Content Security Policy

Walter Ebert

PHP Usergroup
Frankfurt am Main
21. November 2013

http://www.flickr.com/photos/murdelta/5963788863/

Walter Ebert

@wltrd

walterebert.de

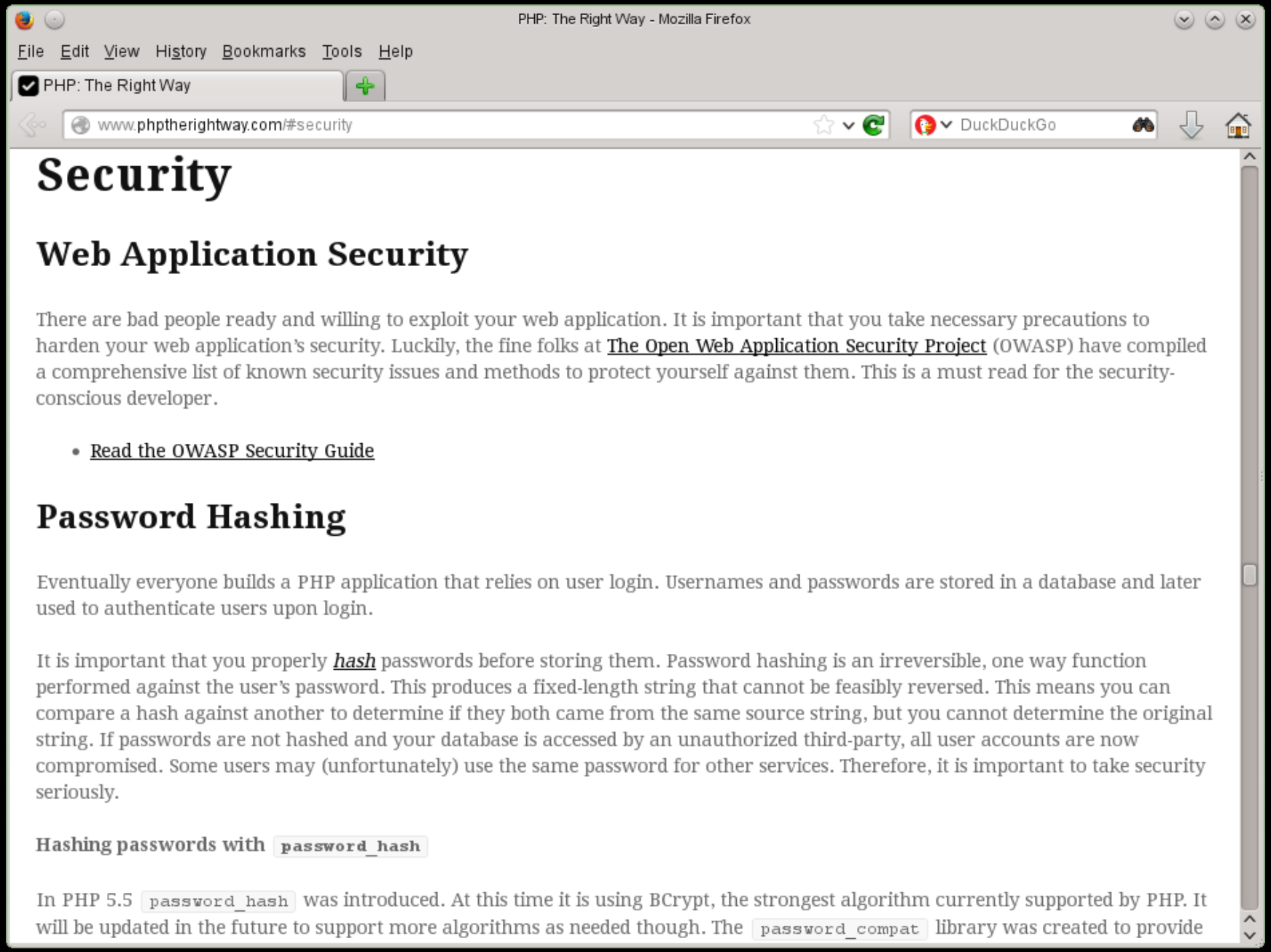
XSS

Cross-Site-Scripting ist eine Art der HTML Injection. Cross-Site-Scripting tritt dann auf, wenn eine Webanwendung Daten annimmt, die von einem Nutzer stammen, und diese Daten dann an einen Browser weitersendet, ohne den Inhalt zu überprüfen. Damit ist es einem Angreifer möglich, auch Skripte indirekt an den Browser des Opfers zu senden und damit Schadcode auf der Seite des Clients auszuführen.

https://de.wikipedia.org/wiki/Cross-Site-Scripting

Schützt den Benutzer

Nicht die Anwendung



http://www.phptherightway.com/#security

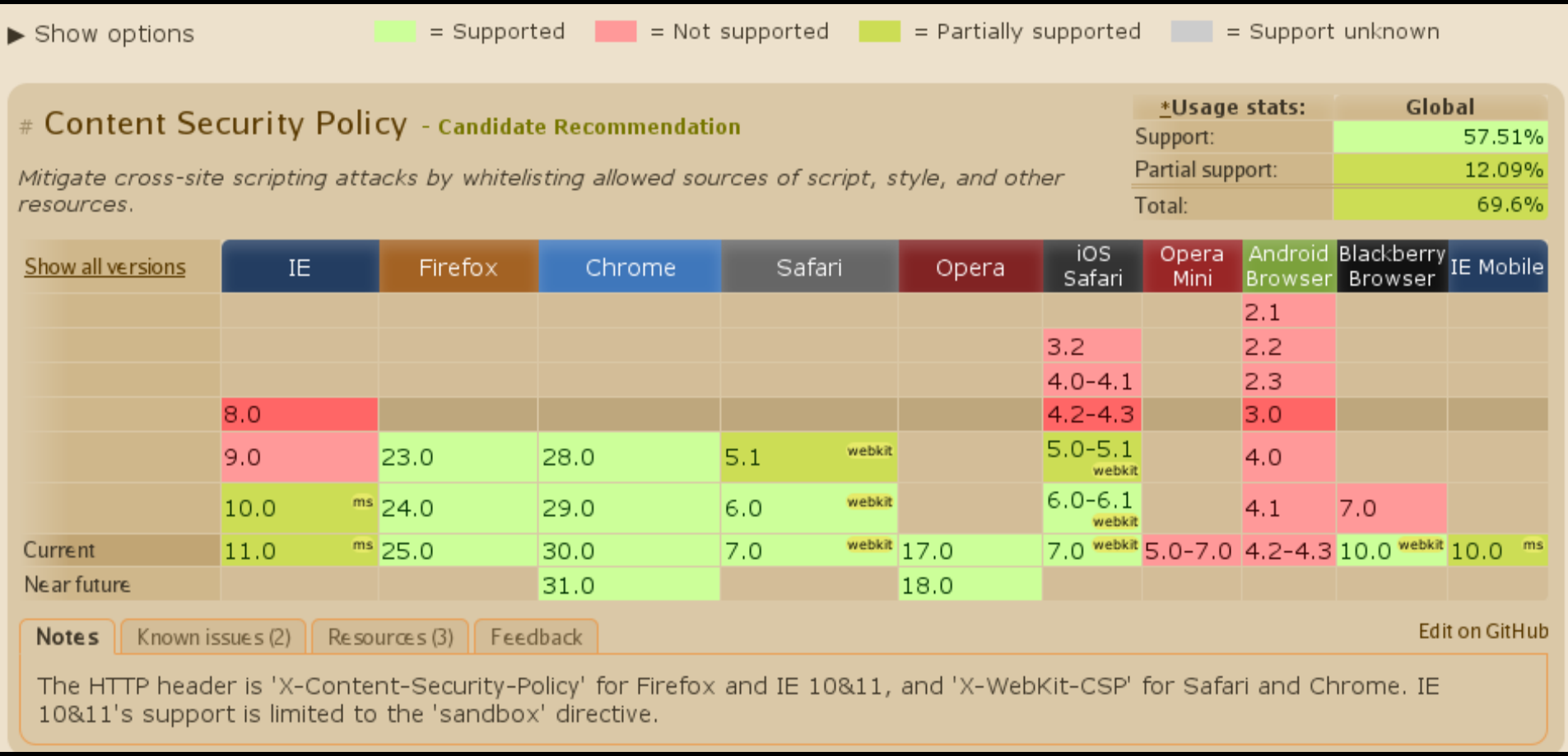
W3C Content Security Policy

CSP 1.0

http://www.w3.org/TR/CSP/

CSP 1.1 (In Arbeit)

https://dvcs.w3.org/hg/content-security-policy/raw-file/tip/csp-specification.dev.html



http://caniuse.com/#search=csp

Konfiguration

Apache

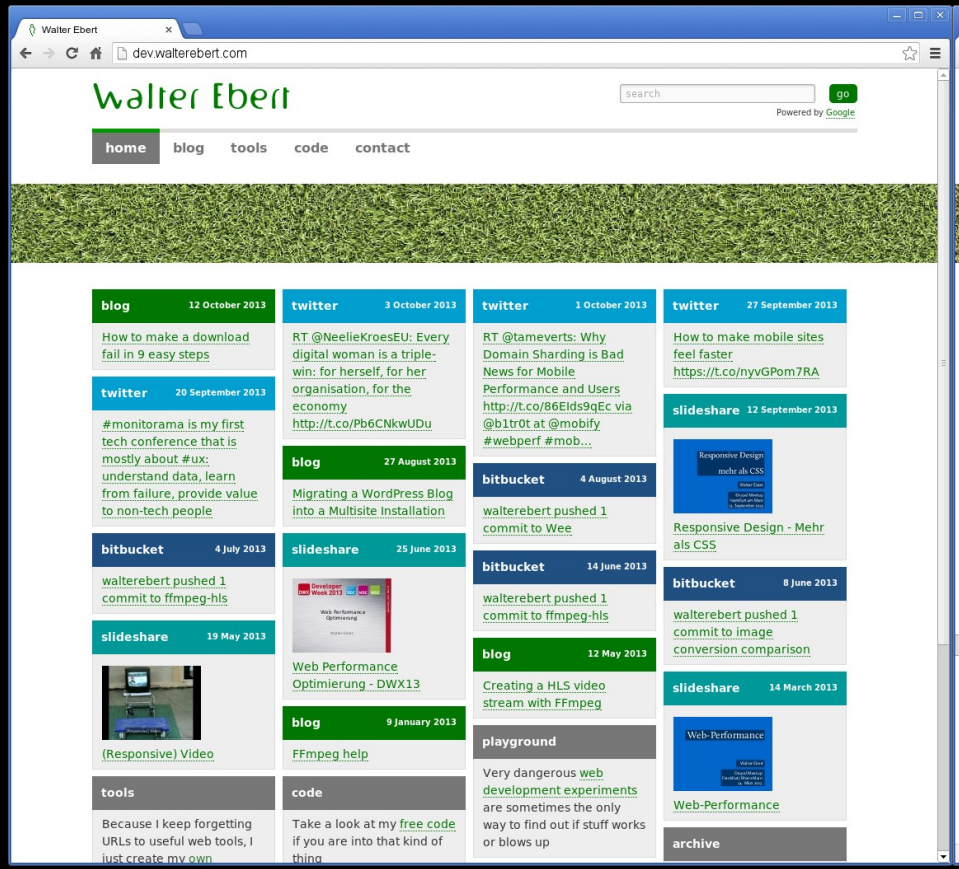
```
<IfModule mod_headers.c>
Header set Content-Security-Policy "default-src 'self';"
</IfModule>
```

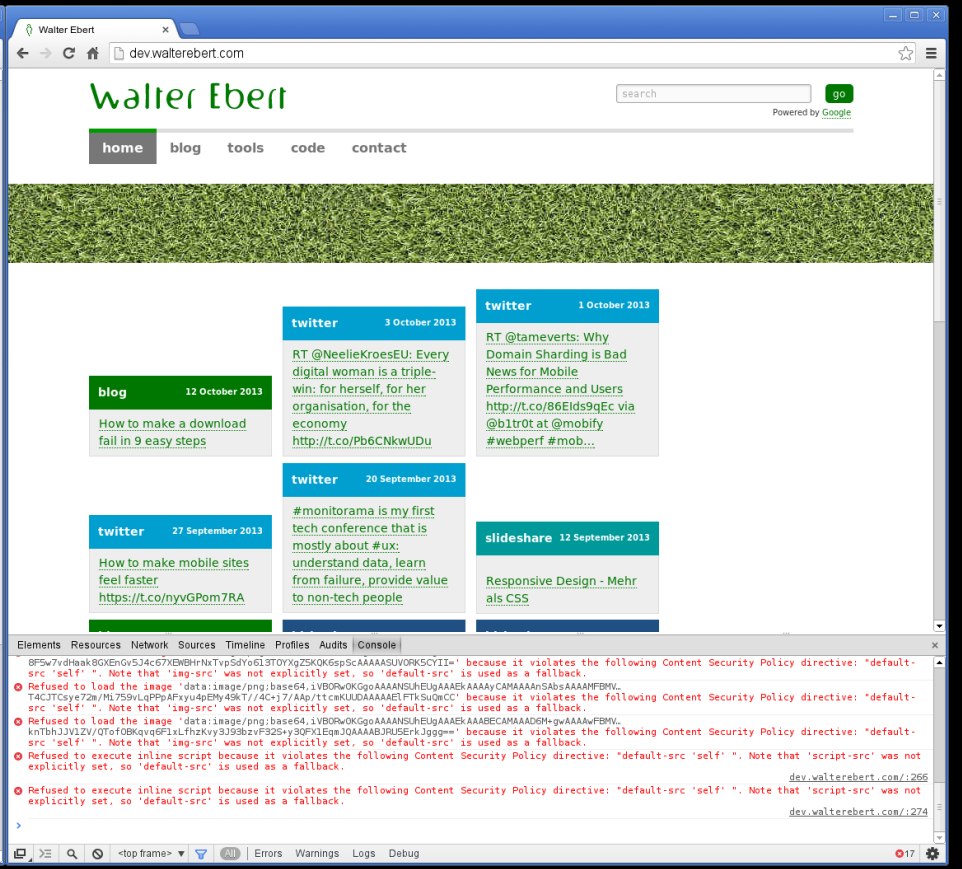
PHP

```
header("Content-Security-Policy: default-src 'self';");
```

```
$ curl -I http://dev.walterebert.com

HTTP/1.1 200 OK
Date: Sat, 02 Nov 2013 12:49:57 GMT
Server: Apache/2.2.22
X-Powered-By: PHP/5.3.17
Cache-Control: max-age=0
Expires: Sat, 02 Nov 2013 12:49:57 GMT
Content-Security-Policy: default-src 'self';
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
```


Walter Ebert
dev.walterebert.com
Walter Ebert
search
go
Powered by Google
home
blog
tools
code
contact
blog 12 October 2013
How to make a download fail in 9 easy steps
twitter 20 September 2013
#monitorama is my first tech conference that is mostly about #ux: understand data, learn from failure, provide value to non-tech people
bitbucket 4 July 2013
walterebert pushed 1 commit to ffmpeg-hls
slideshare 19 May 2013
(Responsive) Video
tools
Because I keep forgetting URLs to useful web tools, I just create my own
twitter 3 October 2013
RT @NeelieKroesEU: Every digital woman is a triple-win: for herself, for her organisation, for the economy http://t.co/Pb6CNkwUDu
blog 27 August 2013
Migrating a WordPress Blog into a Multisite Installation
slideshare 25 June 2013
Web Performance Optimierung - DWX13
blog 9 January 2013
FFmpeg help
code
Take a look at my free code if you are into that kind of thing
twitter 1 October 2013
RT @tameverts: Why Domain Sharding is Bad News for Mobile Performance and Users http://t.co/86Elds9qEc via @b1t0t at @mobify #webperf #mob...
bitbucket 4 August 2013
walterebert pushed 1 commit to Wee
bitbucket 14 June 2013
walterebert pushed 1 commit to ffmpeg-hls
blog 12 May 2013
Creating a HLS video stream with FFmpeg
playground
Very dangerous web development experiments are sometimes the only way to find out if stuff works or blows up
twitter 27 September 2013
How to make mobile sites feel faster https://t.co/nyvGPom7RA
slideshare 12 September 2013
Responsive Design - Mehr als CSS
bitbucket 8 June 2013
walterebert pushed 1 commit to image conversion comparison
slideshare 14 March 2013
Web-Performance
archive


Walter Ebert
dev.walterebert.com
Walter Ebert
search
go
Powered by Google
home
blog
tools
code
contact
blog 12 October 2013
How to make a download fail in 9 easy steps
twitter 3 October 2013
RT @NeelieKroesEU: Every digital woman is a triple-win: for herself, for her organisation, for the economy http://t.co/Pb6CNkwUDu
twitter 1 October 2013
RT @tameverts: Why Domain Sharding is Bad News for Mobile Performance and Users http://t.co/86Elds9qEc via @b1t0t at @mobify #webperf #mob...
twitter 20 September 2013
#monitorama is my first tech conference that is mostly about #ux: understand data, learn from failure, provide value to non-tech people
twitter 27 September 2013
How to make mobile sites feel faster https://t.co/nyvGPom7RA
slideshare 12 September 2013
Responsive Design - Mehr als CSS
Elements Resources Network Sources Timeline Profiles Audits Console
Refused to load the image '…
Refused to load the image '…
Refused to execute inline script because it violates the following Content Security Policy directive: "default-src 'self' ". Note that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.
dev.walterebert.com/:266
Refused to execute inline script because it violates the following Content Security Policy directive: "default-src 'self' ". Note that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.
dev.walterebert.com/:274
Errors Warnings Logs Debug

Reporting

Apache

```
<IfModule mod_headers.c>
Header set Content-Security-Policy-Report-Only \
  "default-src 'self'; report-uri /csp-reporter.php;"
</IfModule>
```

PHP

```
header("Content-Security-Policy-Report-Only: default-src 'self';
  report-uri /csp-reporter.php;");
```

csp-reporter.php

```
<?php
header('HTTP/1.1 204 No Content');

$data = file_get_contents('php://input');
if (is_string($data) and json_decode($data)) {
    syslog(LOG_INFO, $data);
}
```

HTTP POST


```
{
  "csp-report":
  {
    "document-uri":"http://dev.walterebert.com/",
    "referrer":"",
    "violated-directive":"default-src 'self' ",
    "original-policy":"default-src 'self'; report-uri /csp-reporter.php;",
    "blocked-uri":"http://cdn.slidesharecdn.com",
    "status-code":200
  }
}
```

Chrome

{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","violated-directive":"default-src 'self' ","original-policy":"default-src 'self' ; report-uri /csp-reporter.php;","blocked-uri":"http://cdn.slidesharecdn.com","status-code":200}}

{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","violated-directive":"default-src 'self' ","original-policy":"default-src 'self' ; report-uri /csp-reporter.php;","blocked-uri":"data","status-code":200}}

{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","violated-directive":"default-src 'self' ","original-policy":"default-src 'self' ; report-uri /csp-reporter.php;","blocked-uri":"","status-code":200}}

Firefox

{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"https://cdn.slidesharecdn.com/ss_thumbnails/responsive-design-drupal-meetup-frankfurt-130912115128-phpapp01-thumbnail-2.jpg?1379004938","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"https://cdn.slidesharecdn.com/ss_thumbnails/web-performance-optimierung-developer-week-2013-130625082350-phpapp02-thumbnail-2.jpg?1372582510","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"https://cdn.slidesharecdn.com/ss_thumbnails/webperfdays-amsterdam-2013-responsive-video-130519125920-phpapp02-thumbnail-2.jpg?1378556655","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"self","violated-directive":"inline script base restriction","source-file":"http://dev.walterebert.com/","script-sample":"\n// Responsive menu\nif (typeof window.ma...","line-number":14}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"https://cdn.slidesharecdn.com/ss_thumbnails/web-performance-drupal-meetup-frankfurt-2013-130314172209-phpapp01-thumbnail-2.jpg?1363299801","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"http://cdn.slidesharecdn.com/ss_thumbnails/responsive-design-drupal-meetup-frankfurt-130912115128-phpapp01-thumbnail-2.jpg?1379004938","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"http://cdn.slidesharecdn.com/ss_thumbnails/web-performance-optimierung-developer-week-2013-130625082350-phpapp02-thumbnail-2.jpg?1372582510","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"http://cdn.slidesharecdn.com/ss_thumbnails/webperfdays-amsterdam-2013-responsive-video-130519125920-phpapp02-thumbnail-2.jpg?1378556655","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"http://cdn.slidesharecdn.com/ss_thumbnails/web-performance-drupal-meetup-frankfurt-2013-130314172209-phpapp01-thumbnail-2.jpg?1363299801","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"","violated-directive":"default-src http://dev.walterebert.com:80"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"self","violated-directive":"inline script base restriction","source-file":"http://dev.walterebert.com/","script-sample":"\n\tif (typeof window.matchMedia === \"unde...","line-number":266}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"self","violated-directive":"inline script base restriction","source-file":"http://dev.walterebert.com/","script-sample":"\n/* Modernizr 2.6.2 (Custom Build) | MIT...","line-number":274}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/img/logo2.svg","referrer":"http://dev.walterebert.com/","blocked-uri":"self","violated-directive":"inline style base restriction","source-file":"http://dev.walterebert.com/img/logo2.svg","script-sample":"fill:#007a00;stroke:none;"}}
{"csp-report":{"document-uri":"http://dev.walterebert.com/","referrer":"","blocked-uri":"self","violated-directive":"inline script base restriction","source-file":"http://dev.walterebert.com/","script-sample":"try { for(var lastpass_iter=0; lastpass..."}}

Direktiven

default-src : Alle Ressourcen

img-src : Bilder

style-src : Stylesheets

media-src : Audio + Video

frame-src : iframes

connect-src : AJAX, WebSockets, EventSource

font-src : Schriften

object-src : Flash, Java, usw.

Keywords

***** : Alles erlauben

'none' : Nichts erlauben

'self ' : Nur Ursprungsdomain (nicht Subdomains)

'unsafe-inline' : Inline JavaScript + CSS

'unsafe-eval ' : JavaScript eval()

Beispiele

```
# Lokal + Inline CSS/JS + Data URI
default-src 'self'; style-src 'unsafe-inline'; script-src 'unsafe-inline'; img-src data:;

# Lokal + CDN
default-src 'self' *.amazonaws.com;

# Lokal + Bilder von Überall
default-src 'self'; img-src: *;

# Nur SSL
default-src https:;

# Explizite Freigaben
default-src 'none'; style-src 'self'; script-src 'self'; img-src 'self';
```

Browserunterschiede

Firefox

```
default-src 'self'; script-src 'unsafe-inline';
```

Chrome

```
default-src 'self'; script-src 'self' 'unsafe-inline';
```

```
$ curl -I http://walterebert.com
HTTP/1.1 200 OK
Date: Mon, 18 Nov 2013 19:38:14 GMT
Server: Apache
Cache-Control: max-age=0, no-cache
Content-Security-Policy: default-src 'self'; img-src data: http: https: *.slidesharecdn.com *.slideshare.net; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; report-uri /csp-reporter.php;
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
```

Beispiele blockierter URIs

mx://res/reader-mode/reader.html

chromenull://

chromeinvoke://1fb8adb44a3b9f7b1671bf5082dbf486

chromeinvokeimmediate://95dc806b80bec27e456ff17770b82cf8

chrome-extension://noojglkidnpfjbincgijbaiedldjfbhh

android-webview

safari-extension://com.wotservicesoy.wot-ff6ww26hl3

safari-extension://com.avast.wrc-6h4hrtu5e3

moz-icon://noscript?size=32&contentType=video/ogg

http://cdncache-a.akamaihd.net

https://d3ijcis4e2ziok.cloudfront.net

https://translate.googleapis.com

Walter Ebert

@wltrd

walterebert.de

walterebert.com

slideshare.net/walterebert

DrupalCamp Frankfurt, 12.-13. April 2014

drupal-am-main.de

Referenzen

http://content-security-policy.com/

https://www.owasp.org/index.php/Content_Security_Policy

http://www.html5rocks.com/en/tutorials/security/content-security-policy/

https://developer.mozilla.org/en-US/docs/Security/CSP

http://caniuse.com/#search=csp

http://mathiasbynens.be/notes/csp-reports

http://www.w3.org/TR/CSP/

https://dvcs.w3.org/hg/content-security-policy/raw-file/tip/csp-specification.dev.html