

Safe and unsafe content on the web site

If the domain name is redirected to the secure HTTPS protocol after the certificate is installed, there may be a broken pad in the browser's address bar. Which also displays a warning message for browsers.

The broken pad and warning messages are displayed because we display secure and unsafe items at the same time as the web page code. The website will only be completely safe - the green pad in the browser heading will appear - if all elements are displayed via HTTPS.

Example:

```
<a href="http://www.example.com/pictures/picture.jpg">View Image</a>
```

In the above HTML example, the URL of the image in the link is referred to as unsafe (http: //). That is, the visitor can view the rest of the content via a secure connection but not the image itself, so the visitor will see mixed content in the browser. The problem can be caused by external sources, JavaScript, and CSS files.

THIS PROBLEM CAN BE IMPROVED IN TWO WAYS:

USING RELATIVE LINKS

For content (such as images uploaded to the web page, CSS, and Javascript files) that can be accessed from the web site in a relative way.

Example:

```
<a href="/picture/picture.jpg">View Image</a>
```

ALL INCLUDED SOURCES ARE CALLED THROUGH AN SSL CONNECTION:

In this case, all references to the webpage - whether image, CSS, Javascript, or letter type file - are called via secure SSL (https://).

Example:

```
<script type="text/javascript" src="https://example.com/javascript.js" />
```

Unfortunately, this method can only be used if the remote content page is available through HTTPS.

If it is unavailable, you should unfortunately locally store previously included content and relate it in a relative way, or look for a source where the content you want to link is accessible through a secure connection.

Revision #1

Created 2023-10-18 12:47:17 CEST by DotRoll Knowledge Base

Updated 2023-10-18 12:47:54 CEST by DotRoll Knowledge Base