Let's take your website security to the next level.

Plugins are okay, but what else can we do?

Matt Ryan
matt@capwebsolutions.com
Cap Web Solutions

Who am I and why am I up here?

- Matt Ryan
- Kim asked!

Other misc nuggets - WordCamp Lehigh Valley August 2018

- 40+ years in IT
- Started out in software development
  - Look ma, I can program in Fortran IV
- Network management and infrastructure
- WordPress dev | website care | WP Hosting
  - **It makes me happy**.

WordPress Security Areas

- Lock Down WordPress Admin
- HTTPS – SSL Certificate
- Hardening wp-config.php
- Disable XML-RPC
- Hide WordPress Version
- HTTP Security Headers
- Disable Editing in Dashboard
- Prevent Hotlinking
- DDoS Protection

- Secure WordPress Hosting
- Use Latest PHP Version
- Clever Usernames and Passwords
- Latest Versions
- Two-Factor Authentication
- WordPress Security Plugins
- Database Security
- Secure Connections
- File and Server Permissions
- Always Take WordPress Backups

- **Extras**: Cloudflare Rules & Settings

Low-Hanging Fruit aka Security Deterrents

- Secure WordPress Hosting
- Use Latest PHP Version
- Clever Usernames and Passwords
- Latest Versions of Themes and Plugins
- Two-Factor Authentication for Admin

- WordPress Security Plugins
- Database Security - db prefix
- Secure Connections - SFTP/SSH
- File, Folder & Server Permissions
- Always Take WordPress Backups
    - Daily | Weekly | Monthly

Plugin Magic

- WP 2FA
- Solid Security
- Wordfence

Lock Down Admin

- Change WordPress URL
- Limit login attempts
- Basic HTTP Authentication for login page
    - Adds user/pass just to view the page.

- Just to slow the hackers down.
- Encourage them to move on.

Plugin Magic

- Free WPS Hide Login
- Free Limit Logins Attempts

Topic List

SSL Certificate, TLS & HTTPS

- Use HTTPS for Encrypted Connections
- Get SSL certificate
- Use TLS 1.2 at a minimum

- TLS is actually a more recent version of SSL. It addresses security vulnerabilities found in earlier SSL protocols.

SSL Status Checking - https://www.ssllabs.com/ssltest/

Ref Cloudflare example.

Topic List

Hardening wp-config.php

- Heart & soul of your website
- Contains db login and security keys/salts
  - Move wp-config.php 1 level up
- Add code to wp-load.php to reference new location of config file.

```
<?php
include('/home/parent-folder/wp-config.php');
```

See Filezilla screenshot

- Change your security keys & salts
  - Especially if you've done a few clones or migrations of your site.

wordpress.org salt generator

Topic List

Disable XML-RPC

If you are not using it, turn it off.

There are a few WordPress plugins like Jetpack that rely on XML-RPC, but most sites won't need it.

To disable this completely you can install the free Disable XML-RPC-API plugin.

Or add the code snippet to functions.php

NGINX config file tweak to stop XML-RPC attacks. Produces a 403 error when accessed.

```
location ~* ^/xmlrpc.php$ {
return 403;
}
```

PHP Code Snippet for functions.php:

```
// Disable all XML-RPC functionality
add_filter(   'xmlrpc_methods',   '__return_empty_array' );
```

Topic List

Hide WordPress Version

Hiding your WordPress version touches again on the subject of **WordPress security by obscurity**. The less other people know about your WordPress site configuration the better.

Another place where the WordPress version shows up is in the default `readme.html`

- You can safely delete this file via FTP/SFTP/cPanel file manager.

Code Snippet

```
function wp_version_remove_version() {
  return '';
}

add_filter('the_generator', 'wp_version_remove_version');
```

Topic List

HTTP Security Headers

- Take advantage of HTTP security headers
- Configured at web server level
- Tell browser how to behave when handling your site's content.
- Most important headers
  - Content-Security Policy
  - Strict-Transport-Security
  - X-Frame-Options

Ref: KeyCDN in-depth post

Topic List

Check which headers are currently running

- Launch browser devtools -
  - Ctrl Shift I
- Look at the header on your site's initial response under the Network tab.
  - Demo - Look for:
    - strict-transport-security
    - x-content-type
    - X-frame-options
    - Content-security-policy

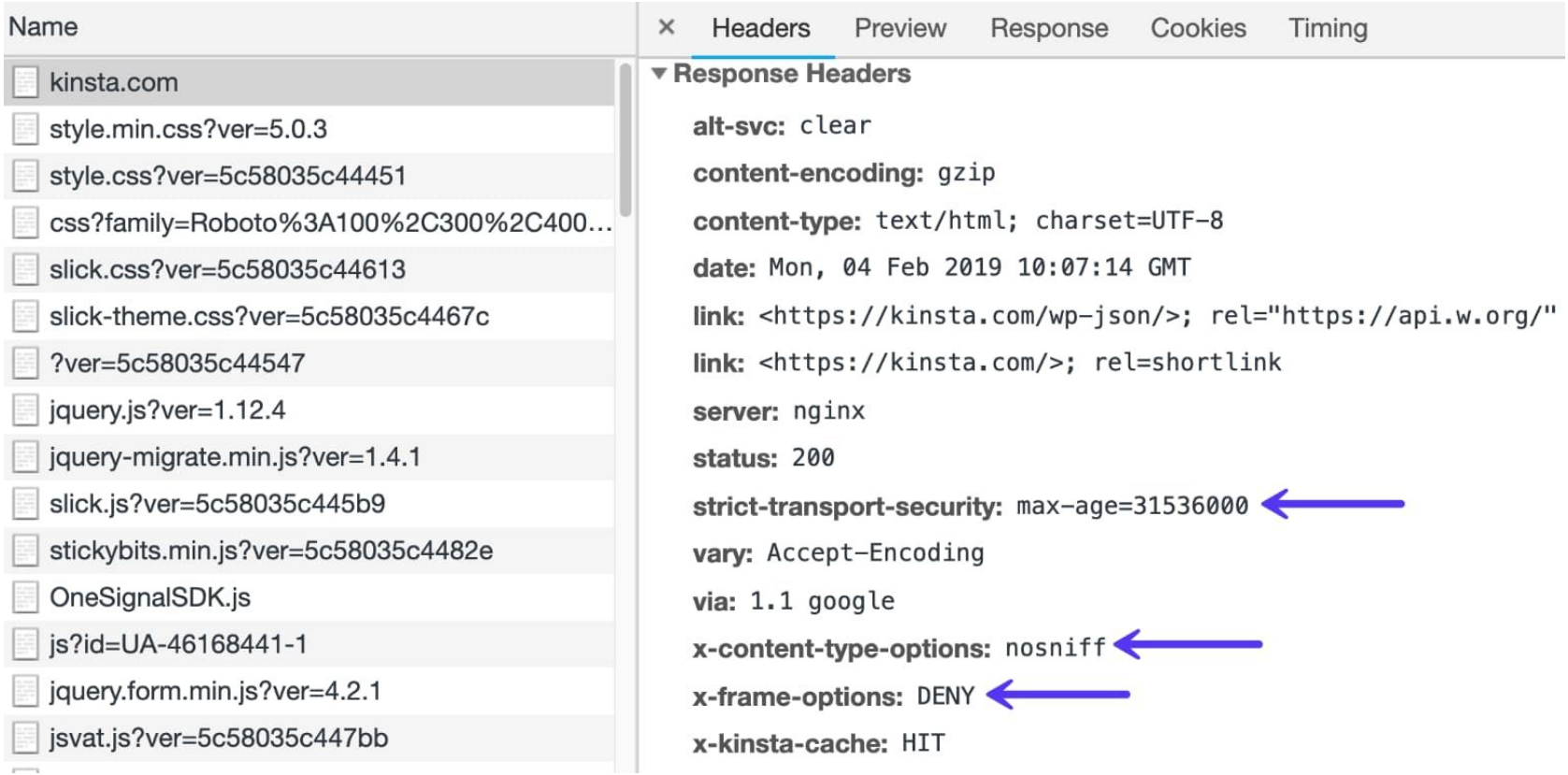
You can also scan your WordPress website with the free securityheaders.io too.

Shows which HTTP security headers you currently have on your site.

Live Demo

Demo - Limited security headers - no Content-security-policy

Topic List



Headers via browser Inspector

Topic List

Content Security Policy Configuration - Code Snippets

- Configure Content- Security-Policy in WordPress by editing the .htaccess file in apache
- Nginx users, this snippet is placed within the configuration file.

Ref: How to Create a Content Security Policy (CSP Header) | GridPane

Code Snippets:

Nginx

```
add_header Content-Security-Policy: "default-src 'none';
script-src 'self' 'unsafe-inline' 'unsafe-eval'
https://*.googletagmanager.com https://cdn.usefathom.com
https://*.usercentrics.eu https://*.cloudflare.com/
https://s3.amazonaws.com https://*.google-analytics.com;
```

Apache

```
<IfModule mod_headers.c>
Header set Content-Security-Policy "default-src 'none';
script-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self';"
</IfModule>
```

Sample conf file on Nginx

Topic List

Security Report Summary

B

Site:	https://capwebsolutions.com/
IP Address:	2606:4700:3036::ac43:d9d5
Report Time:	07 May 2024 10:57:01 UTC
Headers:	✔ X-Frame-Options ✔ X-Content-Type-Options ✔ Strict-Transport-Security ✔ Referrer-Policy ✖ Content-Security-Policy ✖ Permissions-Policy
Advanced:	Solid grade,let's perform a deeper security analysis of your website and APIs: Try Now

SSL Server Test - ssllabs.com

Security Report Summary

A

Site:	https://capwebsolutions.com/
IP Address:	2606:4700:3031::6815:5666
Report Time:	07 May 2024 11:15:11 UTC
Headers:	✔ X-Frame-Options ✔ X-Content-Type-Options ✔ Strict-Transport-Security ✔ Referrer-Policy ✔ Content-Security-Policy ✖ Permissions-Policy
Warning:	Grade capped at A, please see warnings below.
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs: Try Now

Disable Editing in Dashboard

A lot of WordPress sites have multiple users and administrators, which can make WordPress security more complicated.

Bad practice is to give authors or contributors administrator access.

Give users the correct roles and permissions so that they don’t break anything.

It can be beneficial to simply disable the Appearance & Plugin editors in WordPress.

Place the following code in your wp-config.php file to remove the ‘edit_themes’, ‘edit_plugins’ and ‘edit_files’ capabilities of all users.

```
define('DISALLOW_FILE_EDIT', true);
```

Topic List

Prevent Hotlinking

- The concept of Hotlinking is very simple. You find an image on the Internet somewhere and use the URL of the image directly on your site.
- This image will be displayed on your website but it will be served from the original location.
- This is actually theft as it is using the hotlinked site's bandwidth.
- This might not seem like a big deal, but it could generate a lot of extra costs.

Topic List

Prevent Hotlinking - Apache & Nginx - Code Snippets

Apache

Add to .htaccess file.

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER}
!^http(s)?://(www\.)?yourdomain.com [NC]
RewriteRule \.(jpg|jpeg|png|gif)$
http://dropbox.com/hotlink-placeholder.jpg
[NC,R,L]
```

The second row defines the allowed referrer – the site that is allowed to link to the image directly, this should be your website.

Nginx

Add to your config file.

```
location ~ .(gif|png|jpe?g)$ {none blocked
~.google. ~.bing. ~.yahoo mattryan.co
*.mattryan.co;
if ($invalid_referer) {
return 403;
}
}
```

DDoS Protection

DDoS is a type of DOS attack where multiple systems are used to target a single system causing a Denial of Service (DoS) attack.

One of the best recommendations is to use a reputable 3rd party security service like Cloudflare or Sucuri.

Plugin Magic

- AIO Security
- 70+ options on wordpress.org

FREE RECOMMENDATION

Website DDoS protection is Free in all **Cloudflare** service plans!

Topic List

Cloudflare Settings & Configuration Rules

Setup DNSSEC on domain level and cloudflare. Go to Cloudflare > DNS > Settings > DNS SEC and enable it .

Quickstart guide > Automatic HTTPS Rewrites: ON, Always use HTTPS: ON, Brotli: ON

SSL/TLS > Overview > Set SSL to FULL (Strict) and enable SSL/TLS Recommender

SSL/TLS > Edge Certificate > Enable Always Use HTTPS, and Enable HTTP Strict Transport Security (HSTS), Max-Age: 6 months, Include subdomains: On, Preload: On, and set Minimum TLS Version to 1.2

Caching > Configuration > Caching Level to No Query String, and Browser Cache TTL set to Respect Existing Headers, and Always Online™ enabled

Caching > Configuration > Tiered Caching > Smart Tiered Caching Topology enabled

Rules > Settings > Enable Normalize URLs to origin

Rules > Transform Rules > Managed Transform > HTTP request headers > Add TLS client auth headers - Enabled, and Remove visitor IP headers - Enabled

Rules > Transform Rules > Managed Transform > HTTP response headers > Remove "X-Powered-By" headers - Enabled, and Add security headers - Enabled

Network > Pseudo IPv4 > set to Add header

Topic List

Cloudflare Rules

Wrap-up

Topic List

- Lots covered tonight
- Slides will be available with live links
- Blog post forthcoming

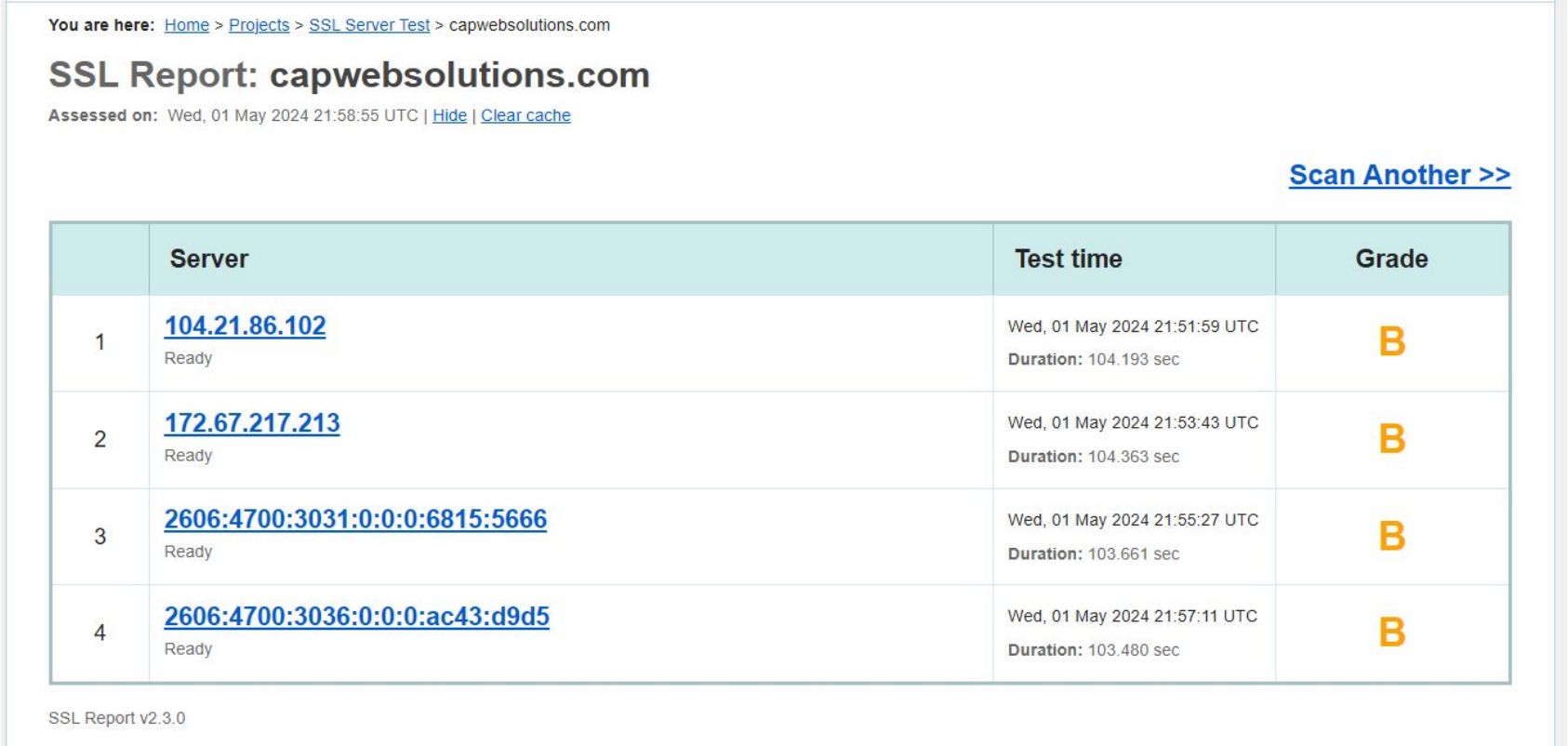
- Cloudflare is your partner - Free tier is all it takes
- Don’t skimp on hosting - think of it as your website’s foundation

- Almost all of these site specific settings can be handled by:
  - Wordfence
  - Solid Security (formerly iThemes Security)
    - “Do it for me”

Thanks for tuning in.

Matt Ryan
matt@capwebsolutions.com
Cap Web Solutions

Cloudflare TLS Example - 1 / 3



You are here: Home > Projects > SSL Server Test > capwebsolutions.com

SSL Report: capwebsolutions.com

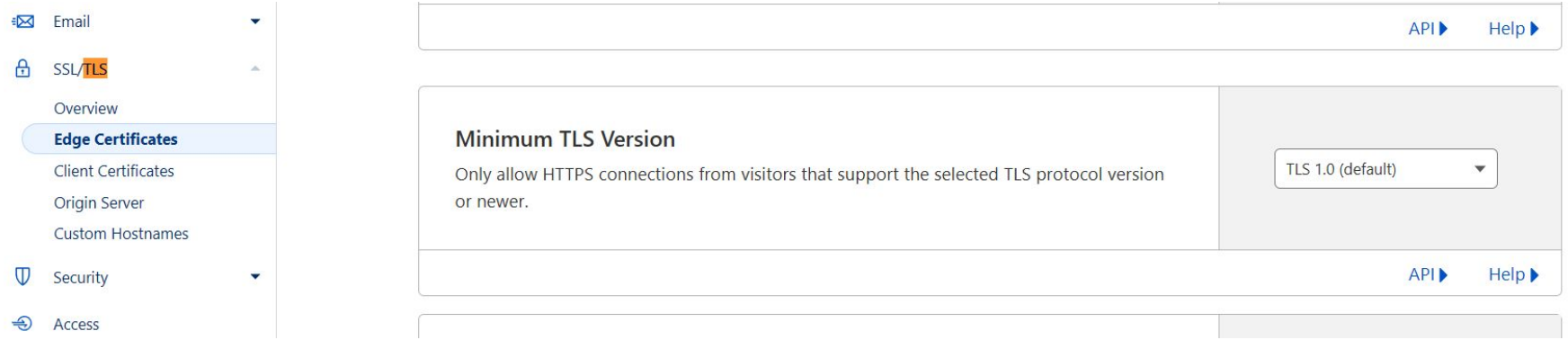
Assessed on: Wed, 01 May 2024 21:58:55 UTC | Hide | Clear cache

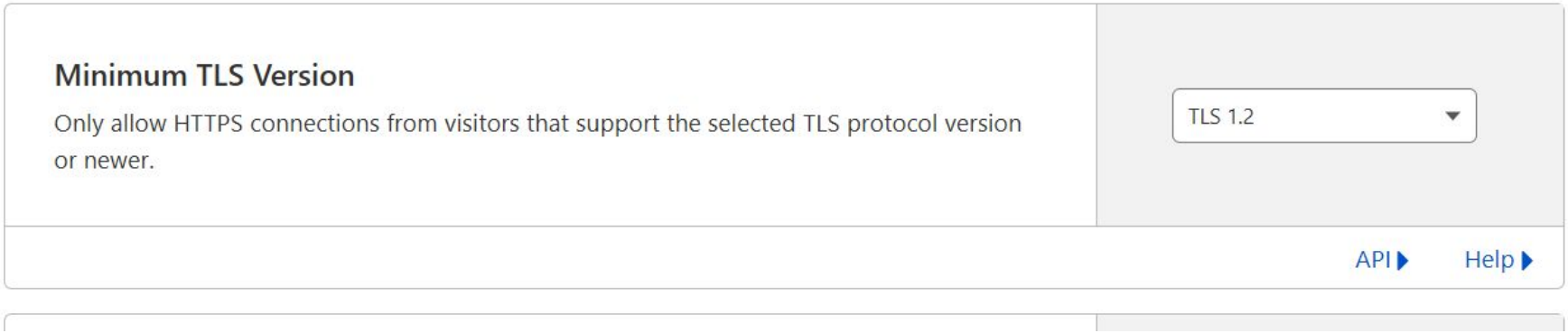
Scan Another >>

	Server	Test time	Grade
1	104.21.86.102 Ready	Wed, 01 May 2024 21:51:59 UTC **Duration:** 104.193 sec	B
2	172.67.217.213 Ready	Wed, 01 May 2024 21:53:43 UTC **Duration:** 104.363 sec	B
3	2606:4700:3031:0:0:0:6815:5666 Ready	Wed, 01 May 2024 21:55:27 UTC **Duration:** 103.661 sec	B
4	2606:4700:3036:0:0:0:ac43:d9d5 Ready	Wed, 01 May 2024 21:57:11 UTC **Duration:** 103.480 sec	B

SSL Report v2.3.0

Cloudflare TLS Example - 2 / 3





Cloudflare TLS Example - 3 / 3

Who Supports TLS 1.2?

After reset TLS version min to TLS 1.2

You are here: Home > Projects > SSL Server Test > capwebsolutions.com

SSL Report: capwebsolutions.com

Assessed on: Thu, 02 May 2024 12:30:07 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	104.21.86.102 Ready	Thu, 02 May 2024 12:24:19 UTC **Duration:** 87.34 sec	A+
2	172.67.217.213 Ready	Thu, 02 May 2024 12:25:46 UTC **Duration:** 87.6 sec	A+
3	2606:4700:3036:0:0:0:ac43:d9d5 Ready	Thu, 02 May 2024 12:27:13 UTC **Duration:** 86.602 sec	A+
4	2606:4700:3031:0:0:0:6815:5666 Ready	Thu, 02 May 2024 12:28:40 UTC **Duration:** 86.805 sec	A+

SSL Report v2.3.0

Return

Db Prefix

[Change WP Database Prefix]

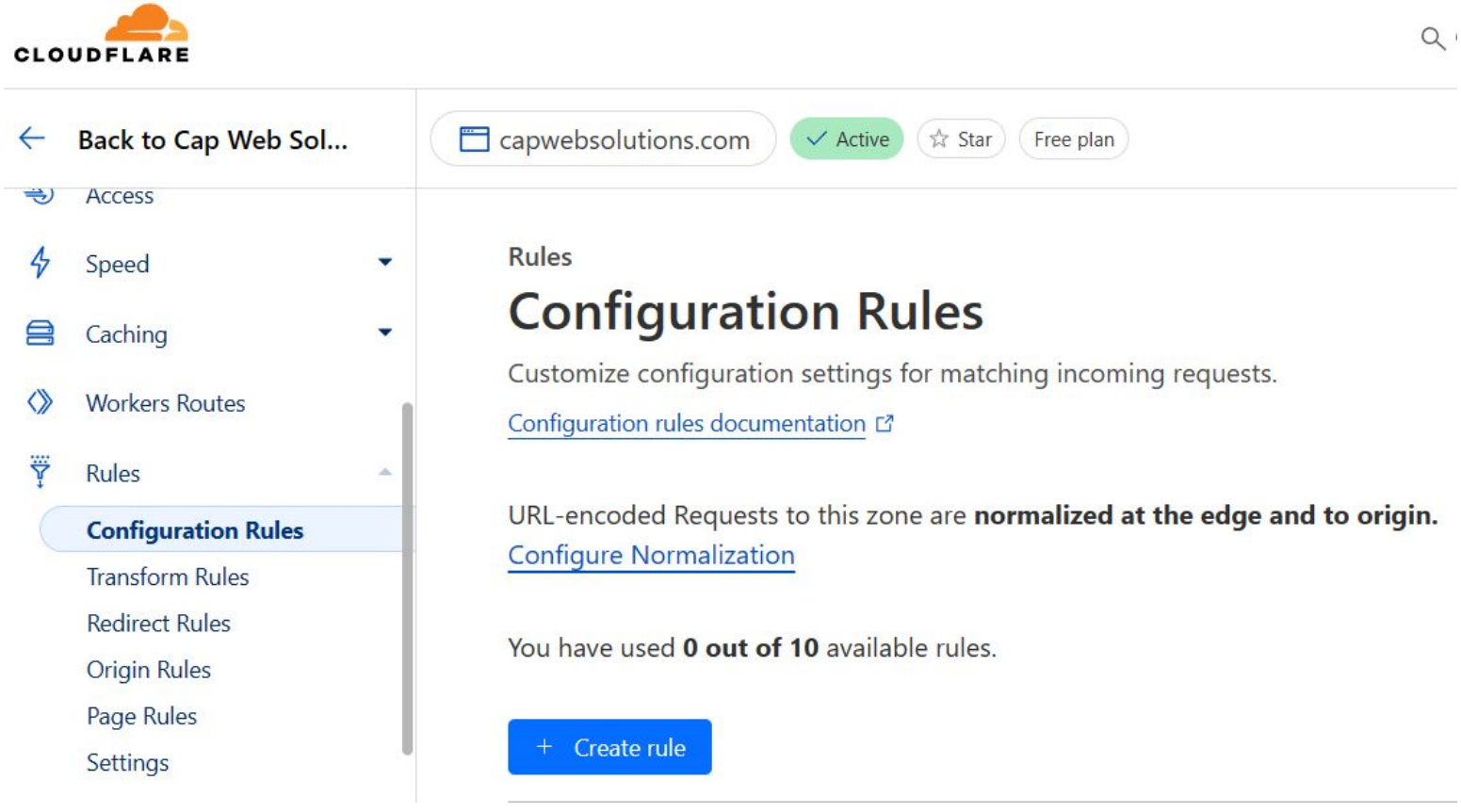
[Return]

Nginx Conf file for Content Security Headers

```
set $CSP "script-src 'self' 'unsafe-inline' 'unsafe-eval' https://*.googletagmanager.com https://cdn.us
set $CSP "${CSP}; connect-src 'self'  https://*.google-analytics.com https://*.analytics.google.com htt
set $CSP "${CSP}; style-src 'self' 'unsafe-inline' https://code.ionicframework.com  https://static.mail
set $CSP "${CSP}; font-src 'self' https://code.ionicframework.com data:";
set $CSP "${CSP}; img-src 'self' https://cdn.usefathom.com https://*.google-analytics.com https://*.ana
set $CSP "${CSP}; frame-src 'self'  https://capwebsolutions.freshdesk.com https://*.cloudflare.com ";
set $CSP "${CSP}; default-src 'self' https://cdn.usefathom.com https://*.wp.com  https://static.cloudfl
add_header Content-Security-Policy $CSP;
```

Return

Cloudflare Rules UI



Return

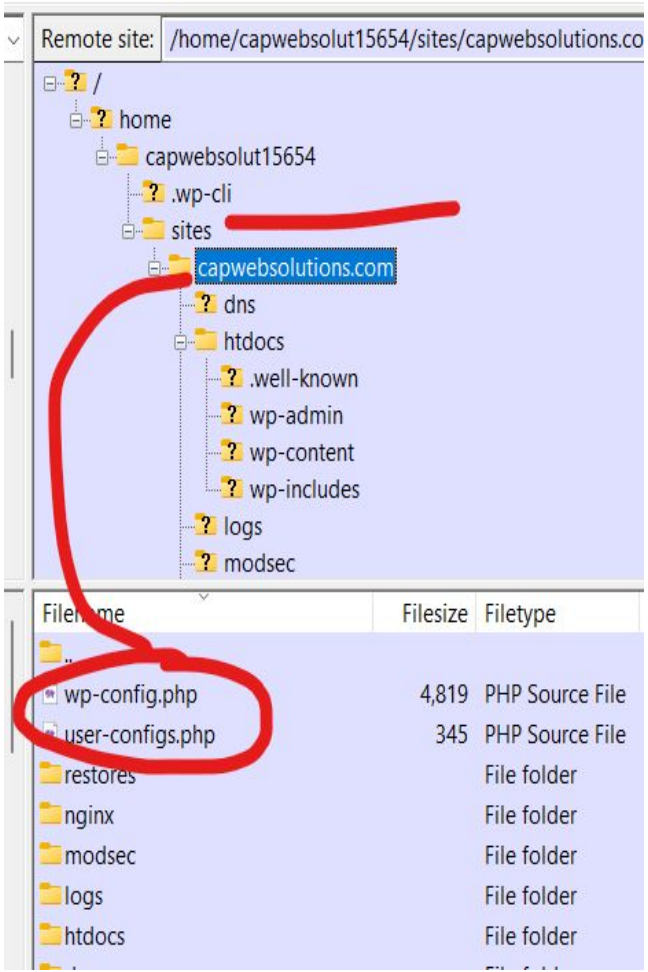
wp-config.php Relocated

Here we see an example from my Gridpane hosting management panel.

The root is sites/capwebsolutions.com

WordPress is installed at /htdocs

wp-load.php instructs WP on how to find the configuration file.



Return