

Mojolicious and Content-Security-Policy

Erik Johansen
DK Hostmaster A/S
Mojoconf 2014
2014-05-24

Content-Security-Policy

HTML response header

Add security constraints to a web page.

Content-Security-Policy

Enforced by your web browser.

Firefox	23.0	...
Chrome	25.0	...
Safari	7.0	...
Opera	15.0	...
Android browser	4.4	
Opera mobile	21.0	
Chrome for Android	33.0	

Content-Security-Policy

Deprecated headers:

X-Content-Security-Policy

X-Webkit-CSP

Check compatibility on
<http://caniuse.com/contentsecuritypolicy>

Content-Security-Policy

What can you restrict ?

Content-Security-Policy

Restricts access by setting
the permitted origins
for each type of content.

Content-Security-Policy

What does it look like ?

Content-Security-Policy

Content-Security-Policy:

```
report-uri    /some_report_uri;
```

```
default-src  'none';
```

```
img-src      'self' https;;
```


Content-Security-Policy

To get enforcement and reports:

```
Content-Security-Policy:  
  report-uri    /content-security-policy-report;  
  default-src  'none';  
  img-src      'self' https;
```

To get enforcement (no reports):

```
Content-Security-Policy:  
  default-src  'none';  
  img-src      'self' https;
```

To get only reports (no enforcement):

```
Content-Security-Policy-Report-Only: ...
```

Content-Security-Policy

Content-Security-Policy:

```
report-uri    /some_report_uri;
```

```
default-src  'none';
```

```
img-src      'self' https;;
```

```
script-src   'self' https;;
```

```
style-src    'self' https;;
```

```
font-src     'self' https;;
```

```
<source type> <origins>... ;
```

Content-Security-Policy

Source types

'default-src'	Default for unspecified source types
'image-src'	Images can be loaded from
'script-src'	Javascript can be loaded from
'font-src'	Fonts can be loaded from
'style-src'	Styles can be loaded from
'frame-src'	Embedded frames can be loaded from
'media-src'	Media (audio/video) can be delivered from
'object-src'	Flash and other plugins can be loaded from
'connect-src'	Connections can be made to (via XHR, WebSockets, and EventSource)
'sandbox'	Sandbox as for inside iframe (same origin policy)

Content-Security-Policy

Origins

<code>'none'</code>	None (no match)
<code>'self'</code>	Same host
<code>'unsafe-inline'</code>	Inline JS/CSS
<code>'unsafe-eval'</code>	<code>eval()</code>
<code>https:</code>	Only <code>https:</code>
<code>https://apis.google.com/</code>	Exact
<code>example.com</code>	Hostname
<code>*://*.example.com:*</code>	Wildcards

Content-Security-Policy

Sandbox options

allow-forms
allow-same-origin
allow-scripts
allow-top-navigation

Sandbox forms
Sandbox SO
Sandbox scripts
Sandbox nav.

Mojolicious

Generate lite app

```
$ mojo generate lite_app \  
content_security_policy.pl
```

```
$ morbo content_security_policy.pl
```

Lite app

content_security_policy.conf

```
{
  secrets => [ 'some_secret' ],
  'content-security-policy' =>
    join("; ",
      "report-uri /content-security-policy-report",

      "default-src    'none'",

      "script-src     'self'",
      "style-src      'self'",

      "font-src       'self'",
      "img-src        'self'",
    ),
}
```

Lite app

main part

```
#!/usr/bin/env perl
use Mojolicious::Lite;

# Documentation browser under "/perldoc"
plugin 'PODRenderer';

my $cfg = plugin 'config';
app->secrets( $cfg->{secrets} );

if ( my $csp = $cfg->{'content-security-policy'} ) {
    # ... (next slide) ...
}

get '/' => sub {
    my $self = shift;
    $self->render('index');
};

app->start;
__DATA__
```


Lite app

main part

```
if ( my $csp = $cfg->{'content-security-policy'} ) {
    $csp =~ s/ {2,}/ /g;

    hook before_dispatch => sub {
        my $self = shift;

        $self->res->headers->header('Content-Security-Policy' => $csp);
    };

    if ( my $report_uri = $csp =~ /\breport-uri\s+([\^ ;]+)/ && $1 ) {
        post $report_uri => sub {
            my $self = shift;
            my $report = $self->req->json;

            $self->app->log->warn("Policy report:",
                $self->dumper( $report )
            ) if $report;

            $self->render( text => "Thanks for the report!" );
        };
    }
}
```

Lite app templates

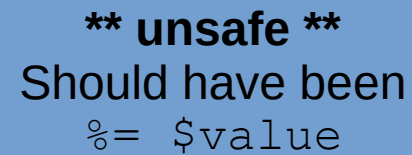
__DATA__

```
@@ index.html.ep
% layout 'default';
% title 'Welcome';
Welcome to the Mojolicious real-time web framework!
```

```
%= form_for "" => begin
  %= text_field 'first_field', size => 50
  %= submit_button
%= end
```

```
% if (my $value = param 'first_field') {
  You typed:
  == $value
% }
```

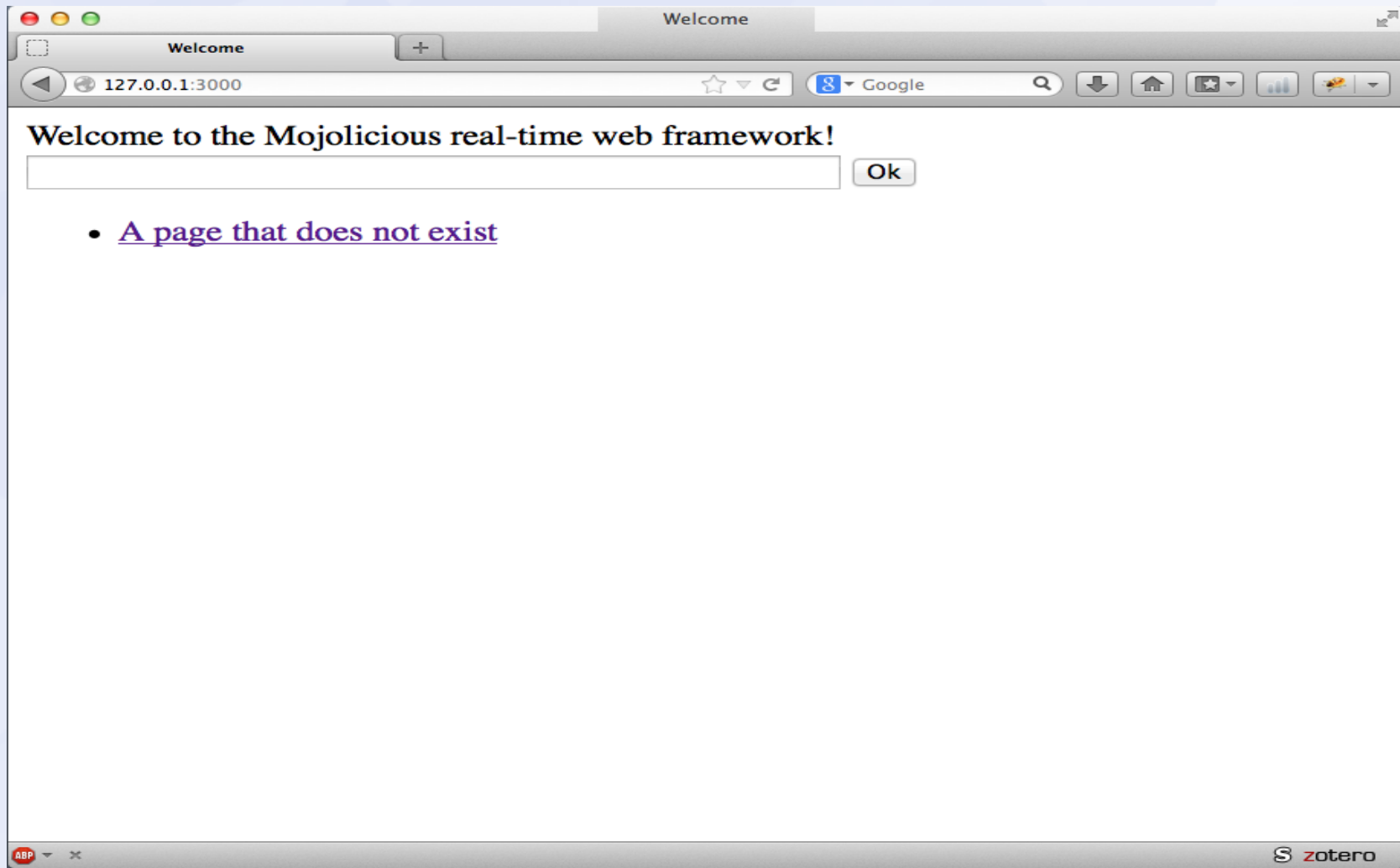
**** unsafe ****
Should have been
%= \$value



```
<ul>
  <li> <a href="/nosuch">A page that does not exist</a> </li>
</ul>
```

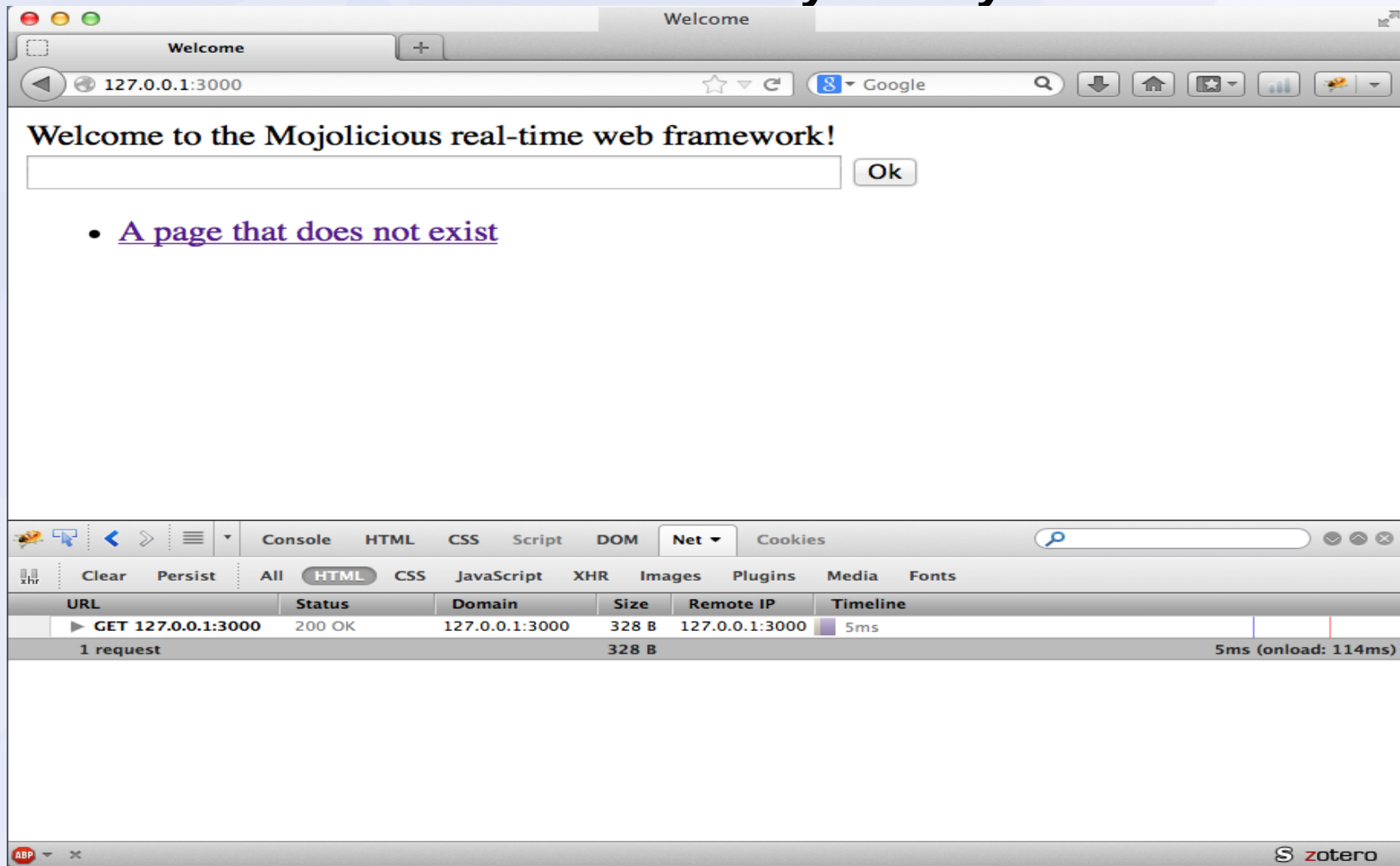
```
@@ layouts/default.html.ep
<!DOCTYPE html>
<html>
  <head><title><%= title %></title></head>
  <body><%= content %></body>
</html>
```

Lite app test



Lite app

Added Content-Security-Policy header



The screenshot shows a web browser window with the address bar set to `127.0.0.1:3000`. The page content includes a heading "Welcome to the Mojolicious real-time web framework!", a text input field, and a button labeled "Ok". Below the input field is a bulleted list with one item: [A page that does not exist](#).

The browser's developer tools are open to the "Net" tab, displaying a network log for the request `GET 127.0.0.1:3000`. The log shows a status of `200 OK`, a size of `328 B`, and a response time of `5ms (onload: 114ms)`.

URL	Status	Domain	Size	Remote IP	Timeline
▶ GET 127.0.0.1:3000	200 OK	127.0.0.1:3000	328 B	127.0.0.1:3000	5ms
1 request			328 B		5ms (onload: 114ms)

Lite app

Added Content-Security-Policy header

The screenshot shows a web browser window with the address bar set to `127.0.0.1:3000`. The page content includes a welcome message, an input field, and a list item:

- [A page that does not exist](#)

The browser's developer tools are open to the 'Network' tab, showing a request to `GET 127.0.0.1:3000` with a status of `200 OK`. The 'Response Headers' section is expanded, displaying the following headers:

Header	Value
Connection	keep-alive
Content-Length	328
Content-Type	text/html; charset=UTF-8
Date	Tue, 15 Apr 2014 16:16:42 GMT
Server	Mojolicious (Perl)
content-security-policy	report-uri /content-security-policy-report; default-src 'none'; script-src 'self'; style-src 'self'; font-src 'self'; img-src 'self'

Lite app

Type `<script>...</script>` into input box. Press OK.

The screenshot shows a web browser window titled "Welcome" with the address bar set to "127.0.0.1:3000". The main content area displays the text "Welcome to the Mojolicious real-time web framework!" followed by an input field containing "Hello world <script>alert(2345)</script>" and an "Ok" button. Below the input field is a bulleted list item: "• [A page that does not exist](#)".

The browser's developer tools are open to the "Net" tab, showing a request log for "GET 127.0.0.1:3000" with a status of "200 OK". The "Response Headers" section is expanded, displaying the following details:

Header	Value
Connection	keep-alive
Content-Length	328
Content-Type	text/html; charset=UTF-8
Date	Tue, 15 Apr 2014 16:16:42 GMT
Server	Mojolicious (Perl)
content-security-policy	report-uri /content-security-policy-report; default-src 'none'; script-src 'self'; style-src 'self'; font-src 'self'; img-src 'self'

The "Request Headers" section is also visible, with a "view source" link. The browser's status bar at the bottom shows "zotero".

Lite app

The javascript does not run.

The screenshot shows a web browser window titled 'Welcome' with the address bar displaying '127.0.0.1:3000/?first_field=Hello+world+<script>alert(2345)</script>'. The page content includes a heading 'Welcome to the Mojolicious real-time web framework!', a text input field containing 'Hello world <script>alert(2345)</script>', and a button labeled 'Ok'. Below the input field, it says 'You typed: Hello world'. A bulleted list contains a link: '• [A page that does not exist](#)'. At the bottom, a network log is visible with the following data:

URL	Status	Domain	Size	Remote IP	Timeline
▶ GET ?first_field=Hell	200 OK	127.0.0.1:3000	446 B	127.0.0.1:3000	6ms
▶ POST content-secur	200 OK	127.0.0.1:3000	22 B	127.0.0.1:3000	7ms
2 requests			468 B (22 B from cache)	148ms (onload: 154ms)	

Lite app

Instead browser sends a JSON report.

The screenshot shows a web browser window with the following content:

127.0.0.1:3000/?first_field=Hello+world+<script>alert(2345)</script>

Welcome to the Mojolicious real-time web framework!

Hello world <script>alert(2345)</script> [Ok]

You typed: Hello world

- [A page that does not exist](#)

The developer console shows a CSP report:

```
Object { document-uri="http://127.0.0.1:3000/?...82345%29%3C%2Fscript%3E",  
referrer="http://127.0.0.1:3000/", blocked-uri="self", more... }
```

Source:

```
{ "csp-report": { "document-uri": "http://127.0.0.1:3000/?first_field=Hello+world+%3Cscript%3Ealert%282345%29%3C%2Fscript%3E", "referrer": "http://127.0.0.1:3000/", "blocked-uri": "self", "violated-directive": "script-src", "source-file": "http://127.0.0.1:3000/?first_field=Hello+world+%3Cscript%3Ealert%282345%29%3C%2Fscript%3E", "script-sample": "alert(2345)", "line-number": 12 } }
```


Lite app

The JSON report is written to the log.

```
[Wed Apr 16 17:01:55 2014] [debug] 200 OK (0.005466s, 182.949/s).
[Wed Apr 16 17:01:55 2014] [debug] POST "/content-security-policy-report".
[Wed Apr 16 17:01:55 2014] [debug] Routing to a callback.
[Wed Apr 16 17:01:55 2014] [warn] Policy report:
{
  "csp-report" => {
    "blocked-uri" => "self",
    "document-uri" => "http://127.0.0.1:3000/?first_field=Hello+world+%3Cscript%3Ealert%282345%29%3C%2Fscript%3E",
    "line-number" => 12,
    "referrer" => "http://127.0.0.1:3000/",
    "script-sample" => "alert(2345)",
    "source-file" => "http://127.0.0.1:3000/?first_field=Hello+world+%3Cscript%3Ealert%282345%29%3C%2Fscript%3E",
    "violated-directive" => "script-src http://127.0.0.1:3000"
  }
}

[Wed Apr 16 17:01:55 2014] [debug] 200 OK (0.001660s, 602.410/s).
```

Mojolicious

Side effects

Any side effects ?

Mojolicious

Side effects

Mojolicious "not_found" page
uses inline styles and scripts
and will be refused by a strict policy.

Lite app

Use /nosuch link.

The screenshot shows a web browser window with the following content:

- Address bar: `127.0.0.1:3000/?first_field=Hello+world+<script>alert(2345)</script>`
- Page content: "Welcome to the Mojolicious real-time web framework!"
- Input field: "Hello world <script>alert(2345)</script>" with an "Ok" button.
- Text below input: "You typed: Hello world"
- List item:
 - [A page that does not exist](#) ← (indicated by a blue arrow)

The browser's developer console is open, showing a CSP report:

```
Object { document-uri="http://127.0.0.1:3000/?...82345%29%3C%2Fscript%3E",  
referrer="http://127.0.0.1:3000/", blocked-uri="self", more... }
```

The source code snippet in the console is:

```
{ "csp-report": { "document-uri": "http://127.0.0.1:3000/?first_field=Hello+world+%3Cscript%3Ealert%282345%29%3C%2Fscript%3E", "referrer": "http://127.0.0.1:3000/", "blocked-uri": "self", "violated-directive": "script-src", "source-file": "http://127.0.0.1:3000/?first_field=Hello+world+%3Cscript%3Ealert%282345%29%3C%2Fscript%3E", "script-sample": "alert(2345)", "line-number": 12 } }
```

Mojolicious

Error page when unsafe-inline denied

Page not found (development mode)

Page not found (development m... +

127.0.0.1:3000/nosuch

Google

mojolicious

[Documentation](#) [Wiki](#) [GitHub](#) [CPAN](#) [MailingList](#) [Blog](#) [Twitter](#)

Search

Page not found... yet!

None of these routes could generate a response for your GET request for /nosuch, maybe you need to add a new one?

Console HTML CSS Script DOM Net Cookies

Clear Persist All HTML CSS JavaScript XHR Images Plugins Media Fonts

URL	Status	Domain	Size	Remote IP	Timeline
▶ GET nosuch	404 Not Found	127.0.0.1:3000	18.1 KB	127.0.0.1:3000	41ms
▶ http://127.0.0.1:3000/content-security-policy-report			22 B	127.0.0.1:3000	8ms
▶ POST content-secur	200 OK	127.0.0.1:3000	22 B	127.0.0.1:3000	10ms
▶ POST content-secur	200 OK	127.0.0.1:3000	22 B	127.0.0.1:3000	8ms
▶ POST content-secur	200 OK	127.0.0.1:3000	22 B	127.0.0.1:3000	9ms
▶ POST content-secur	200 OK	127.0.0.1:3000	22 B	127.0.0.1:3000	13ms
6 requests			18.2 KB (110 B from cache)		437ms (onload: 457ms)

zotero

Mojolicious

Side effects

If you want it to look nice again.

Mojolicious

Side effects

One way is to allow
unsafe-inline scripts
and
unsafe-inline css
in development mode.

Lite app

content_security_policy.conf

```
{
  secrets => [ 'some_secret' ],

  'content-security-policy' =>
    join("; ",
      "report-uri /content-security-policy-report",

      "default-src    'none'",

      "script-src     'self'",
      "style-src      'self'",

      "font-src       'self'",
      "img-src        'self'",
    ),
}
```


Lite app

content_security_policy.development.conf

```
{
  secrets => [ 'some_development_secret' ],

  'content-security-policy' =>
    join("; ",
      "report-uri /content-security-policy-report",

      "default-src    'none'",

      # for mojo not_found page
      "script-src     'self' 'unsafe-inline'",
      "style-src      'self' 'unsafe-inline' https://google-code-
prettify.googlecode.com",

      "font-src       'self'",
      "img-src        'self'",
    ),
}
```

Mojolicious

Now it looks ok

Page not found (development mode)

Page not found (development m...)

127.0.0.1:3000/nosuch

Google

mojolicious

Page not found... yet!

None of these routes could generate a response for your **GET** request for **/nosuch**, maybe you need to add a new one?

Pattern	Methods	Name
/perldoc/:module	*	perldocmodule
/content-security-		

Console HTML CSS Script DOM Net Cookies

Clear Persist All HTML CSS JavaScript XHR Images Plugins Media Fonts

URL	Status	Domain	Size	Remote IP	Timeline
▶ GET nosuch	404 Not Found	127.0.0.1:3000	18.0 KB	127.0.0.1:3000	15ms
1 request			18.0 KB		15ms (onload: 487ms)

ABP x Zotero

Mojolicious

Now it looks ok

Page not found (development mode)

Page not found (development m...

127.0.0.1:3000/nosuch

Google

mojolicious

Page not found... yet!

None of these routes could generate a response for your **GET** request for **/nosuch**, maybe you need to add a new one?

Pattern	Methods	Name
/perldoc/:module	*	perldocmodule
/content-security-policy-report	POST	contentsecuritypolicyreport
/	GET	

Method: GET

URL: /nosuch

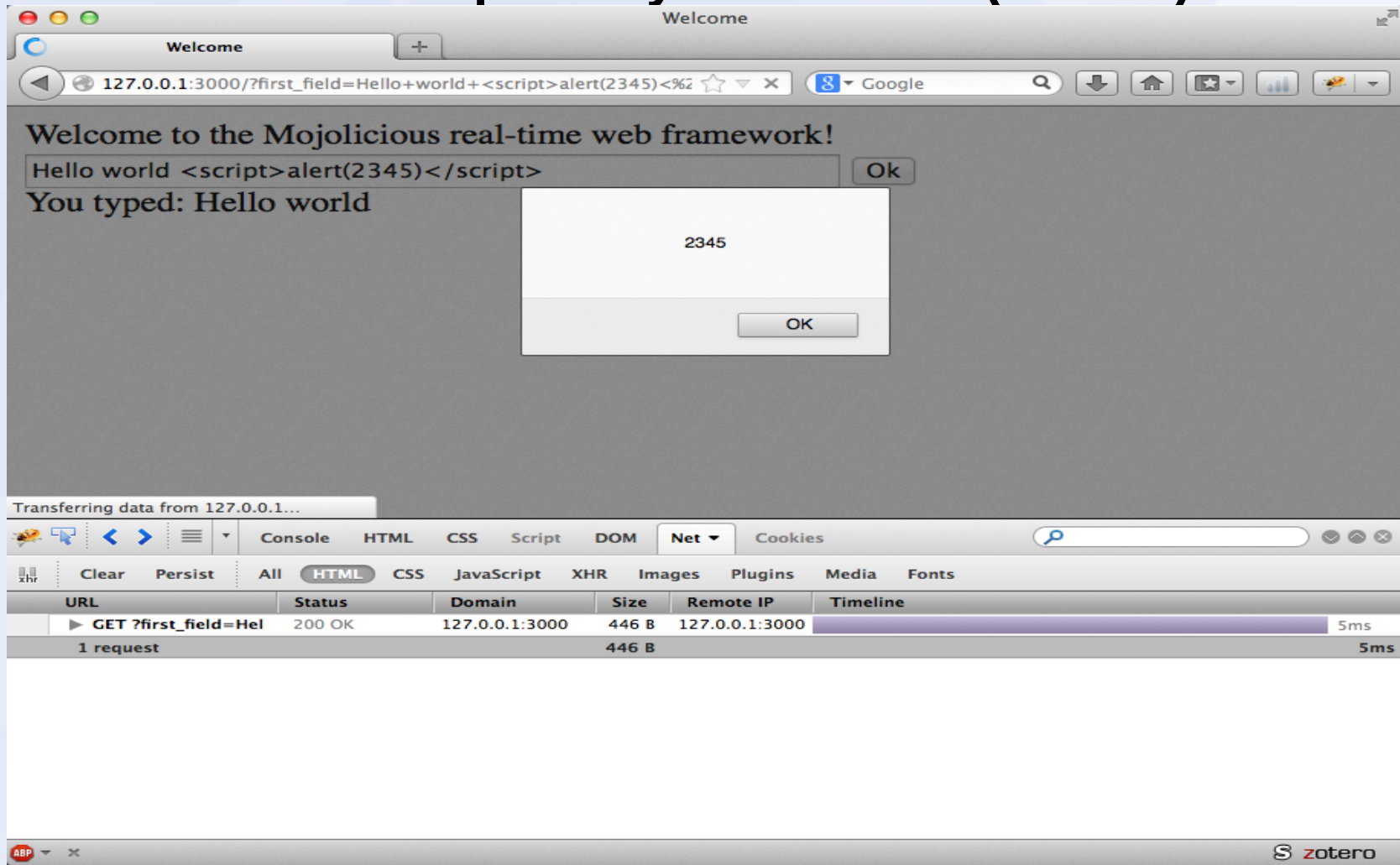
zotero

Mojolicious

But then...

Lite app

Other scripts may run as well (unsafe)



End of presentation...

References

Download this presentation:

<http://www.uniejo.dk/presentations/2014-05-24-csp.pdf>

Download test script:

<http://www.uniejo.dk/presentation/2014-05-24-csp.tgz>

Read more on
"HTML5 Rocks":

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

"Content Security Policy Best Practices":

https://www.isecpartners.com/media/106598/csp_best_practices.pdf

End of presentation...