Malware Cleanup

Malware is one of the most common issues with Wordpress Sites , this is mainly due to plugins which are not updates or simply bad user practices.Recommended approach to cleanup -

This guide assumes that wp cli is availbile -

--allow-root if logged in as root

Search

Check maldet logs if detection were made

```
cat /usr/local/maldetect/logs/event_log | grep hits
```

grep search based on signatures found

```
grep -r -e 'exp' --include=*.php
```

Delete files which have a string insdie them

```
grep -rlZ 'exp' . --include=*.ico | xargs -0 rm -f --
```

Reset Wordpress

Change directory to the WordPress install directory , In most cases the best way to start is check core files are infected and replace them if required , First Check if checksums are ok -

```
wp core verify-checksums --allow-root
```

Before changing any files, please get the wordpress version to know which version needs to be downloaded.

```
cat wp-includes/version.php | grep wp_version
```

Then remove the core files and reinstall wordpress (overwrite files only)

```
rm -rf wp-admin ; rm -rf wp-includes
rm -rf {SITEUID}
wp core download --force --skip-content --version= --allow-root
```

** You can also reset plugins **

```
wp plugin install {name} --force --allowroot
```

Scan with Third party plugin

As a third step we will use Wordfence to do a final scan to find files which we might have missed . Sometimes this will fail with cahcing so disable caching.

Delete files

Delete files with confirmation

```
find . -type f -name "*.php" -exec rm -i {} \;
```

Find all PHP usuall in uploads and delte them

```
find . -name "*.php" -type f {-delete}
```

Quick edit files

:n for next files , :N for prev file , dd to delte line , :wn to write and move to next

```
grep -rl pattern |  xargs -o vim
```

Myssql cache

Sometimes malware will insert meta tags in post_content (use query to replace)

```
UPDATE wp_posts SET post_content = replace(post_content, "<script
src='https://for.dontkinhooot.tw/stat.js?n=ns1'  type='text/javascript'></script>", "")
```

Rules

New Rules for nginx to disable php in wp-content

```
# Deny access to hidden files and files inside wp-content/uploads
location /wp-content/uploads/{
        location ~ \.php$ {
                deny all;
            }
}
```

```
  # Deny access to hidden files and files inside wp-content/uploads
location /wp-content/ {
        location ~ \.php$ {
                deny all;
            }
}
```

Revision #8
Created 24 June 2021 05:18:15 by Vikas
Updated 23 September 2022 08:08:38 by Vikas