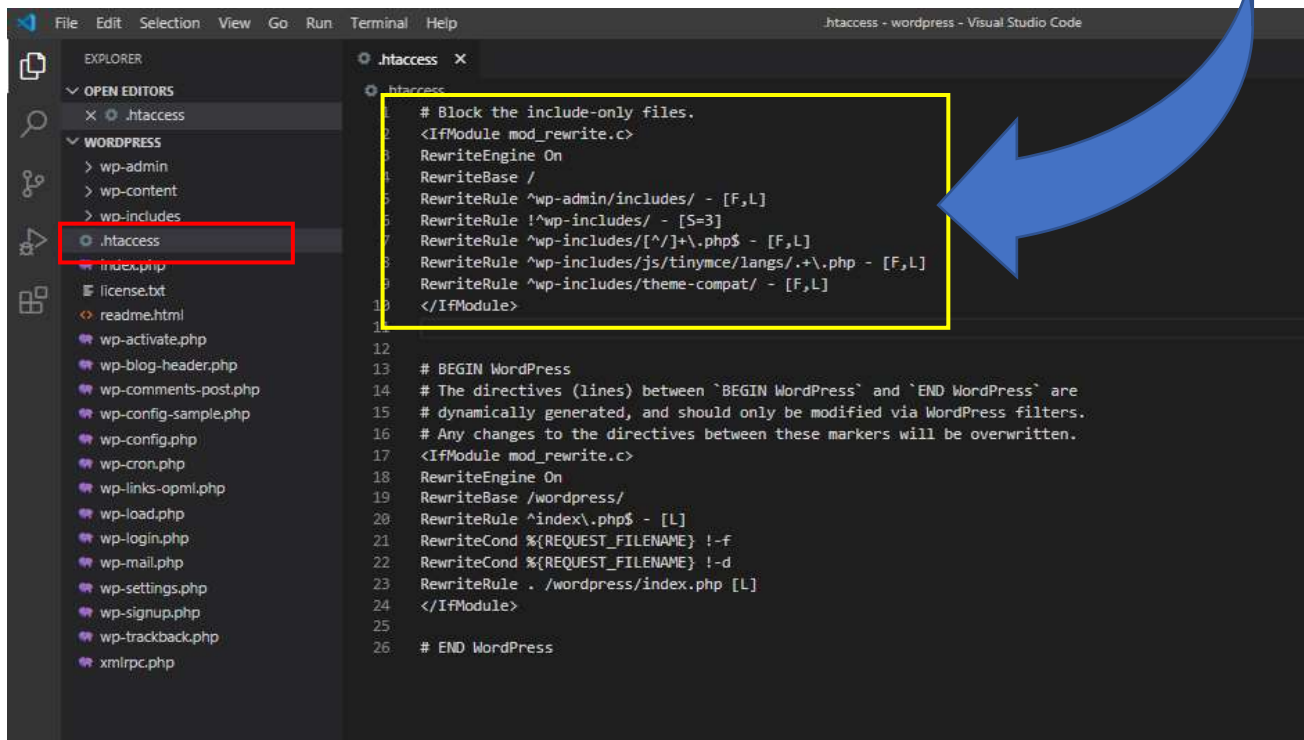
Adding server-side password protection to /wp-admin/ adds a second layer of protection around your blog's admin area, the login screen, and your files. This forces an attacker or bot to attack this second layer of protection instead of your actual admin files.

A second layer of protection can be added where scripts are generally not intended to be accessed by any user.

One way to do that is to block those scripts using mod\_rewrite in the .htaccess file.

```
# 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>
```

This should place above the line **# BEGIN WordPress**

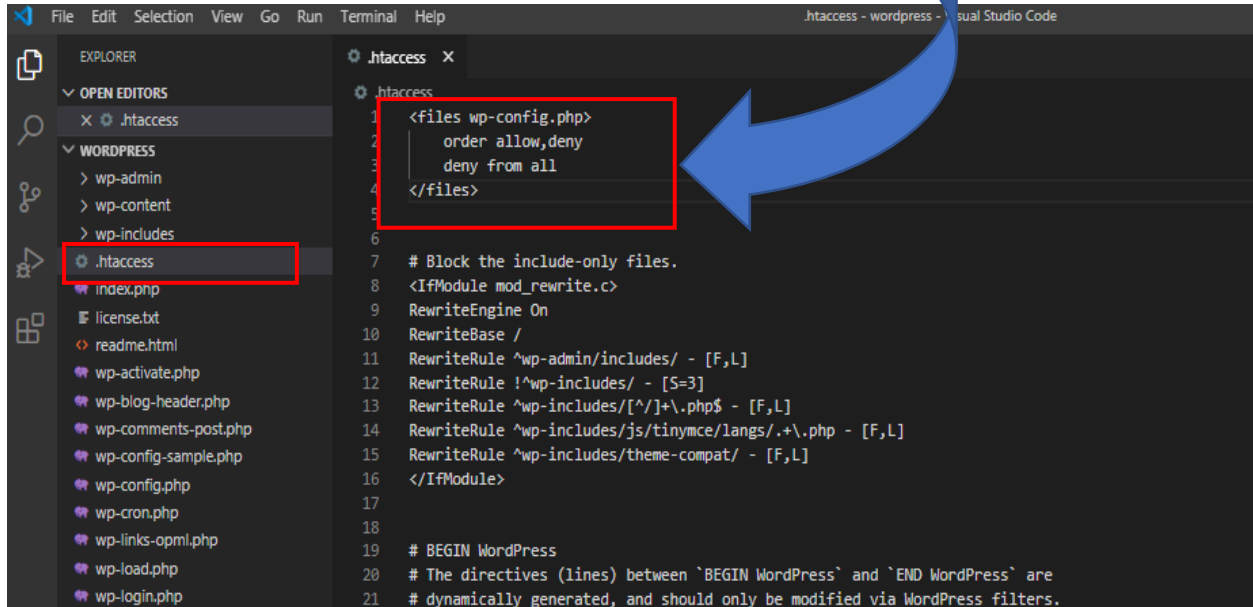


```
File Edit Selection View Go Run Terminal Help .htaccess - wordpress - Visual Studio Code
EXPLORER
OPEN EDITORS
  .htaccess
WORDPRESS
  wp-admin
  wp-content
  wp-includes
    .htaccess
    index.php
    license.txt
    readme.html
    wp-activate.php
    wp-blog-header.php
    wp-comments-post.php
    wp-config-sample.php
    wp-config.php
    wp-cron.php
    wp-links-opml.php
    wp-load.php
    wp-login.php
    wp-mail.php
    wp-settings.php
    wp-signup.php
    wp-trackback.php
    xmlrpc.php
  .htaccess
  1 # Block the include-only files.
  2 <IfModule mod_rewrite.c>
  3 RewriteEngine On
  4 RewriteBase /
  5 RewriteRule ^wp-admin/includes/ - [F,L]
  6 RewriteRule !^wp-includes/ - [S=3]
  7 RewriteRule ^wp-includes/[^\.]+\.\php$ - [F,L]
  8 RewriteRule ^wp-includes/js/tinymce/langs/.+\.\php - [F,L]
  9 RewriteRule ^wp-includes/theme-compat/ - [F,L]
 10 </IfModule>
 11
 12 # BEGIN WordPress
 13 # The directives (lines) between `BEGIN WordPress` and `END WordPress` are
 14 # dynamically generated, and should only be modified via WordPress filters.
 15 # Any changes to the directives between these markers will be overwritten.
 16 <IfModule mod_rewrite.c>
 17 RewriteEngine On
 18 RewriteBase /wordpress/
 19 RewriteRule ^index\.\php$ - [L]
 20 RewriteCond %{REQUEST_FILENAME} !-f
 21 RewriteCond %{REQUEST_FILENAME} !-d
 22 RewriteRule . /wordpress/index.php [L]
 23 </IfModule>
 24
 25 # END WordPress
```

## 5. Securing wp-config.php

If you use a server with .htaccess, you can put this in that file (at the very top) to deny access to anyone surfing for it:

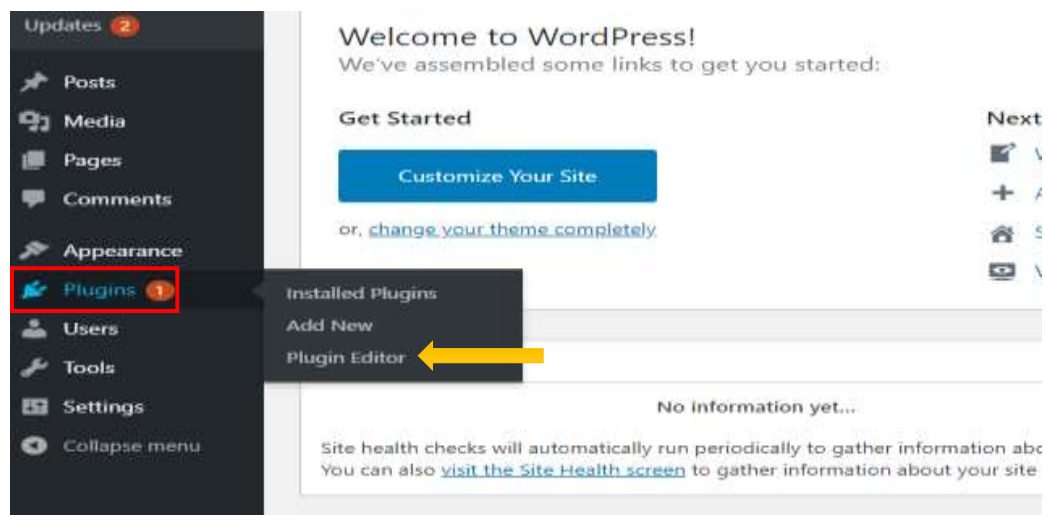
```
<files wp-config.php>
order allow,deny
deny from all
</files>
```



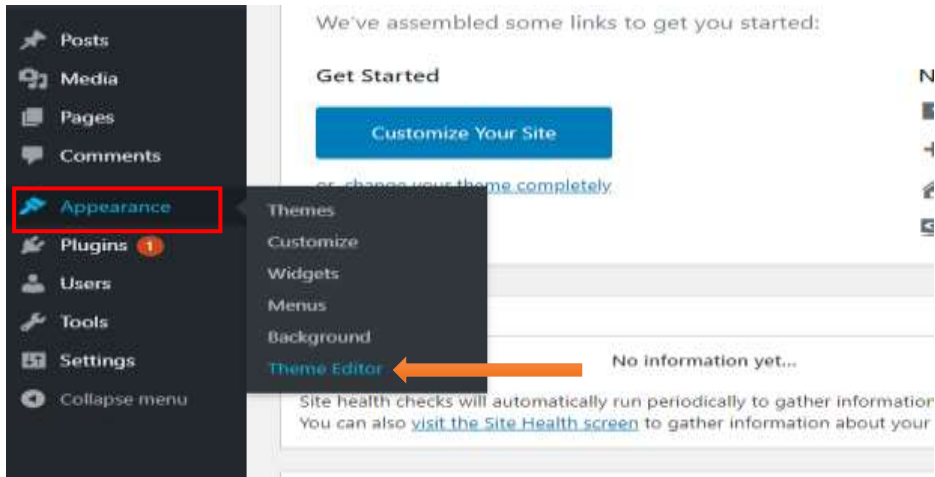
## 6. Disable file editing in WordPress admin

The WordPress dashboard by default allows administrators to edit php files, such as plugin and theme files.

Plugins → Plugin Editor

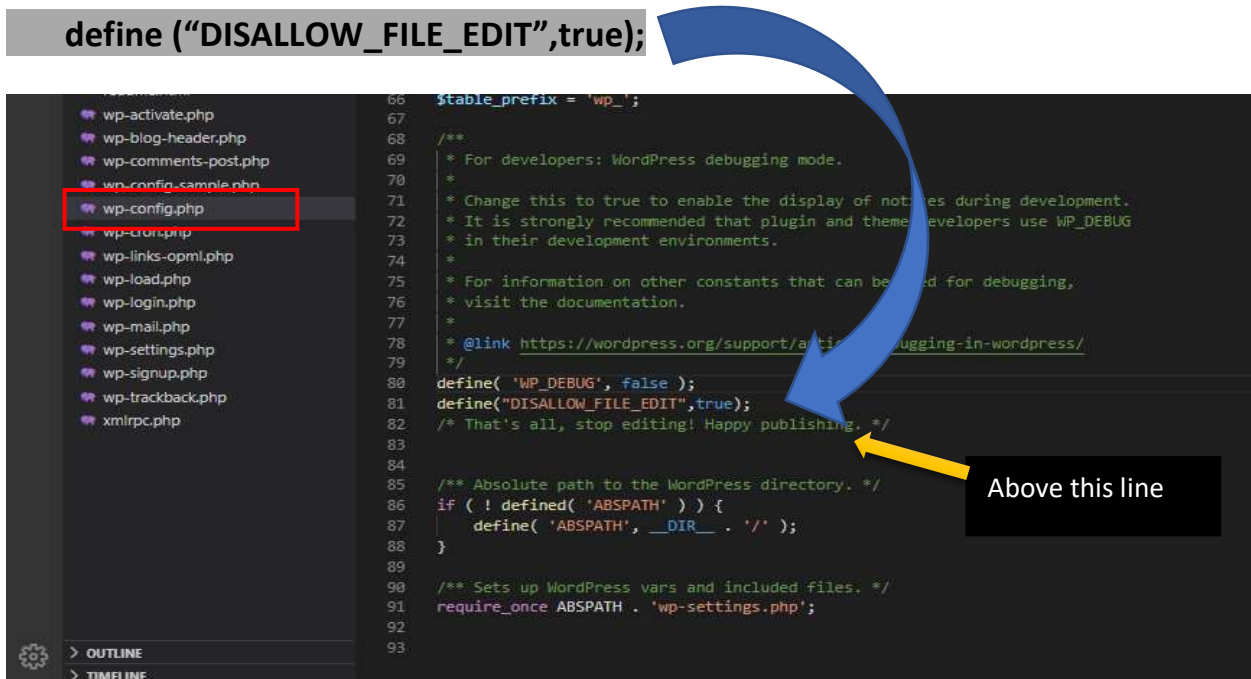


## Appearance → Theme Editor

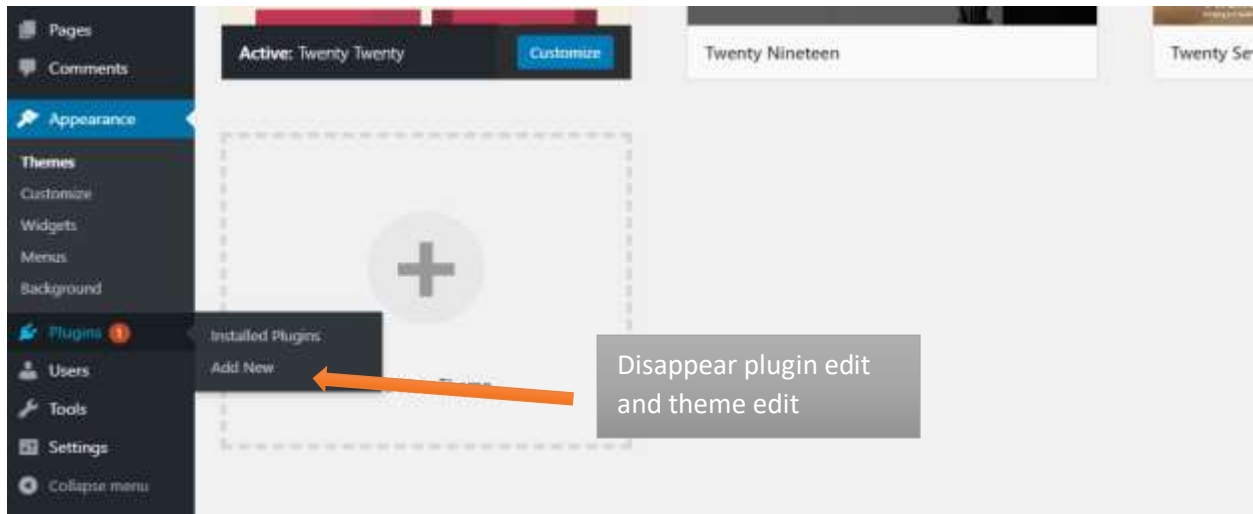


This is often the first tool an attacker will use if able to login, since it allows code execution.

## How to disable file editing in WordPress



After entering that line of code



This will not prevent an attacker from uploading malicious files to your site, but might stop some attacks.

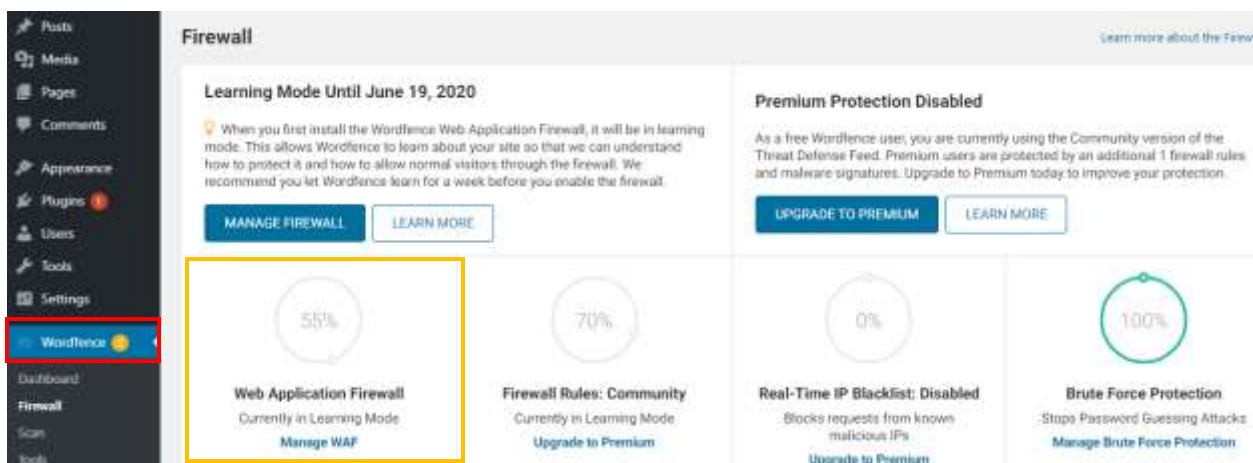
## 7. Use a web application firewall (WAF)

There are many plugins and services that can act as a firewall for your website.

We recommend wordfence plugin for this because others can have some security issues.

[Wordfence plugin installation](#)

After installation you can see;



When we select WAF plugin, we should check:

- Features they provide
- Updates frequency

Special for something like this

- Blacklist (ip range allowed).
- Whitelist (ip range allowed).
- Dynamic blacklist.
- Events recording which can be viewed by admins from back end.
- Alert of strict mode.
- File integrity checker
- Malware scanner

## 8. Security through obscurity

Rename the administrative account

When creating an administrative account, avoid easily guessed terms such as admin or webmaster as usernames because they are typically subject to attacks first.

The screenshot shows a database management interface. On the left, a tree view displays the database structure for 'wordpress'. A yellow box labeled 'Your WordPress Database' has a blue arrow pointing to the 'wordpress' folder. The 'wp\_users' table is highlighted with a red box. On the right, a table view shows the contents of the 'wp\_users' table. The first row has 'ID' 1, 'user\_login' 'admin', and 'user\_pass' 'SP\$Bjml1.qRn2kxyc7sbxzddZ72Q/9'. The 'admin' username is highlighted with a yellow box. Below the table, there are options for 'Query results operations' and 'Bookmark this SQL query'.

The screenshot shows a SQL query editor window titled 'Run SQL query/queries on table wordpress.wp\_users:'. The query text is: `1 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' value in the query.

+ Options		ID	user_login	user_pass
<input type="checkbox"/>	Edit  Copy  Delete	1	newuser	\$P\$Bjml1.qRn2kx.cy7sboxzddZ72Q/9M
<input type="checkbox"/> Check all <span style="margin-left: 20px;">With selected:</span> Edit  Copy  Delete  Export				

## 9. Data backups

No matter the size of your WordPress website, finding a way to keep it safe from issues such as updates gone wrong, hacking, user error and crashes should be of the utmost importance.

How to backup a WordPress site with an easy-to-use, free backup plugin. we recommend UpdraftPlus plugin for this.

Step 1


The screenshot shows the WordPress dashboard's 'Plugins' page. The 'Add New' button is highlighted with a red box. Below the button, there are filters for 'All (2)', 'Inactive (2)', and 'Update Available (1)'. A table lists installed plugins, with 'Akismet Anti-Spam' visible. A notification at the bottom indicates a new version (4.1.6) is available for Akismet.

Step2

The screenshot shows the search bar on the WordPress dashboard. The word 'updraft' is entered into the search field and is highlighted with a red box. To the left of the search field is a 'Keyword' dropdown menu.

Step 3

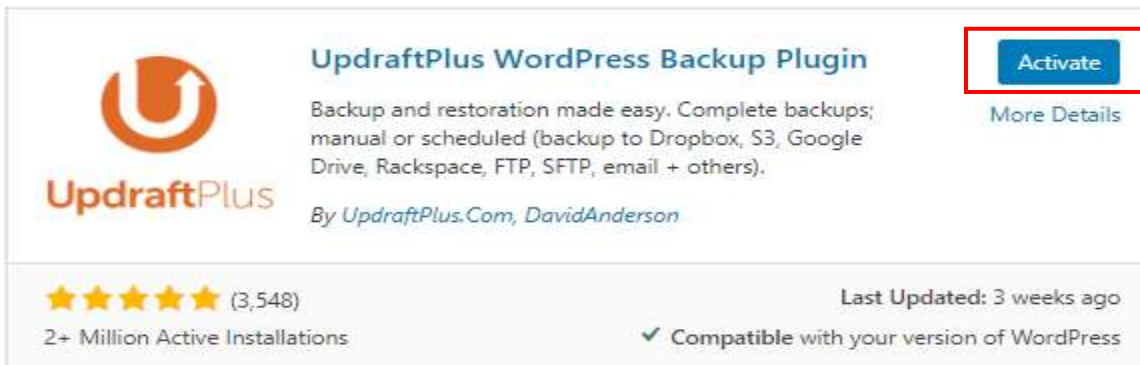


 **UpdraftPlus WordPress Backup Plugin** [Install Now](#)  
More Details

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) Last Updated: 3 weeks ago  
2+ Million Active Installations  Compatible with your version of WordPress

Step 4

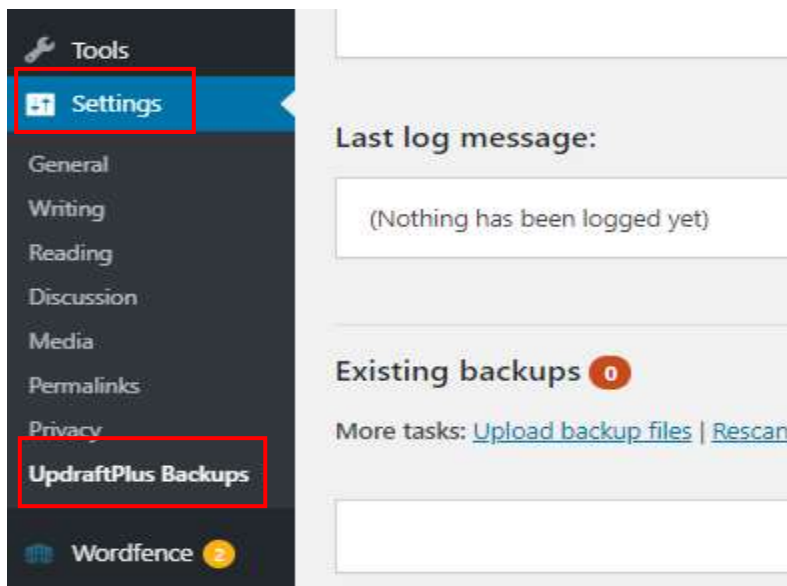



 **UpdraftPlus WordPress Backup Plugin** [Activate](#)  
More Details


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) Last Updated: 3 weeks ago  
2+ Million Active Installations  Compatible with your version of WordPress

Step 5




 Tools


 **Settings**

General  
Writing  
Reading  
Discussion  
Media  
Permalinks  
Privacy

**UpdraftPlus Backups**

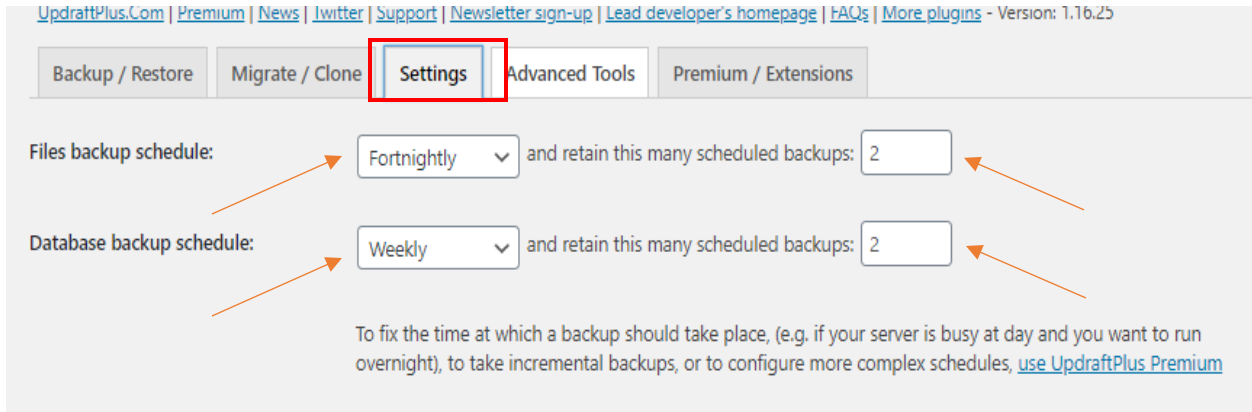
Wordfence 

Last log message:  
(Nothing has been logged yet)

Existing backups  0

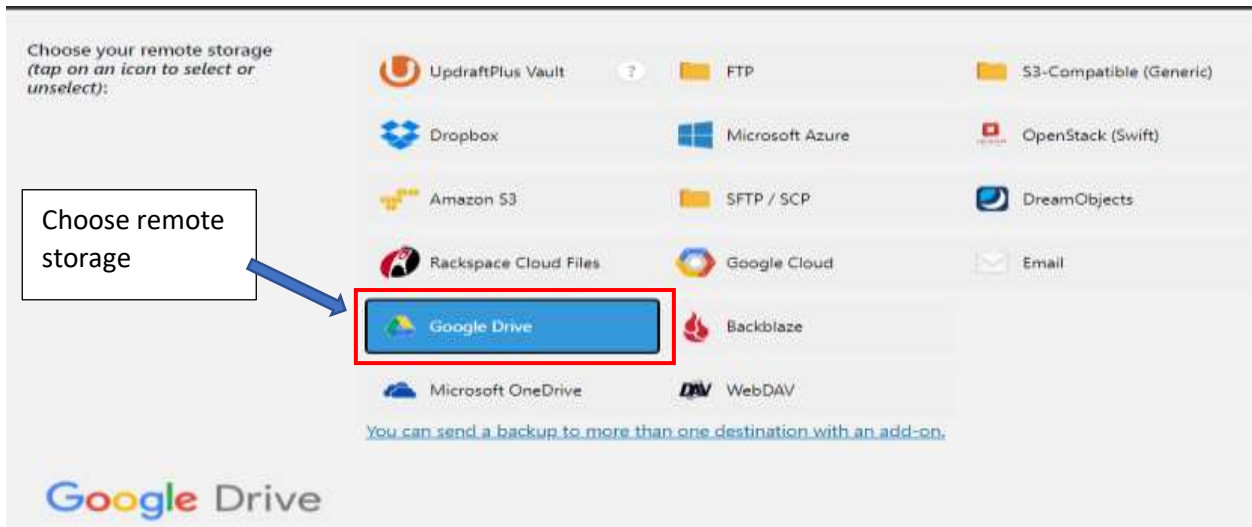
More tasks: [Upload backup files](#) | [Rescan](#)

## Step 6

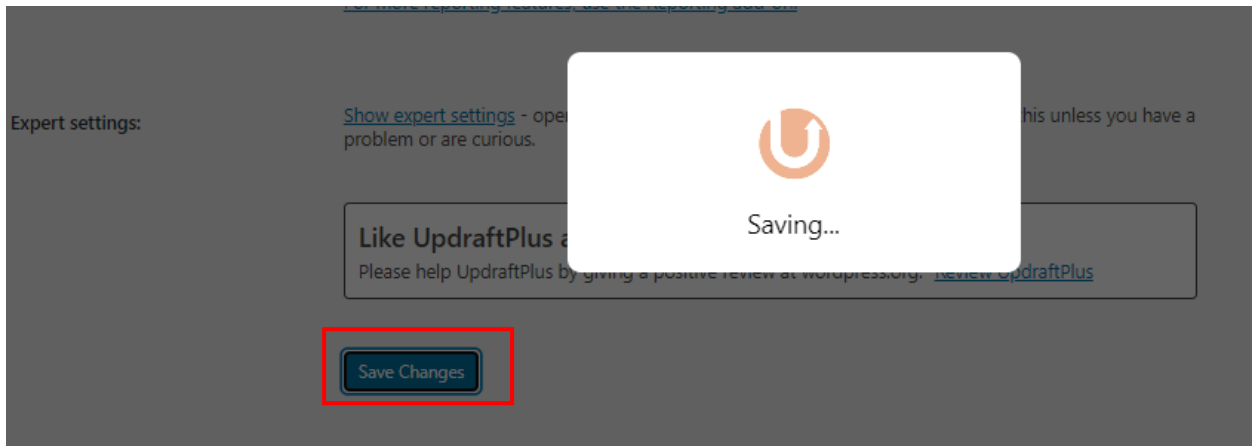


## Step 7

If we select Google drive option for remote storage (we can select other options also);



## Step 8



## Step 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.](#)



## Step 10



Sign in with Google

Choose an account  
to continue to **UpdraftPlus**

## Step 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

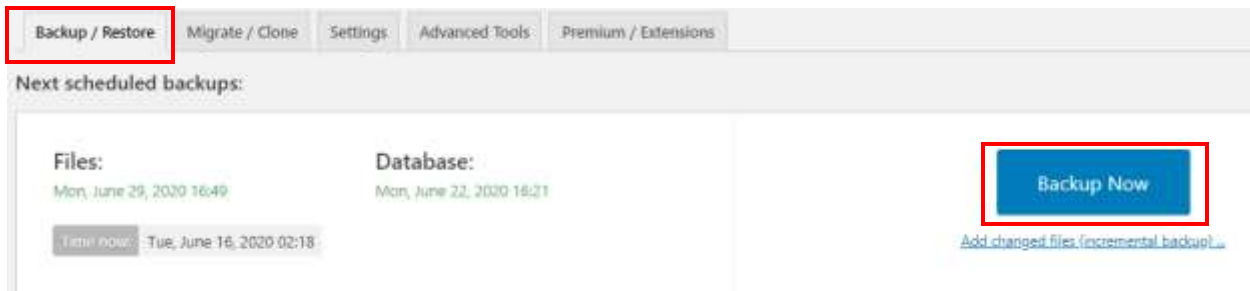
Allow

## Step 12



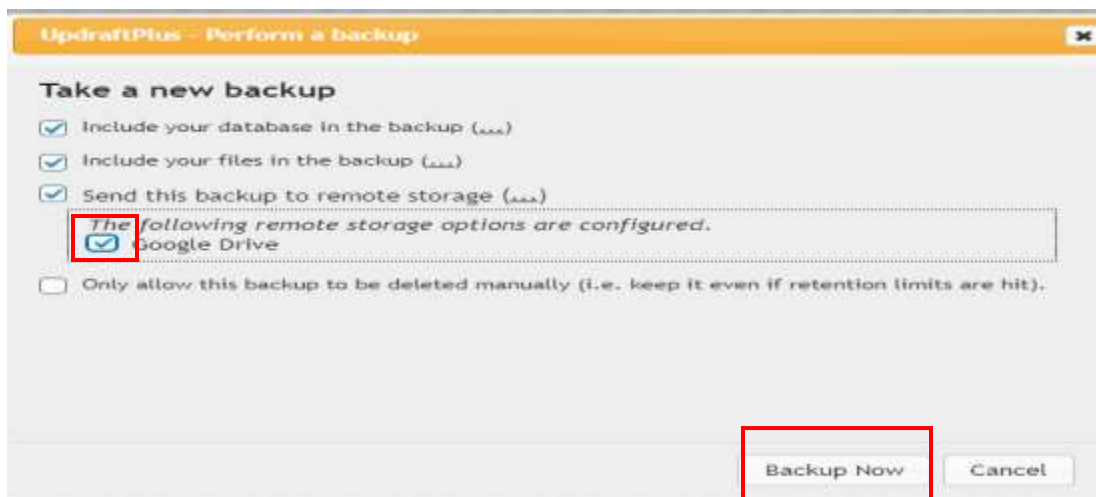
The image shows a confirmation screen for UpdraftPlus. At the top is the UpdraftPlus logo, a white 'U' with a circular arrow inside, on an orange background. Below the logo, the text reads: "To complete setup for Google Drive press the button below. This will take you back to your UpdraftPlus settings on the site http://localhost. You will then be able to send backups to Google Drive." A URL is provided: "The button will take you to: http://localhost/wordpress/wp-admin/options-general.php?action=updraftmethod-goo". A link to the privacy policy is also present: "Please read [this privacy policy](#) concerning use of our Google Drive authorisation app (none of your backup data is sent to us)". At the bottom center is a button labeled "Complete setup".

## Step 13



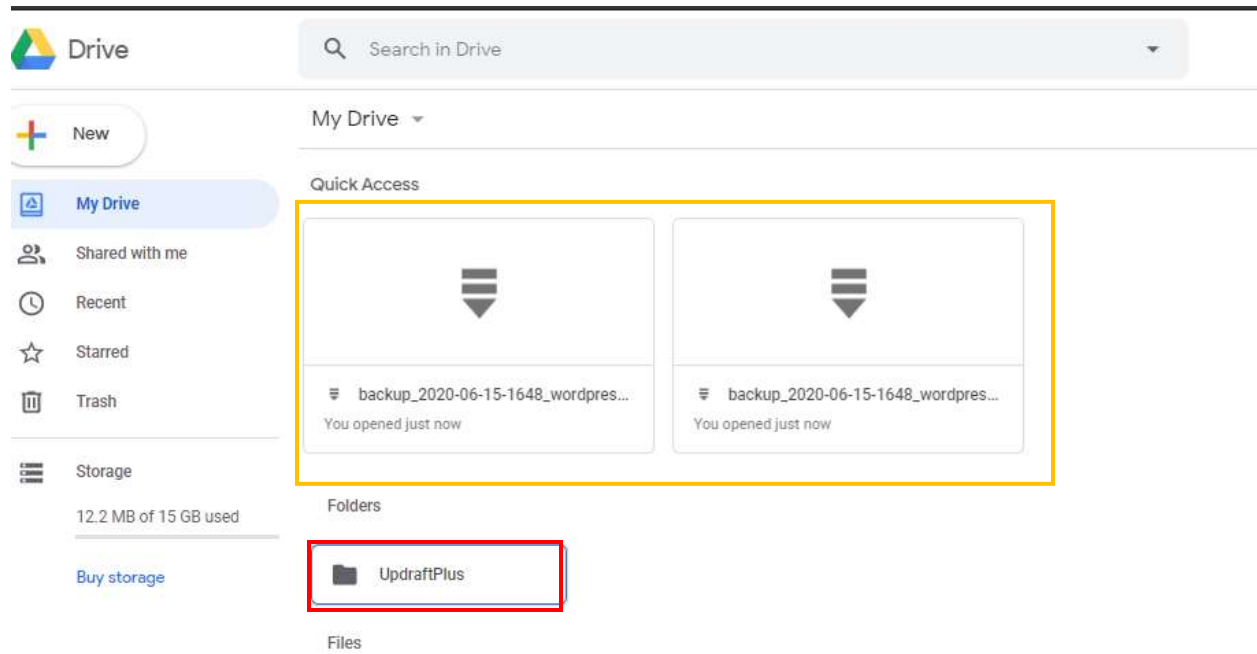
The image shows a portion of the WordPress dashboard. A navigation menu at the top includes "Backup / Restore" (highlighted with a red box), "Migrate / Clone", "Settings", "Advanced Tools", and "Premium / Extensions". Below the menu, the section "Next scheduled backups:" displays two backup schedules: "Files: Mon, June 29, 2020 16:49" and "Database: Mon, June 22, 2020 16:21". A "Time now:" indicator shows "Tue, June 16, 2020 02:18". On the right side, there is a blue "Backup Now" button (highlighted with a red box) and a link "Add changed files (incremental backup...)".

## Step 14

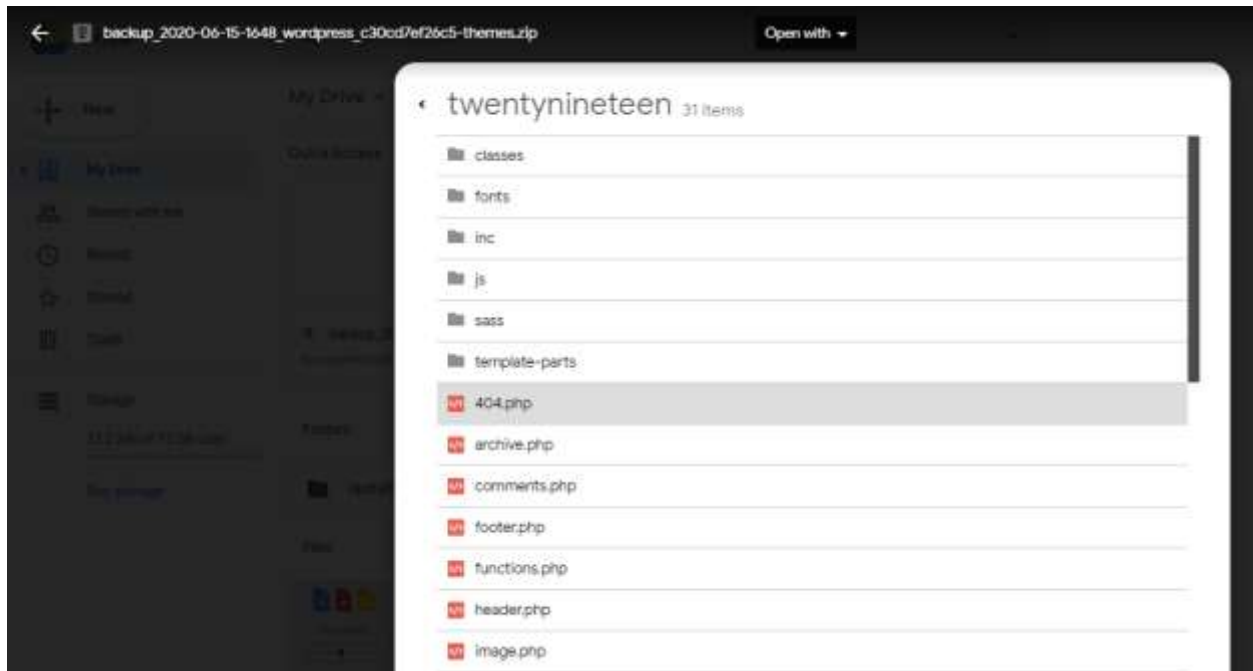


The image shows a dialog box titled "UpdraftPlus - Perform a backup". Under the heading "Take a new backup", there are three checked options: "Include your database in the backup", "Include your files in the backup", and "Send this backup to remote storage". A message box with a checkmark icon states: "The following remote storage options are configured. Google Drive". At the bottom of the dialog, there are two buttons: "Backup Now" (highlighted with a red box) and "Cancel".

## Step 15

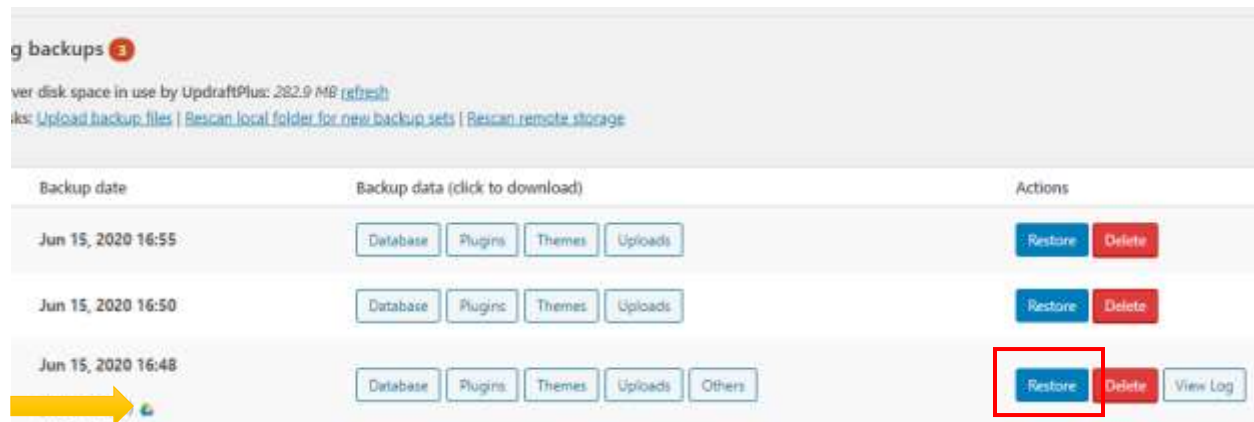


## Step 16

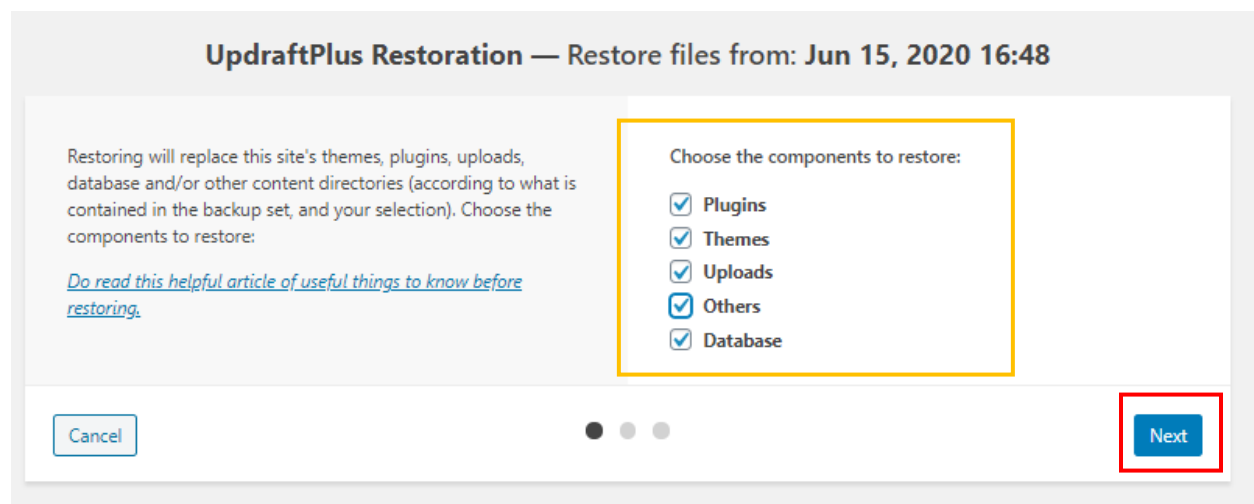


# How to restore your WordPress site from a backup

## Step 1



## Step 2



## 10. Block user-enumeration

- via functions.php

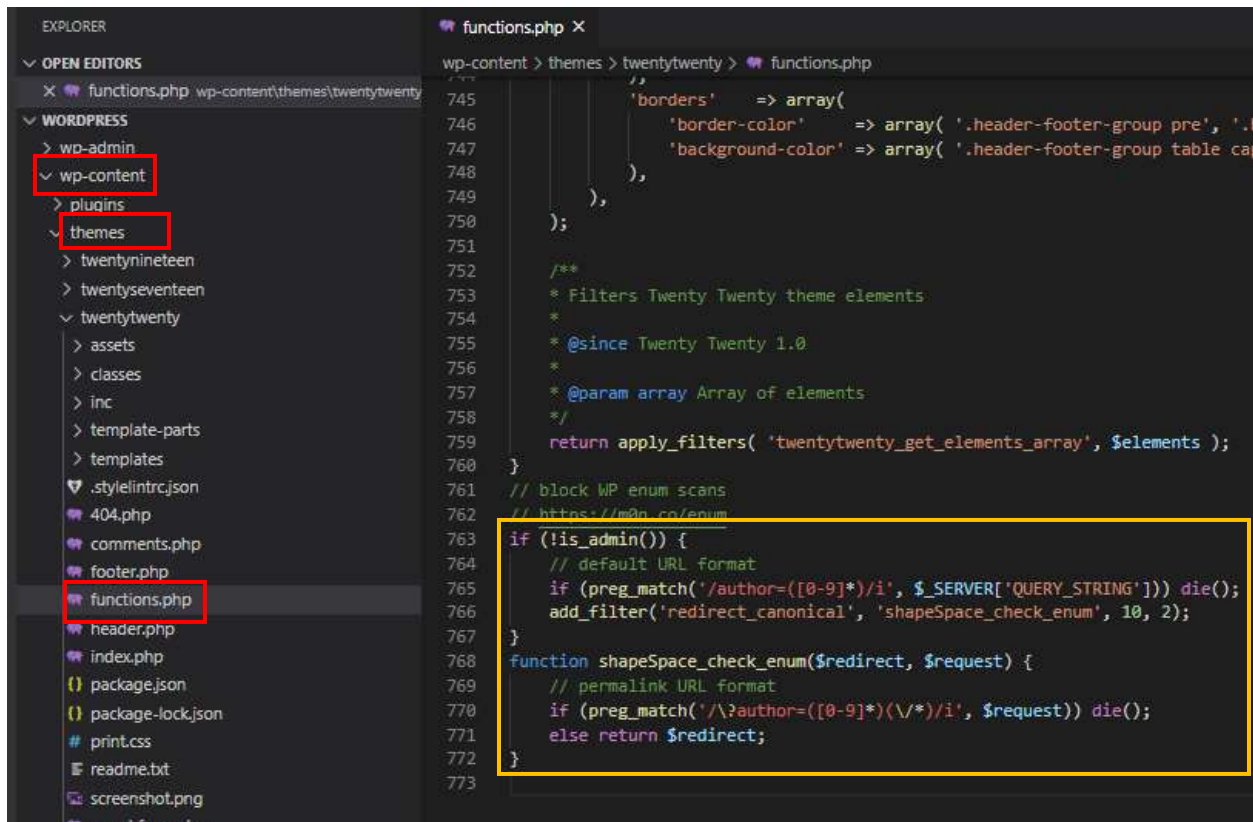
Add the following code to your theme's functions file:

```
// 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;
}

```



- Via .htaccess

Add the following code to the site's root .htaccess file.

```

# 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. Rest Api disabled via functions.php

Add the following code to your theme's functions file (Wp-content/ themes/ functions.php ):

```

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;
});

```

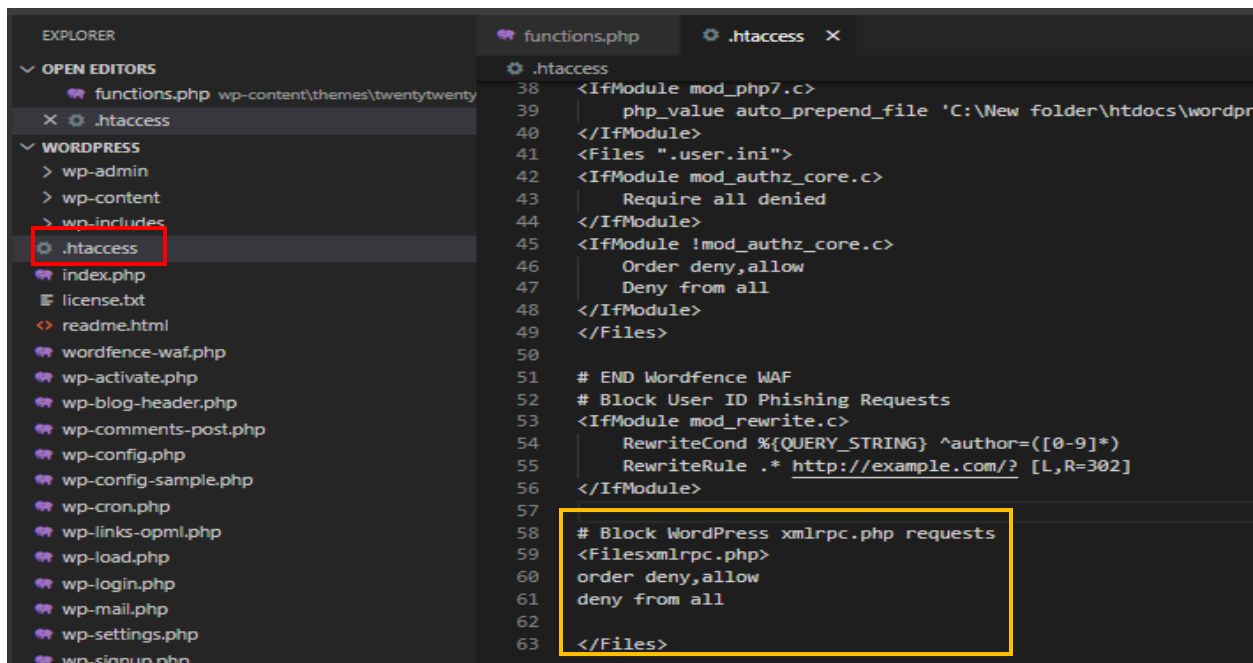
## 12. Disable XML-RPC in WordPress using .htaccess file

Add the following code to the site's root .htaccess file.

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

order deny,allow
deny from all

</Files>
```



The screenshot shows a code editor with two panes. The left pane is the Explorer view showing the file structure of a WordPress installation, with the .htaccess file in the wp-includes directory highlighted with a red box. The right pane shows the content of the .htaccess file, with the code for blocking XML-RPC requests highlighted with a yellow box. The code in the .htaccess file is as follows:

```
38 <IfModule mod_php7.c>
39     php_value auto_prepend_file 'C:\New folder\htdocs\wordpress\wp-includes\functions.php'
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
63 </Files>
```