

```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /flexbones/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /flexbones/index.php [L]
</IfModule>

# END WordPress

## Load uploads from the staging or production servers

<IfModule mod_rewrite.c>
# Attempt to load files from production if
# they're not in our local version
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule app/uploads/(.*) \
    http://myproductionsite.com/app/uploads/$1 [NC,L]
</IfModule>

### SECURITY
# General Security Hardening measures

# XSS-Protection
# https://kb.sucuri.net/warnings/hardening/headers-x-xss-protection

<IfModule mod_headers.c>
    Header set X-XSS-Protection "1; mode=block"
</IfModule>

# X-Frame-Options
# https://kb.sucuri.net/warnings/hardening/headers-x-frame-clickjacking

<IfModule mod_headers.c>
    Header always append X-Frame-Options SAMEORIGIN
</IfModule>

# V-Contact Title: #####
```

```
# X-Content-Type: nosniff
# https://kb.sucuri.net/warnings/hardening/headers-x-content-type
```

```
<IfModule mod_headers.c>
  Header set X-Content-Type-Options nosniff
</IfModule>
```

```
# Wordpress recommend the following
# http://codex.wordpress.org/Hardening\_WordPress
# Block the include-only files.
```

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /flexbones/
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>
```

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