How WordPress uses Database?

WordPress uses PHP as a scripting language (to store and retrieve data from database) and MySQL is used for database management, using SQL queries within the PHP markup. For example, if you log into a WordPress powered business website, It is SQL that actually logs you in, extracts your user ID and validates it, and ensures that the correct profile data is displayed on the front-end.

PHP and SQL work hand-in-hand. This helps WordPress to create a dynamic content-based experience for users. It allows you to customize content specific to certain users, such as admins, editors, and subscribers.

Plugins and themes also use WordPress database to store data. They use SQL within PHP markup to query the database and output content dynamically. Other plugins like WP-DB Manager, can be used to easily manage the database.

How to secure WordPress Database?

WordPress Database is the brain of a WordPress website as it stores all the information about and on the website like posts, pages, comments, tags, users, categories, custom fields, and other site options. This makes it a juicy target for malicious actors. Spammers and hackers run automated codes for SQL injections. Here is how you can secure the WordPress database.

1. Change Administrator Username

Like every other CMS, WordPress also has a default administrator login. Not changing the default admin login makes it easier for malicious actors to illegitimately gain access to your website and database.

In WordPress the default username is `admin`. Change it now if you haven't already.

1. Go to *phpMyAdmin.*
2. Run the following query. This changes the username from `admin` to `anything`.

```
UPDATE {database_prefix}users SET user_login='anything' WHERE user_login='admin';
```

3. In case of a WordPress multisite, you can use the `grant_super_admin()` function to grant super admin access and super admin privileges.

2. Change Administrator ID

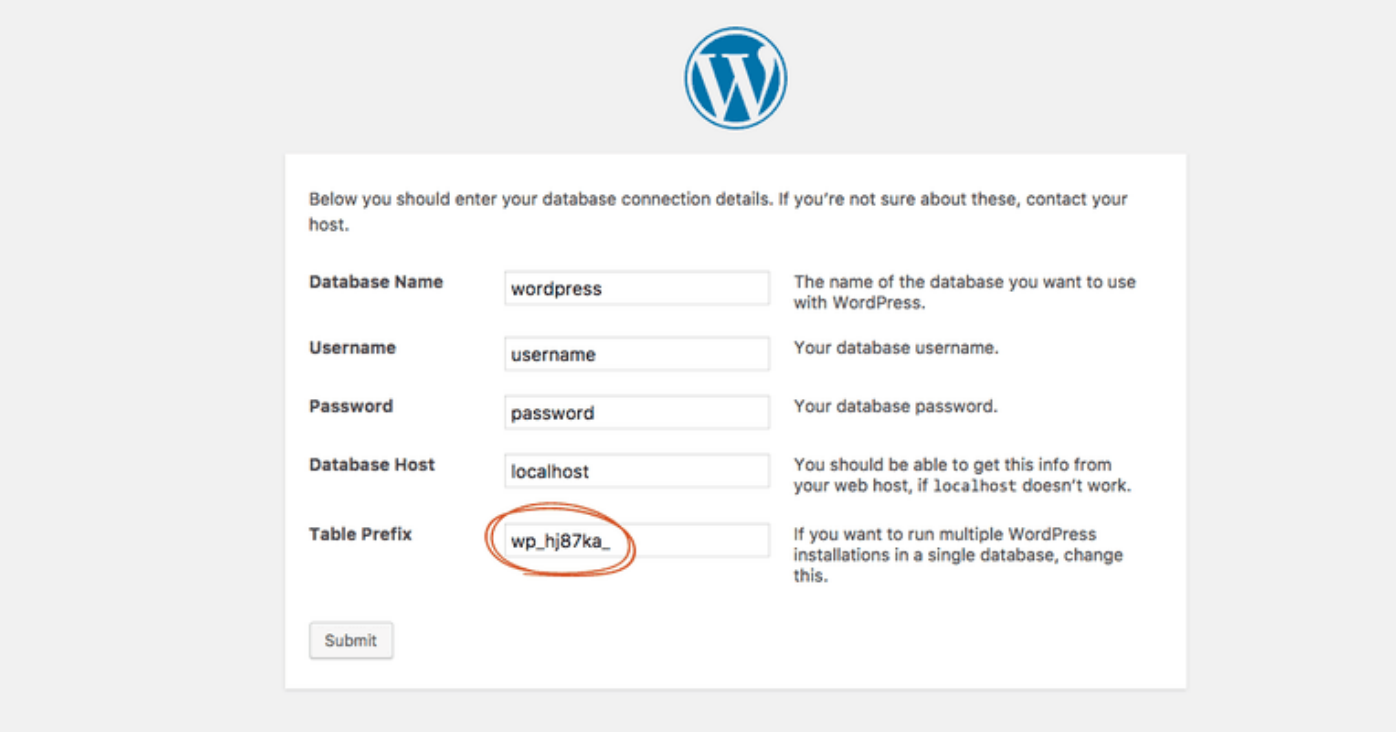
In WordPress, the default admin name is `admin` and default admin user ID is 1. Many SQL-injection attacks have exploited this. So, you should change this in the earliest to secure WordPress database. To change the admin user ID,

1. Go to *phpMyAdmin*
2. Run the following queries.

```
UPDATE wp_users SET ID = 2807 WHERE ID = 1; UPDATE wp_posts SET post_author = 2807 WHERE post_author = 1; UPDATE wp_comments SET user_id = 2807 WHERE user_id = 1; UPDATE wp_usermeta SET user_id = 2807 WHERE user_id = 1; ALTER TABLE wp_users AUTO_INCREMENT = 2808
```

3. Change Database Prefix

The default WordPress Database prefix is `wp_` . For a secure WordPress database, it is highly recommended that you change the default prefix during the WordPress installation process itself.



Change WordPress Database Prefix

If you haven't already, do it now. Follow these steps:

1. Access your website through an FTP client
2. Navigate to your configuration file *wp_config.php* in the root directory
3. Find the line with *wp_* prefix and change it.
   `$table_prefix = 'wp_ga2807_';`

4. Strict Database User Privileges

Strict user privileges better secure WordPress database. MySQL user specified in the *wp-config.php* file should have strict privileges. During installation, database user has all privileges to set necessary tables and objects but it should be a temporary measure. After installation, the MySQL user needs only DATA READ and DATA WRITE privileges.

5. Create Backups

Create back up before making any changes to your website or database. I repeat, create back up! Creating regular backups can be very helpful in case of an infection. You can simply restore the backup and remove the infected files.

But even with the back up restored the vulnerability that the attacker exploited remains unaddressed. You can signup for the Astra vulnerability assessment and penetration testing to uncover all the hidden backdoors and security vulnerabilities in your website.

6. Delete Custom Tables

It is recommended that you delete custom tables from your database after removing a website extension from your site, otherwise over the lifetime you'll collect a heap of unused tables in your database. Some plugins do come with the option to auto-delete all its data from the website and database when you uninstall it.