Be a good internet citizen

Secure your site and your users

Daniele Howell
Jørgen Tellnes
Vidar Drageide

skandia:banken

Who are we?

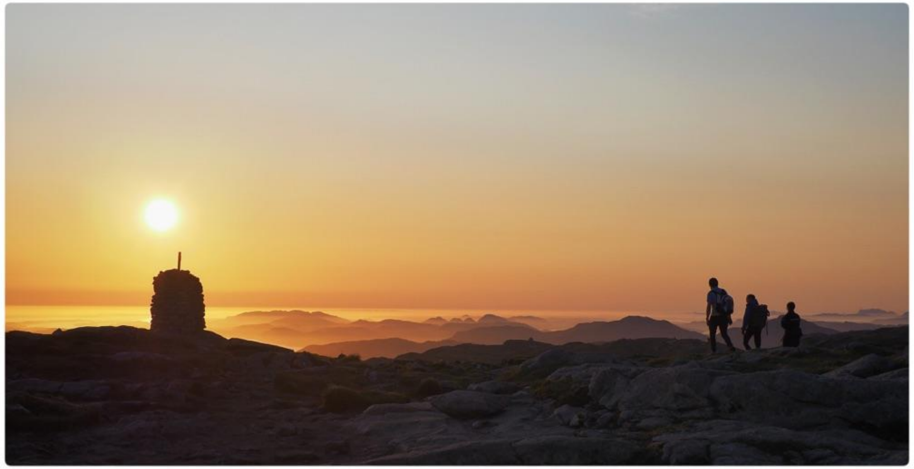
- Security (development) Team at Skandiabanken
  - Daniele
  - Vidar
  - Jørgen

skandia:banken

J

What do we do?

- Online bank security
- Development (authentication, signing, app security, etc)
- Security testing (pentesting)
- TLS config, security headers
- Super epic mountain voyages →



J

What’s this?

- We often focus on securing our own services
  - Our users and customers aren’t security experts
  - It’s **our** responsibility to help them stay safe
- We are all internet citizens – we need to raise the bar
- At minimum, proper TLS and security headers
- None of this is hard nor expensive, it just requires vigilance

J

Why encryption at all?

- You open your customers to interposition attacks (MITM)
  - Stolen secrets
  - Tampered content
- Solution: **always** encrypt
  - Development: encrypted
  - Staging: encrypted
  - Production: encrypted
- It’s not hard

V

skandia:banken

DEMO

Dwall

V

skandia:banken

Structure

13:30 – 15:00:

- PKI, TLS, certificates, current state of web security
- Security headers, CSP

15:00 – 15:15

- Stimulant break

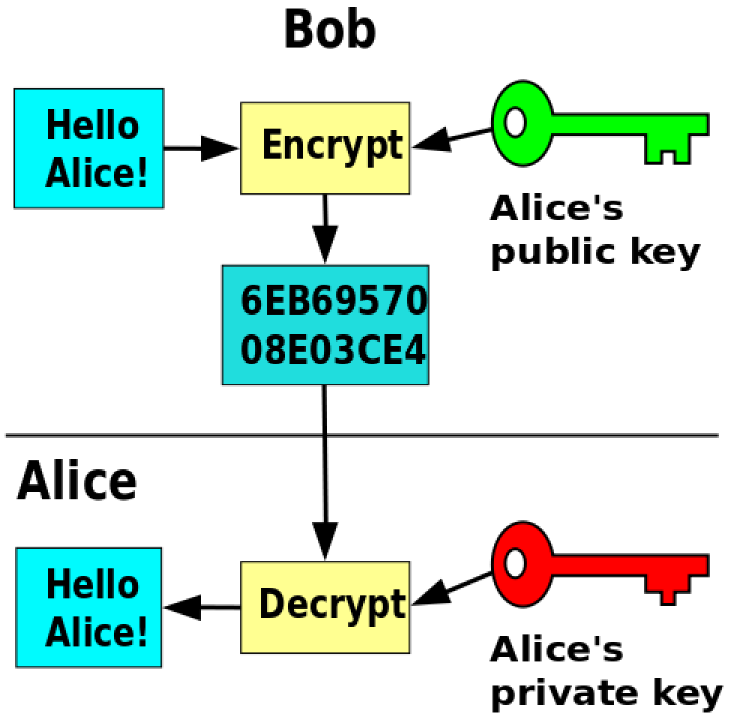
15:15 – 16:45

- Workshop section – we’ll build a site using best practices

V

PKI in 5 minutes – asymmetric cryptography

- Public-private key pairs
- Ensure that only the recipient can read your message
- Can be used for signatures
  - Recipient can use the public key to:
    - Verify that content is unchanged
    - Verify that only the private key owner has generated the signature
  - Signatures are **not** encryption



PKI in 5 minutes – Certificates

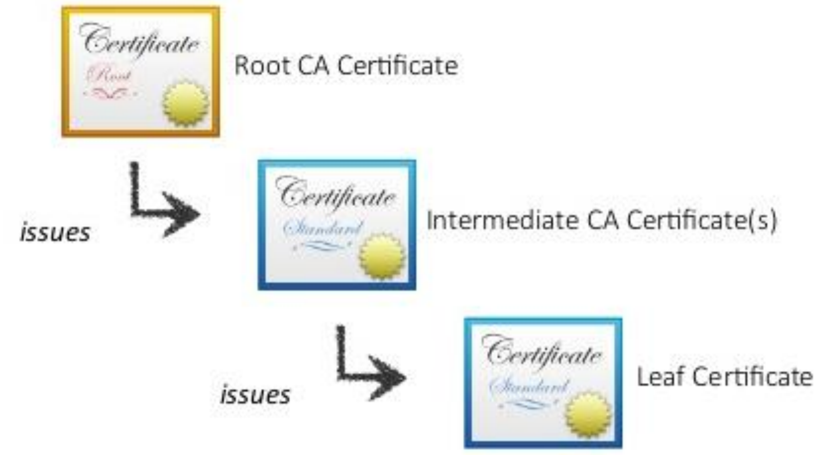
- «ID card» for server
- Contains servers public key
- Signed (issued) by a trusted third party

- Essential fields
  - Subject (hostname)
  - Expiry (notBefore, notAfter)
  - many many more

J

PKI in 5 minutes

- PKI – Public Key Infrastructure
- Certification Authority (CA)
  - Issues certificates
- Trust chain built using signatures
- Walk the chain up to a trusted cert
- Root certificate is explicitly trusted
  - (> 90 default roots in your browser)



skandia:banken

SSL and TLS

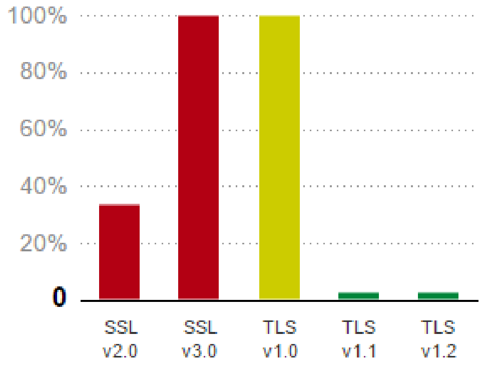
- Secure Sockets Layer (SSL)
  - SSL 2.0 in 1995, SSL 3.0 in 1996
- New name – TLS (Transport Layer Security)
  - TLS 1.0 in 1999
  - TLS 1.1 in 2006
  - TLS 1.2 in 2008
  - TLS 1.3 – working draft, prelim. support in Chrome/Firefox this year

J

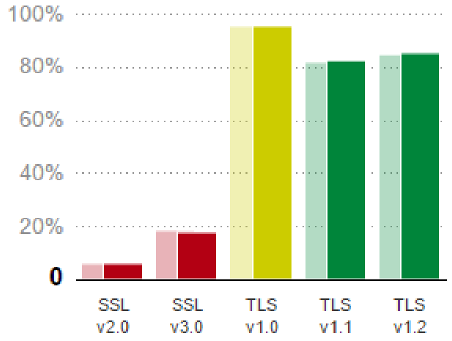
SSL and TLS

- Slow adoption – but we are getting there
- Held back by old browsers

April 2012



March 2017

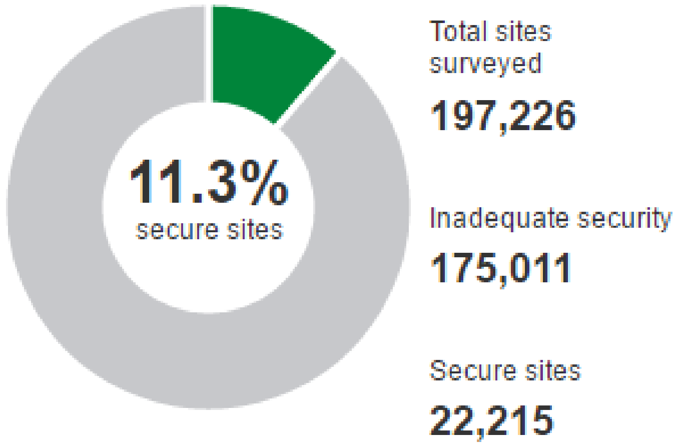


skandia:banken

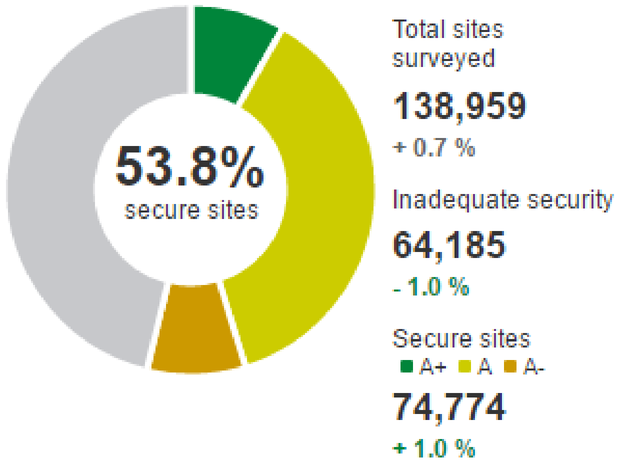
J

Current state of TLS and web security

April 2012:



March 2017:

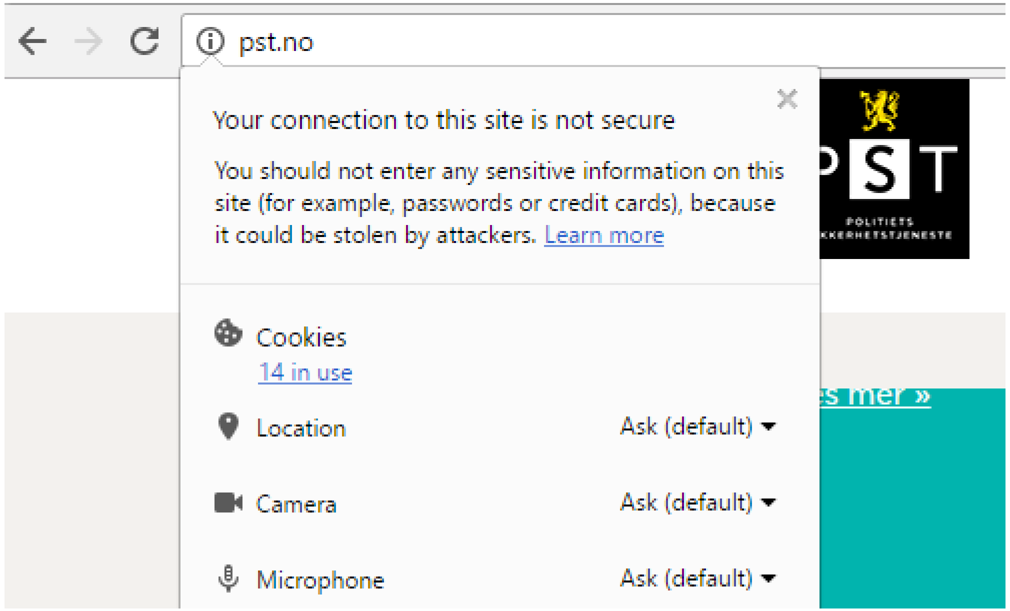


https://www.trustworthyinternet.org/ssl-pulse/ - scan of alexa top list

J

Current state of TLS and web security

- Let's encrypt probably has a lot of the credit for this
- But still only ~50% TLS
- Some glaring omissions
- Advanced techniques still rare
  - HSTS found in about 5-10%
  - HPKP adoption at < 1%



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Cookies
14 in use

Location Ask (default)

Camera Ask (default)

Microphone Ask (default)

skandia:banken

J

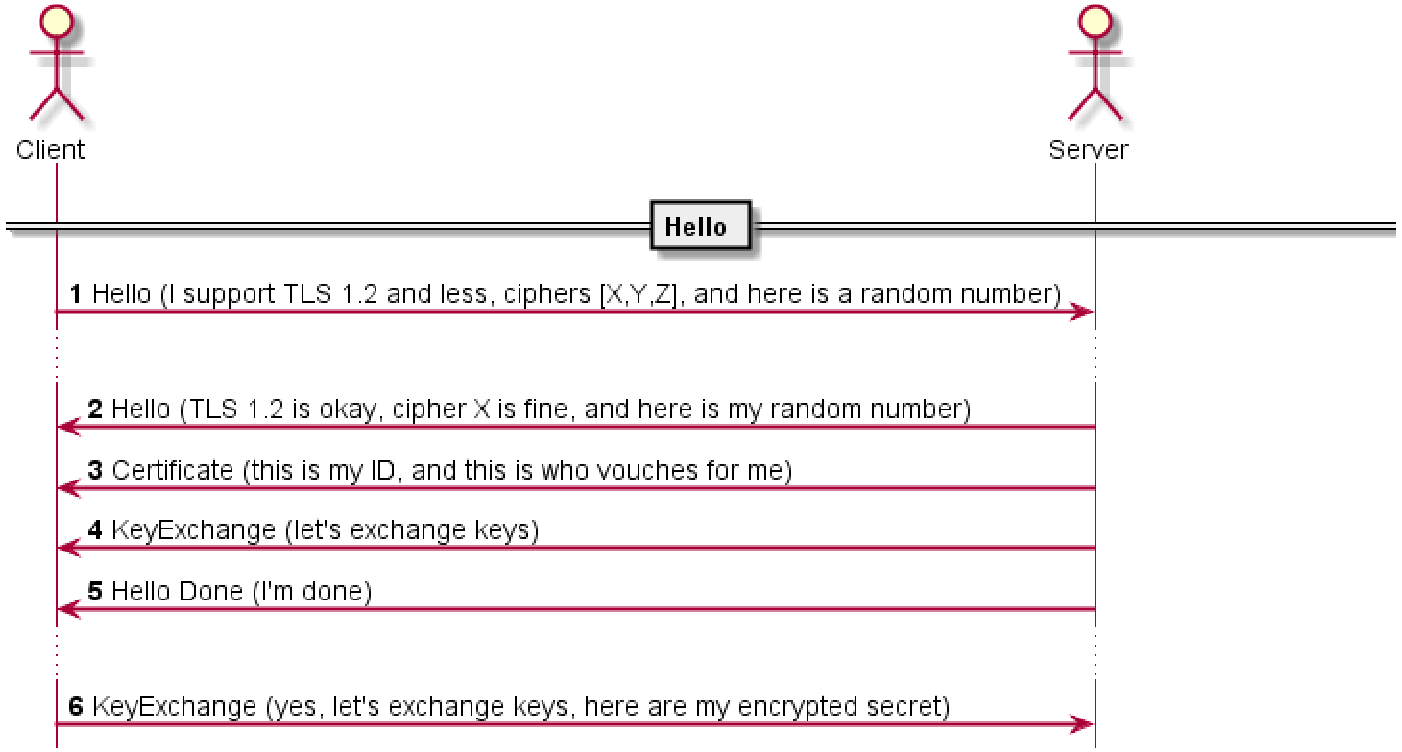
Weak TLS configuration

- Let’s breeze through the TLS handshake first

skandia:banken

J

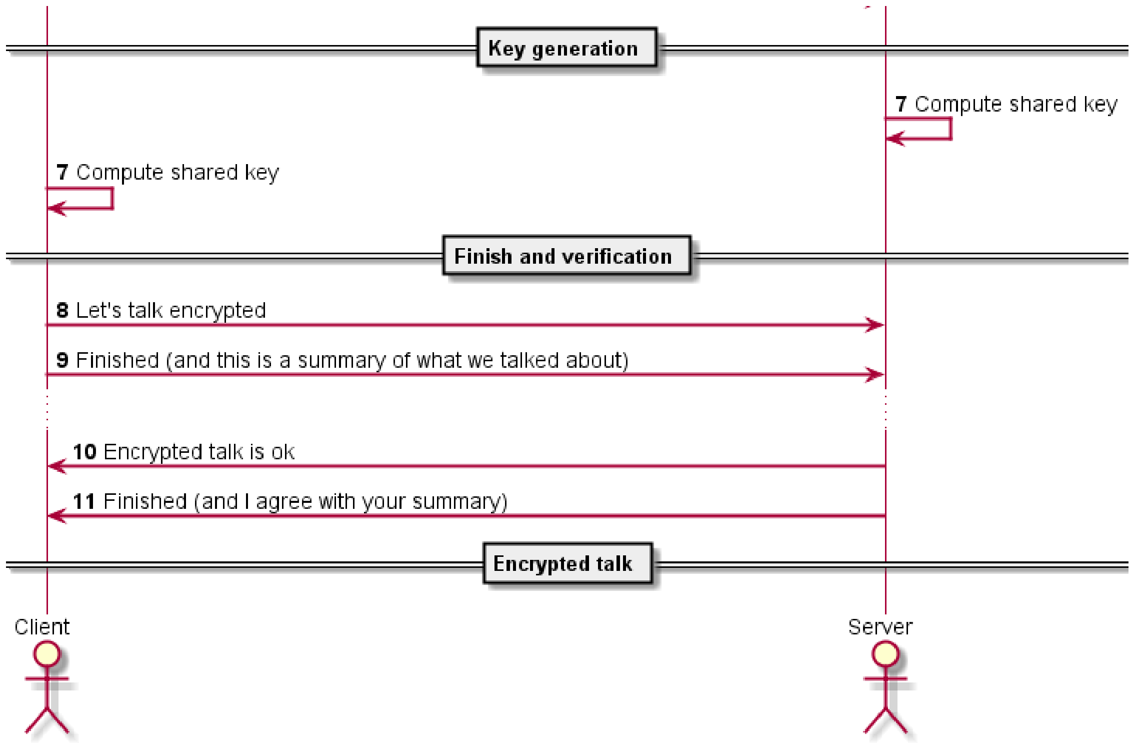
Weak TLS configuration - TLS in 3 minutes


Client
Server
Hello
1 Hello (I support TLS 1.2 and less, ciphers [X,Y,Z], and here is a random number)
2 Hello (TLS 1.2 is okay, cipher X is fine, and here is my random number)
3 Certificate (this is my ID, and this is who vouches for me)
4 KeyExchange (let's exchange keys)
5 Hello Done (I'm done)
6 KeyExchange (yes, let's exchange keys, here are my encrypted secret)

skandia:banken

J

Weak TLS configuration - TLS in 3 minutes



skandia:banken

J

Weak TLS configuration

- Ciphers (encryption algorithms) are important
- Bad ciphers
  - ECB, RC4, null ciphers
- Ciphers with short keys
  - DES, 3DES
- Bad hash algorithms
  - SHA1, MD5

skandia:banken

Weak TLS configuration

- Old TLS/SSL version support is a risk - actual exploitable vulnerabilites:
  - BEAST
  - POODLE
  - DROWN – vuln. if just one server uses SSL v2
  - Missing Perfect Forward Secrecy – not NSA future-proof
- Qualys SSL Labs has a super sweet validator

skandia:banken

Let’s Encrypt

- Launched on April 12, 2016
  - Project started in 2012 by a team from Mozilla, EFF and University of Michigan
- Completely free
- Wildly popular (> 25 million active certificates)
- Easy to use
- Secure
  - The private key is always generated and managed on your own servers
- Transparent
  - All certificates issued or revoked will be publicly recorded and available for anyone to inspect

skandia:banken

D

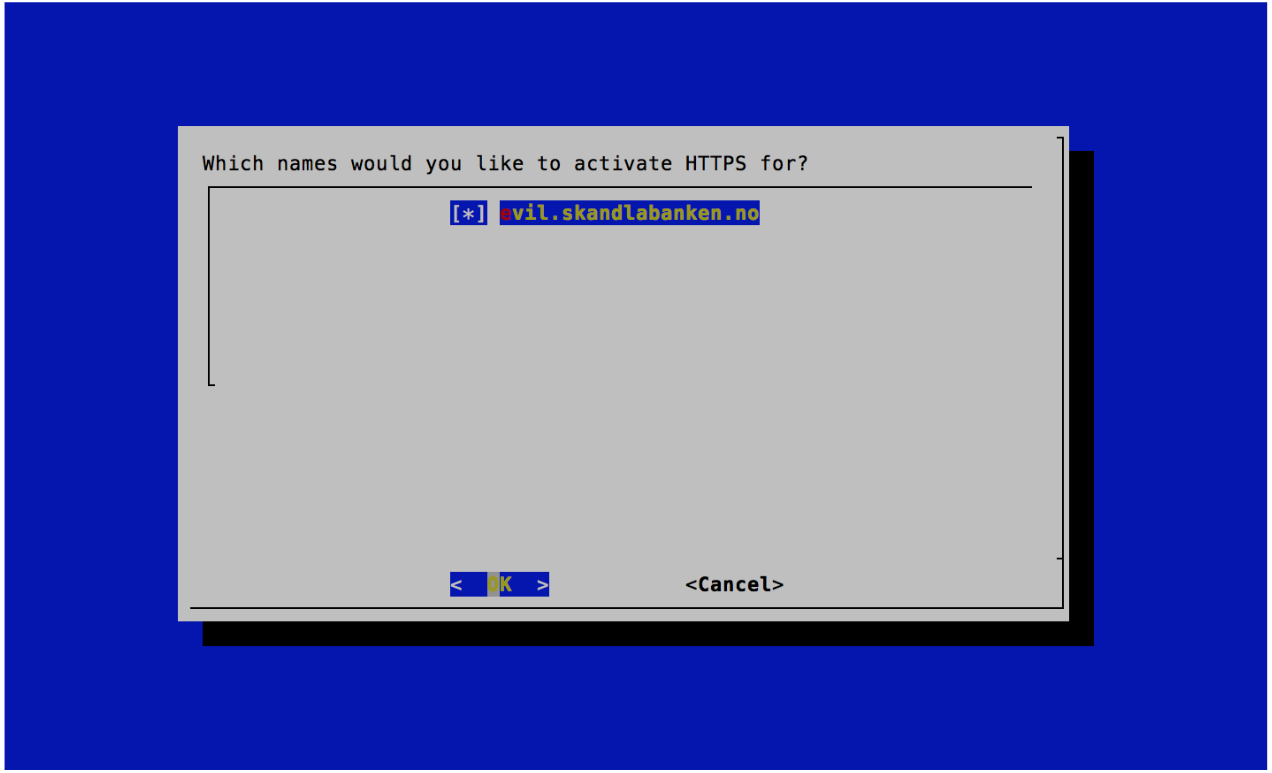
Let’s Encrypt

- Requires control over the domain
  - Uses Automatic Certificate Management Environment (ACME) protocol https://ietf-wg-acme.github.io/acme/
  - Typically runs on your web host
- Without Shell Access
  - Needs support from your hosting provider
  - Azure offers Let’s Encrypt Extension (hassle to setup but awesome results)
- With Shell Access
  - Uses Certbot ACME client to automate certificate issuance and installation
  - Easy to use

skandia:banken

D

Let’s Encrypt



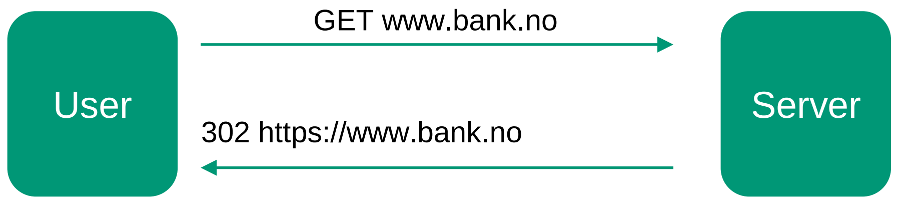
```
Which names would you like to activate HTTPS for?

                [*] evil.skandlabanken.no

                < OK >          <Cancel>
```

skandia:banken

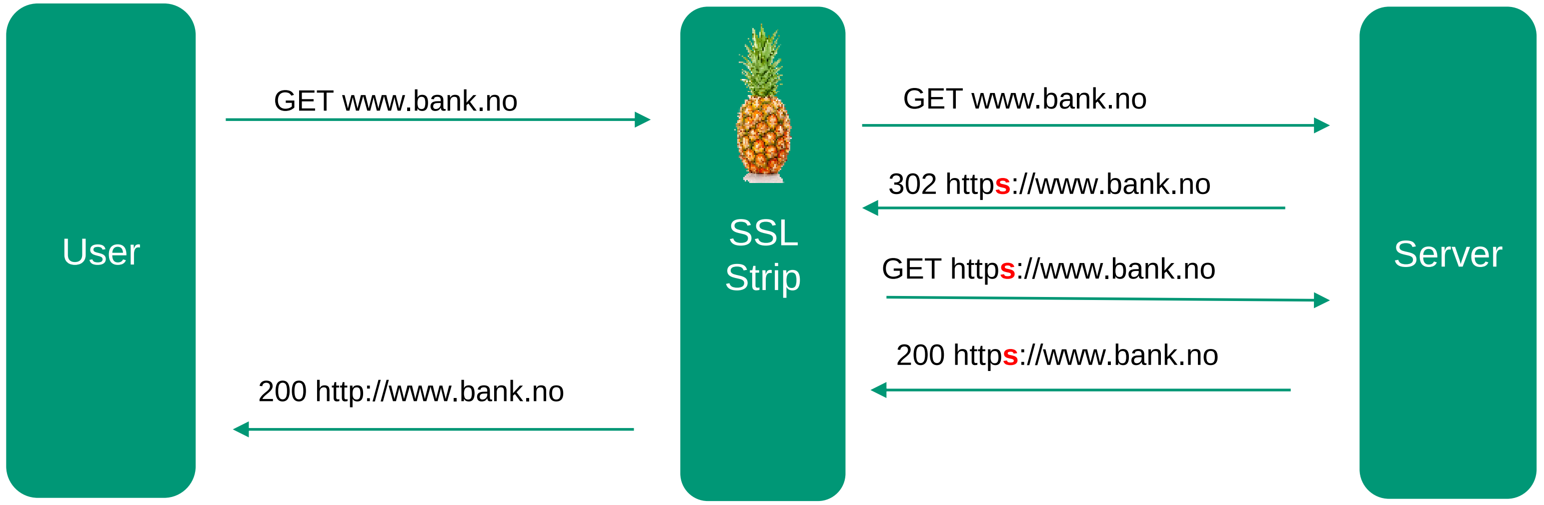
D

TLS stripping attack (downgrade attacks)

- Courtesy of Moxie Marlinspike – Blackhat DC 2009
- Downgrade the users connection to a given domain from TLS/SSL to plaintext.



Simplified SSL-strip



V

DEMO

sslstrip

V

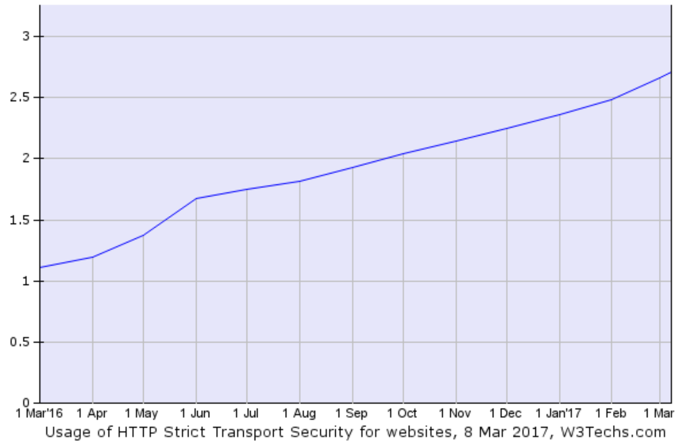
skandia:banken

HTTP Strict Transport Security (HSTS)

- *”Use only HTTPS from now until $time$”*

```
Strict-Transport-Security: max-age=[seconds]; includeSubDomains; preload
```

- For the next *[seconds]*, the user agent should only access the server securely
- Used by only 2.7% of all surveyed websites (w3techs.com)
- Reduces ability to intercept requests and responses between a user and a web server.



skandia:banken

D

Still bad on first visit «ever»

- HSTS is just a vaccine
- For the first visit ever on the page your browser cannot know that your site serves the HSTS header

D

DEMO

sslstrip despite HSTS

V

skandia:banken

HSTS preloading

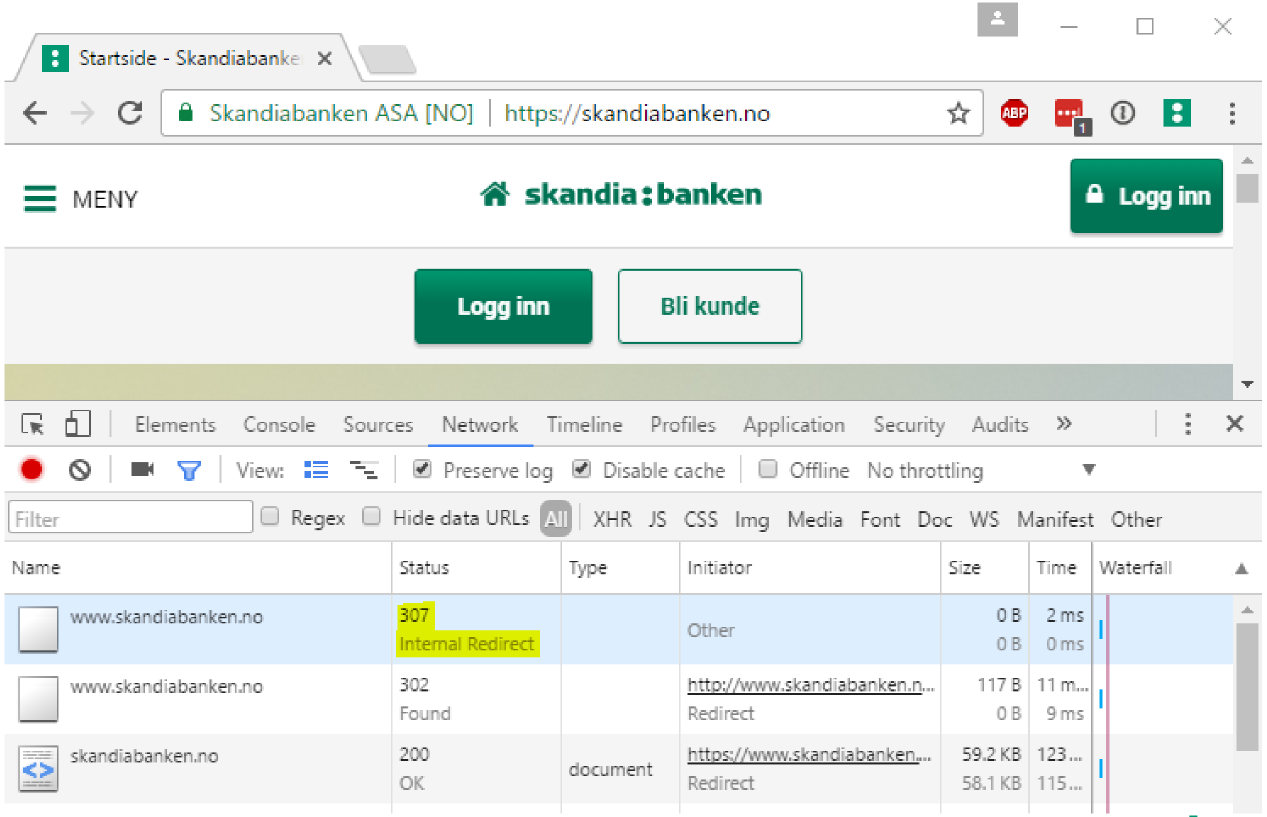
- Hard-coded list of «preloaded» HSTS headers

Process:

1. Add «preload» and «includeSubdomains»
2. Submit to https://hstspreload.org
3. Allow 6-8 weeks for delivery
4. Result: **TLS even on the first request**

D

HSTS preloading



Name	Status	Type	Initiator	Size	Time	Waterfall
www.skandiabanken.no	307 Internal Redirect		Other	0 B / 0 B	2 ms / 0 ms	
www.skandiabanken.no	302 Found		http://www.skandiabanken.n... Redirect	117 B / 0 B	11 m... / 9 ms	
skandiabanken.no	200 OK	document	https://www.skandiabanken... Redirect	59.2 KB / 58.1 KB	123... / 115...	

skandia:banken

D

Keep your cookies secure

- Secure and HttpOnly

```
Set-Cookie: sessid=[snip]; Path=/; Domain=.example.com; Secure; HttpOnly
```

- Otherwise the cookies may be sent unencrypted
- Request to **http**://yoursecuredomain.com will include your cookies
- From stortinget.no (what's missing?):

```
Set-Cookie: ASP.NET_SessionId=flt[…]zb; path=/; HttpOnly
```

Security headers

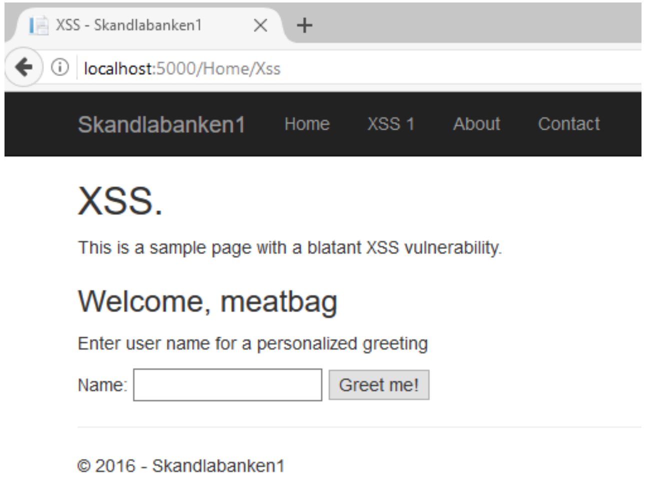
- Partnership between server and client
- Server defines the rules for the website
- Uses HTTP headers

- May reduce the impact of vulnerabilities
- Publicly visible scorecard

V

Headers to consider

- Content-Security-Policy (CSP)
- HTTP Strict Transport Security (HSTS)
- HTTP Public Key Pinning (HPKP)
- X-XSS-Protection
- X-Frame-Options
- X-Content-Type-Options
- Referrer Policy



XSS.

This is a sample page with a blatant XSS vulnerability.

Welcome, meatbag

Enter user name for a personalized greeting

Name: [ ] Greet me!

© 2016 - Skandlabanken1

V

Content Security Policy

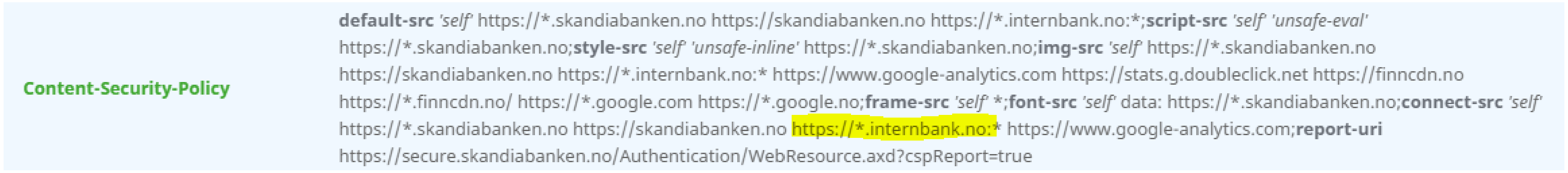
- Unification of security headers
- Reminder: Security headers and CSP is **not** a first-line defence
- Level 2 support in all browsers except IE/Edge (yet)
  - Hash/nonce based whitelisting
- CSP Level 3 is in working draft status

J

Content Security Policy

- Content-Security-Policy
- Content-Security-Policy-Report-Only
  - Violation reports only, no blocking
- **Report-uri.io** – excellent (free!) service

- Dangers
  - Information leakage (internal domains, preproduction, etc)



Content-Security-Policy	**default-src** *'self'* https://*.skandiabanken.no https://skandiabanken.no https://*.internbank.no:*;**script-src** *'self' 'unsafe-eval'* https://*.skandiabanken.no;**style-src** *'self' 'unsafe-inline'* https://*.skandiabanken.no;**img-src** *'self'* https://*.skandiabanken.no https://skandiabanken.no https://*.internbank.no:* https://www.google-analytics.com https://stats.g.doubleclick.net https://finncdn.no https://*.finncdn.no/ https://*.google.com https://*.google.no;**frame-src** *'self'* *;**font-src** *'self'* data: https://*.skandiabanken.no;**connect-src** *'self'* https://*.skandiabanken.no https://skandiabanken.no https://*.internbank.no:* https://www.google-analytics.com;**report-uri** https://secure.skandiabanken.no/Authentication/WebResource.axd?cspReport=true

J

CSP directives

- Fetch directives – i.e. «from where can i fetch what resource»
  - `default-src`
  - `script-src`
  - `font-src`
  - `img-src`
  - …
- Document directives
  - `sandbox`
  - `plugin-types`
- Navigation directives
  - `form-action`
  - `frame-ancestors`
- Reporting directives
  - `report-uri`

skandia:banken

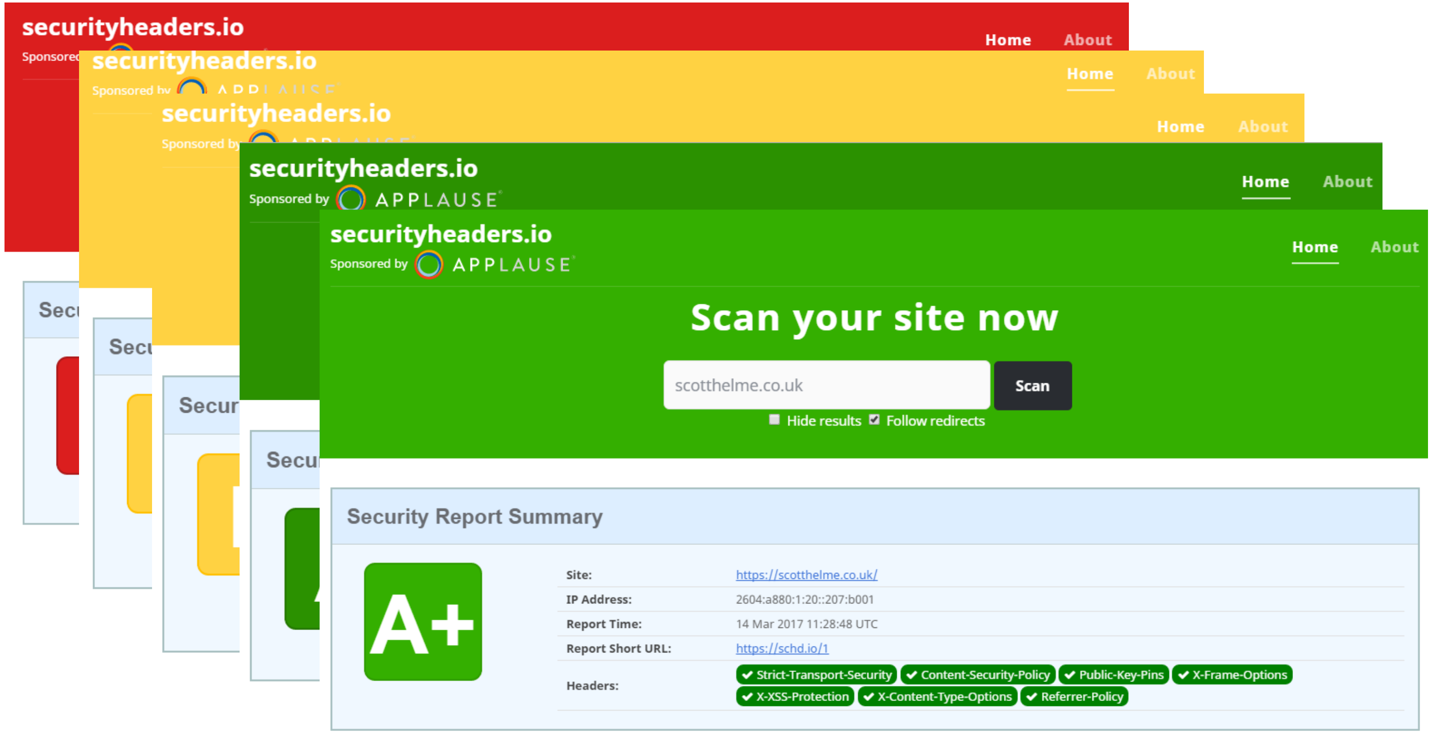
J

Securityheaders.io

- Excellent validator and public scorecard
- By Scott Helme (@scotthelme)

V

Securityheaders.io



Security Report Summary

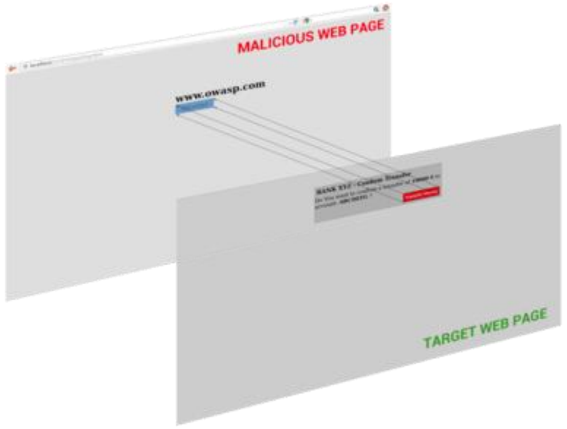
Site:	https://scotthelme.co.uk/
IP Address:	2604:a880:1:20::207:b001
Report Time:	14 Mar 2017 11:28:48 UTC
Report Short URL:	https://schd.io/1
Headers:	✓ Strict-Transport-Security ✓ Content-Security-Policy ✓ Public-Key-Pins ✓ X-Frame-Options ✓ X-XSS-Protection ✓ X-Content-Type-Options ✓ Referrer-Policy

V

Ui-redressing (clickjacking) attacks

DEMO

- Trick the user into performing clicks on the target webpage
  - Abuses iFrames, z-index and transparent layers



V

Clickjacking defence

- Control who's allowed to iframe your site
- X-Frame-Options:

```
X-Frame-Options: ALLOW-FROM https://example.com
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
```

- CSP – frame-ancestors

```
Content-Security-Policy: frame-ancestors <source>;
```

V

skandia:banken

Referrer-Policy

- Brand-spanking new header (this year)

```
Referrer-Policy: no-referrer-when-downgrade
```

- Control the value of the referer header
  - Stop information leakage
  - Varying degrees (‘no-referrer’ to ‘unsafe-url’)

V

Summary

- TLS
  - Weak TLS, vulnerabilities
- Security headers
  - Use them – run scans!
- Content security policy
  - Partially replaces security headers
  - Beware of legacy browsers
- Public scorecards
  - SSL Labs and securityheaders.io is effective public shaming

skandia:banken

Questions?

skandia:banken

Get ready for some coding

Development environment:

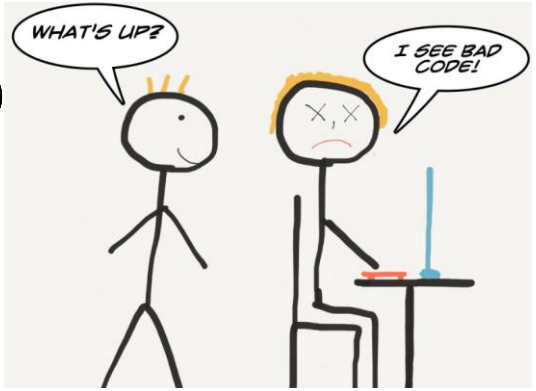
- Any text editor (we use Visual Studio Code with C# ext.)
- .NET Core 1.1.1 https://www.microsoft.com/net/core
- Git https://git-scm.com/downloads

Workshop projects and handouts:

https://github.com/jorgis/boosterconf2017

Host environment:

- Azure App Service - Free trial
  https://azure.microsoft.com/en-us/try/app-service/web/



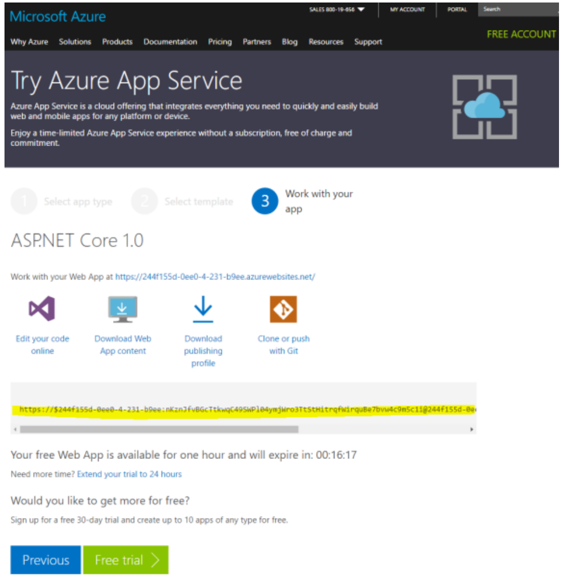
skandia:banken

D

Publishing your project to Azure

- Go to https://azure.microsoft.com/en-us/try/app-service/
- Select Web App → Choose ASP.NET Core 1.0
- Sign in using whatever
- Click “Extend to 24 hours”
- Select “Clone or Push with Git” to get your git remote url

- Open our github repo, add Azure remote and push
  - git remote add Azure [your-url]
  - git push Azure master *(you may have to use --force)*



Try Azure App Service

Azure App Service is a cloud offering that integrates everything you need to quickly and easily build web and mobile apps for any platform or device.

Enjoy a time-limited Azure App Service experience without a subscription, free of charge and commitment.

ASP.NET Core 1.0

Work with your Web App at https://244f155d-0ee0-4-231-b9ee.azurewebsites.net/

```
https://$244f155d-0ee0-4-231-b9ee:nKznJfvBGcTtkwqC49SWPl04ymjWro3TtStHitrqfWirquBe7bvw4c9m5c1i@244f155d-0e
```

Your free Web App is available for one hour and will expire in: 00:16:17

Need more time? Extend your trial to 24 hours

Would you like to get more for free?

Sign up for a free 30-day trial and create up to 10 apps of any type for free.

skandia:banken

D

Workshop

- Open **workshop.pdf** in the Handouts folder of the github repo
  - https://github.com/jorgis/boosterconf2017
- Form small groups – **2-3 people**
- We'll help as best we can – ask us anything

Wrapping it up

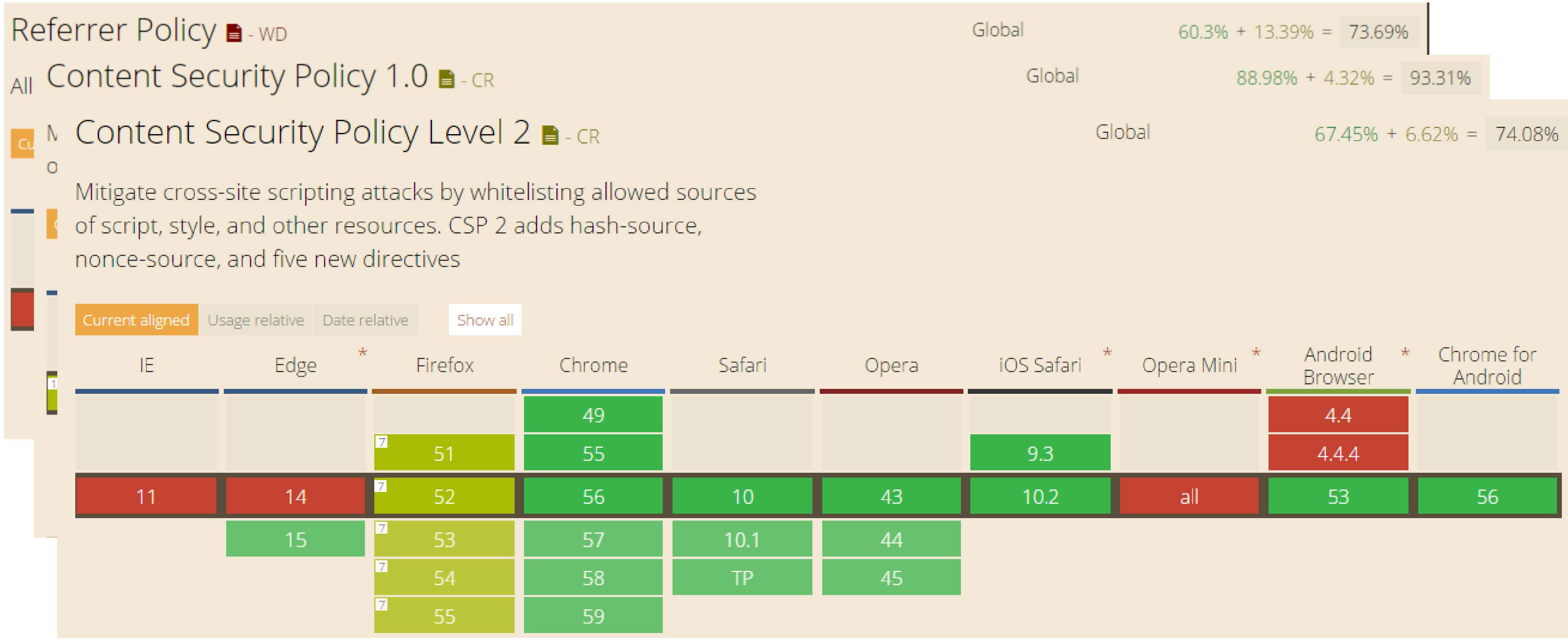
J

Pitfalls

- HSTS and HPKP can be DoS-generators
  - HPKP Ransom
- HSTS includeSubdomains can be dangerous
- Preload is impossibly hard to disable – be careful!
- Too tight controls can ruin your site
  - Always start with *-Report-Only
- Don’t forget old browsers – also use legacy headers
  - Browser support is always a pain

skandia:banken

Pitfalls – browser support



Referrer Policy - WD — Global 60.3% + 13.39% = 73.69%

All

Content Security Policy 1.0 - CR — Global 88.98% + 4.32% = 93.31%

Content Security Policy Level 2 - CR — Global 67.45% + 6.62% = 74.08%

Mitigate cross-site scripting attacks by whitelisting allowed sources of script, style, and other resources. CSP 2 adds hash-source, nonce-source, and five new directives

Current aligned | Usage relative | Date relative | Show all

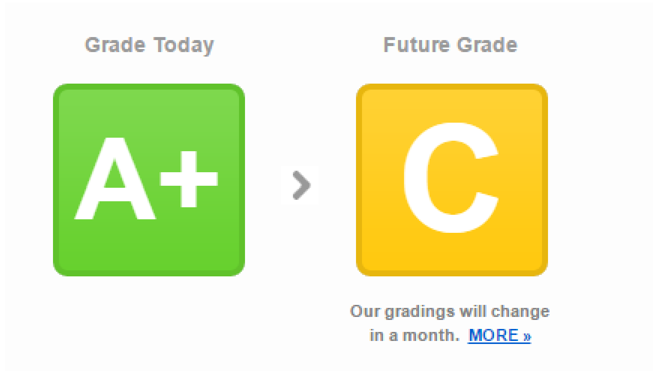
IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49					4.4	
		[7] 51	55			9.3		4.4.4	
11	14	[7] 52	56	10	43	10.2	all	53	56
	15	[7] 53	57	10.1	44				
		[7] 54	58	TP	45				
		[7] 55	59						

skandia:banken

J

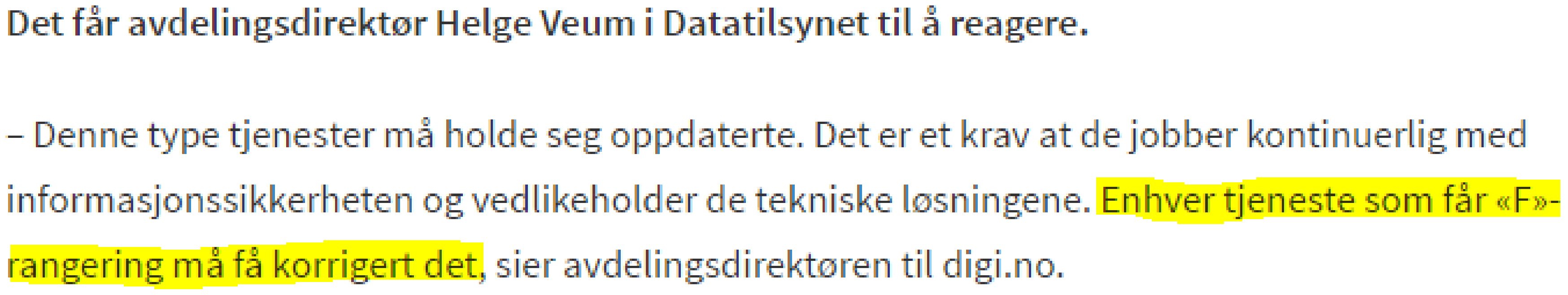
Summary

- It isn't hard – although crypto is always scary
- It's not just for you – it also benefits your users
- Adding security headers is easy
  - Determining your actual policy is hard
- Use SSL Labs and securityheaders.io
  - Run periodic scans – things change



skandia:banken

Summary



Det får avdelingsdirektør Helge Veum i Datatilsynet til å reagere.

– Denne type tjenester må holde seg oppdaterte. Det er et krav at de jobber kontinuerlig med informasjonssikkerheten og vedlikeholder de tekniske løsningene. Enhver tjeneste som får «F»-rangering må få korrigert det, sier avdelingsdirektøren til digi.no.

J

Summary – what’s next?

- TLS in HTTP/2 (and no browser supporting unencrypted connections)
- TLS1.3
  - Enabled in Firefox
  - Chrome backtracked
- CSP level 3
  - Currently a W3C draft
  - Out-of-band reporting
  - More directives
- In the app world – App Transport Security, Android Network Security Configuration

J

skandia:banken

Thanks

Daniele Howell

daniele.howell@skandiabanken.no

@daniele_mh

Jørgen Tellnes

jorgen.tellnes@skandiabanken.no

Vidar Drageide

vidar.drageide@skandiabanken.no

@vidard