# WordPress Security Analysis (Passive)

**http://foss-notes.blog.nomagic.uk**

This report details the results of a passive (non-intrusive) security analysis of the target WordPress site.

WordPress Version:

**5.2.3**

Version does not appear to be latest 5.1.1 - update now.

**Reputation Check**

**PASSED**

| | |
|---|---|
| Google Check: | OK |
| Spamhaus Check: | OK |
| Abuse CC: | OK |
| Dshield Blocklist: | OK |
| Talos Blacklist: | OK |

**Server information**

| | |
|---|---|
| Web Server: | **Apache** |
| X-Powered-By: | **None** |
| IP Address: | **88.99.140.69** |
| Hosting Provider: | **Hetzner Online GmbH** |
| Shared Hosting: | **69 sites found on IP** |

## WordPress Plugins

The following plugins were detected through analysis of the HTML source from the sites main page.

| | |
|---|---|
| **advanced-access-manager** | latest release (5.9.9.1)<br>0 |
| **wp-featherlight** | latest release (1.3.0)<br>https://cipherdevelopment.com/wp-featherlight/ |
| **wp-super-cache** | latest release (1.7.0)<br>https://wordpress.org/plugins/wp-super-cache/ |

Plugins are a source of many security vulnerabilities within WordPress installations, always keep them updated to the latest version available and check the developers plugin page for information about security related updates and fixes.

There are likely more plugins installed than those listed here as the detection method used here is passive. While these results give an indication of the status of plugin updates, a more comprehensive assessment should be undertaken by brute forcing the plugin paths using a **dedicated tool**.

## WordPress Theme

The theme has been found by examining the path `/wp-content/themes/ *theme name* /`

| | | |
|---|---|---|
| **Canyon** | 0.2.3 | https://designcanyon.com/canyon/ |

While plugins get a lot of attention when it comes to security vulnerabilities, themes are another source of security vulnerabilities within WordPress installations, always keep them updated to the latest version available and check the developers theme page for information about security related updates and fixes.

The theme listed here is the **active theme** found in the HTML source of the page. A comprehensive assessment should include checking for other themes that are installed but not active as these can also contain exploitable security vulnerabilities. In a "black box" assessment or penetration test detection of all themes can be undertaken by **brute forcing the theme path**. Remove all unused themes to minimise the attack surface of the WordPress installation. Remove all unused themes to minimise the attack surface of the WordPress installation.

## User Enumeration

✔ It was **not possible to easily enumerate usernames** from the user ID's. This is a good thing, as it can add difficulty to brute force password attacks if the username is not able to be determined.

It is recommended to rename the `admin` user account to reduce the chance of brute force attacks occurring. As this will reduce the chance of automated password attackers gaining access.

Keep in mind that if the author archives are enabled it is usually **possible to enumerate all users** within a WordPress installation. Including a renamed `admin` account.

Only the first two user ID's were tested during this scan. Try the **advanced membership options** or a dedicated tool for more detailed enumeration of users, themes and plugins.

## Directory Indexing

In the test we attempted to list the directory contents of the uploads and plugins folders to determine if **Directory Indexing** is enabled. This vulnerability type is known as information leakage and can reveal sensitive information regarding your site configuration or content.

| | |
|---|---|
| /wp-content/uploads/ | **Indexing Disabled** |
| /wp-content/plugins/ | **Indexing Disabled** |

Directory indexing was tested on the `/wp-content/uploads/` and `/wp-content/plugins/` directores. Note that other directories may have this web server feature enabled, so ensure you check other folders in your installation. It is good practice to ensure directory indexing is disabled for your full WordPress installation either through the web server configuration or `.htaccess`.

## Linked Sites

Google Safe browse checks have been performed on each of the linked sites. Links with poor reputation could be a threat to users of the site. Hosting and location are also included in the results.

| | Externally Linked Host | Hosting Provider | Country |
|---|---|---|---|
| | designcanyon.com | SingleHop LLC | United States |

Search performed against Google Safe Browse website security testing
Check for malicious URL against multiple malware scanners using Virus Total

## Loaded Resources

Compromised sites will often be linked to malicious `javascript` or `iframes` in an attempt to attack users of your WordPress installation. Look over the listed resources, you should be familiar with all scripts and investigate ones you are not sure. In addition removal of unneeded javascript will speed up your website.