SAMPLE SITE

Site Audit Report

http://www.sampleproject.com

Table Of Contents

Site Audit Report Checklist

General Items

PASS	Site free of malware (Website scan)
PASS	Google Transparency Report
PASS	Site not listed on blacklists
FIXED	404 Page Detection
PASS	Suspicious Logins Scan

FIXED	Copyright Information
FIXED	Avoiding Comment Spamming
FIXED	Captcha Validation
FIXED	File Change Detection
FIXED	File Permissions
FIXED	Redirect All HTTP Page Requests to HTTPS

Security Tools & Parameters

FIXED	Two-Factor Authentication
FIXED	Privilege Escalation
FAIL	Away Mode

FIXED	Network Brute Force Protection
FIXED	Trusted Devices
FIXED	Local Brute Force Protection

WordPress Core Inspection

FIXED	No publicly available logs
FIXED	No public PHPinfo files
FIXED	Code Review
FIXED	WordPress Core Updated
FIXED	Protecting System Files
FIXED	Directory Browsing

FIXED	Filter Suspicious Query Strings in the URL
FIXED	Filter Non-English Characters
FIXED	Filter Long URL Strings
FIXED	Remove File Writing Permissions
FIXED	Disable PHP in Uploads
FIXED	Reduce Comment Spam
FIXED	Disable File Editor in WordPress Admin

Themes and Plugins

PASS	Only utilized themes installed
FIXED	All themes updated & actively maintained
FIXED	Theme core files unmodified
PASS	No high-risk theme functions installed

FIXED	Only utilized plugins installed
FIXED	All plugins updated & actively maintained
PASS	No high-risk plugins installed
PASS	No redundant plugins
FIXED	Validation of Contact Form

Administrative and General User Accounts

FAIL	Valid administrative users
PASS	Password audit
PASS	PASS Unique ID for administrators
FIXED	Remove the default admin
PASS	No Extraneous admin users
🟩	

	No public transaction or error logs
FIXED	Banned Users Management
FIXED	User Logging
FIXED	User Security Check
FAIL	Passwordless Login

Hosting Issues

FIXED	Backups being stored
PASS	No publicly accessible backups
PASS	No credit card data stored on site

FIXED	PHP version updated
PASS	No suspicious cron jobs
PASS	Strong CPANEL/Hosting Password
PASS	Strong FTP Password

Database

FIXED	Database Backups
PASS	Only one MySQL database user
FIXED	MySQL user has appropriate permissions
PASS	Strong MySQL database user password

PASS	Remote database access disabled
PASS	No custom MySQL database connections
PASS	PhpMyAdmin updated
PASS	Tables are optimized
FIXED	WordPress database table prefix

Speed & Performance

FIXED	Image Optimization
FIXED	Cache Management
FIXED	Lazyload
FIXED	Minification
FIXED	Combine CSS & JavaScript files
FIXED	Google Fonts Optimization

	Database Optimization
FIXED	Remove Query Strings from Static Resources
FIXED	Defer JS Loading
FIXED	CDN
FIXED	Speed Score Optimization

Failure/Fixed Action Items

General Items

❑ **404 Page Detection.** Fixed

404 Detection functionality has been added to the website so that a user or host hitting multiple 404 page would be banned from accessing the website.

❑ **Copyright Information.** Fixed

Copyright information is updated on the website footer.

❑ **Avoiding Comment Spamming.** Fixed

All spam comments have been removed from website blog. We have setup a couple of tools which shall help us reduce the amount of generic spam.

> **Note**: If required, we can completely disable the default commenting feature on the website blog.

❑ **Captcha Validation.** Fixed

We have protected your website from bots by verifying that the person submitting comments or logging in is indeed human. We have used reCaptcha V3 invisible via API integration.

❑ **File Change Detection .** Fixed

We have added File Change Detection so that admin will get notifications if there is a file on ftp gets changed. This shall help admin users to read log to troubleshoot certain things on the website.

❑ **File Permissions.** Fixed

We have setup appropriate permissions to file and directories on the site.

❑ **Redirect All HTTP Page Requests to HTTPS.** Fixed

The site is configured with a valid certificate and we setup to redirects all http traffic to your site to the https address, thus requiring everyone to access the site via SSL. In other words, we are forcing everyone to use a secure connection to the site.

Security Tools & Parameters

❑ **Two-Factor Authentication.** Fixed

An additional layer of security have been added to the login section of your website. User need to provide a ONE TIME PASSWORD (OTP) to gain access to the admin dashboard. The OTP is sent to the email id associated with the user account. Users can visit their profile to enable/manage this two-factor authentication feature for their account. Or admin can also generate backup codes to get access.

❑ **Privilege Escalation.** Fixed

Added a feature to allow administrators to temporarily grant extra access to a user of the site for a specified period of time. For example, a contractor can be granted developer access to the site for 24 hours after which his or her status would be automatically revoked.

❑ **Away Mode.** Fail Client's Attention Required

We recommend to setup an **AWAY MODE** so that you can disable your administrative panel during off business hours.

> ***Note:*** *Please let us know if we should go ahead and set it up. Please suggest the exact timings for the same.*

❑ **Network Brute Force Protection.** Fixed

The network protection will automatically report the IP addresses of failed login attempts and will block them for a length of time necessary to protect your site based on the number of other sites that have seen a similar attack.

❑ **Trusted Devices.** Fixed

We have added a function to set trusted devices in the admin site so that it identifies the devices users use to login and can apply additional restrictions to unknown devices.

❑ **Local Brute Force Protection.** Fixed

We have protected your site against attackers that try to randomly guess login details to your site. We are banning the host user from attempting to login again after the specified bad login threshold has been reached.

WordPress Core Inspection

❑ **No publicly available logs.** Fixed

We have setup the website so that there are no logs available to a default URL on the website to avoid any threat.

❑ **No public PHPinfo files.** Fixed

We made sure there is no PHP information file available at the FTP so that no one get access to the system information from the website.

❑ **Code Review.** Fixed

Code review of framework files have been completed.

> **No script/code injection or unwanted customization noticed.**

❑ **WordPress Core Updated.** Fixed

WordPress Core Framework has been upgraded to Version 5.4.2

❑ **Protecting System Files.** Fixed

We are now protecting default framework system files from public access**.**

❑ **Directory Browsing.** Fixed

We are now hiding directory browsing in case an index file is not present in a folder.

❑ **Filter Suspicious Query Strings in the URL.** Fixed

We are now blocking suspicious query strings to be executed in the URL as these are very often signs of someone trying to gain access to your site. However, in some cases some plugins and themes can also be blocked. We strongly recommend not to use these plugins as they can remain vulnerable.

❑ **Filter Non-English Characters.** Fixed

We are now filtering out non-english characters from the query string.

❑ **Filter Long URL Strings.** Fixed

We are now limiting the number of characters that can be sent in the URL. Hackers often take advantage of long URLs to try to inject information into your database.

❑ **Remove File Writing Permissions.** Fixed

We are now disabling the system files *(wp-config.php file and .htaccess file)* to be writable and preventing scripts and users from being able to access them.

❑ **Disable PHP in Uploads.** Fixed

We are now disable PHP execution in the uploads directory to eliminate any suspicious php file upload via a plugin or a comments section.

❑ **Reduce Comment Spam.** Fixed

We have setup the configurations to cut down on comment spam.

❑ **Disable File Editor in WordPress Admin.** Fixed

We are now hiding the file editor that is available by default in the admin dashboard to avoid unwanted injections or mistakes while editing them online.

Themes and Plugins

❑ **All themes updated & actively maintained.** Fixed

- Default theme (**2020**) have been upgraded to its latest version.
- Current ACTIVE theme (**Enfold**) is stable and working as expected.

❑ **Theme core files unmodified.** Fixed

Active theme has been tested and found no visible alterations to the core files.

❑ **Only utilized plugins installed.** Fixed

No extraneous plugins found installed on the website. The scan is completed.

❑ **All plugins updated & actively maintained.** Fixed

Following plugins have been upgraded to their respective latest versions:

- **Contact Form 7** - Upgraded from version 5.1.9 to 5.2.
- **iThemes Security Pro** - Upgraded from version 6.6.0 to 6.6.1.
- **MC4WP: Mailchimp for WordPress** - Upgraded from version 4.7.8 to 4.8.
- **NextScripts: Social Networks Auto-Poster** - Upgraded from version 4.3.15 to 4.3.16.
- **Smash Balloon Instagram Feed** - Upgraded from version 2.4.4 to 2.4.5.
- **WooCommerce** - Upgraded from version 4.2.2 to 4.3.1.
- **WPBakery Visual Composer** - Upgraded from version 5.0.1 to 6.2.
- **WP Rocket** - Upgraded from version 3.6.1 to 3.6.2.1.
- **Yoast SEO** - Upgraded from version 14.4.1 to 14.6.1.

❑ Validation of Contact Form. Fixed

We have validated configuration in all forms which have been created using CONTACT FORM 7 plugin. No invalid contact form was found.

Administrative and General User Accounts

❑ Valid administrative users. Fail

Please log in to your admin dashboard and validate the following administrative user accounts:

- **Test user** - not active since last 1 year

❑ Remove the default admin. Fixed

We found an admin username of "admin" or a user ID of "1". We renamed the username and its ID in the database to safeguard the user login section.

❑ No public transaction or error logs. Fixed

Scanned to make sure no public transaction or error logs available that might provide attackers information about your site configuration.

❑ Banned Users Management. Fixed

A new functionality for managing banned users has been added to the website. Admin can login and manage users who are listed as banned or add new hosts/IPs in the banned user list. Any IP addresses or user agents found in the lists below will not be allowed any access to your site. We have also enabled HackRepair.com blacklist feature which include the blacklist developed by Jim Walker.

❑ User Logging. Fixed

We have logged user actions such as login, saving content and others.

❑ User Security Check. Fixed

We have added a tool where you can check all logged-in users and manage their login status and verify their activities.

❑ Passwordless Login. Fail Client's Attention Required

Password-less Login feature can be added to your admin site which will help you log in bypassing the password and Two-Factor requirements. You shall receive an email with a special login link from the WordPress login page

> **Note:** Please provide an SMTP account (basically an email id login) that we can use to send out emails from website. Website need to send emails with OTP to the users for which it needs to send email smoothly.

Hosting Issues

❑ Backups being stored. Fixed

We have saved a current backup of the files on the hosting server and our local archives. We have also setup scheduled a weekly backups.

❑ PHP version updated. Fixed

Your site was running on an insecure version of PHP.

> We upgraded the PHP version to the latest stable available and tested the website to make sure it is compatible with the latest version of PHP.

Database

❑ Database Backups. Fixed

We have saved a current backup of the database on the hosting server and our local archives. We have also scheduled a DB backup.

❑ MySQL user has appropriate permissions. Fixed

We ensured the MySQL database user has appropriate permissions to access and modify the database.

❑ WordPress database table prefix. Fixed

Database tables are not using WordPress default prefix.

Speed & Performance

❑ Image Optimization. Fixed

- We are automatically optimizing and compressing the images that you will upload from now on.
- We have detected unnecessarily large oversized images on your website and reduced their size to improve **load time.** The optimized images include the original uploads and the various sizes created by WordPress System.
- Our system have also checked which PNG files can be converted to JPG for fast loading and converted them to JPGs. We ignored the PNG files with transparent properties.

Total Savings
450 MB

Total Images Optimized
212

❑ Cache Management. Fixed

Caching creates an ultra-fast load time, essential for improving Search Engine Optimization and increasing conversions.

- We activated page caching on your website and preloading all the URLs to ensure that your site's cache is always warm.
- We optimized your website to speed up your site for mobile visitors.
- Optimized the rendering of web browsers and save bandwidth, we facilitated the work of the browser (gzip compression, expires headers, etags).
- We have set up the browser caching so that static contents (JS, CSS, images) are stored in the browser. When a visitor goes to another page on your website, your static content does not need to be loaded again.
- We are hosting your Google scripts locally on your server to help satisfy the Page Speed recommendation for Leverage browser caching.

❑ Lazyload. Fixed

We have set up the Lazy Load on your website so that images are loaded only as your visitor scrolls down the page, improving the load time of the page. YouTube, Facebook, Yahoo and other major websites are using this technique. Now yours can too.

❑ Minification. Fixed

We reduced the weight of your HTML, JavaScript and CSS files through minification. Lighter files means faster load time! Minifying HTML, CSS and JS, removes white space and comments to reduce the size.

❑ Combine CSS & JavaScript files. Fixed

We combined JavaScript and CSS files of your website's internal, 3rd party and inline JS reducing HTTP requests.

❑ Google Fonts Optimization. Fixed

We optimized fonts used on the website (thanks to Google Fonts Optimization) to reduce HTTP requests for a faster website.

❑ Database Optimization. Fixed

We cleaned up your database to remove bloat and reduce its size, boosting your site's performance. We also schedule regular clean-ups to keep things running smoothly.

❑ Remove Query Strings from Static Resources. Fixed

We improved your GT Metrix grade by removing query strings from CSS/JS files. Cache busting is retained by encoding the version number into the URL.

❑ Defer JS Loading. Fixed

We ensured that the JavaScript files are loaded after the end of the rendering of the page. Thus, the loading time of your website will be reduced.

❑ CDN. Fixed

We have successfully set up **CDN (Content Delivery Network)** on your website via your current hosting provider to speed up your website. Now your website is loading various assets from a third party URL resulting less loading time.

❑ Speed Score Optimization. Fixed

We perform lossless **image optimization** throughout the website, manage your **website cache**, **Minifying** scripts and styles, **File optimization** and perform various **compression techniques** to improve page speed.

These scores tell you how well your front-end is optimized for loading time.

Google Page Speed Grade

A (93%)

Previous: 44%

Yahoo! YSlow Grade

B (89%)

Previous: 32%

Page load time: 2s ▼ (previous: 7s)
Total page size: 1.9MB ▼ (previous: 8.9MB)
Total number of requests: 22 ▼ (previous: 75)

Security Elements Reviewed

General Items

- **Site free of malware (Website scan).**

  Scans the website to look for malware, backdoors, trojans, or other malicious and suspicious scripts. We check for known malware, blacklisting status, website errors, and out-of-date software. We do this malware scan using **Sucuri SiteCheck** which is the most reliable and stable scanning tool. Although the **Sucuri team** does its best to provide the best results, 100% accuracy is not realistic and is not guaranteed.

- **Google Transparency Report.**

  Google safe browsing transparency report can often indicate problems. We scan the domain for safe browsing at Google. Domain clean by Google Safe Browsing, Norton Safe Web, McAfee, Sucuri, ESET, PhishTank, Yandex, Opera, Spamhaus

- **Site not listed on blacklists.**

  We review the following blacklists to ensure your site is not listed:
  - McAfee Site Advisor
  - Norton SafeWeb

    etc.

- **404 Page Detection.**

  Our 404 detection looks at a user who is hitting a large number of non-existent pages and getting a large number of 404 errors. 404 detection assumes that a user who hits a lot of 404 errors in a short period of time is scanning for something (presumably a vulnerability) and locks them out accordingly. This also gives the added benefit of helping you find hidden problems causing 404 errors on unseen parts of your site. All errors will be logged in the "**View Logs**" section.

- **Suspicious Logins Scan.**

  We look for logins that appear to be from suspicious locations.

- **Copyright Information.**

  Check the copyright information is updated on the website footer.

- **Avoiding Comment Spamming.**

  Check to make sure necessary action steps taken to minimize the comment spamming.

- **Captcha Validation.**

  Protecting your site from bots by verifying that the person submitting comments or logging in is indeed human. Results of previous malware scans can be found on the logs page.

- **File Change Detection .**

  Even the best security solutions can fail. How do you know if someone gets into your site? You will know because they will change something. File Change detection will tell you what files have changed in your WordPress installation alerting you to changes not made by yourself.

- **File Permissions.**

  Lists file and directory permissions of key areas of the site.

- **Redirect All HTTP Page Requests to HTTPS.**

  SSL is an important feature for every site. It protects user accounts from being compromised, protects the content from modifications by ISPs and attackers, protects potentially-sensitive information submitted to the site from network sniffing, could speed up performance of your site (depending on server configuration), and could improve your site search engine rankings. Your site might support SSL. If the site is configured with a valid certificate that is not self-signed, it is highly recommended that you redirects all http traffic to your site to the https address, thus requiring everyone to access the site via SSL. In other words, it will force everyone to use a secure connection to the site.

Security Tools & Parameters

- **Two-Factor Authentication.**

  Two-Factor Authentication greatly increases the strength of a user account by requiring a secondary code in addition to a username and password when logging in. Once Two-Factor Authentication is enabled here, users can visit their profile to enable two-factor for their account. The following settings allow you to enforce the use of two-factor on accounts based on different criteria.

- **Privilege Escalation.**

  Enabling this feature will allow administrators to temporarily grant extra access to a user of the site for a specified period of time. For example, a contractor can be granted developer access to the site for 24 hours after which his or her status would be automatically revoked.

- **Away Mode.**

  As most sites are only updated at certain times of the day it is not always necessary to provide access to the WordPress dashboard 24 hours a day, 7 days a week. The options below will allow you to disable access to the WordPress Dashboard for the specified period. In addition to limiting exposure to attackers this could also be useful to disable site access based on a schedule for classroom or other reasons.

- **Network Brute Force Protection.**

  Local brute force protection looks only at attempts to access your site and bans users per the lockout rules specified locally. Network brute force protection takes this a step further by banning users who have tried to break into other sites from breaking into yours. The network protection will automatically report the IP addresses of failed login attempts and will block them for a length of time necessary to protect your site based on the number of other sites that have seen a similar attack.

- **Trusted Devices.**

  Trusted Devices identifies the devices users use to login and can apply additional restrictions to unknown devices.

- **Local Brute Force Protection.**

  Protect your site against attackers that try to randomly guess login details to your site. If one had unlimited time and wanted to try an unlimited number of password combinations to get into your site they eventually would, right? This feature will ban the host user from attempting to login again after the specified bad login threshold has been reached.

WordPress Core Inspection

- **No publicly available logs.**

  We make sure there are no logs available to a default URL on the website.

- **No public PHPinfo files.**

  We make sure there is no PHPinfo file available at the FTP

- **Code Review.**

  We review the WordPress Core files and database for any unwanted customization. Customization to core files are never recommended because they get overwritten on software upgrades.

- **WordPress Core Updated.**

  Make sure the core WordPress framework is up-to date after due stability tests.

- **Protecting System Files.**

  Prevent public access to readme.html, readme.txt, wp-config.php, install.php, wp-includes, and

.htaccess. These files can give away important information on your site and serve no purpose to the public once WordPress has been successfully installed.

- **Directory Browsing.**

  Prevents users from seeing a list of files in a directory when no index file is present.

- **Filter Suspicious Query Strings in the URL.**

  These are very often signs of someone trying to gain access to your site but some plugins and themes can also be blocked.

- **Filter Non-English Characters.**

  Filter out non-english characters from the query string. This should not be used on non-english sites and only works when "Filter Suspicious Query String" has been selected.

- **Filter Long URL Strings.**

  Limits the number of characters that can be sent in the URL. Hackers often take advantage of long URLs to try to inject information into your database.

- **Remove File Writing Permissions.**

  Prevents scripts and users from being able to write to the wp-config.php file and .htaccess file. Note that in the case of this and many plugins this can be overcome however it still does make the files more secure. Turning this on will set the UNIX file permissions to 0444 on these files and turning it off will set the permissions to 0664.

- **Disable PHP in Uploads.**

  Disable PHP execution in the uploads directory. This blocks requests to maliciously uploaded PHP files in the uploads directory.

- **Reduce Comment Spam.**

  This option will cut down on comment spam by denying comments from bots with no referrer or without a user-agent identified.

- **Disable File Editor in WordPress Admin.**

  Disables the file editor for plugins and themes requiring users to have access to the file system to modify files. Once activated you will need to manually edit theme and other files using a tool other than WordPress.

Themes and Plugins

- **Only utilized themes installed.**

  We recommend that you do not have extraneous themes installed.

- **All themes updated & actively maintained.**

  We check to ensure that the theme(s) installed are updated and are actively maintained by their developers.

- **Theme core files unmodified.**

  Modifying theme files is not recommended. If you need to make changes, use a child theme.

- **No high-risk theme functions installed.**

  We look for high risk theme functionality such as uploading scripts, remote tunnel access, etc.

- **Only utilized plugins installed.**

  We recommend that you do not have extraneous plugins installed.

- **All plugins updated & actively maintained.**

We check to ensure that all plugins, both premium and repository, are updated to the current versions. We check to see if plugin development appears to be abandoned. We check to ensure installed plugins have been updated in the last 2 years.

- **No high-risk plugins installed.**

  We look for functions within plugins that might allow for uploading, administrative tunnels, etc.

- **No redundant plugins.**

  We look for plugins that may have overlapping functionality.

- **Validation of Contact Form.**

  Validating various forms which have been created using CONTACT FORM 7 plugin.

Administrative and General User Accounts

- **Valid administrative users.**

  We check to see that administrative users appear to be valid.

- **Password audit.**

  We check to see that all passwords appear to be strong and unique.

- **PASS Unique ID for administrators.**

  We evaluate whether administrators appear to have unique user IDs and that logins are not shared. Each user should have their own login for PCI compliance.

- **Remove the default admin.**

  We highly recommend to remove users with a username of "admin" or a user ID of "1".

- **No Extraneous admin users.**

  We check to see if there are an inordinate number of administrative users. We recommend limiting administrative access and using contributor, editor, store manager, and other user types.

- **No public transaction or error logs.**

  We check for any public transaction or error logs that might provide attackers information about your site configuration.

- **Banned Users Management.**

  This feature allows you to completely ban hosts and user agents from your site without having to manage any configuration of your server. Any IP addresses or user agents found in the lists below will not be allowed any access to your site.

- **User Logging.**

  Log user actions such as login, saving content and others.

- **User Security Check.**

  Every user on your site affects overall security. See how your users might be affecting your security and take action when needed.

- **Passwordless Login.**

  This login method is called Password-less Login which is used to login bypassing the password and Two-Factor requirements. You can request to receive an email with a special login link from the WordPress login page. This email shall contain a link that will take you to the admin dashboard. Alternatively, you can also login with a password that you set for your login just in case the email takes time to reach you for certain reasons.

Hosting Issues

- **Backups being stored.**

  We look for evidence that backups are being made of your site.

- **No publicly accessible backups.**

  We look for publicly available backups that might contain sensitive site information.

- **No credit card data stored on site.**

  We look for evidence of credit card information stored on your site or in your database.

- **PHP version updated.**

  We look to see that the server is running an updated version of PHP.

- **No suspicious cron jobs.**

  We look for suspicious cron jobs.

- **Strong CPANEL/Hosting Password.**

  We evaluate whether the hosting panel password is strong and appears to be unique from other passwords.

- **Strong FTP Password.**

  We check to see if the FTP password is strong and appears to be unique from other passwords.

Database

- **Database Backups.**

  One of the best ways to protect yourself from an attack is to have access to a database backup of your site. If something goes wrong, you can get your site back by restoring the database from a backup and replacing the files with fresh ones. Use the button below to create a backup of your database for this purpose. You can also schedule automated backups and download or delete previous backups.

- **Only one MySQL database user.**

  We look for extra MySQL database users.

- **MySQL user has appropriate permissions.**

  We ensure the MySQL database user has appropriate permissions to access and modify the database.

- **Strong MySQL database user password.**

  We evaluate the MySQL database userâ€™s password.

- **Remote database access disabled.**

  We look for remote database access capabilities on your site.

- **No custom MySQL database connections.**

  We review the site code to look for any extraneous database connections.

- **PhpMyAdmin updated.**

  We determine if the hostâ€™s version of PhpMyAdmin does not have security issues.

- **Tables are optimized.**

  We check to see if database tables require optimization.

- **WordPress database table prefix.**

  We ensure that database tables are not using WordPress default prefix.

Speed & Performance

- **Image Optimization.**

  When you upload images to your site, we will automatically optimize and compress them for you. We detect unnecessarily large oversize images on your website to reduce their size and decrease **load times** that includes the original uploads and the various sizes created by WordPress System. We do it via our Bulk Optimizer. Our system will also check which PNG files can be converted to JPG for fast loading and convert them. We ignore the PNG files with transparent properties.

- **Cache Management.**

  Caching creates an ultra-fast load time, essential for improving Search Engine Optimization and increasing conversions. We activate page caching on your website and preload all the URLs to ensure that your site's cache is always warm.

  We speed up your site for mobile visitors.

  To optimize the rendering of web browsers and save bandwidth, we facilitate the work of the browser (gzip compression, expires headers, etags).

  With browser caching, static contents (JS, CSS, images) are stored in the browser. When a visitor goes to another page on your website, your static content does not need to be loaded again. We will host your Google scripts locally on your server to help satisfy the Page Speed recommendation for Leverage browser caching.

- **Lazyload.**

  We set up the Lazy Load on your website so that images are loaded only as your visitor scrolls down the page, improving the load time of the page. YouTube, Facebook, Yahoo and other major websites are using this technique. Now yours can too.

- **Minification.**

  We reduce the weight of your HTML, JavaScript and CSS files through minification. Lighter files means faster load time! Minifying HTML, CSS and JS, removes whitespace and comments to reduce the size.

- **Combine CSS & JavaScript files.**

  We combine JavaScript and CSS files of your website's internal, 3rd party and inline JS reducing HTTP requests.

- **Google Fonts Optimization.**

  We optimize fonts used on the website (thanks to Google Fonts Optimization) to reduce HTTP requests for a faster website.

- **Database Optimization.**

  We clean up your database to remove bloat and reduce its size, boosting your site's performance. We also schedule regular clean-ups to keep things running smoothly.

- **Remove Query Strings from Static Resources.**

  We improve your GT Metrix grade by removing query strings from CSS/JS files. Cache busting is retained by encoding the version number into the URL.

- **Defer JS Loading.**

  We ensure that the JavaScript files are loaded after the end of the rendering of the page. Thus, the loading time of your website will be reduced.

- **CDN.**

  We shall assist you in setting up **CDN (Content Delivery Network)** to speed up your website. Some hosting providers already provide this facility. We will help you figure out what and how to perform this activity.

- **Speed Score Optimization.**

PageSpeed and **YSlow** focus on the front-end performance of your website – including elements that are largely in your control, like images, files and general site structure. These scores tells you how well your front-end is optimized for loading time. We perform lossless image optimization throughout the website, manage your website cache, Minifying scripts and styles, File optimization and perform various compression techniques to improve page speed.