Will New HTTP headers save us?

John Wilander, OWASP/Omegapoint, IBWAS'10

John Wilander
consultant at Omegapoint
in Sweden

Researcher in application security

Co-leader OWASP Sweden

Certified Java Programmer

omega
point.

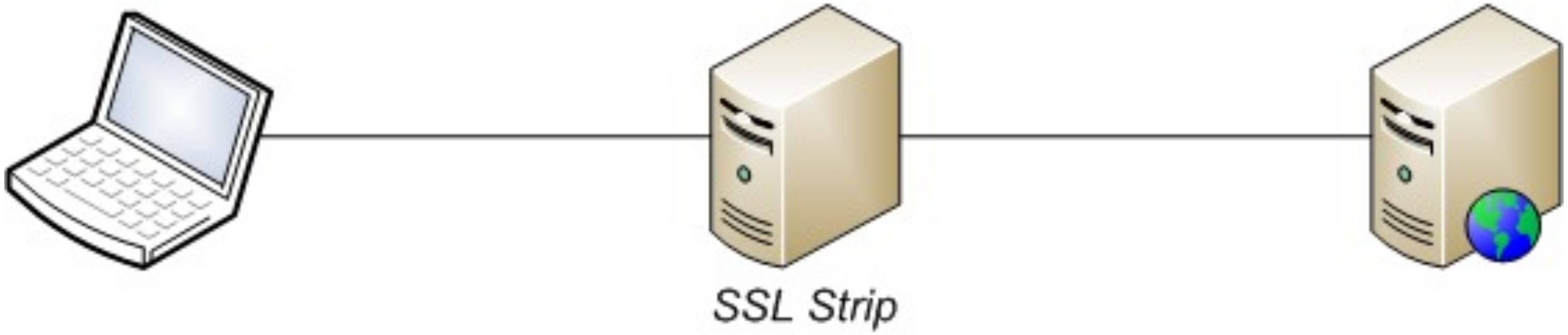
1. HTTP Strict Transport Security (Paypal)
2. X-Frame-Options (Microsoft)
3. Content Security Policy (Mozilla)

4. Set-Cookie (new IETF draft)
5. X-Do-Not-Track (FTC initiative, Stanford proposal)

HTTP Strict Transport Security

`http://tools.ietf.org/html/draft-hodges-strict-transport-sec-02`

Moxie's SSL Strip



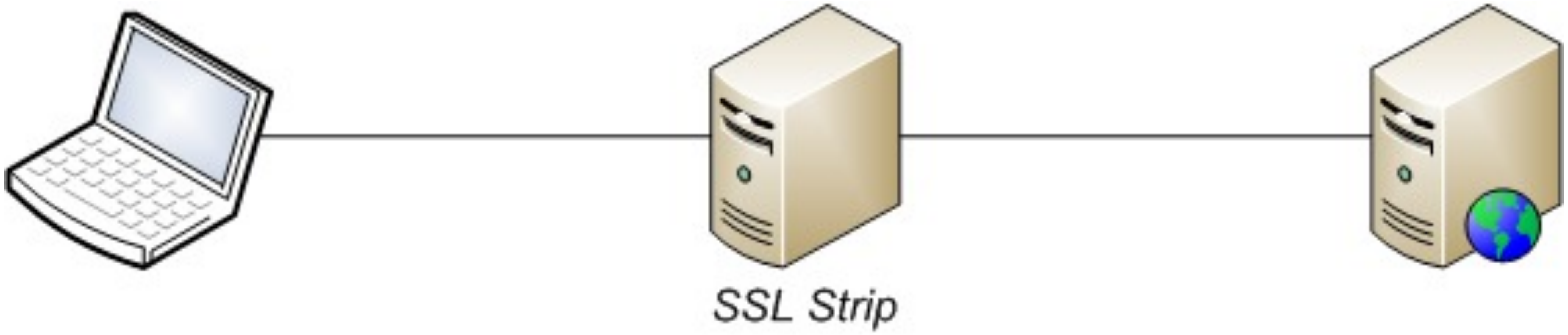
Terminates SSL

Changes https to http

Normal https to the server

Acts as client

Moxie's SSL Strip



Secure cookie?	Strip the secure attribute off all cookies.
Encoding, gzip?	Strip all encodings in the request.
Cached content?	Strip all if-modified-since in the request.
Sessions?	Redriect to same page, set-cookie expired

Enforce SSL without warnings for X seconds
and
potentially do it for all my sub domains too

```
Strict-Transport-Security: max-age=86400

Strict-Transport-Security: max-age=86400;
includeSubdomains
```

X-Frame-Options

http://blogs.msdn.com/b/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx

No page is allowed to frame me
or
Only my domain is allowed to frame me

```
X-Frame-Options: DENY

X-Frame-Options: SAMEORIGIN
```

Content Security Policy

https://developer.mozilla.org/en/Introducing_Content_Security_Policy

Only allow scripts from white listed domains
and
only allow scripts from files, i e no inline scripts

`'self'`	same URL scheme and port number
`'none'`	no hosts match

```
X-Content-Security-Policy: allow 'self' trustedscripts.foo.com
```

Trust scripts from my URL+port and from `trustedscripts.foo.com`

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

Trust scripts and images from my URL+port

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

New Cookie RFC (draft)

http://www.ietf.org/id/draft-ietf-httpstate-cookie-19.txt

X-Do-Not-Track (idea)

`http://donottrack.us/`

FTC Do not track

Federal Trade Commission's idea is that users would be able to choose to have their browser tell any Website not to track them for advertising purposes, and that setting wouldn’t be wiped out if a user clears browser cookies

Request header: `X-Do-Not-Track`

Potential Bad Stuff

Response Splitting

```
<%
  response.sendRedirect("/by_lang.jsp?lang="+
  request.getParameter("lang"));
%>
```

Response Splitting

```
<%
  response.sendRedirect("/by_lang.jsp?lang="+
  request.getParameter("lang"));
%>
```

```
HTTP/1.1 302 Moved Temporarily
Date: Wed, 24 Dec 2010 12:53:28 GMT
Location: http://10.1.1.1/by_lang.jsp?
lang=English
Set-Cookie:
JSESSIONID=1pMRZOiOQzZiE6Y6iivsREg82pq9Bo1ape7h
4YoHZ62RXj
Strict-Transport-Security: max-age=10000
X-Content-Security-Policy: allow ‘self’
X-Frame-Options: DENY

<html> ... </html>
```

```
HTTP/1.1 302 Moved Temporarily
Date: Wed, 24 Dec 2010 12:53:28 GMT
Location: http://10.1.1.1/by_lang.jsp?
lang=English[CRLF]Content-Length=0[CRLF]
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=sessionFixation
X-Content-Security-Policy: allow attacker.com
Strict-Transport-Security: max-age=1
<html> ... </html>
Set-Cookie:
JSESSIONID=1pMRZOiOQzZiE6Y6iivsREg82pq9Bo1ape7h
4YoHZ62RXj

<html> ... </html>
```

Meta Headers

```
<META HTTP-EQUIV="X-Content-Security-Policy" CONTENT="allow attacker.com">
```

From the specs

- For security reasons, you can't use the <meta> element to configure the X-Content-Security-Policy header.
- The X-Frame-Options directive is ignored if specified in a META tag.
- UAs MUST NOT heed http-equiv="Strict-Transport-Security" attribute settings on <meta> elements in received content.

So, will new HTTP headers save us?

john.wilander@owasp.org
Twitter: @johnwilander
Blog: appsandsecurity.blogspot.com

OWASP