# Guide To Fixing Mixed Content

Companion Guide To HTTPS Checker & HTTPS Reporter

httpschecker.net

## About Us

The httpschecker.net service offers our HTTPS Checker scanning app and HTTPS Reporter real-time issue reporting tool to identify mixed content issues. We typically follow a “freemium” model so as many businesses as possible can benefit from our apps for free, with advanced features or scaled up versions available to purchase.

To get HTTPS Checker & HTTPS Reporter visit https://httpschecker.net/

# Introduction

This guide is intended to help you understand how to fix mixed content issues and can be used as an accompaniment to our HTTPS Checker and HTTPS Reporter tools.

To read more about what mixed content is, read our "***HTTPS, Mixed Content & Why It Matters***" PDF which you can download from httpschecker.net.

You can also read the excellent guide from Jo-el  van Bergen on Google's Developer pages about how to Prevent Mixed Content.

# Finding Pages With Mixed Content Issues

There are 3 ways you can find mixed content:

1. **Roll your sleeves up and get stuck in**. Visit each individual HTTPS page in a modern browser like Chrome and use their developer tools to see if there are errors on the page. The problem with this method is it is time-consuming for larger sites.

2. **Sit back and wait.** Passively collect issues from across your entire site by implementing a Content Security Policy. This reports issues found on pages as and when they are visited by users. Our HTTPS Reporter tool can collate these reports as they come in so you have an easy fix list to work from. The drawback with this method is it could take quite some time to identify all the issues for a site, so you might wish to perform an active crawl of your site first, especially if preparing to migrate to https.

3. **Actively find and fix issues.** Use a specialised tool to crawl your pages and report on issues which you can solve in a planned fashion. Our HTTPS Checker tool was created for this purpose since there was no other at-scale tool available. Once done, use HTTPS Reporter to report ad hoc issues.

For more detailed information on finding and fixing issues, refer to Google's post.

## Finding Secure Versions Of Content & Fixing Issues

Mixed content issues occur when there are "HTTP" resources being used on a HTTPS page. For example, an image file is called via a URL starting "http://" rather than "https://" i.e. the "s" part is missing. Other files causing issues might include javascript, fonts, css, audio and video.

To fix the issue check whether the secure version of the file is available. Open a new tab and change the file's address to start "https://" and see if it is available without any error messages and the "green padlock" is present in the browser.

*If the HTTPS version is available:*

Change your web page so the file's URL starts with "https://" and re-publish it. Refresh the page and make sure the issue is fixed.

REMEMBER: You Can Use Relative Links In Your Content

❏ Use *protocol relative* URL's for external links e.g.. "//www.site.com/file.xx" rather than "http://www.site.com/file.xx". This allows your site to load the link via HTTPS once it is available.

- ❏ Similarly, use *relative* links for internal files e.g. “/file.xx” rather than “http://www.site.com/file.xx”.

*If the HTTPS version isn’t available, either:*

1. Find the file on a different server which uses HTTPS and use this one.
2. Download then add the file to your own website it it’s allowed, or source an alternative you can use on your site.
3. Remove the file from your site entirely.

## Keeping Your Site Free From Mixed Content Issues

To keep your site free from new issues once it is fixed:

- ❏ Check every page that has content added or changed is secure via your range of supported browsers or install a plug-in to your site that checks content you post does not create issues.
- ❏ Implement a Content Security Policy on your site then collect and action reports of issues as they occur, for example via our HTTPS Reporter tool.
- ❏ Run a scan over your site on a periodic basis and action any issues found. Our HTTPS Checker tool can be used for this.

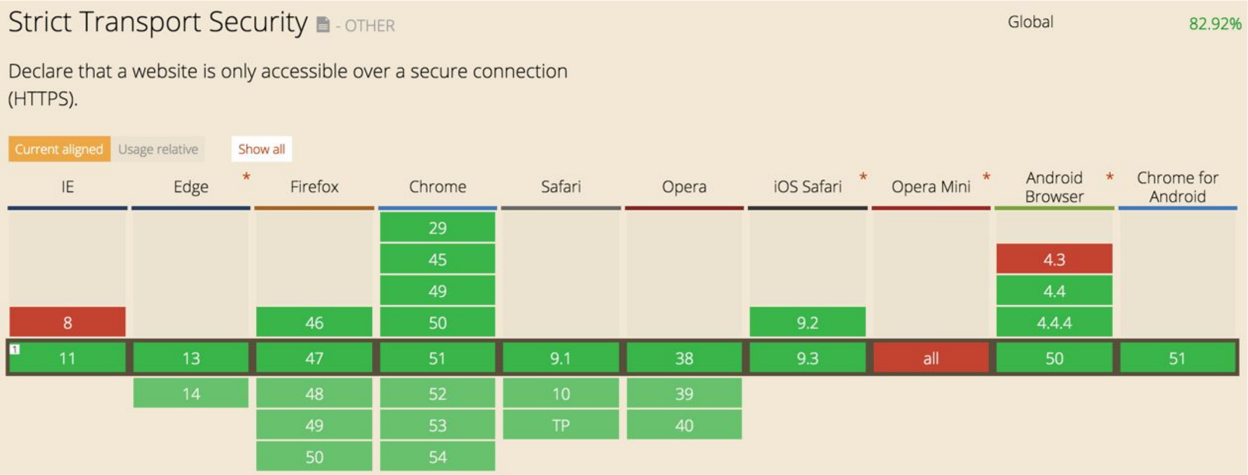
## Content Security Policy

For more information on understanding and implementing Content Security Policy, visit Google’s Developer pages. When implementing policies you have to consider browser usage and compatibility as well so the following links will help:

- ❏ Strict Transport Security - Supported Browsers
  Declare that a website is only accessible over a secure connection (HTTPS).

❏ Content Security Policy 1.0 - Supported Browsers

Mitigate cross-site scripting attacks by whitelisting allowed sources of script, style, and other resources.



Strict Transport Security - OTHER

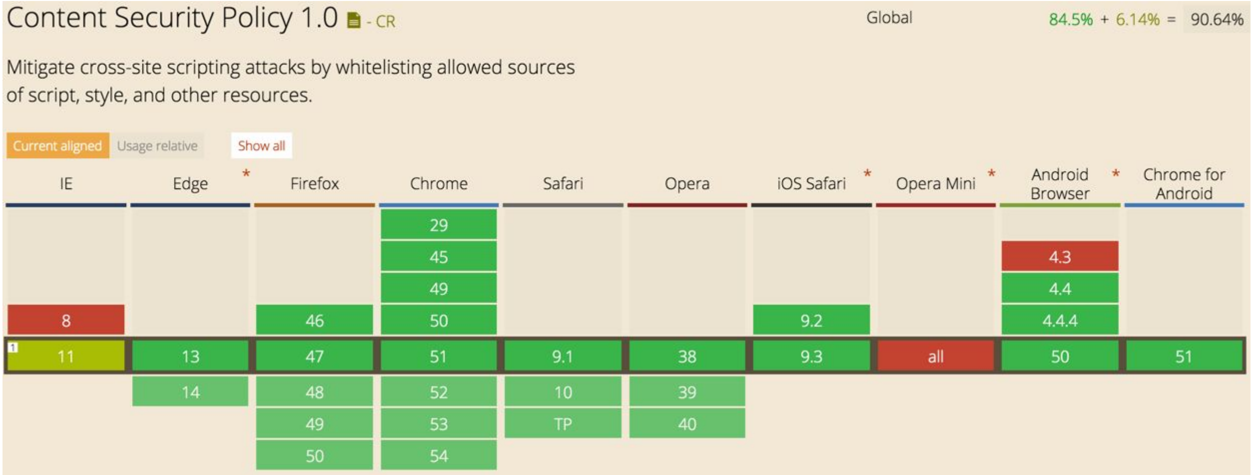
Global 82.92%

Declare that a website is only accessible over a secure connection (HTTPS).

Current aligned Usage relative Show all

| IE | Edge * | Firefox | Chrome | Safari | Opera | iOS Safari * | Opera Mini * | Android Browser * | Chrome for Android |
|---|---|---|---|---|---|---|---|---|---|
| | | | 29 | | | | | | |
| | | | 45 | | | | | 4.3 | |
| | | | 49 | | | | | 4.4 | |
| 8 | | 46 | 50 | | | 9.2 | | 4.4.4 | |
| 1 11 | 13 | 47 | 51 | 9.1 | 38 | 9.3 | all | 50 | 51 |
| | 14 | 48 | 52 | 10 | 39 | | | | |
| | | 49 | 53 | TP | 40 | | | | |
| | | 50 | 54 | | | | | | |

*Illustration: Compatible browsers for Strict Transport Security policy (HSTS) as of 21st July 2016*



Content Security Policy 1.0 - CR

Global 84.5% + 6.14% = 90.64%

Mitigate cross-site scripting attacks by whitelisting allowed sources of script, style, and other resources.

Current aligned Usage relative Show all

| IE | Edge * | Firefox | Chrome | Safari | Opera | iOS Safari * | Opera Mini * | Android Browser * | Chrome for Android |
|---|---|---|---|---|---|---|---|---|---|
| | | | 29 | | | | | | |
| | | | 45 | | | | | 4.3 | |
| | | | 49 | | | | | 4.4 | |
| 8 | | 46 | 50 | | | 9.2 | | 4.4.4 | |
| 1 11 | 13 | 47 | 51 | 9.1 | 38 | 9.3 | all | 50 | 51 |
| | 14 | 48 | 52 | 10 | 39 | | | | |
| | | 49 | 53 | TP | 40 | | | | |
| | | 50 | 54 | | | | | | |

*Illustration: Compatible browsers for Content Security Policy 1.0 as of 21st July 2016*