

Beveiliging en cross-site verwijzingen

Vanaf december 2018 is Ruimtelijkeplannen.nl volledig gebruik gaan maken van het https-protocol. Dit https-protocol zorgt er voor dat het webverkeer tussen gebruiker en webserver geheel beveiligd plaats vindt. Webrowsers kunnen hierdoor niet meer de melding geven dat de website (mogelijk) onveilig is.

N.B. Alle aanwezige planinformatie was al geheel beveiligd en is ook geheel gewaarmerkt, daaraan is niet veranderd.

Desondanks zijn er enkele situaties waarin gebruikers nog steeds meldingen kunnen krijgen dat de website onveilig is of niet volledig beveiligd is. Deze worden veroorzaakt doordat in een van de planteksten een verwijzing naar een http-locatie buiten Ruimtelijkeplannen.nl is opgenomen welke niet bereikbaar is via https. Het gaat hierbij om een weblocatie bij bijvoorbeeld een stedenbouwkundig bureau, softwareleverancier of een gemeente.

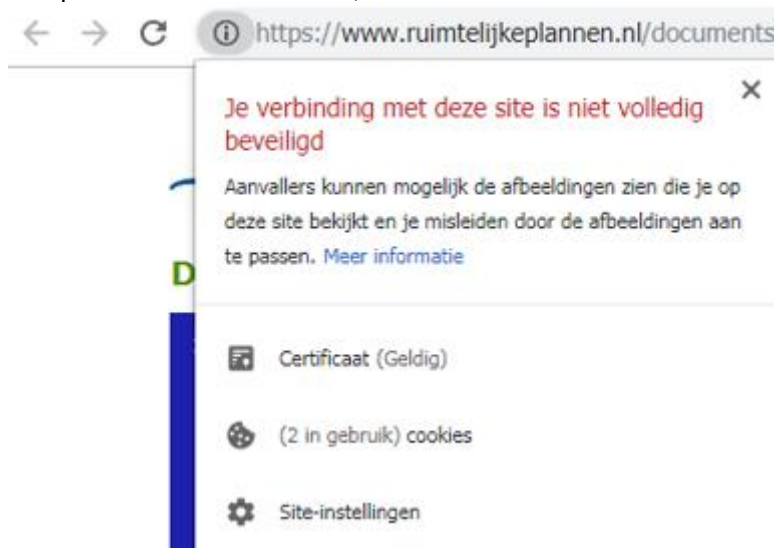
De situatie komt voornamelijk voor bij verwijzingen welke opgenomen zijn in planteksten in (x)htm(l)-formaat. Het betreft voornamelijk verwijzingen naar opmaakbestanden (css) of afbeeldingen.

De oplossing in alle situaties is dat op de webserver van de externe organisatie een redirect van http naar https wordt ingesteld. Hiermee kan worden ingesteld dat webverkeer welke binnenkomt via http automatisch wordt doorgestuurd naar https.

Verschillende organisaties hebben hun webserver al voor http en https ingesteld, oftewel de afbeeldingen of andere verwijzingen zijn zowel via http als via https bereikbaar. Om er voor te zorgen dat het webverkeer altijd via het beveiligde https-protocol verloopt dient mogelijk de redirect van http naar https nog ingesteld te worden.

VOORBEELDEN:

Onderstaand een deel uit het webbrowserscherf (Google Chrome) van een plantekst. Dit betreft een plantekst in html-formaat;



Deze melding wordt veroorzaakt doordat de afbeelding alleen via http bereikbaar is. Wanneer deze afbeelding rechtstreeks wordt geopend in de webbrowser dan verschijnt onderstaande tekst ("Niet beveiligd") aan het begin van het browserscherf (Google Chrome);



De plantekst (source van een html) bevat een verwijzing welke te herleiden is naar een onbeveiligde http-verbinding;

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="nl" xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8"/>
<title>Doorwerth 2013: Regels</title>
<link href="opmaak.css" rel="stylesheet" type="text/css"/>
</head>
<body>
```

De geel gemarkeerde opmaak.css bevat een link naar het css-bestand. Dit css-bestand bevat vervolgens een verwijzing naar een afbeelding op een http-locatie. Deze verwijzing in dit css-bestand staat onderstaand geel gemarkeerd weergegeven;

```
div#koptekst {
width:100%; /* nodig voor has-layout in IE */
background:#FFF url(http://opmaak.<naam>.nl/<gemeente>/opmaak_logo.jpg) no-repeat 0 15px;
padding-top:100px;
```

Onderstaand nog een voorbeeld van een regel uit een plantekst (html). In deze situatie verwijst deze rechtstreeks naar de externe locatie.

```
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<title>Bebouwde kommen; herziening 2017</title>
<link href="opmaak-stri.css" rel="stylesheet" type="text/css" />
<link href="NL.IMRO.0848.BP150BEBOUWDEKOM-VA01.css" rel="stylesheet" type="text/css" />
<script src="http://lib.<organisatie>.nl/rotekst/template/Rotekst.js" type="text/javascript"></script>
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js"></script>
</head>
<body>
```