Adding JWT to WordPress

One of the things I've struggled with when working with headless WordPress is getting stuff that I need to be authenticated to accomplish; for example, I can get a list of posts and get an individual post but I can't create, update and delete posts from a remote client.

While reviewing a Udemy Course on the subject (Zach Gordon's Headless WordPress REST API Authentication I discovered that the reason this happens is that WordPress doesn't provide third party clients authentication by default. SO if you want to authenticate you have to set up your own authentication infrastructure in WordPress.

This post will cover how to implement JSON Web Token (JWT) authentication on a WordPress installation.

I chose JWT as my login solution not just because it's what the course I took used but because other options are too cumbersome and do way more than what I need them to, opening too many potential security holes.

I will use the JWT Authentication for WP REST API plugin as suggested in Gordon's course. It hasn't been tested in about a year but it works, for now, so I'll continue using it.

The first step is to download and install the plugin. You can do so from inside your WordPress installation by going to the plugins menu and selecting add new, searching for JWT authentication and then installing the plugin. **Don't activate it yet, we still need to configure it**.

The next steps are done outside of the administrator's GUI.

We first need to add

```
RewriteEngine on
RewriteCond %{HTTP:Authorization} ^(.*)
RewriteRule ^(.*) - [E=HTTP_AUTHORIZATION:%1]
```

CONFIGURATE THE SECRET KEY The JWT needs a secret key to sign the token this secret key must be unique and never revealed.

To add the secret key edit your wp-config.php file and add JWT_AUTH_SECRET_KEY constant

```php
define('JWT_AUTH_SECRET_KEY', 'your-top-secret-key');
```

You can use a string from the [WordPress Salt Generator](#) as the value for the key.

The `wp-api-jwt-auth` plugin has the option to activate CORs support.

To enable the CORs Support edit your `wp-config.php` file and add a JWT_AUTH_CORS_ENABLE constant

```php
define('JWT_AUTH_CORS_ENABLE', true);
```

Finally activate the plugin. The best way to test it is to point your browser to `https://<your-server-ulr>/wp-json/jwt-auth/v1`. It should return a list of the available endpoints.

We're ready to begin working with WordPress as a headless CMS