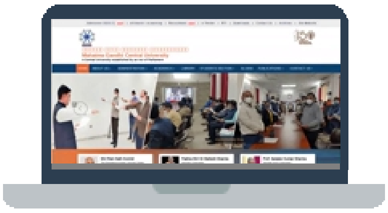
Web performance and quality report



http://mgcub.ac.in/

This report is provided by Dareboost, an online tool for web performance and quality analysis and monitoring.

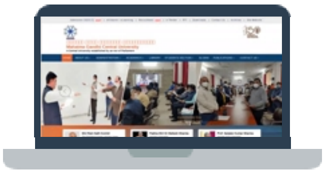
Summary

60%

14 Issues

14 Improvements

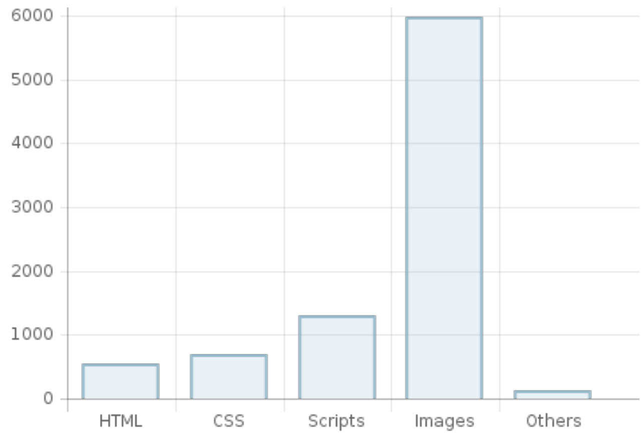
62 Successes



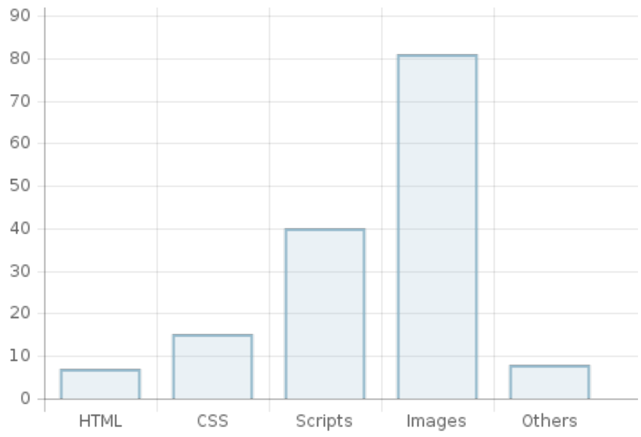
SIMULATED VISITOR: Chrome Washington DC 10.0/2.0Mbps (Latency: 28 ms)

First Byte	Start Render	Fully Loaded	Speed Index
0.52 sec	3.13 sec	8.89 sec	4742 ms

Weight by resources type



Requests by resources type



Detected technologies

- Apache
- Font Awesome
- Google Font API
- OWL Carousel
- OpenSSL
- PHP
- Twitter Bootstrap
- Windows Server
- YouTube
- jQuery

Tips and best practices

Browser rendering

Your Optimization Priorities

0/100

#2353

❗ Defer parsing of JavaScript

JavaScript can significantly slow down a page display, especially if it is necessary to download an external script.

Defer the use of JavaScript as much as possible to provide a faster start for the page display.

How can I fix this?

First of all, distinguish what portions of your JS is critical and must be loaded as soon as possible, and put them in a specific external file. Keep this file as streamlined as possible, and defer the parsing or execution of all other JS files.

Use one of the methods below to defer parsing for external JavaScript files:

- use the async attribute;
- use the defer attribute;
- append the script to the DOM in JavaScript during the onload event;
- make sure your scripts are placed at the bottom of the page (ideally at the end of the body).

2.3MiB of JavaScript is parsed during initial page load. Defer parsing JavaScript to reduce blocking of page rendering.

- www.youtube.com/s/[...]e.js (1.3MiB)
- www.facebook.com/r[...]g5Kz (223.6KiB)
- www.facebook.com/r[...]g5Kz (152.9KiB)
- www.youtube.com/s/[...]r.js (133.5KiB)
- www.facebook.com/r[...]g5Kz (103.8KiB)
- www.facebook.com/r[...]g5Kz (88.2KiB)
- mgcub.ac.in/js/ven[...]in.js (78.4KiB)
- www.facebook.com/p[...]ppId (54.2KiB of inline JavaScript)
- www.facebook.com/r[...]g5Kz (52.0KiB)
- mgcub.ac.in/js/jss[...]ni.js (42.7KiB)
- and 18 others

0/100

#2416

❗ You should reduce the number of DOM elements

The number of DOM elements influences the complexity of the webpage and DOM access in JavaScript.

A well-designed webpage can offer rich content while maintaining a reasonable number of DOM elements. Read more about this here.

We recommend creating pages that contain less than 1000 DOM elements.

This page contains too many DOM elements (4118 elements).

0/100

#2575

❗ Avoid Mutation Events in your scripts

To capture DOM events, do not use Mutation Events. Alternatives exist.

Good concept, bad implementation

When developing complex JavaScript applications, you may need to know when the DOM node tree has changed. Introduced in 2000 in the DOM, Level 2 specification to provide a solution to this need, Mutations Events are browser-initiated events that let you know when a DOM node is added, removed, or deleted.

Mutation Events, however, present major performance problems. First, they are synchronous, i.e. they prevent other events in the queue from being fired (if those events are used to update the UI, this will cause some lag). Second, they are implemented as browser events, thus traverse the DOM tree from the targeted HTML element to the parent element which listens for the event, clogging the JavaScript thread along the way.

Mutation Events have been deprecated in 2016 in the DOM, Level 3 specification.

Mutation Observers to the rescue

If you need to watch for changes being made to the DOM tree, you should use the `MutationObserver` interface (DOM4 Living Standard). Mutation Observers are asynchronous, processed in batches, and observe specific or all changes to a node. They are more efficient in terms of CPU usage than browser events and therefore cause fewer to no UI freeze.

Learn how to use Mutation Observers (Mozilla Developer Network).

Detected mutations events:

Please find below the Mutation Events that Dareboost found in your code:

`DOMSubtreeModified` :

- https://www.facebook.com/rsrc.php/v3/yx/r/lDNjdSJxnmr.js?_nc_x=Ij3Wp8lg5Kz (1 times)

Cache policy

Your Optimization Priorities

41/100

#2352

! Specify a 'Vary: Accept-Encoding' header

The following publicly cacheable, compressible resources should have a "Vary: Accept-Encoding" header:

Resources from "mgcub"

- mgcub.ac.in/css/an[...]n.css
- mgcub.ac.in/css/bo[...]p.css
- mgcub.ac.in/css/bo[...]n.css
- mgcub.ac.in/css/fo[...]n.css
- mgcub.ac.in/css/jq[...]i.css
- mgcub.ac.in/css/li[...]s.css
- mgcub.ac.in/css/ma[...]p.css
- mgcub.ac.in/css/ma[...]n.css
- mgcub.ac.in/css/ni[...]t.css
- mgcub.ac.in/css/ow[...]l.css
- and 14 others

Resources hosted by a third-party

It appears these files are hosted by a third-party, so they may not be within your control. However, you should consider any alternative to these resources to improve your page performance.

- static.doubleclick[...]s.js
- syndication.twitte[...]ings

The `Vary: Accept-Encoding` header allows to cache two versions of the resource on proxies: one compressed, and one uncompressed. So, the clients who cannot properly decompress the files are able to access your page via a proxy, using the uncompressed version. The other users will get the compressed version.

0/100

#70

! Do not use too long inline scripts

Any script with a significant size should let the browser cached them in order to reduce loading time/improve performance of your returning visitor.

Inline scripts / cache policy

"inline" scripts allow to integrate easily small portions of scripts directly in the HTML code. Example:

Example

```
<script type="text/javascript">
   (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']...,'/analytics.js','ga');
   ga('create', 'UA-11111111-1', 'mywebsite.com');
</script>
```

By doing so, you avoid making a request to the server to retrieve the resource. So inline scripts represent a performance gain if you want to integrate small scripts.

However, once a script has a fairly substantial size, we advise you to outsource it and perform a request to retrieve it. So you will benefit from the cache mechanism.

What should I do?

Outsource your scripts with more than 1500 characters in one or more separate files.

You should **group the following scripts in one or more distinct files**:

-
  ```
  jQuery(document).ready(function ($) {

        var options = {
           $FillMode: 2, //[Optional] The way to fill image in slide, 0 stretch, 1 ...
  ```

-
  ```
  $(document).ready(function () {
                          document.title = "Mahatma Gandhi Central University, Motihari (Bihar)";
           ...
  ```

Compliance

Your Optimization Priorities

0/100

#99

! 5 links to Word documents are detected

.doc and *.docx* documents do not guarantee compatibility with all major operating systems. It's recommended to use PDF documents.

You should use PDF format for these links:

- pdf/20201205140836eb49ba6c32.docx
- pdf/20201205140836eb49ba6c32.docx
- pdf/20201020070227f5a54d2878.docx
- pdf/2020093001361735d0017e60.docx
- pdf/20200930013617c6353bedcd.docx

Data amount

Your Optimization Priorities

0/100

#2384

Enable compression

Compressing resources with gzip or deflate can reduce the number of bytes sent over the network.

Enable compression for the following resources to reduce their transfer size by 1.1MiB (84% reduction).

- Compressing http://mgcub.ac.in/ could save 421.9KiB (92% reduction).
- Compressing mgcub.ac.in/css/bo[...]n.css could save 152.8KiB (87% reduction).
- Compressing mgcub.ac.in/css/bo[...]p.css could save 133.7KiB (86% reduction).
- Compressing mgcub.ac.in/css/ma[...]n.css could save 93.8KiB (86% reduction).
- Compressing mgcub.ac.in/js/jss[...]ni.js could save 83.5KiB (78% reduction).
- Compressing mgcub.ac.in/js/ven[...]in.js could save 55.2KiB (65% reduction).
- Compressing mgcub.ac.in/css/an[...]n.css could save 47.7KiB (92% reduction).
- Compressing mgcub.ac.in/js/ven[...]in.js could save 35.0KiB (73% reduction).
- Compressing mgcub.ac.in/js/owl[...]in.js could save 29.2KiB (73% reduction).
- Compressing mgcub.ac.in/css/jq[...]i.css could save 27.0KiB (76% reduction).
- and 13 others

This page is delivered by an Apache server. Check if it uses the mod_deflate module.

0/100

#2443

Reduce the page weight (8.7MB)

The page weight is too high, slowing down its display, especially on low-speed connections. This can lead to frustration for users paying for data (see whatdoesmysitecost.com).

Evaluate the Weight of my Web Page

According to HTTPArchive, in July 2019, the average weight of a web page is 1,95MB.

How to reduce the weight of my page?

You can report to our "Data amount" category to discover the possible optimizations in your case. Images are often involved.
Moreover, make sure to build your web pages to load data that is essential to the user experience (rendering optimization of the critical path).
For other content (social networking plugins, advertising, content at the bottom of the page ...), it is better to delay the loading (asynchronous, lazy-loading ...), so they don't override priority contents.

We have established the weight distribution of the page by resource type:

- **Images :** 69,16% of total weight
- **JavaScript :** 15,10% of total weight
- **CSS :** 7,98% of total weight
- **Texts :** 6,24% of total weight
- **Font :** 1,33% of total weight
- **JSON :** 0,18% of total weight

Here is the weight of the 10 heaviest resources over the network, and that are necessary to load the page:

- http://mgcub.ac.in/images/slider/Slider21.png (766kB)
- http://mgcub.ac.in/images/slider/Slider24.png (672kB)
- www.youtube.com/s/player/5dd3f3b2/pl[...]et/en_US/base.js (500kB)
- http://mgcub.ac.in/ (469kB)
- http://mgcub.ac.in/images/slider/Slider30.png (362kB)
- http://mgcub.ac.in/images/slider/Slider31.png (358kB)
- http://mgcub.ac.in/images/slider/Slider29.png (344kB)
- http://mgcub.ac.in/images/slider/Slider27.png (315kB)
- http://mgcub.ac.in/images/slider/Slider32.png (307kB)
- http://mgcub.ac.in/images/slider/Slider23.png (271kB)

0/100

#2436

❗ 2 images are resized on browser side

If your images are larger than their display area, the browser will download unnecessary data (and perform unsupervised resizing).

Avoid resizing images on the browser side

Resizing images on the browser side to reduce their rendering size is not recommended.

When the browser needs to display an image on your page, it does everything it can to adapt it to its rendering surface. If the image is too large, it will reduce it.

Provide images adapted to the display dimensions to prevents unnecessary data from being sent over the network, which reduces page loading time.

And because embedded browser algorithms are not as good as those of image manipulation tools, you will get a more satisfying visual result by resizing your images upfront, rather than letting the browser do it.

Serve Responsive Images

Several methods exist, to serve images adapted to the browser regardless of screen resolution or device pixel density. We recommend reading the following resources:

- "Responsive images" on the Mozilla Developer Network
- Picturefill, to start using the <picture> element in browsers that do not support it
- RICG, group of developers working on responsive images

Don't resize the following images:

- http://mgcub.ac.in/images/address2.jpg (displayed size: 184x108)
- http://mgcub.ac.in/images/rotate.png (displayed size: 75x80)

The other tips

0/100

#2364

❗ Minify HTML

Compacting HTML code, including any inline JavaScript and CSS contained in it, can save many bytes of data and speed up download and parse times.

Minify HTML for the following resources to reduce their size by 286.2KiB (62% reduction).

- Minifying http://mgcub.ac.in/ could save 286.2KiB (62% reduction).

50/100

#2387

❗ Minify CSS

Compacting CSS code can save many bytes of data and speed up download and parse times.

Minify CSS for the following resources to reduce their size by 95.4KiB (20% reduction).

- Minifying mgcub.ac.in/css/bo[...]n.css could save 31.9KiB (19% reduction).
- Minifying mgcub.ac.in/css/bo[...]p.css could save 31.8KiB (21% reduction).
- Minifying mgcub.ac.in/css/ma[...]n.css could save 23.1KiB (22% reduction).
- Minifying mgcub.ac.in/css/jq[...]i.css could save 5.8KiB (17% reduction).
- Minifying mgcub.ac.in/css/ma[...]p.css could save 1.5KiB (23% reduction).
- Minifying mgcub.ac.in/css/ow[...]l.css could save 1.3KiB (31% reduction).

There are many tools to minify CSS files. You can try YUI Compressor or cssmin.js, recommended by Google.

50/100

#2388

! Minify JavaScript

Compacting JavaScript code can save many bytes of data and speed up downloading, parsing, and execution time.

Minify JavaScript for the following resources to reduce their size by 78.4KiB (13% reduction).

Resources from "mgcub"

- Minifying mgcub.ac.in/js/jss[...]ni.js could save 61.8KiB (58% reduction).
- Minifying http://mgcub.ac.in/js/main.js could save 5.9KiB (49% reduction).
- Minifying mgcub.ac.in/js/hov[...]nt.js could save 4.9KiB (71% reduction).
- Minifying mgcub.ac.in/js/jqu[...]in.js could save 2.4KiB (50% reduction).

Resources hosted by a third-party

It appears these files are hosted by a third-party, so they may not be within your control. However, you should consider any alternative to these resources to improve your page performance.

- Minifying www.youtube.com/s/[...]e.js could save 3.3KiB (1% reduction).

There are many tools to minify JavaScript files. You can try YUI Compressor or JSMin, recommended by Google.

90/100

#2389

✓ Optimize your images

Properly formatting and compressing images can save many bytes of data.

Optimize the following images to reduce their size by 54.3KiB (9% reduction).

Resources from "mgcub"

- Losslessly compressing mgcub.ac.in/images[...]3.jpg could save 18.9KiB (20% reduction).
- Losslessly compressing mgcub.ac.in/images[...]i.png could save 14.7KiB (45% reduction).
- Losslessly compressing mgcub.ac.in/images[...]e.png could save 5.8KiB (3% reduction).
- Losslessly compressing mgcub.ac.in/images[...]1.jpg could save 5.4KiB (5% reduction).
- Losslessly compressing mgcub.ac.in/images[...]2.jpg could save 4.3KiB (5% reduction).

Resources hosted by a third-party

It appears these files are hosted by a third-party, so they may not be within your control. However, you should consider any alternative to these resources to improve your page performance.

- Losslessly compressing www.facebook.com/r[...].png could save 2.6KiB (82% reduction).
- Losslessly compressing www.facebook.com/r[...].png could save 2.6KiB (66% reduction).

Images may contain data unnecessary for their use on the web. This data can increase their size significantly. Some tools automatically remove this unnecessary data without loss of quality and thus reduce your image sizes.

Many image optimization algorithms depend on each image format. Some of them are included in graphic software like Photoshop or GIMP:

- PNG: Zopfli-png, PNGOUT, OptiPNG, AdvPNG, PNGCrush, PNGQuant...
- JPG: JPEGOptim, MozJPEG, Jpegtran, Guetzli...

FileOptimizer (Windows), ImageOptim (Mac) or Trimage (Linux) are software that combine several algorithms in one place. They will find the best possible optimization and encoding for every image, with or without quality loss.

Number of requests

Your Optimization Priorities

46/100

#2418

❗ Group 13 JavaScript files

Each HTTP request affects the performance of your webpage (e.g., roundtrip time and bandwidth usage).

For example, it is better to request a unique 50 kB file instead of requesting 10 files that are 5 kB in size.

How should I distribute scripts?

Distribute your scripts by integrating them directly into your HTML or grouping them in files. We recommend using the latter method to take advantage of caching mechanisms.

You should consider grouping the following resources:

- http://mgcub.ac.in/js/vendor/jquery-3.2.1.min.js
- http://mgcub.ac.in/js/popper.min.js
- http://mgcub.ac.in/js/vendor/bootstrap.min.js
- http://mgcub.ac.in/js/easing.min.js
- and 9 others

58/100

#2419

❗ Group 6 CSS files

Each HTTP request affects the performance of your webpage (e.g., roundtrip time and bandwidth usage).

For example, it is better to request a unique 50 kB file instead of requesting 10 files that are 5 kB in size.

How should I distribute styles?

Distribute your styles by integrating them directly into your HTML or grouping them in files. We recommend using the latter method to take advantage of caching mechanisms.

You should consider grouping the following resources:

- http://mgcub.ac.in/css/linearicons.css
- http://mgcub.ac.in/css/font-awesome.min.css
- http://mgcub.ac.in/css/magnific-popup.css
- http://mgcub.ac.in/css/nice-select.css
- http://mgcub.ac.in/css/owl.carousel.css
- http://mgcub.ac.in/css/jquery-ui.css

Quality

Your Optimization Priorities

0/100

#71

Avoid HTML code in comments

Comments allow you to detail a portion of code and help you navigate more efficiently in the DOM. However, make sure no sensitive information is exposed in your comments.

1 of your 3 comments contains HTML code. You should remove the code for your production version. You'll save 113 useless characters:

- `<!--<link href="https://fonts.googleapis.com/css?family=Poppins:100,200,400,300,500,600,700" rel="stylesheet">-->`

0/100

#2517

The !important declaration is used 109 times

If you abuse of this declaration, you should consider a review of your CSS code. We tolerate 10 occurrences of the !important declaration before penalizing your score.

Here are the !important detected:

http://mgcub.ac.in/css/magnific-popup.css

- `.mfp-wrap {outline: none !important}` (line 20, col 3)
- `.mfp-hide {display: none !important}` (line 84, col 3)

http://mgcub.ac.in/css/animate.min.css

- `.flipInX {-webkit-backface-visibility: visible!important}` (line 11, col 28027)
- `.flipInX {backface-visibility: visible!important}` (line 11, col 28073)
- `.flipInY {-webkit-backface-visibility: visible!important}` (line 11, col 29368)
- `.flipInY {backface-visibility: visible!important}` (line 11, col 29414)
- `.flipOutX {-webkit-backface-visibility: visible!important}` (line 11, col 30202)
- `.flipOutX {backface-visibility: visible!important}` (line 11, col 30248)
- `.flipOutY {-webkit-backface-visibility: visible!important}` (line 11, col 30926)
- `.flipOutY {backface-visibility: visible!important}` (line 11, col 30972)

http://mgcub.ac.in/css/nice-select.css

- `.nice-select {text-align: left !important}` (line 20, col 3)
- `.nice-select.wide .list {left: 0 !important}` (line 72, col 7)
- `.nice-select.wide .list {right: 0 !important}` (line 73, col 7)
- `.nice-select .list:hover .option:not(:hover) {background-col...` (line 112, col 7)

http://mgcub.ac.in/css/main.css

- `h1, h2, h3, h4, h5, h6 {line-height: 1.2em !important}` (line 116, col 5)
- `.fz-48 {font-size: 48px !important}` (line 214, col 5)
- `.fw400 {font-weight: 400 !important}` (line 226, col 5)
- `.ml-0 {margin-left: 0 !important}` (line 298, col 5)
- `.ml-5 {margin-left: 5px !important}` (line 302, col 5)
- `.mr-0 {margin-right: 0 !important}` (line 326, col 5)
- `.mr-5 {margin-right: 5px !important}` (line 330, col 5)
- `.mb-0-i {margin-bottom: 0px !important}` (line 358, col 5)
- and 87 others

0/100

#2383

Separate the CSS styles from the HTML tags

Separating HTML tags and CSS directives improves code readability and promotes factorization.

How to define CSS styles

CSS styles are used to format the page. You can use one of three main methods to define them:

- declare styles in a specific CSS file;
- declare "inline" styles (<style> tag in your HTML template);
- declare styles with the "style" attribute of a HTML tag.

How can I improve my page?

We recommend grouping your CSS styles in `<style>` tags or in separate files. That way, the HTML is only responsible for providing the structure of the page, and its layout is outsourced. The `<style>` attribute should only be generated by some JavaScript code (e.g., if you need to know the screen size).

This page uses 56 `style` attribute(s):

-
  ```
  <div style="position: absolute;bottom:24px;text-align: left;background: rgba(10,16,29,0.7);width: 18%;height:40px;left:750px;border-radius:10px;float:left;">
  ```

-
  ```
  <div style="position:absolute;top:8px;left:15px;width:auto;z-index:1;font-size:16px;line-height:22px;font-weight:500;text-align:left;color:#ffffff;letter-spacing:1px;right:15px;">
  ```

-
  ```
  <span style="color:#FE9E3E;">
  ```

-
  ```
  <div style="position: absolute;bottom:24px;text-align: left;background: rgba(10,16,29,0.7);width: 15%;height:40px;left:750px;border-radius:10px;float:left;">
  ```
- and 52 others

The other tips

90/100

#2527

☑ 2 CSS properties are duplicated

Using several times the same property within a same CSS rule can affect the readability of the CSS. It is also an optimization opportunity: by removing duplicated properties, you will reduce the file size.

CSS properties

The CSS properties allow to apply a style to a set of elements. It is unnecessary to define 2 times the same property with the same value in a same rule.

How to improve it?

Remove one occurrence of the duplicated property. For example, the following properties:

Example

```
.myClass {
  margin: 10px;
  ...
  margin: 10px;
}
```

Should be replaced by:

Example

```
.myClass {
  margin: 10px;
}
```

The following files define the same property several times (with the same value) in a single rule:

http://mgcub.ac.in/css/main.css

- `.primary-btn {position: relative}` (line 2394, col 5)
- `.nav-side-menu li a {letter-spacing: 1px}` (line 5564, col 5)

SEO

Your Optimization Priorities

0/100

#78

Define at least <h1> and <h2> tags in your page

We recommend putting page keywords in at least the h1 and h2 tags. Search engines use the h1, h2, and h3 tags for SEO purposes.
This page contains:

- 2 <h3> element(s)

0/100

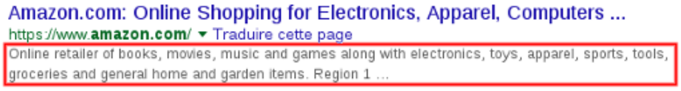
#84

You should define a 'description' meta tag

The page should define a unique description.

Description in search engines

The description of the page may be directly displayed in search engine results pages (SERP):



Amazon.com: Online Shopping for Electronics, Apparel, Computers ...
https://www.**amazon.com**/ ▾ Traduire cette page
Online retailer of books, movies, music and games along with electronics, toys, apparel, sports, tools, groceries and general home and garden items. Region 1 ...

It allows you to control at best the entry preview in search engines, and to improve the click rate to your page. Learn more.

How to define a page's description?

Use `<meta name="description" content="page description">` and place it in the `<head>` tag.

No <meta> `description` has been found on this page. Please provide a <meta> `description`.

0/100

#2503

robots.txt file should be defined

Indicate to web crawlers which URLs should be explored on your website.

The robots.txt file

Place your robots.txt file in the root of the website. It will be interpreted by the robots in charge of your SEO. It delivers instructions to specify the pages to explore by robots, like Google bot.

Note that these directives are indicative only. A lambda robot will not be blocked by the restrictions specified by the file.

We have not detected the robots.txt file on this website, you should define one:

- http://mgcub.ac.in/robots.txt

The other tips

0/100

#2399

Your site should use more Open Graph properties

You can help social networks understand information related to the page by using Open Graph properties.

The Open Graph properties explained

Several properties allow social networks to learn more about the page's content. We recommend using at least the required properties:

- `<meta property="og:title" content="The title" />` Example
- `<meta property="og:type" content="The type" />` Example
- `<meta property="og:url" content="http://url.com/" />` Example
- `<meta property="og:image" content="http://image.jpg" />` Example

This information is used to improve links between your page and various social networks, including Facebook. Read more about Open Graph here.

This page declares some Open Graph properties, **however the following are missing**:

- `<meta property="og:url" content="http://url.com/" />`
- `<meta property="og:image" content="http://image.jpg" />`

Your Optimization Priorities

0/100

#2548

! You should use a secure connection (HTTPS)

This test was run on a URL using the HTTP protocol. You should redirect to HTTPS.

HTTPS guarantees the confidentiality and security of communications over the internet: data is encrypted, so protected against attacks and data corruption.

Google is multiplying its actions to push more and more websites towards HTTPS. Google first added HTTPS in its SEO criteria (see the announcement). Since then, Chrome has been evolving and now highlights the absence of a secure environment in various cases where information is collected from users. Other browsers are also following this trend.

Setting up HTTPS on a website sometimes causes some reservations (cost, impacts on performance, compatibility with technical partners...). But the market has changed in recent years and you should not worry about migrating to HTTPS. You should consider switching your site to HTTPS.

How to set up the HTTPS protocol

You have to set up a certificate you got from a reliable certification authority. Learn more by contacting your website host who can help you getting this certificate. Besides, the following page help you in your migration procedure to the HTTPS protocol.

A free certificate? Try Let's Encrypt!

Let's Encrypt is a free, automated, and open certificate authority. Many hosting providers offer to enable the generation and automatic renewal of free certificates directly from the administration interface of your domain. Contact your website host for more information.

0/100

#2434

The Content Security Policy is missing

Protect your website from cross-site scripting (XSS) attacks by setting up a restrictive Content-Security-Policy.

XSS attacks explained

XSS attacks are a type of attack in which malicious data is maliciously added to websites. The number of vulnerabilities allowing these attacks is quite large, which is why it is as useful to prevent them as to limit their harmful effects.

You can protect your pages against these attacks and their effects by restricting execution to code portions either legitimized by the domain to which they belong or by a unique integrity token. The code that does not match this security policy will not be executed and the user will be informed.

You can learn more about XSS attacks on the Open Web Application Security Project (OWASP) Website.

Configure a "Content-Security-Policy" (CSP) HTTP header

Set up a "Content-Security-Policy" (CSP) HTTP header to prevent or limit the damage caused by an XSS attack. To specify a security policy configure your server so the response of the first resource contains the "Content-Security-Policy" HTTP header.

Here's an example:

Example

```
Content-Security-Policy: script-src 'self' https://apis.google.com
```

In this case, only scripts coming from the current host or https://apis.google.com will be executed.

Read more about the CSP HTTP header by consulting the CSP directives specification.

Please, be careful, if the header is misconfigured, some of your content, scripts, or styles may be blocked. That could cause unwanted side effects. Moreover, the restrictions apply to all pages of the website. We recommend you test the different pages of your website before deploying this header in your production environment.

CSP can be configured with your Apache server. Make sure that the mod_headers module is enabled. Then, you can specify your content security policy (in your .htaccess file, for example). Here is an example :

Example

```
<IfModule mod_headers.c>
Header set Content-Security-Policy "script-src 'self' https://www.google.com"
</IfModule>
```

This example allows scripts from the same origin (same scheme, host and port) and google.com.

No Content Security Policy on this page: it is more easily exposed to XSS attacks.

0/100

#2481

This page is exposed to "clickjacking" type attacks

Keep malicious people from integrating your pages into their websites.

Clickjacking explained

This kind of attack happens when your page gets integrated with a malicious website via <frame> or <iframe> tags. By doing this, attackers can persuade users that they are on your own page when they are not. The unsuspecting user may enter personal information that is visible on and thus vulnerable to the malicious website.

To avoid this, always indicate which domains have permission to integrate your pages.

How to prevent clickjacking?

There are two main ways to prevent that behavior.

1/ Configure a "X-Frame-Options" HTTP header. Configure your server so the main resource response includes the "X-Frame-Options" HTTP header.

Three values may be defined:

- `DENY` to prevent any frame or iframe from integrating the page;
- `SAMEORIGIN` to authorize only frames from the same domain name;
- `ALLOW-FROM uri` to indicate the domains allowed to integrate a page into frame (however is not compatible with some browsers)

2/ Define an explicit `frame-ancestors` directive into a Content-Security-Policy HTTP Header. "frame-ancestors" directive is a newer, hence supported by fewer browsers, approach that will allow your website to authorize multiple domains instead of only the current origin. Setting this directive to 'none' is similar to `X-Frame-Options: DENY`.

Which approach to choose? If you only have the current domain to allow, do set up the two security features, for better compatibility with older browsers. If you want to allow multiple domains, you should only implement the frame-ancestors security policy.

The "X-Frame-Options" HTTP header can be configured with your Apache server. Make sure that the mod_headers module is enabled. Then, you can specify the header (in your .htaccess file, for example). Here is an example:

Example

```
<IfModule mod_headers.c>
Header always set X-FRAME-OPTIONS "DENY"
</IfModule>
```

Neither the "X-Frame-Options" HTTP header nor the "frame-ancestors" security police are configured on this page; you are more likely to be exposed to clickjacking.

The other tips

0/100

#2492

2 iframes could be secure with a sandbox attribute

Restrict as much as possible the actions that can be processed by external content embedded on your website.

External contents

You should pay a special attention to external contents (social networks widgets, ads, etc.) embedded via the <iframe> tag. To limit the risks, the W3C has added the `sandbox` attribute in the HTML5 specifications. It restricts the available actions from an iframe (on major modern browsers).

How to fix the issue?

Add the `sandbox` attribute on your iframe tags to control as much as possible the behavior of its content. Be sure to **use the correct values for this attribute**.

A security policy is missing for the folowing iframes:

-
  ```
  <iframe src="https://www.facebook.com/plugins/page.php?href=https%3A%2F%2Fwww.facebook.com%2FMGCUB2016%2F&tabs=timeline&width=340&height=337&small_header=false&adapt_container_width=true&hide_cover=false&show_facepile=true&appId" width="340" height="337" style="border:none;overflow:hidden" scrolling="no" frameborder="0" allowTransparency="true" allow="encrypted-media">
  ```

-
  ```
  <iframe width="100%" height="337" src="https://www.youtube.com/embed/watch?v=UayWciWna2E&list=UUX35-ZgGBrtFKwZ131_Su1Q" frameborder="0" allow="autoplay; encrypted-media" allowfullscreen>
  ```

0/100

#2484

Disable the auto detection of resource type

Protect yourself from malicious exploitation via MIME sniffing.

MIME-Type sniffing explained

Internet Explorer and Chrome browsers have a feature called "MIME-Type sniffing" that automatically detects a web resource's type. This means, for example, that a resource identified as an image can be read as a script if its content is a script.

This property allows a malicious person to send a file to your website to inject malicious code. We advise you to disable the MIME-Type sniffing to limit such activity.

Chrome has been working on a feature called Site Isolation which provides extensive mitigation against exploitation of these types of vulnerabilities. Site Isolation is more effective when MIME types are correct.

How to prevent MIME-Type sniffing

Configure a "X-Content-Type-Options" HTTP header. Add the "X-Content-Type-Options" HTTP header **in the responses of each resource**, associated to the "nosniff" value. It allows you to guard against such misinterpretations of your resources.

The "X-Content-Type-Options" HTTP header can be configured with your Apache server. Make sure that the mod_headers module is enabled. Then, you can specify the header (in your .htaccess file, for example). Here is an example:

Example

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

On this page, **you should configure the following resources**, that risk being misinterpreted:

Resources from "mgcub"

- http://mgcub.ac.in/css/linearicons.css
- http://mgcub.ac.in/css/font-awesome.min.css
- http://mgcub.ac.in/css/bootstrap.css
- http://mgcub.ac.in/css/magnific-popup.css
- http://mgcub.ac.in/css/bootstrap.min.css
- http://mgcub.ac.in/css/nice-select.css
- http://mgcub.ac.in/css/animate.min.css
- http://mgcub.ac.in/css/owl.carousel.css
- http://mgcub.ac.in/css/jquery-ui.css
- http://mgcub.ac.in/css/main.css
- http://mgcub.ac.in/js/vendor/jquery-3.2.1.min.js
- http://mgcub.ac.in/js/popper.min.js
- http://mgcub.ac.in/js/vendor/bootstrap.min.js
- http://mgcub.ac.in/js/easing.min.js
- http://mgcub.ac.in/js/hoverIntent.js
- and 9 others

Resources hosted by a third-party

It appears these files are hosted by a third-party, so they may not be within your control. However, you should consider any alternative to these resources to improve your page performance.

- https://platform.twitter.com/widgets.js
- platform.twitter.com/js/moment~timeline~tweet.ae[...]a43cb146e35371430188e.js
- https://platform.twitter.com/js/timeline.687eed636a16648c9f0b1f72d7fa68bd.js
- platform.twitter.com/css/timeline.32f7f89e2e680e[...]efb27966ae.light.ltr.css

Apache

Your Optimization Priorities

0/100

#74

! You should not expose your Apache server version

The `Server` HTTP header in your server responses indicates your apache version: `Apache/2.4.46`. It will be more difficult for a hacker to attack your website if he does not know the version you use. Think to change this value.

For instance, if you are on a Linux server, edit your */etc/apache2/conf.d/security* file. You will have to change the ServerSignature and the ServerTokens values, as shown bellow:

Example

```
# Hide the version from the 'Server' HTTP Header.
# (e.g.): display only "Server: Apache"
ServerTokens Prod
```

Example

```
# Do not add a trailing footer line under server-generated document,
# containing the server name and its version.
ServerSignature Off
```

However, keep in mind that the best way to protect your system from attacks is to regularly update your Apache server.

PHP

Your Optimization Priorities

0/100

#2573

Do not expose your PHP version

Hide your version of PHP to limit your exposure to attacks and increase your server's security.

Dareboost has detected `PHP 7.3.21`.

Why hide the PHP version?

Knowing the version of PHP used on a server helps an attacker to target security holes and exploit vulnerabilities.

How to hide the PHP version

To hide your PHP version, you need to find your php.ini configuration file and locate the keyword `expose_php` to set its value to `off`.

Example

```
# php.ini
# expose_php = off
```

Once the php.ini file modified, you will need to restart your web server.