Overall data for: http://structuralfire.com

Your SEO Score is **53/100**

- **26 Passed Checks**
- **21 Failed Checks**
- **2 Warnings**

Title Tag

The **title** tag is required in all HTML documents and it defines the title of the document. This tag displays the page title in browsers toolbar and in the search-engine results (SERPs). It also provides a title for the page when it is added to favorites. A descriptive **title** tag is important in helping search engines determine your web page's relevancy for certain keywords.

The meta title of your page has a length of 56 characters. Most search engines will truncate meta titles to 70 characters.

> Structural Fire Safety Engineering - Bogazici University

Meta Description

The meta description tag is meant to be a short and accurate summary of your page content. This description can affect your search engine rankings and can also show up directly in search engine results (and affect whether or not the user clicks through to your site).

> The meta-description tag is missing from your page. You should include this tag in order to provide a brief description of your page which can be used by search engines or directories.

HOW TO FIX

In order to pass this test you must include a meta-description tag in your page header (**<head>** section):

```
<head>
 <meta name="description" content="type_your_description_here">
</head>
```

Note that in HTML the **<meta>** tag has no end tag but in XHTML this tag must be properly closed. Meta description can have any length but a good practice is to keep this under 160 characters (search engines generally truncate snippets longer than this value).

Google Search Results Preview

Check how your page might look in the Google search results page (SERP's). A Google search result uses your webpage title, URL, and meta-description in order to display relevant summarized information about your site. If these elements are too long, Google will truncate their content, so you are advised to set your webpage title under 70 characters and your webpage description under 160 characters in order to optimize readability.

Structural Fire Safety Engineering - Bogazici University
http://structuralfire.com/

Most Common Keywords Test

Check the most common keywords and their usage (number of times used) on your web page.

There is likely no optimal keyword density (search engine algorithms have evolved beyond keyword density metrics as a significant ranking factor). It can be useful, however, to note which keywords appear most often on your page and if they reflect the intended topic of your page. More importantly, the keywords on your page should appear within natural sounding and grammatically correct copy.

- research - 22 times
- selamet - 19 times
- serdar - 19 times
- related - 15 times
- website - 15 times

Keyword Usage

This describes if your most common keywords are used in your page title and meta-description.

Your most common keywords are not appearing in one or more of the meta-tags above. Your primary keywords should appear in your meta-tags to help identify the topic of your webpage to search engines.

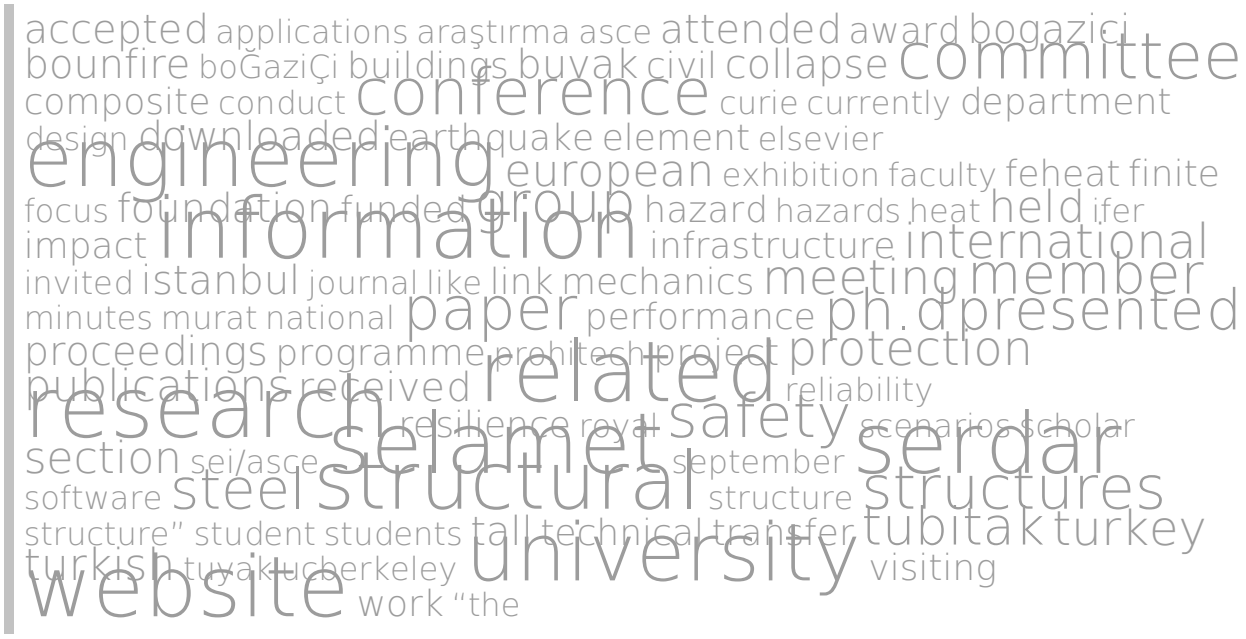
- Keyword(s) not included in Meta-Title
- Keyword(s) not included in Meta-Description

HOW TO FIX

First of all, you must make sure that your page is using the title and meta-description tags. Second, you must adjust these tags content in order to include some of the primary keywords displayed above.

Keywords Cloud

The Keyword Cloud is a visual representation of keywords used on your website. This will show you which words are frequently used in the content of your webpage. Keywords having a higher density are presented in larger fonts and displayed in an alphabetic order.



<h1> Headings Status

This indicates if any H1 headings are used in your page. H1 headings are HTML tags than can help emphasize important topics and keywords within a page.

Your page contains H1 headings. Their contents are listed below:

> Glosey

<h2> Headings Status

This indicates if any H2 headings are used in your page. H2 headings can be helpful for describing the sub-topics of a page.

Your page does not contain any H2 headings. H2 headings help describe the sub-topics of your webpage to search engines. While less important than good meta-titles and descriptions, H1 and H2 headings may still help define the topics of your page to search engines.

HOW TO FIX

In order to pass this test you must indentify the most important sub-topics from your page and insert those sub-topics between `<h2>...</h2>` tags.
Example:

```
<h2>First sub-topic goes here</h2>
...
<h2>Another sub-topic</h2>
```

Robots.txt Test

Check if your website is using a robots.txt file. Search engines send out tiny programs called spiders or robots to search your site and bring information back so that your pages can be indexed in the search results and found by web users. If there are files and directories you do not want indexed by search engines, you can use the "robots.txt" file to define where the robots should not go.
These files are very simple text files that are placed on the root folder of your website: www.yourwebsite.com/robots.txt.
There are two important considerations when using "robots.txt":
- the "robots.txt" file is a publicly available file, so anyone can see what sections of your server you don't want robots to use;
- robots can ignore your "robots.txt", especially malware robots that scan the web for security vulnerabilities;

Your site lacks a "robots.txt" file. This file can protect private content from appearing online, save bandwidth, and lower load time on your server. A missing "robots.txt" file also generates additional errors in your apache log whenever robots request one. Read more about the robots.txt file, and how to create one for your site.

HOW TO FIX

In order to pass this test you must create and properly install a **robots.txt** file.
For this, you can use any program that produces a text file or you can use an online tool (Google Webmaster Tools has this feature).
Remember to use all lower case for the filename: **robots.txt**, not **ROBOTS.TXT**.
A simple **robots.txt** file looks like this:

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /images/
Disallow: /pages/thankyou.html
```

This would block all search engine robots from visiting "cgi-bin" and "images" directories and the page "http://www.yoursite.com/pages/thankyou.html"

TIPS:

- You need a separate **Disallow** line for every URL prefix you want to exclude
- You may not have blank lines in a record because they are used to delimit multiple records
- Notice that before the **Disallow** command, you have the command: **User-agent: ***. The **User-agent:** part specifies which robot you want to block. Major known crawlers are: Googlebot (Google), Googlebot-Image (Google Image Search), Baiduspider (Baidu), Bingbot (Bing)
- One important thing to know if you are creating your own **robots.txt** file is that although the wildcard (*) is used in the **User-agent** line (meaning "any robot"), it is not allowed in the **Disallow** line.

- Regular expressions are not supported in either the **User-agent** or **Disallow** lines

Once you have your **robots.txt** file, you can upload it in the top-level directory of your web server. After that, make sure you set the permissions on the file so that visitors (like search engines) can read it.

Sitemap Test

This test will check if your website is using a "sitemap" file: sitemap.xml, sitemap.xml.gz or sitemapindex.xml.
Sitemaps are an easy way for webmasters to inform search engines about pages on their sites that are available for crawling. In its simplest form, a sitemap is an XML file that lists URLs for a site along with additional metadata about each URL (when it was last updated, how often it usually changes, and how important it is, relative to other URLs in the site) so that search engines can more intelligently crawl the site.

Your site lacks a sitemap file. Sitemaps can help robots index your content more thoroughly and quickly. Read more on Google's guidelines for implementing the sitemap protocol.

HOW TO FIX

In order to pass this test you must create a sitemap.xml file for your website. Some of the best practices are listed below:

- It is strongly recommended that you place your sitemap at the root directory of your website: **http://yourwebsite.com/sitemap.xml** But in some situations, you may want to produce different sitemaps for different paths on your site (e.g., security permission issues)
- Sitemaps should be no larger than 10MB (10,485,760 bytes) and can contain a maximum of 50,000 URLs. This means that if your site contains more than 50,000 URLs or your sitemap is bigger than 10MB, you must create multiple sitemap files and use a **Sitemap index file**
- All URLs listed in the sitemap must reside on the same host as the sitemap. For instance, if the sitemap is located at **http://www.yourwebsite.com/sitemap.xml**, it can't include URLs from **http://subdomain.yourwebsite.com**
- Once you have created your sitemap, let search engines know about it by submitting directly to them, pinging them, or adding the sitemap location to your **robots.txt** file
- Sitemaps can be compressed using gzip, reducing bandwidth consumption

sitemap.xml example:

```
<?xml version="1.0" encoding="UTF-8"?>
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
<url>
 <loc>http://www.yourwebsite.com</loc>
 <lastmod>2013-01-01</lastmod>
 <changefreq>weekly</changefreq>
 <priority>0.9</priority>
</url>
<url>
 <loc>http://www.yourwebsite.com/articles/100</loc>
 <changefreq>weekly</changefreq>
</url>
<url>
 <loc>http://www.yourwebsite.com/articles/101</loc>
 <lastmod>2013-01-02</lastmod>
 <changefreq>weekly</changefreq>
</url>
```

```
<url>
 <loc>http://www.yourwebsite.com/articles/102</loc>
 <lastmod>2013-01-02T13:00:12+00:00</lastmod>
 <priority>0.5</priority>
</url>
</urlset>
```

Broken Links Test

Check your website for broken or dead links. This tool scans your website to locate internal and external broken links that are not only frustrating to your visitors, but damaging to your websites overall ranking with the major search engines.

From 50 distinct anchor links analyzed, none of them appear to be broken.

Underscores in Links Test

Check your URL internal links for underscore characters. Google's suggestions for URL structure specify using hyphens or dashes (-) rather than underscores (_). Unlike underscores, Google treats hyphens as separators between words in a URL.

Congratulations! We have not found underscores in your in-page URLs!

Image Alt Test

Check images on your webpage for required alt attributes. If an image cannot be displayed (wrong source, slow connection, etc), the alt attribute provides alternative information. Using keywords and human-readable captions in the alt attributes is a good SEO practice because search engines cannot really see the images. For images with a decorative role (bullets, round corners, etc) you are advised to use an empty alt or a CSS background image.

Your webpage has **28** 'img' tags and none of them contain the required 'alt' attribute.

HOW TO FIX

In order to pass this test you must add an **alt** attribute to every **<img>** tag used into your webpage. An image with an alternate text specified is inserted using the following HTML line:

```
<img src="image.png" alt="text_to_describe_your_image">
```

Remember that the point of alt text is to provide the same functional information that a visual user would see. Search engines, users who disabled images in their browsers and other agents who are unable to see the images on your webpage can read the alt attributes assigned to the image since they cannot view it.
Learn more about **optimizing images for SEO**.

Inline CSS Test

Check your webpage HTML tags for inline CSS properties. An inline CSS property is added by using the style attribute for a specific tag. By mixing content with presentation you might lose some advantages of the style sheets. Is a good practice to move all the inlines CSS rules into an external file in order to make your page "lighter" in weight and decreasing the code to text ratio.

Congratulations! Your web page does not use inline CSS styles.

Deprecated HTML Tags

Check if your webpage is using old, deprecated HTML tags. These tags will eventually lose browser support and your web pages will render differently. Check this list with all HTML tags.

We found some HTML deprecated tags. You are advised to change these old tags with equivalent tags or proper CSS rules.

> <font>: found 1 time

HOW TO FIX

In order to pass this test you must identify into your code all deprecated HTML tags listed above and replace them with proper tags or CSS rules. Some examples are given below:

- for `<applet>` tag, the equivalent tag is `<object>`
- for `<center>` tag, the alternative CSS property is `text-align`
- for `<font>` tag, the alternative CSS properties are `font-family` and `font-size`
- for `<s>`, `<strike>` and `<u>` tags, the alternative CSS property is `text-decoration`

Google Analytics Test

Check if your page is connected with Google Analytics. Google Analytics is the most popular analytics package for websites, this tool provides you with great insights about your site visitors, demographics and very comprehensive metrics that help you analyze every aspect of your site. It is a good practice to use analytics in order to learn how your visitors behave and gain tips on how to continuously improve your website.

Congratulations! Your website is using the correct version of Google Analytics tracking code.

Favicon Test

Check if your site is using and correctly implementing a favicon. Favicons are small icons that appear in your browser's URL navigation bar. They are also saved next to your URL's title when bookmarking that page and they can help brand your site, making it easy for users to navigate to your site among a list of bookmarks.

We've found a favicon in your page's HTML code, but it's not accessible.

HOW TO FIX

You must check the access rights and the path to icon file.

SEO Friendly URL Test

Check if your website URL and internal URLs are SEO friendly. In order for links to be SEO friendly, they should be clearly named for what they are and contain no spaces, underscores or other characters. You should avoid the use of parameters when possible, as they are make URLs less inviting for users to click or share.

Congratulations! This URL and all internal links on this page are SEO friendly.

JS Error Checker

Check your source code for JavaScript errors. These errors may prevent users from properly viewing your pages and impact their user experience. Sites with poor user experience tend to rank poorly in search engines.

Congratulations! There are no severe JavaScript errors on your web page.

Social Media Check

Check if your page is connected to at least one of the most important social networks. Social signals are getting increasing importance as ranking factors for search engines because it leverages the social intelligence (via our interactions) to determine more accurate relevancy for searches. That's why connecting your website to a social network is a must nowadays to make sure your site is social enabled.

Congratulations! Your website is connected successfully with social media using: Facebook; Twitter;

HTML Page Size Test

Check your page's HTML size. HTML size is the size of all the HTML code on your web page - this size does not include images, external javascripts or external CSS files.

Congratulations! Your HTML size is **21.20 Kb** and this is under the average web page size of **33 Kb**. This leads to a faster page loading time than average.

HTML Compression/GZIP Test

Check if your page is correctly using HTML compression. Compression works by finding similar strings within a text file, and replacing those strings temporarily to make the overall file size smaller. This form of compression is particularly well-suited for the web because HTML and CSS files usually contain plenty of repeated strings, such as white spaces, tags, and style definitions.

Your page do not use any HTML compression!
You should compress your HTML to reduce your page size and page loading times - this will help your site retain visitors and increase page views. If you were using compression, you could be compressing your HTML size by **72 %** - from **21.20 Kb** to **5.92 Kb** which would further reduce your page loading time.

HOW TO FIX

Your two options for file compression are **Deflate** and **GZIP**.

- Deflate is an option which comes automatically with the Apache server and which is simple to set up.
- GZIP on the other hand needs to be installed and requires a bit more work to install.

However, GZIP does achieve a higher compression rate and therefore might be a better choice if your website uses pages which have a lot of images or large file sizes.

Setting up file compression for your website will depend on which type of server you?re using for your website. Most likely, you?ll be using Apache, which means you can enable compression by adding a few deflate codes to your **.htaccess** file.

```
# compress text, html, javascript, css, xml:
AddOutputFilterByType DEFLATE text/plain
AddOutputFilterByType DEFLATE text/html
AddOutputFilterByType DEFLATE text/xml
AddOutputFilterByType DEFLATE text/css
AddOutputFilterByType DEFLATE application/xml
AddOutputFilterByType DEFLATE application/xhtml+xml
AddOutputFilterByType DEFLATE application/rss+xml
AddOutputFilterByType DEFLATE application/javascript
AddOutputFilterByType DEFLATE application/x-javascript
```

For more advanced information regarding deflate you can check this Apache **documentation**.

Site Loading Speed Test

Test your website using real browsers to determine the loadtime speed. How fast your page loads is one of the most important factors in search engine rankings. Pages that take longer than 5 seconds to load can lose up to 50% users. Faster loading webpages offer higher traffic, better conversions and increased sales over slower loading pages.

Your site loading time is around **2.902 seconds** and this is under the average loading speed which is **5 seconds**.

Page Objects

Check if the full list of objects requested by your page can be retrieved. If your page contains objects that cannot be retrieved your page won't be displayed correctly, this impacts the user experience and search engines will penalize you accordingly.

Your page has more than 20 http requests, which can slow down page loading. You can try reducing http requests through various methods such as using text instead of images, using css sprites, using data URIs instead of images, or combining several external files together into one.

HTML Pages: 2

http://structuralfire.com/
http://structuralfire.com/favicon.ico

CSS Files: 6

http://structuralfire.com/css/style.css
http://structuralfire.com/css/reset.css
http://structuralfire.com/css/skeleton.css
http://structuralfire.com/css/superfish.css
http://structuralfire.com/css/flexslider.css
http://structuralfire.com/css/forms.css

Scripts: 7

http://structuralfire.com/js/jquery-1.7.1.min.js

http://structuralfire.com/js/script.js
http://structuralfire.com/js/superfish.js
http://structuralfire.com/js/jquery.responsivemenu.js
http://structuralfire.com/js/jquery.flexslider-min.js
http://structuralfire.com/js/FF-cash.js
http://www.google-analytics.com/analytics.js

Images: 11

http://structuralfire.com/images/news_icon.png
http://structuralfire.com/images/serdarnew.jpg
http://structuralfire.com/images/icon1.jpg
http://structuralfire.com/images/icon2.jpg
http://structuralfire.com/images/icon3.jpg
http://structuralfire.com/images/bg-light.png
http://structuralfire.com/images/photo.JPG
http://structuralfire.com/images/bogazicilogo.jpg
http://structuralfire.com/images/bg-png.png
http://structuralfire.com/images/menu-arrow.png
http://structuralfire.com/images/bg-content.png

Flash Files: 0

Page Cache Test (Server Side Caching)

Check if your page is serving cached pages. A page cache is a mechanism for the temporary storage (caching) of web documents, such as HTML pages and images to reduce bandwidth usage, server load, and perceived lag. A web cache stores copies of documents passing through it; subsequent requests may be satisfied from the cache if certain conditions are met. Common caching methods are Quickcache and jpcache

It does not appear that you are caching your pages. Cached pages serve up static html and avoid potentially time consuming queries to your database. It also helps lower server load by up to 80%. Caching most visibly benefits high traffic pages that access a database, but whose content does not change on every page view. Common caching methods include Alternative PHP Cache, Quickcache, and jpcache. Caching mechanisms also typically compress HTML, further reducing page size and load time.

HOW TO FIX

In order to pass this test you are advised to use a caching mechanism for your pages. There are three methods which can be used to caching your web pages:

1. **Alternative PHP caching**
   - **Alternative PHP Cache** (APC) is an open source framework which caches data using intermediate PHP code. Most web programmers who are familiar with the PHP programming language can easily set up Alternative PHP Cache for your site.
2. **Quickcache**
   - **Quickcache** is a lightweight page caching solution which was formerly known as **jpcache**. Quickcache caches the page output rather than compiling the PHP page, making it a superior version of page caching to the Alternative PHP caching. Quickcache can be quickly downloaded from their website and can reduce your page load time up to 80%.
3. **WP Super Cache**
   - If you have a Wordpress website, **WP Super Cache** can be installed within seconds and

without no programming knowledge.

Flash Test

Check if your page uses Flash. Flash is an outdated technology that was widely used in the past to deliver rich multimedia content. Nowadays this evolved to newer, more mature technologies and standards based on HTML 5, so it's not considered a good practice to use it. Flash content does not work well on mobile devices, and it's not Search Engine friendly.

Congratulations! Your website does not include flash objects (an outdated technology that was sometimes used to deliver rich multimedia content). Flash content does not work well on mobile devices, and is difficult for crawlers to interpret.

Image Expires Tag Test

Checks if your page is using an image expires tag, which specifies a future expiration date for your images. Browsers will see this tag and cache the image in the user's browser until the specified date (so that it does not keep re-fetching the unchanged image from your server). This speeds up your site the next time that user visits your site and requires the same image.

Your site is not using expires headers for your images. An expires tag can help speed up the serving of your webpages for users that regularly visit your site and see the same images. Learn more about how to add expires headers to your images.

HOW TO FIX

In order to reduce the number of HTTP requests, you can use the HTTP Expires header to set an expiration time for your images or any other content type. You can add the following lines into your **.htaccess** file:

```
<IfModule mod_expires.c>
    ExpiresActive on

    ExpiresByType image/jpg "access plus 1 month"
    ExpiresByType image/jpeg "access plus 1 month"
    ExpiresByType image/gif "access plus 1 month"
    ExpiresByType image/png "access plus 1 month"
</IfModule>
```

JS Minification Test

This checks if any of external javascript files used in your page is minified

Some of your website's JavaScript files are not minified!

MINIFIED JAVASCRIPT FILES:

http://structuralfire.com/js/jquery-1.7.1.min.js

http://structuralfire.com/js/jquery.responsivemenu.js

http://structuralfire.com/js/jquery.flexslider-min.js

http://www.google-analytics.com/analytics.js

NOT MINIFIED JAVASCRIPT FILES:

http://structuralfire.com/js/script.js

http://structuralfire.com/js/superfish.js

http://structuralfire.com/js/FF-cash.js

HOW TO FIX

In order to pass this test you must minify all of your external JavaScript files. For this task you can use an online JS minifier like **YUI Compressor**, **Closure Compiler** or **JSMin**.

CSS Minification Test

This checks if any of external css files used in your page is minified

Some of your website's CSS files are not minified!

MINIFIED CSS FILES:

http://structuralfire.com/css/reset.css

NOT MINIFIED CSS FILES:

http://structuralfire.com/css/style.css

http://structuralfire.com/css/skeleton.css

http://structuralfire.com/css/superfish.css

http://structuralfire.com/css/flexslider.css

http://structuralfire.com/css/forms.css

HOW TO FIX

In order to pass this test you must minify all of your external CSS files. For this task you can use an online CSS minifier like **YUI Compressor** or **cssmin.js**.

Nested Tables Test

Check if your site is using nested tables, which can slow down page rendering in the user's browser.

Congratulations, your page does not use nested tables. This speeds up page loading time and optimizes the user experience.

Frameset Test

Check to see if your website is using frames. The "frameset" tag is used to display multiple HTML documents in one page. When search engines use robots or spiders to get information from your page, they have to sort through a bunch or unrelated pages, making it difficult to index a single page. This can create a decrease in search engine page rankings.

Congratulations! Your webpage does not use frames.

Doctype Test

Check for doctype declaration. A document type declaration, or DOCTYPE, defines which version of (X)HTML your webpage is actually using and this is essential to a proper rendering and functioning of web documents in compliant browsers.

Congratulations! Your website has a doctype declaration:

```
<!DOCTYPE html>
```

URL Canonicalization Test

Test your site for potential URL canonicalization issues. Canonicalization describes how a site can use slightly different URLs for the same page (for example, if http://www.example.com and http://example.com displays the same page but do not resolve to the same URL). If this happens, search engines may be unsure as to which URL is the correct one to index. Learn more about canonicalization issues.

http://structuralfire.com and http://www.structuralfire.com/ should resolve to the same URL, but currently do not.

HOW TO FIX

In order to pass this test you must consider using a 301 re-write rule in your **.htaccess** file so that both addresses (**http://example.com** and **http://www.example.com**) resolve to the same URL.
- If you want to redirect **http://www.example.com** to **http://example.com**, you can use this:

```
RewriteCond %{HTTP_HOST} ^www\.example\.com$
RewriteRule ^/?$ "http\:\/\/example\.com\/" [R=301,L]
```

- If you want to redirect **http://example.com** to **http://www.example.com**, you can use this:

```
RewriteCond %{HTTP_HOST} !^www.example.com$ [NC]
RewriteRule ^(.*)$ http://www.example.com/$1 [L,R=301]
```

Note that you must put the above lines somewhere after **RewriteEngine On** line.

IP Canonicalization Test

Test your site for potential IP canonicalization issues. Canonicalization describes how a site can use slightly different URLs for the same page (for example, if your site's IP address and domain name display the same page but do not resolve to the same URL). If this happens, search engines may be unsure as to which URL is the correct one to index. Learn more about canonicalization issues.

Your site's IP 51.255.67.49 does not redirect to your site's domain name. This could cause duplicate content problems if a search engine indexes your site under both its IP and domain name.

HOW TO FIX

In order to pass this test you must consider using a 301 re-write rule in your **.htaccess** file so that your site's IP points to your domain name.
If your site is running on apache server, you could put these lines in your **.htaccess** after **RewriteEngine on** line:

```
RewriteCond %{HTTP_HOST} ^XXX\.XXX\.XXX\.XXX
RewriteRule (.*) http://www.yourdomain.com/$1 [R=301,L]
```

Note that you must proper format the first line using your IP (replace X characters with proper digits from your IP) and the second line using your domain name.

HTTPS Test

Check if your website is using a secure communication protocol over the Internet. Using an HTTPS URL indicates that an additional encryption/authentication layer was added between client and server. The data transferred is encrypted so that it cannot be read by anyone except the recipient. HTTPS must be used by any Web site that is collecting sensitive customer data such as banking information or purchasing information. If you are making a transaction online, you should make sure that it is done over HTTPS so that the data remains secure. Even for sites that do not collect senstive customer information, search engines suggest that switching to https is an increasingly good idea and may help improve rankings.

Your website is not using https, a secure communication protocol. Even for sites that do not collect senstive customer information, search engines suggest that switching to https is an increasingly good idea and may help improve rankings. Note: if your site relies primarily on adsense income, be aware that using https may be detrimental to ad earnings.

HOW TO FIX

If your website needs a secured authentication or an encrypted transfer of data, you need to install an SSL certificate in order to provide a secure connection over HTTPS protocol. **HERE** is a "step by step" guide to purchase and install an SSL certificate.

Safe Browsing Test

Check if your website is listed with malware or phishing activity. Any site containing malware or suspicious for phising activity is seen as a threat and risk to the online community and hence will get a a lower ranking. This test checks if the most relevant online databases that track malware and phishing list your website.

This site is not currently listed as suspicious (no malware or phishing activity found).

Server Signature Test

Check if your server's signature is ON. A server signature is the public identity of your web server and contains sensitive information that could be used to exploit any known vulnerability, so it's considered a good practice to turn it OFF as you don't want to disclose what software versions you are running.

Your server signature is on. Turning off your server signature is generally a good idea from a security standpoint. Read more on how to turn off server signature and improve your website's security.

> Server: Apache/2.4.18

HOW TO FIX

By default, the Apache webserver sends HTTP headers with some information about your server version, operating system, modules installed, etc. These informations can be used by hackers in order to exploit vulnerabilities (specially if you are running an older version). These information can be hidden or changed with very basic configurations.
Open Apache?s configuration file (**httpd.conf** or **apache.conf**) and search for **ServerSignature**. If you find it, edit it to:

```
ServerSignature Off
ServerTokens Prod
```

If you don't find it, just add these two lines at the end of the file.
Note that, after you modify the configuration file, you must restart the Apache server.

Directory Browsing Test

Check if your server allows directory browsing. If directory browsing is disabled, visitors will not be able to browse your directory by accessing the directory directly (if there is no index.html file). This will protect your files from being exposed to the public. Apache web server allows directory browsing by default. Disabling directory browsing is generally a good idea from a security standpoint.

Congratulations! Your server has disabled directory browsing.

Libwww-perl Access Test

Check if your server allows access from User-agent Libwww-perl. Botnet scripts that automatically look for vulnerabilities in your software are sometimes identified as User-Agent libwww-perl. By blocking access from libwww-perl you can eliminate many simpler attacks.

Your server appears to allow access from User-agent Libwww-perl. Botnet scripts that automatically look for vulnerabilities in your software are sometimes identified as User-Agent libwww-perl. By blocking access from libwww-perl you can eliminate many simpler attacks. Read more on blocking Libwww-perl access and improving your website's security.

HOW TO FIX

In order to pass this test you must block the libwww-perl user-agent in your **.htaccess** file.
If your site is running on apache server, you could put these lines in your **.htaccess** after **RewriteEngine on** line:

```
RewriteCond %{HTTP_USER_AGENT} libwww-perl.*
RewriteRule .* ? [F,L]
```

Plaintext Emails Test

Check your webpage for plaintext email addresses. Any e-mail address posted in public is likely to be automatically collected by computer software used by bulk emailers (a process known as e-mail address harvesting). A spam harvester can read through the pages in your site and extract email addresses which are then added to bulk marketing databases and the result is more spam in your inbox.

We found 1 email addresses in your page code. We advise you to protect email links in a way that hides them from the spam harvesters.

HOW TO FIX

In order to pass this test you must make your email addresses invisible to email spiders. Note that the best option is to replace your entire contact mechanism with a contact form and using the POST method while submitting the form. Other solutions are listed below:

- replace the at (@) and dot (.) characters
- replace text with images
- use email obfuscators
- hide email addresses using JavaScript or CSS trick

Media Query Responsive Test

Check if your page implements responsive design functionalities using media query techniques. The '@media' rule allows different style rules for different media in the same style sheet. Media query techniques allows different content to be optimized depending on the output device and this is a must nowadays to make sure your website looks good on ALL devices and platforms.

Congratulations, your website uses media query technique, which is the base for responsive design functionalities.

Mobile Snapshot

Check how your page renders on a mobile device by providing a snapshot for you to quickly check if it looks good.

Microdata Schema Test

This test will check if your web page take the advantages of HTML Microdata specifications in order to markup structured data. By using microdata in your web pages, you can help search engines to better understand your content and to create rich snippets in search results.

Your webpage doesn't take the advantages of HTML Microdata specifications in order to markup structured data. View Google's guide for getting started with microdata.

HOW TO FIX

HTML5 Microdata is an easy way to add semantic markup to your web pages. Search engines rely on this markup to improve the display of search results, making it easier for people to find the right web pages.
Here is a simple example of how to use HTML5 microdata in your contact web page:

```
<div itemscope itemtype="http://schema.org/Person">
   <span itemprop="name">Joe Doe</span>
   <span itemprop="company">The Example Company</span>
   <span itemprop="tel">604-555-1234</span>
   <a itemprop="email" href="mailto:joe.doe@example.com">joe.doe@example.com</a>
</div>
```

Noindex Tag Checker

Check if your webpage is using the noindex meta tag. The usage of this tag instructs search engines not to show your page in search results.

Your webpage does not use the noindex meta tag. This means that your webpage will be read and indexed by search engines.

Canonical Tag Checker

Check if your webpage is using the canonical link tag. This tag is used to nominate a primary page when you have several pages with duplicate content.

Your page does not use the canonical link tag.

Nofollow Tag Checker

Check if your webpage is using the nofollow meta tag. This tag will tell search engines not to crawl any outgoing links from your webpage.

Your webpage does not use the nofollow meta tag. This means that search engins will crawl all links from your webpage.

Disallow Directive Checker

Check if the robots.txt file is excluding some parts of your website. Search engines will look for a robots.txt file in the root of your domain whenever they crawl your website. The Disallow directive is used when you want to advise a search engine not to crawl and index a file, page, or directory.

Your site lacks a "robots.txt" file. This file can protect private content from appearing online, save bandwidth, and lower load on your server. A missing "robots.txt" file also generates additional errors in your apache log whenever robots request one.

SPF records checker

This test will check if your DNS server has an SPF record. SPF (Sender Policy Framework) allows email systems to check if the sender of a message comes from a legitimate source and refuse an email if the source is not legitimate. SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record or TXT record in the Domain Name System (DNS).

Your DNS server is not using an SPF record. SPF (Sender Policy Framework) allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record or TXT record in the Domain Name System (DNS). You can find more information about SPF records here.

HOW TO FIX

An **SPF record** is a type of **Domain Name Service (DNS)** record that allows email systems to check if the sender of a message comes from a legitimate source and refuse an email if the source is not legitimate. Adding an SPF record is as easy as adding CNAME, MX or A records in your DNS zone. You can find more information **here**.

Before creating the SPF record for your domain, it is important to have access at your domain's DNS zone and to know what mail servers your domain is likely to use and plan how you want any non-authorised email to be handled.

Example:
Let's say that you are planning to send emails using Google Apps and you also want to ensure that no other mail servers are authorised. You can use an SPF record like this:

```
v=spf1 include:_spf.google.com -all
```

"v=spf1" - This sets the SPF version
"include:_spf.google.com" - This includes Google mail servers in your list of authorized sending servers
"-all" - This means that any server not previously listed is not authorized

If you are using your own VPS to send email and not any other service like Mandrill, Google Apps, etc. then you can create an SPF record like this:

```
v=spf1 mx -all
```

Note:
Setting an SPF record for your domain can help in reducing the chances of a spammer using your domain name in unsolicited emails. Research carefully what mail servers your domain is likely to use and plan how you want any non-authorised email to be handled.