

Content Security Policy

Walter Ebert

Bereich

der vorbildlichen
**ÖRDNUNG, SICHERHEIT
SAUBERKEIT
und DISZIPLIN**

PHP Usergroup
Frankfurt am Main
21. November 2013

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.

Schützt den Benutzer

Nicht die Anwendung



Security

Web Application Security

There are bad people ready and willing to exploit your web application. It is important that you take necessary precautions to harden your web application's security. Luckily, the fine folks at [The Open Web Application Security Project](#) (OWASP) have compiled a comprehensive list of known security issues and methods to protect yourself against them. This is a must read for the security-conscious developer.

- [Read the OWASP Security Guide](#)

Password Hashing

Eventually everyone builds a PHP application that relies on user login. Usernames and passwords are stored in a database and later used to authenticate users upon login.

It is important that you properly *hash* passwords before storing them. Password hashing is an irreversible, one way function performed against the user's password. This produces a fixed-length string that cannot be feasibly reversed. This means you can compare a hash against another to determine if they both came from the same source string, but you cannot determine the original string. If passwords are not hashed and your database is accessed by an unauthorized third-party, all user accounts are now compromised. Some users may (unfortunately) use the same password for other services. Therefore, it is important to take security seriously.

Hashing passwords with `password_hash`

In PHP 5.5 `password_hash` was introduced. At this time it is using BCrypt, the strongest algorithm currently supported by PHP. It will be updated in the future to support more algorithms as needed though. The `password_compat` library was created to provide

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>

► Show options

■ = Supported

■ = Not supported

■ = Partially supported

■ = Support unknown

Content Security Policy - Candidate Recommendation

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

*Usage stats:	Global
Support:	57.51%
Partial support:	12.09%
Total:	69.6%

Show all versions	IE	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	IE Mobile			
								2.1					
						3.2		2.2					
						4.0-4.1		2.3					
	8.0					4.2-4.3		3.0					
	9.0	23.0	28.0	5.1	webkit	5.0-5.1 webkit		4.0					
	10.0	ms	24.0	29.0	6.0	6.0-6.1 webkit		4.1	7.0				
Current	11.0	ms	25.0	30.0	7.0	7.0	webkit	5.0-7.0	4.2-4.3	10.0	webkit	10.0	ms
Near future			31.0			18.0							

[Notes](#)
[Known issues \(2\)](#)
[Resources \(3\)](#)
[Feedback](#)

[Edit on GitHub](#)

The HTTP header is 'X-Content-Security-Policy' for Firefox and IE 10&11, and 'X-WebKit-CSP' for Safari and Chrome. IE 10&11's support is limited to the 'sandbox' directive.

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

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/86Eids9qEc> via @b1tr0t 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

archive

Responsive Design mehr als CSS

Responsive Design - Mehr als CSS

bitbucket 8 June 2013

walterebert pushed 1 commit to image conversion comparison

slideshare 14 March 2013

Web-Performance

Web-Performance

Walter Ebert

dev.walterebert.com

Walter Ebert

home blog tools code contact

blog 12 October 2013

How to make a download fail in 9 easy steps

twitter 27 September 2013

How to make mobile sites feel faster <https://t.co/hyvGPom7RA>

slideshare 12 September 2013

Responsive Design - Mehr als CSS

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/hyvGPom7RA>

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 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

slideshare 12 September 2013

Responsive Design - Mehr als CSS

twitter 1 October 2013

RT @tameverts: Why Domain Sharding is Bad News for Mobile Performance and Users <http://t.co/86Eids9qEc> via @b1tr0t at @mobify #webperf #mob...

Elements Resources Network Sources Timeline Profiles Audits Console

8f5w7vdh8ak8GXEnGv534c67EWBhNkTvPsdYo6L3TOYqZSKQ6p5cAAAAASUv0K5CYII=' because it violates the following Content Security Policy directive: 'default-src 'self' '. Note that 'img-src' was not explicitly set, so 'default-src' is used as a fallback.

⊗ Refused to load the image '. T4CJT0csy47Zm/Pu759hLqPp0AFyUyqE9y4SR7/4c+17Aa0/1tWU0AAAAR1FR5u0CC' because it violates the following Content Security Policy directive: 'default-src 'self' '. Note that 'img-src' was not explicitly set, so 'default-src' is used as a fallback.

⊗ Refused to load the image '. knTh3JVLZV/0ToFOkveqfP3LhZkV3359bczF925+y8P3LEm3QMAAEDJrUSEh4Jgg==' because it violates the following Content Security Policy directive: 'default-src 'self' '. Note that 'img-src' was not explicitly set, so 'default-src' is used as a fallback.

⊗ 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}}
```


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://95dc806b8obec27e456ff1777ob82cf8>

<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://cdn-cache-a.akamaihd.net>

<https://d3jicis4e2ziok.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>