Content Security Policy

Security

Otago Polytechnic
Dunedin, New Zealand

The problem

Why might we be vulnerable to Cross Site Scripting?

The problem

Basically, we want to be able to supply resources like JavaScript to our pages without allowing anyone else to do so.

Content Security Policy

Content Security Policy (CSP) is a candidate standard that allows us to specify the legitimate sources for scripts, styles, media and other resources that can be loaded into a web page. Resources from other locations are blocked.

Example

```
Content-Security-Policy:    default-src 'self';
                            style-src 'self' http://cdn.examp
                            script-src http://cdn.example.com
```

We specify the policy in our HTTP headers that we send with our web pages.

How do we do this?

We can configure our web servers to send the headers automatically with every response, or we can specify the headers in our web application code.
In PHP:

```
header("Content-Security-Policy: default-src 'self';
        script-src http://cdn.example.com;")
```

Note that we must specify headers before we send any other output to the client.

CSP directives

```
default-src
script-src
object-src
style-src
img-src
media-src
frame-src
font-src
connect-src
```

CSP Logging

With CSP we can specify a url to which CSP violations will be logged.

```
Content-Security-Policy:    default-src 'self';
    report-uri: https://foo.org.nz/csp-report;
```

CSP Report-Onle

With CSP we can specify a url to which CSP violations will be logged.

```
Content-Security-Policy-Report-Only:    default-src 'self';
    report-uri: https://foo.org.nz/csp-report;
```

Downsides

To use CSP to its fullest potential, you have to build your website so that it complies with the policies.

- No inline JavaScript
- No inline styles
- Any remote script sources (e.g. Google APIs) have to be identified
- etc.

This isn't a problem for new web sites, but legacy sites are likely to have problems.

Downsides

Internet Explorer

Downsides

Older Browsers

Conclusion

CSP is a useful tool for reducing XSS risk, but it doesn't completely solve the problem, especially for older sites and older browsers.

Demo

`http://xss.foo.org.nz/lab4.2`

Be sure to try this on a variety of browsers.