Defeating cross-site scripting with Content Security Policy

Francois Marier <francois@catalyst.net.nz>

templating system

auto-escaping turned ON

auto-escaping turned ON

!=

escaping always ON

browser default: `allow all`

W3C Working Draft

Content Security Policy

W3C Working Draft 29 November 2011

This version:
http://www.w3.org/TR/2011/WD-CSP-20111129/
Latest published version:
http://www.w3.org/TR/CSP/
Latest editor's draft:
http://dvcs.w3.org/hg/content-security-policy/raw-file/tip/
Editors:
Brandon Sterne, Mozilla Corporation
Adam Barth, Google, Inc.

a way to get the **browser** to **enforce** the restrictions you want on your site

```
$ curl --head https://www.libravatar.org/

X-Content-Security-Policy:
  default-src 'self' ;
  img-src     'self' data
```

```
$ curl --head
https://www.libravatar.org/account/login/

X-Content-Security-Policy:
  default-src 'self' ;
  img-src     'self' data ;
  frame-src   'self'
    https://browserid.org ;
  script-src  'self'
    https://browserid.org
```

```
$ curl --head http://fmarier.org/
```

```
X-Content-Security-Policy:
  default-src 'none' ;
  img-src     'self' ;
  style-src   'self' ;
  font-src    'self'
```

<object>
<script>
<style>
<img>
<audio> & <video>
<frame> & <iframe>
<font>

WebSocket & XMLHttpRequest

>= 4

>= 13

>= 10

General Discussion - Add topic

Subject * First Post!

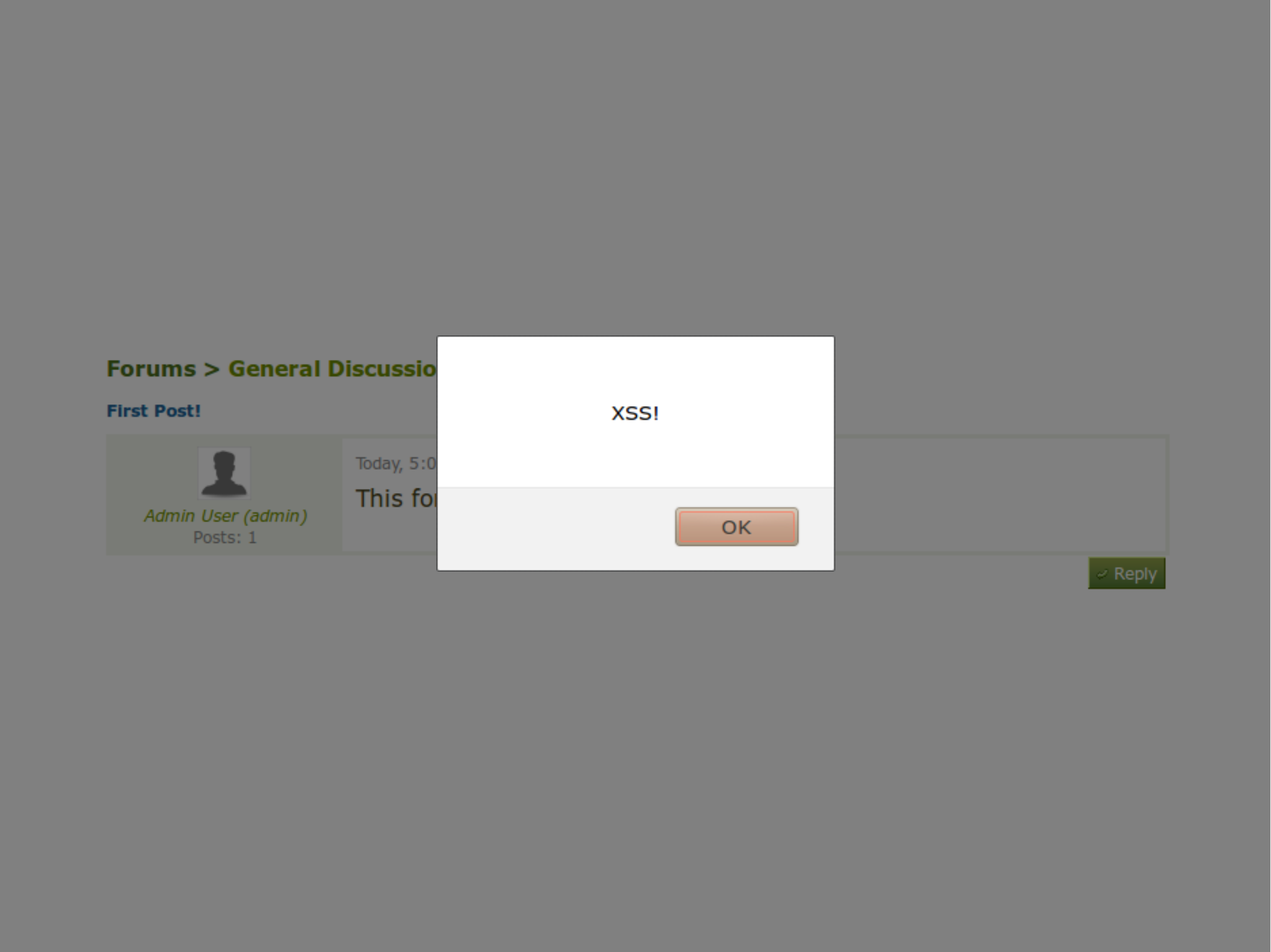
Body *

Font Family | 7 (36pt) | Paragraph

This forum is great!

<script>alert('XSS');</script>

Post Cancel


Forums > General Discussio
First Post!
Admin User (admin)
Posts: 1
Today, 5:0
This fo
XSS!
OK
Reply

Forums > General Discussion

First Post!

Admin User (admin)
Posts: 1

Today, 5:03 PM

This forum is great!

Reply

General Discussion - Add topic

Subject * Photo sharing

Body *

Font Family | Font Size | Paragraph

My favourite photo is:

<img src="http://goatse.cx/hello.jpg">

Post Cancel

Forums > General Discussion

Photo sharing

Admin User (admin)
Posts: 1

Today, 5:22 PM

My favourite photo is:

Reply

Forums > General Discussion

Photo sharing

Admin User (admin)
Posts: 1

Today, 5:22 PM

My favourite photo is:

Reply

not a replacement for
proper XSS hygiene

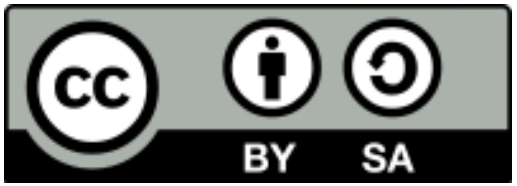
great tool to increase the
depth of your defenses

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

HOWTO:
https://developer.mozilla.org/en/Security/CSP

fmarier

fmarier



Copyright © 2012 François Marier
Released under the terms of the Creative Commons Attribution Share Alike 3.0 Unported Licence

Credits:

Biohazard wallpaper: http://www.flickr.com/photos/rockyx/4273385120/

eliminate inline scripts and styles

```
<script>
do_stuff();
</script>
```

```
<script src=”do_stuff.js”>

</script>
```

eliminate javascript: URIs

```
<a href=”javascript:go()”>
Go!
</a>
```

```
<a id=”go-button” href=”#”>
Go!
</a>

var button =
  document.getElementById('go-button');
button.onclick = go;
```

add headers in web server config

```
<Location /some/page>

  Header set X-Content-Security-Policy
    "default-src 'self' ;
     script-src 'self' http://example.org"

</Location>
```