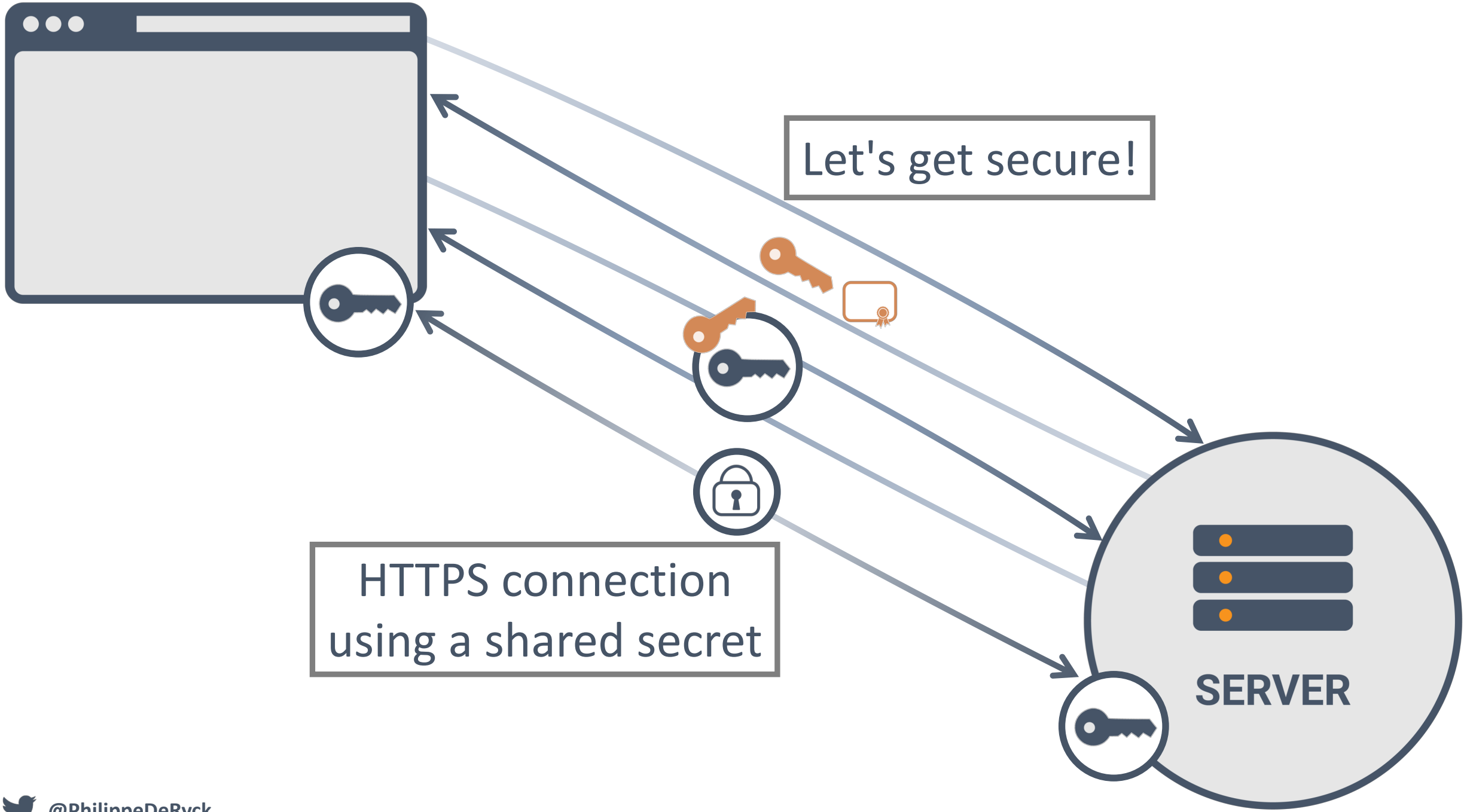
Pragmatic Web Security

Security training for developers

HTTPS FOR DEVELOPERS

PHILIPPE DE RYCK

@PhilippeDeRyck – philippe@PragmaticWebSecurity.com


Let's get secure!
HTTPS connection
using a shared secret
SERVER

- Founder of **Pragmatic Web Security**
  - In-depth web security training for developers
  - Covering web security, API security & Angular security
- 15+ years of security experience
  - Web security instructor and conference speaker
  - Author of ***Primer on client-side web security***
  - Creator of ***Web Security Fundamentals*** on edX
- Course curator of the **SecAppDev course**
  - Yearly security course targeted towards developers
  - More information on ***https://secappdev.org***
- Foodie and professional chef

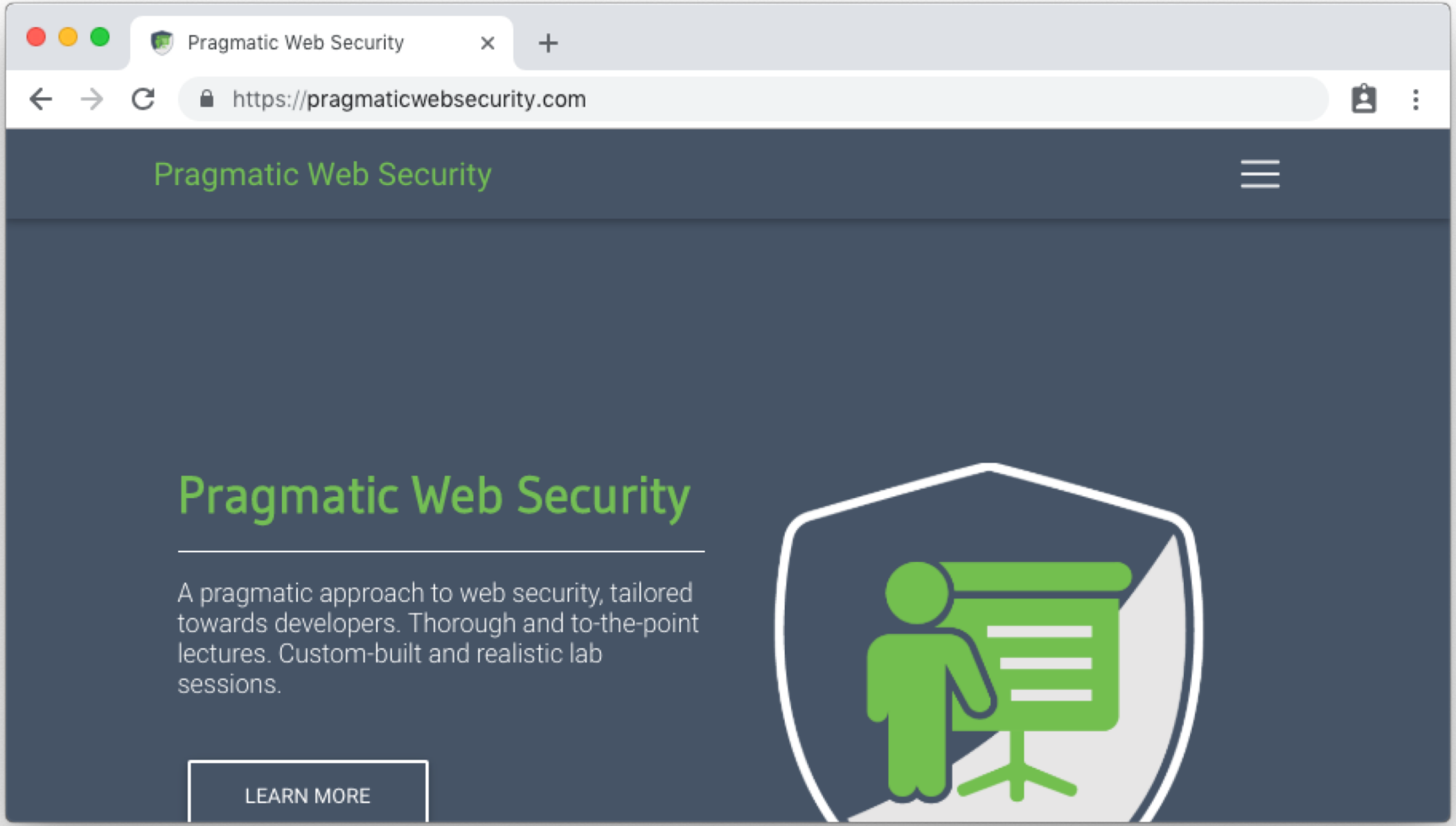
Dr. Philippe De Ryck

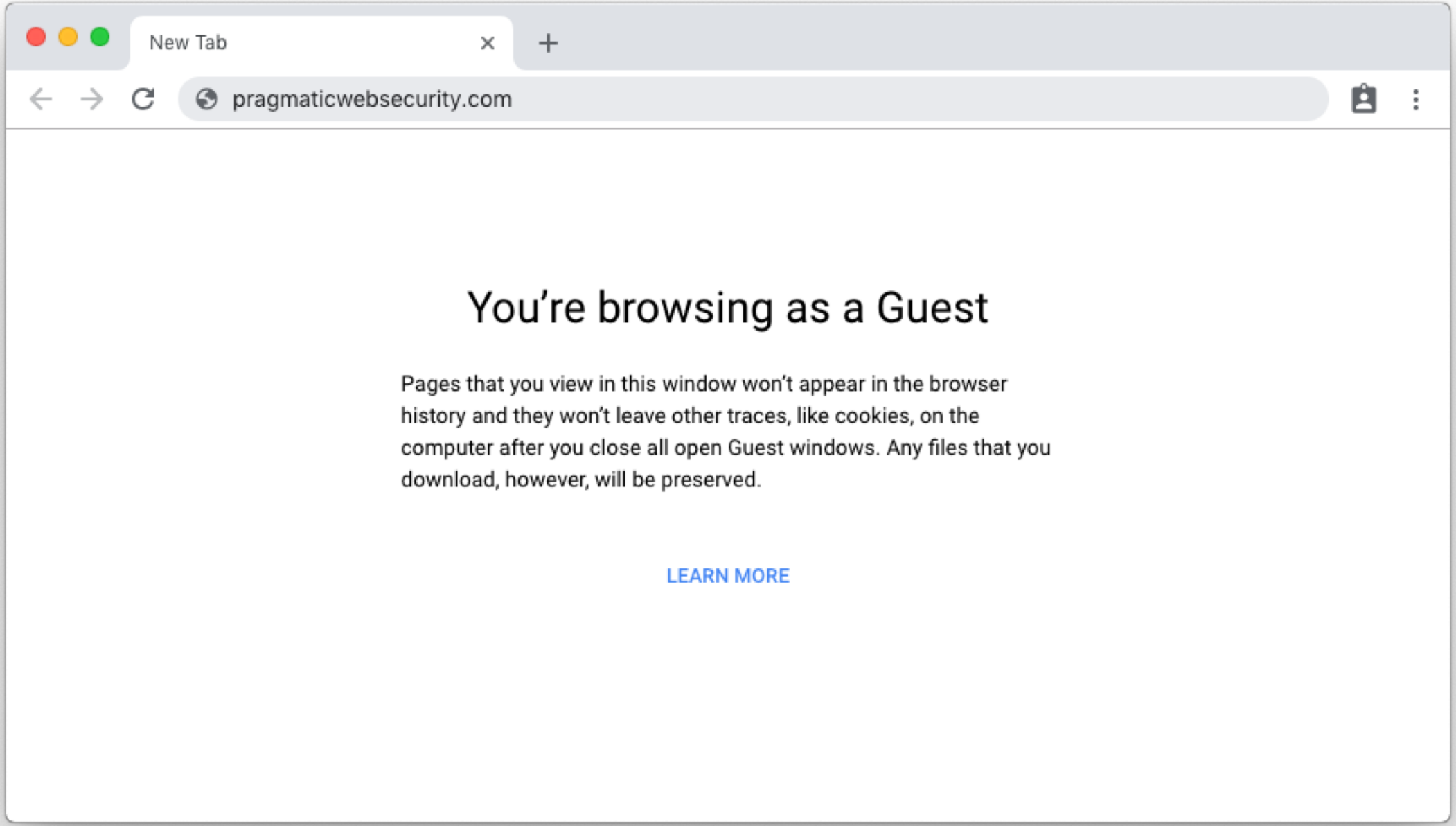
Ph.D. in web security

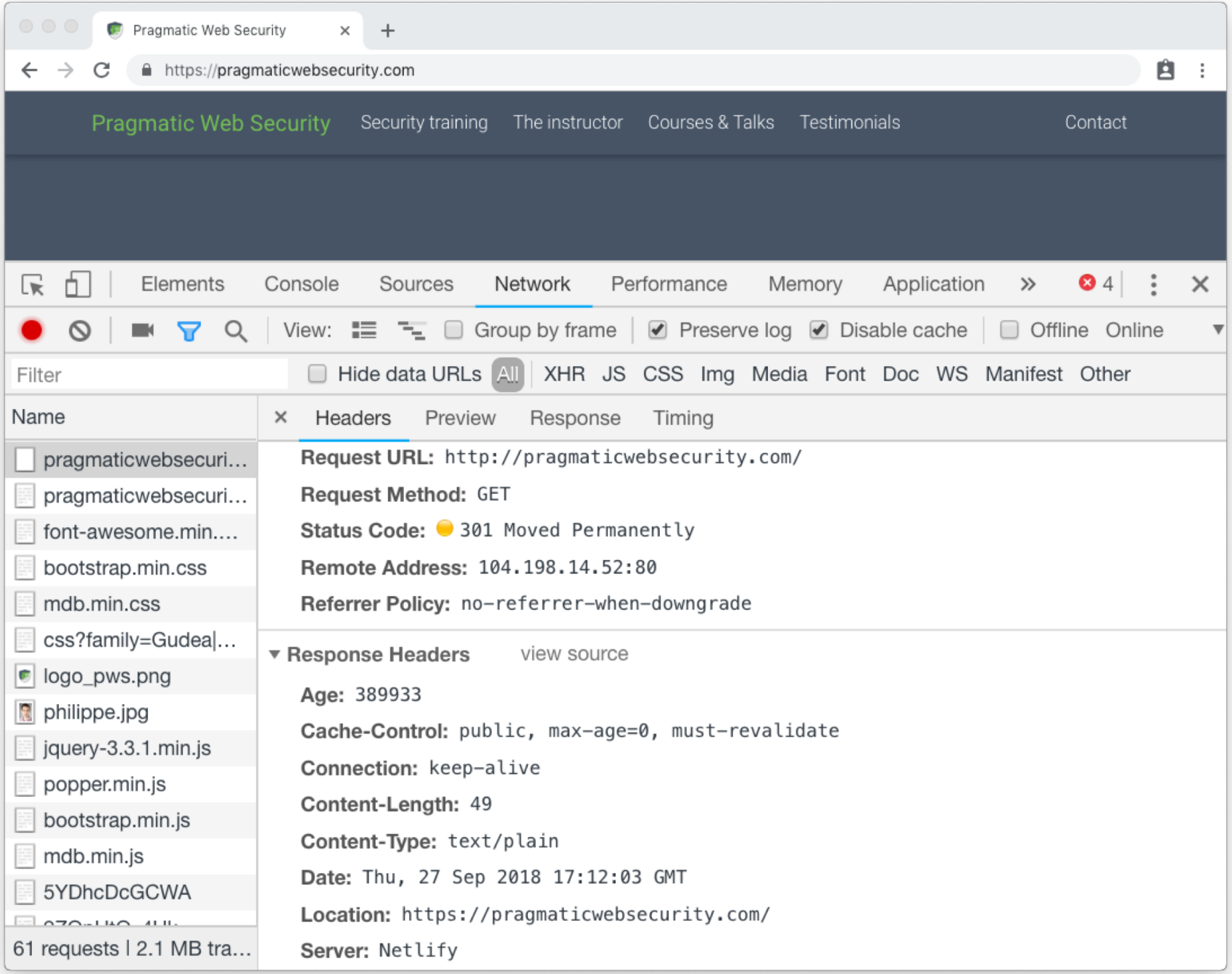
Google developer expert

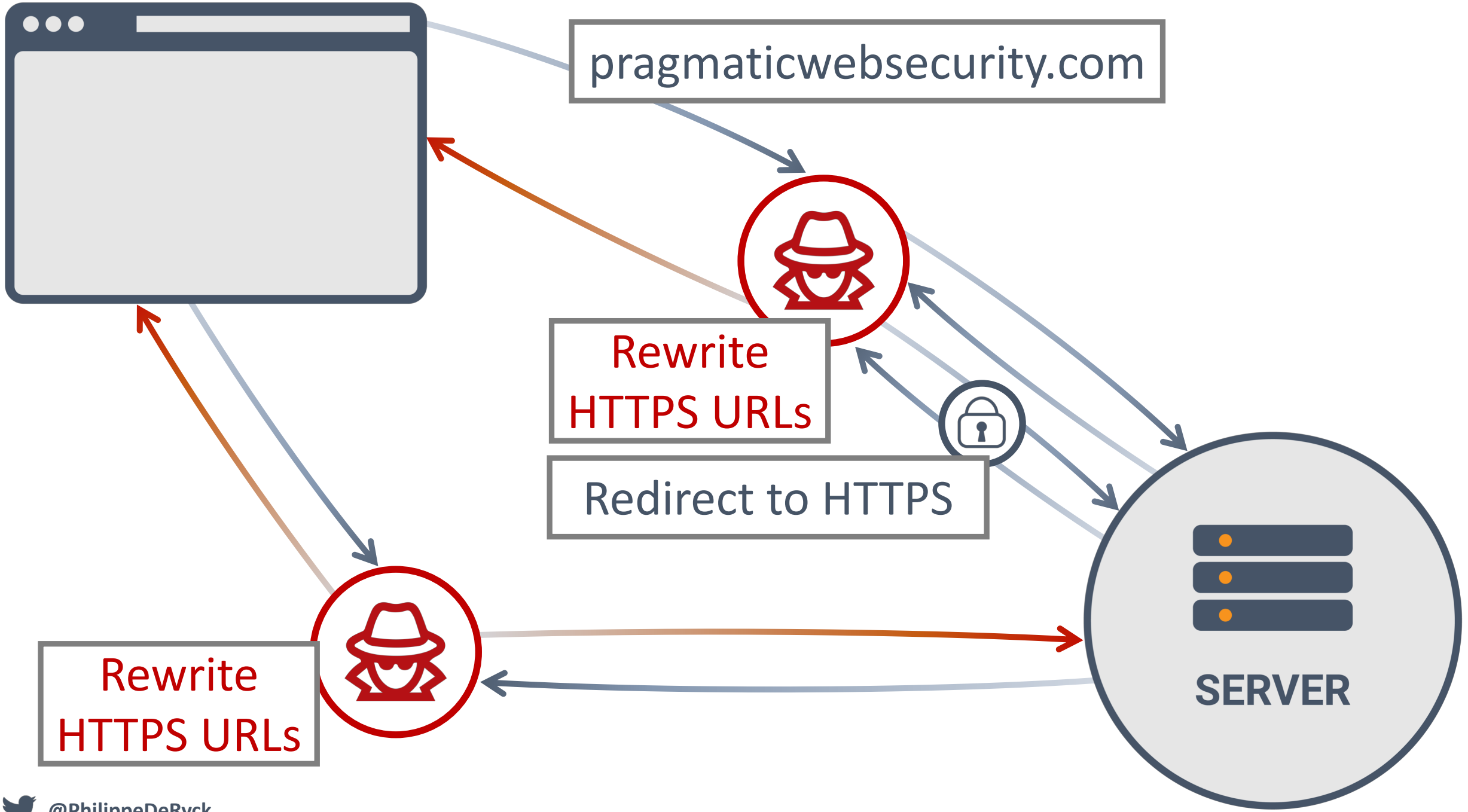
@PhilippeDeRyck

https://PragmaticWebSecurity.com


Pragmatic Web Security
https://pragmaticwebsecurity.com
Pragmatic Web Security
Pragmatic Web Security
A pragmatic approach to web security, tailored towards developers. Thorough and to-the-point lectures. Custom-built and realistic lab sessions.
LEARN MORE


New Tab
pragmaticwebsecurity.com
You’re browsing as a Guest
Pages that you view in this window won’t appear in the browser history and they won’t leave other traces, like cookies, on the computer after you close all open Guest windows. Any files that you download, however, will be preserved.
LEARN MORE


Pragmatic Web Security
https://pragmaticwebsecurity.com
Pragmatic Web Security
Security training
The instructor
Courses & Talks
Testimonials
Contact
Elements
Console
Sources
Network
Performance
Memory
Application
4
View:
Group by frame
Preserve log
Disable cache
Offline
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Name
Headers
Preview
Response
Timing
pragmaticwebsecuri...
pragmaticwebsecuri...
font-awesome.min....
bootstrap.min.css
mdb.min.css
css?family=Gudea|...
logo_pws.png
philippe.jpg
jquery-3.3.1.min.js
popper.min.js
bootstrap.min.js
mdb.min.js
5YDhcDcGCWA
61 requests | 2.1 MB tra...
Request URL: http://pragmaticwebsecurity.com/
Request Method: GET
Status Code: 301 Moved Permanently
Remote Address: 104.198.14.52:80
Referrer Policy: no-referrer-when-downgrade
Response Headers
view source
Age: 389933
Cache-Control: public, max-age=0, must-revalidate
Connection: keep-alive
Content-Length: 49
Content-Type: text/plain
Date: Thu, 27 Sep 2018 17:12:03 GMT
Location: https://pragmaticwebsecurity.com/
Server: Netlify


pragmaticwebsecurity.com
Rewrite
HTTPS URLs
Redirect to HTTPS
Rewrite
HTTPS URLs
SERVER

```
Strict-Transport-Security:
max-age=31536000
```

HTTP Strict Transport Security (HSTS)

- By enabling HSTS, a server instructs the browser to always use HTTPS
  - Typing ***restograde.com*** will result in a request sent over HTTPS
  - All HTTP links will be fetched over HTTPS
  - Even if the user types ***http://restograde.com***, the browser will use HTTPS

```
Strict-Transport-Security:  max-age=31536000
```

- HSTS is enabled by sending the ***Strict-Transport-Security*** response header
  - The header can only be set over a valid HTTPS connection
  - The ***max-age*** property indicates how long HSTS should be enabled (in seconds)

Strict Transport Security - OTHER

Usage % of all users

Global 86.03%

Declare that a website is only accessible over a secure connection (HTTPS).

Current aligned | Usage relative | Date relative | Show all

IE	Edge *	Firefox	Chrome	Safari	iOS Safari *	Opera Mini *	Chrome for Android	UC Browser for Android	Samsung Internet
			49		10.3				4
		60	66		11.2				6.2
1 11	17	61	67	11.1	11.4	all	67	11.8	7.2
	18	62	68	12	12				
		63	69	TP					
			70						

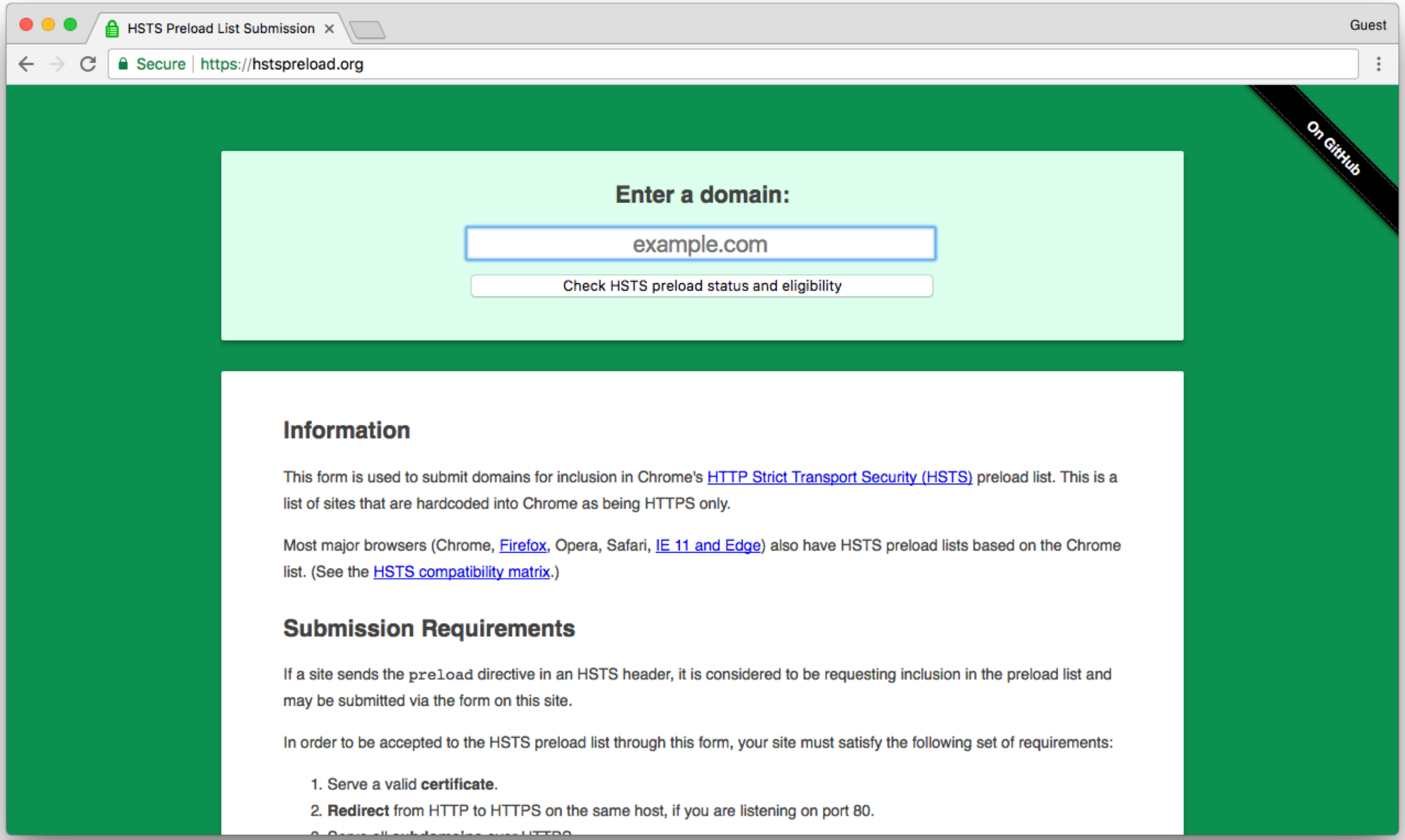
```
Strict-Transport-Security:
max-age=31536000;
includeSubDomains
```

HSTS FOR SUBDOMAINS

- HSTS supports the ***includeSubDomains*** flag
  - This flag extends the policy to all subdomains of the current domain
  - Can be set on any level, not only on registered domains

```
Strict-Transport-Security: max-age=31536000;
    includeSubDomains
```

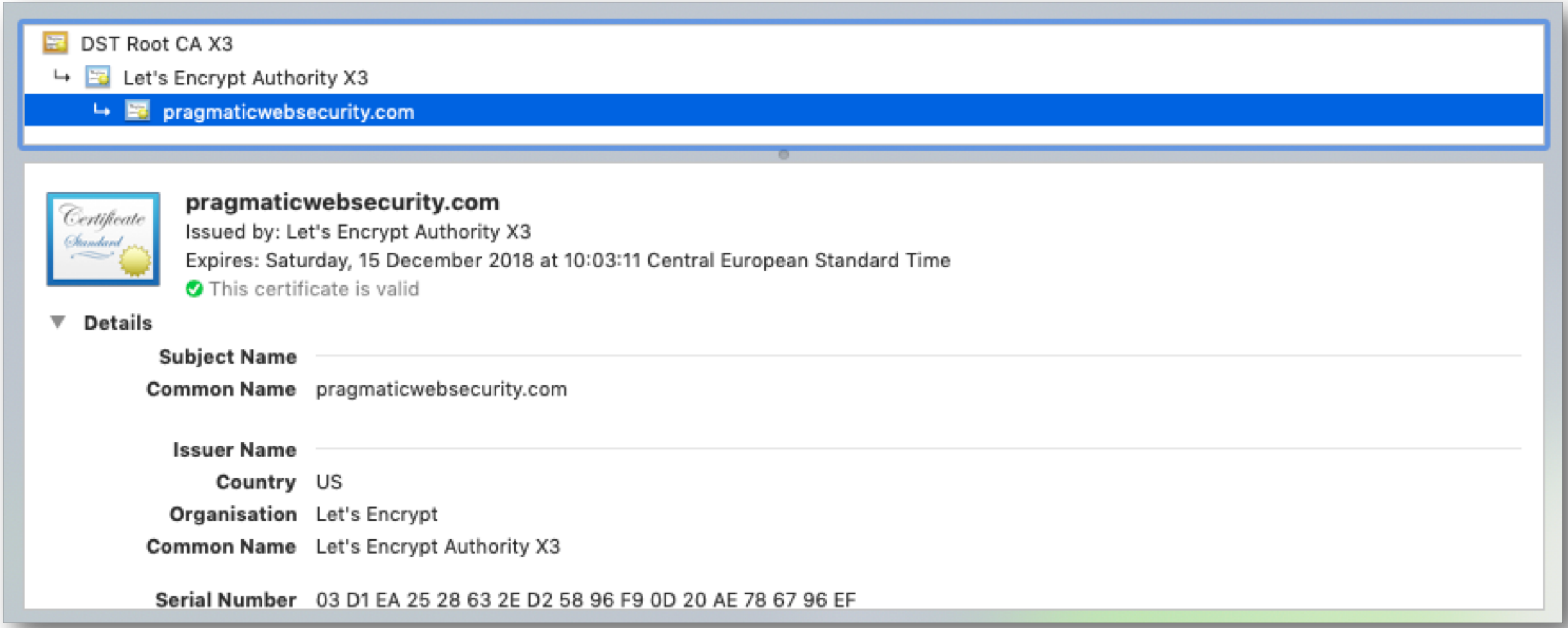
- Implications of enabling HSTS with ***includeSubDomains***
  - The browser will no longer send HTTP requests to any subdomain
  - Can potentially impact legacy services that do not support HTTP
  - Only works when browser sees parent domain, so also enable HSTS on subdomains


HSTS Preload List Submission
Guest
Secure | https://hstspreload.org
On GitHub
Enter a domain:
example.com
Check HSTS preload status and eligibility
Information
This form is used to submit domains for inclusion in Chrome's HTTP Strict Transport Security (HSTS) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only.
Most major browsers (Chrome, Firefox, Opera, Safari, IE 11 and Edge) also have HSTS preload lists based on the Chrome list. (See the HSTS compatibility matrix.)
Submission Requirements
If a site sends the preload directive in an HSTS header, it is considered to be requesting inclusion in the preload list and may be submitted via the form on this site.
In order to be accepted to the HSTS preload list through this form, your site must satisfy the following set of requirements:
1. Serve a valid certificate.
2. Redirect from HTTP to HTTPS on the same host, if you are listening on port 80.

HTTP Strict Transport Security

Enable a long-term HSTS policy for every HTTPS site

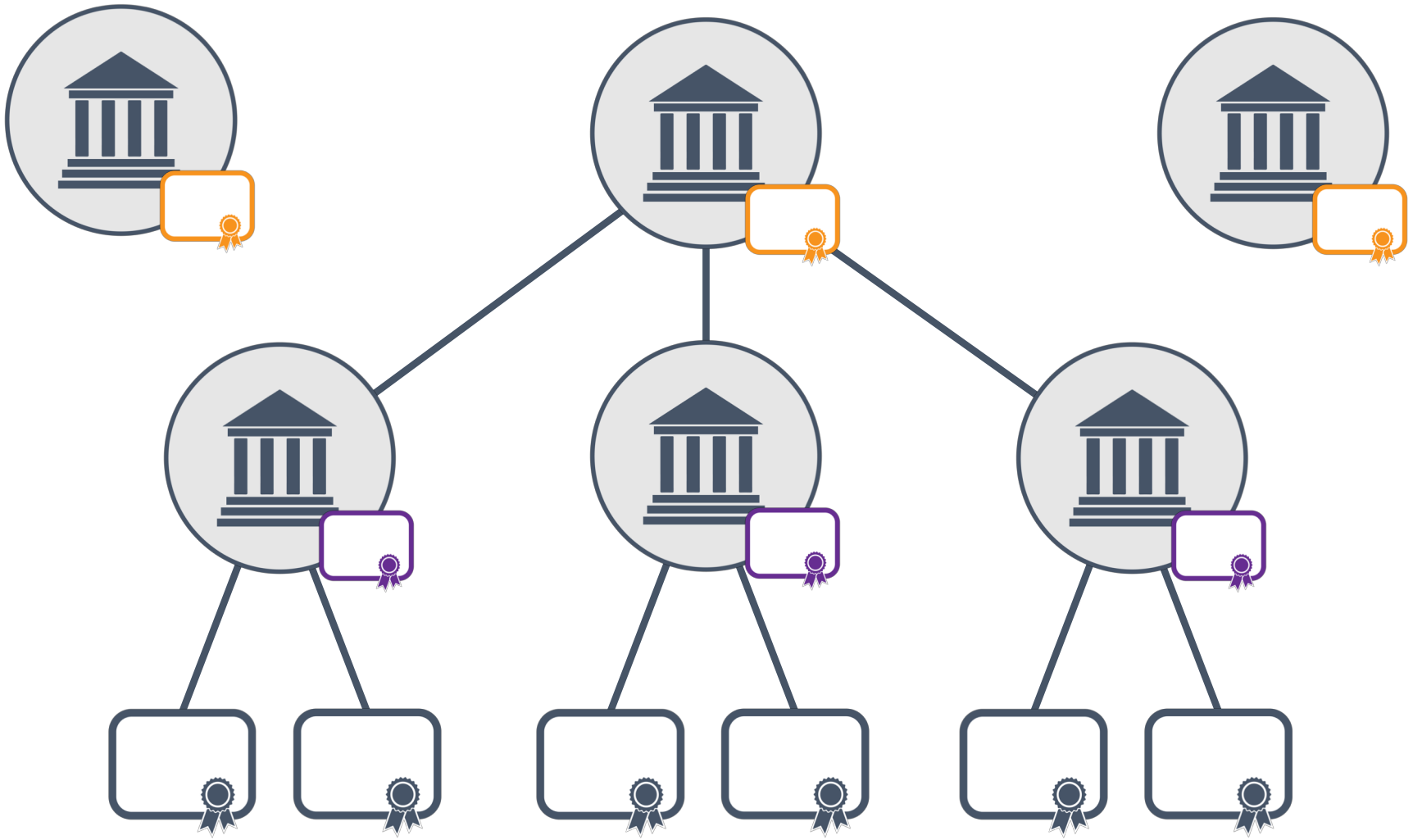
Work towards a global policy with includeSubdomains

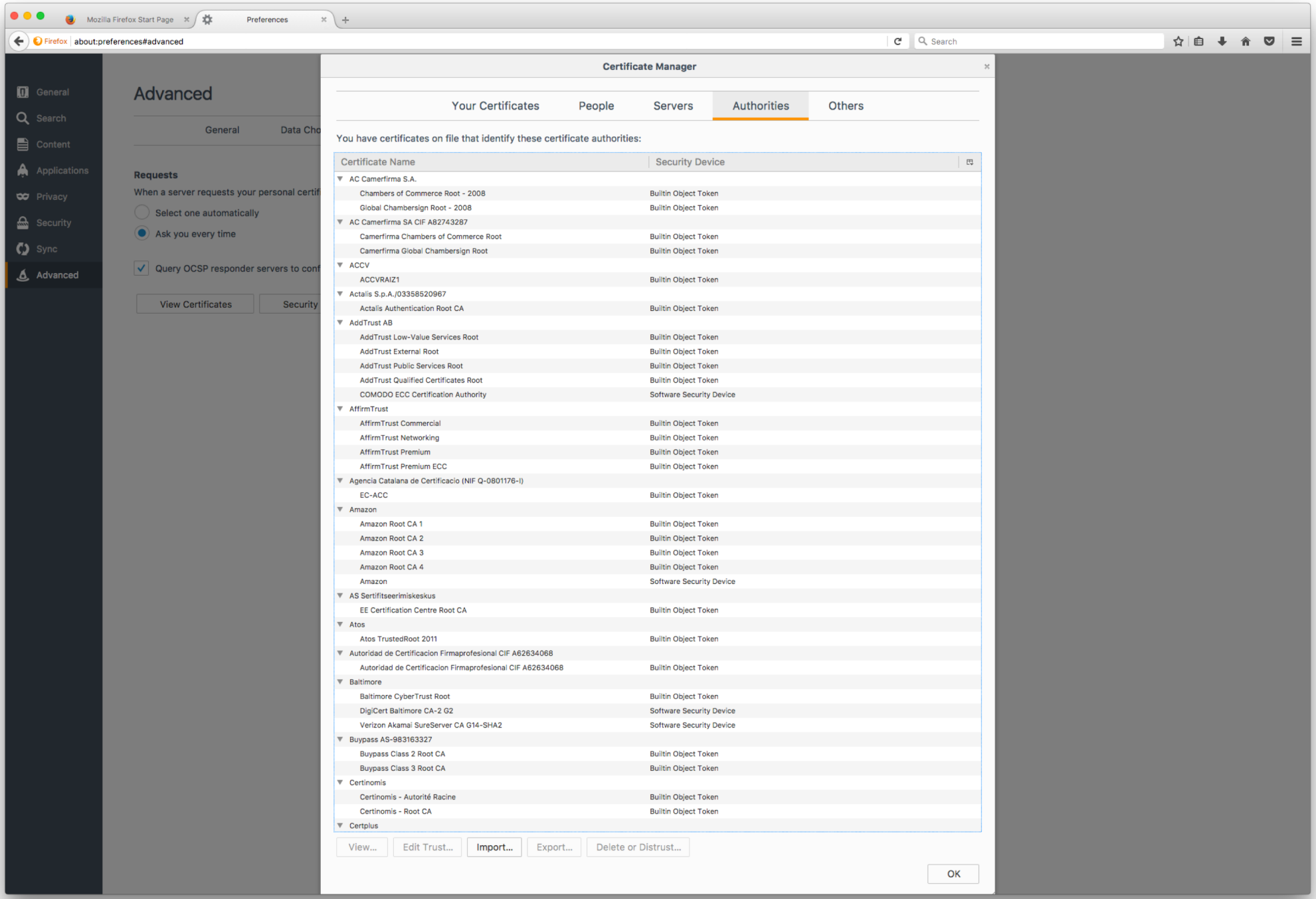

DST Root CA X3
Let's Encrypt Authority X3
pragmaticwebsecurity.com
pragmaticwebsecurity.com
Issued by: Let's Encrypt Authority X3
Expires: Saturday, 15 December 2018 at 10:03:11 Central European Standard Time
This certificate is valid
Details
Subject Name
Common Name pragmaticwebsecurity.com
Issuer Name
Country US
Organisation Let's Encrypt
Common Name Let's Encrypt Authority X3
Serial Number 03 D1 EA 25 28 63 2E D2 58 96 F9 0D 20 AE 78 67 96 EF

ROOT CA

INTERMEDIATE CA

CERTIFICATES




Mozilla Firefox Start Page
Preferences
about:preferences#advanced
Search
General
Search
Content
Applications
Privacy
Security
Sync
Advanced
Advanced
General
Data Cho
Requests
When a server requests your personal certif
Select one automatically
Ask you every time
Query OCSP responder servers to conf
View Certificates
Security
Certificate Manager
Your Certificates
People
Servers
Authorities
Others
You have certificates on file that identify these certificate authorities:
Certificate Name
Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Builtin Object Token
Global Chambersign Root - 2008
Builtin Object Token
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Commerce Root
Builtin Object Token
Camerfirma Global Chambersign Root
Builtin Object Token
ACCV
ACCVRAIZ1
Builtin Object Token
Actalis S.p.A./03358520967
Actalis Authentication Root CA
Builtin Object Token
AddTrust AB
AddTrust Low-Value Services Root
Builtin Object Token
AddTrust External Root
Builtin Object Token
AddTrust Public Services Root
Builtin Object Token
AddTrust Qualified Certificates Root
Builtin Object Token
COMODO ECC Certification Authority
Software Security Device
AffirmTrust
AffirmTrust Commercial
Builtin Object Token
AffirmTrust Networking
Builtin Object Token
AffirmTrust Premium
Builtin Object Token
AffirmTrust Premium ECC
Builtin Object Token
Agencia Catalana de Certificacio (NIF Q-0801176-I)
EC-ACC
Builtin Object Token
Amazon
Amazon Root CA 1
Builtin Object Token
Amazon Root CA 2
Builtin Object Token
Amazon Root CA 3
Builtin Object Token
Amazon Root CA 4
Builtin Object Token
Amazon
Software Security Device
AS Sertifitseerimiskeskus
EE Certification Centre Root CA
Builtin Object Token
Atos
Atos TrustedRoot 2011
Builtin Object Token
Autoridad de Certificacion Firmaprofesional CIF A62634068
Autoridad de Certificacion Firmaprofesional CIF A62634068
Builtin Object Token
Baltimore
Baltimore CyberTrust Root
Builtin Object Token
DigiCert Baltimore CA-2 G2
Software Security Device
Verizon Akamai SureServer CA G14-SHA2
Software Security Device
Buypass AS-983163327
Buypass Class 2 Root CA
Builtin Object Token
Buypass Class 3 Root CA
Builtin Object Token
Certinomis
Certinomis - Autorité Racine
Builtin Object Token
Certinomis - Root CA
Builtin Object Token
Certplus
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK

▼ Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token
▼ AddTrust AB	
AddTrust Low-Value Services Root	Builtin Object Token
AddTrust External Root	Builtin Object Token
AddTrust Public Services Root	Builtin Object Token
AddTrust Qualified Certificates Root	Builtin Object Token
COMODO ECC Certification Authority	Software Security Device
▼ AffirmTrust	
AffirmTrust Commercial	Builtin Object Token
AffirmTrust Networking	Builtin Object Token
AffirmTrust Premium	Builtin Object Token
AffirmTrust Premium ECC	Builtin Object Token
▼ Agencia Catalana de Certificacio (NIF Q-0801176-I)	
EC-ACC	Builtin Object Token
▼ Amazon	
Amazon Root CA 1	Builtin Object Token
Amazon Root CA 2	Builtin Object Token
Amazon Root CA 3	Builtin Object Token

Google boots China's main digital certificate authority CNNIC

Google says a future update in Chrome will remove trust for all certificates from China's main root certificate authority.

By Liam Tung | April 2, 2015 -- 11:46 GMT (12:46 BST) | Topic: Security

Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

4 minute read

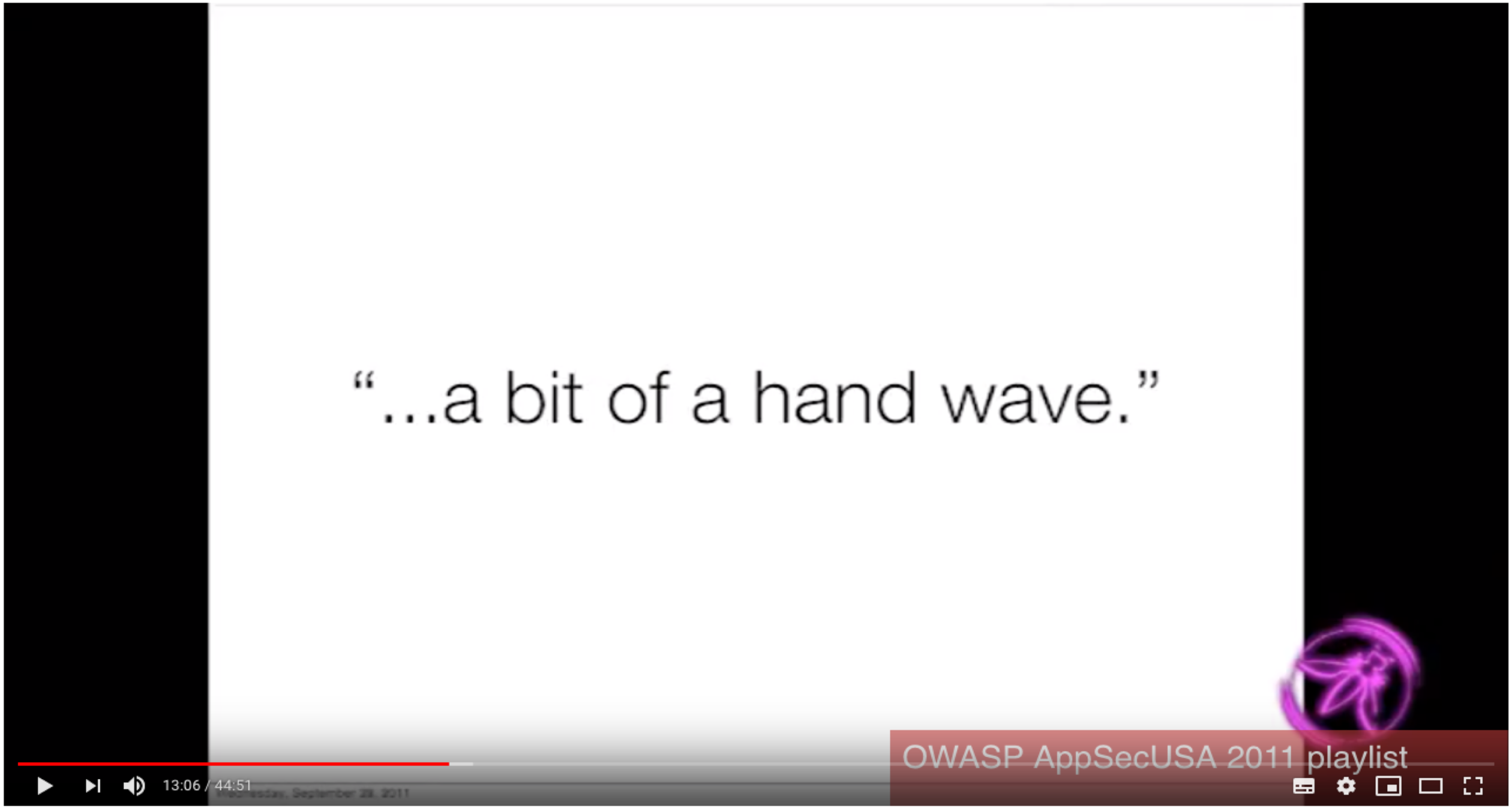
Author:
Dennis Fisher

October 31, 2012
/ 2:49 pm

Share this article:

French Government ANSSI responsible of a MITM against Google SSL-TLS

December 8, 2013 By Pierluigi Paganini



OWASP AppSecUSA 2011: Keynote: SSL and the future of authenticity

https://imgur.com/r/diwhy/p1Xxq70
https://pholder.com/r/diwhy/

@PhilippeDeRyck

Certificate Authority Authorization

```
restograde.com. CAA 0 issue "letsencrypt.org"
restograde.com. CAA 0 issue "globalsign.org"
```

```
restograde.com. CAA 0 issuewild "letsencrypt.org"
```

Certificate Authority Authorization (CAA)

- By adding CAA DNS records, you can specify the set of authorized CAs
  - Only works if CAs check your DNS records before issuing a certificate
  - Since September 2017, this is a mandatory requirement for all CAs

```
restograde.com. CAA 0 issue "letsencrypt.org"
```

- The records allow the configuration of multiple CAs
  - Only applies to this specific domain, not subdomains
  - Wildcard directives are supported as well (but again, does not include subdomains)

```
restograde.com. CAA 0 issue "letsencrypt.org"
restograde.com. CAA 0 issue "globalsign.org"
```

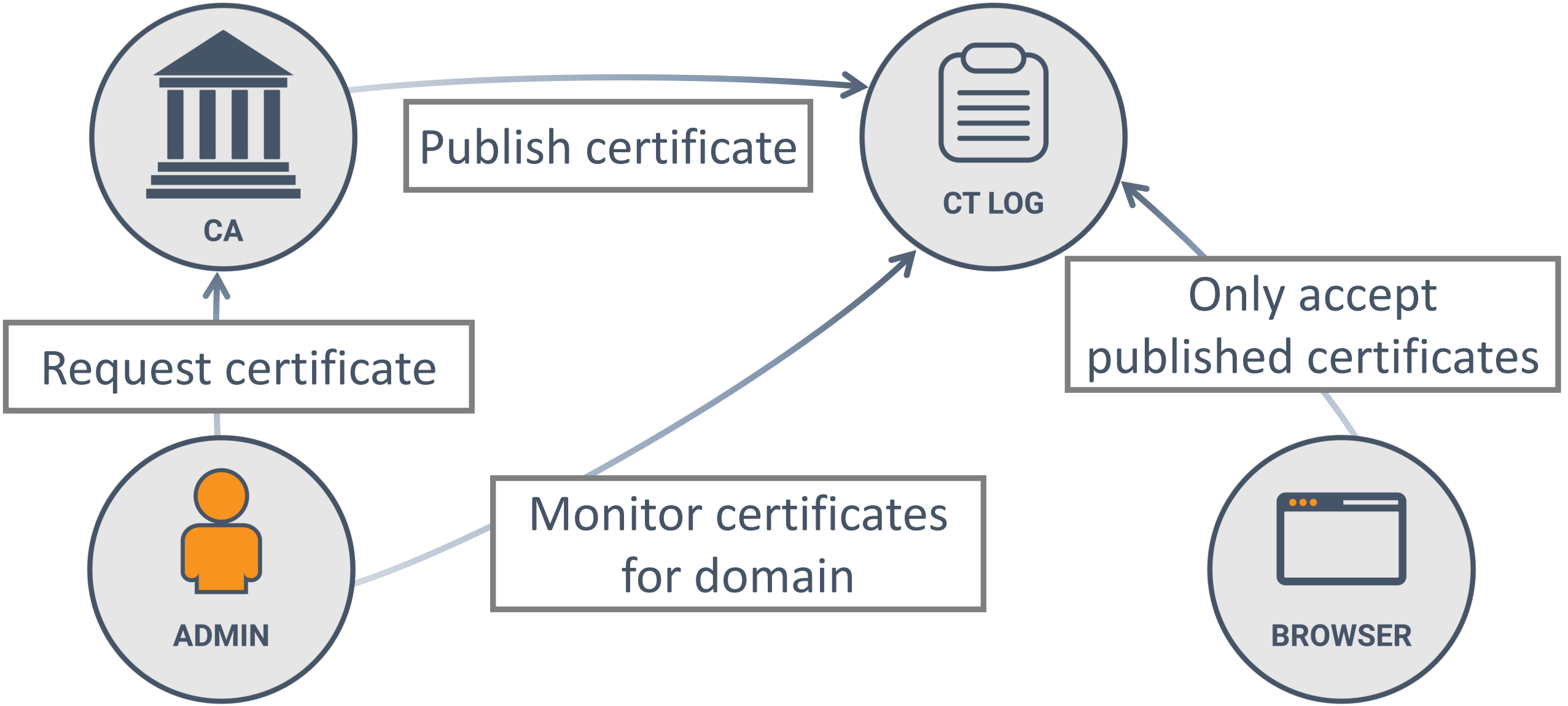
```
restograde.com. CAA 0 issuewild "letsencrypt.org"
```

Certificate Authority Authorization

Add DNS CAA records to restrict the set of valid CAs

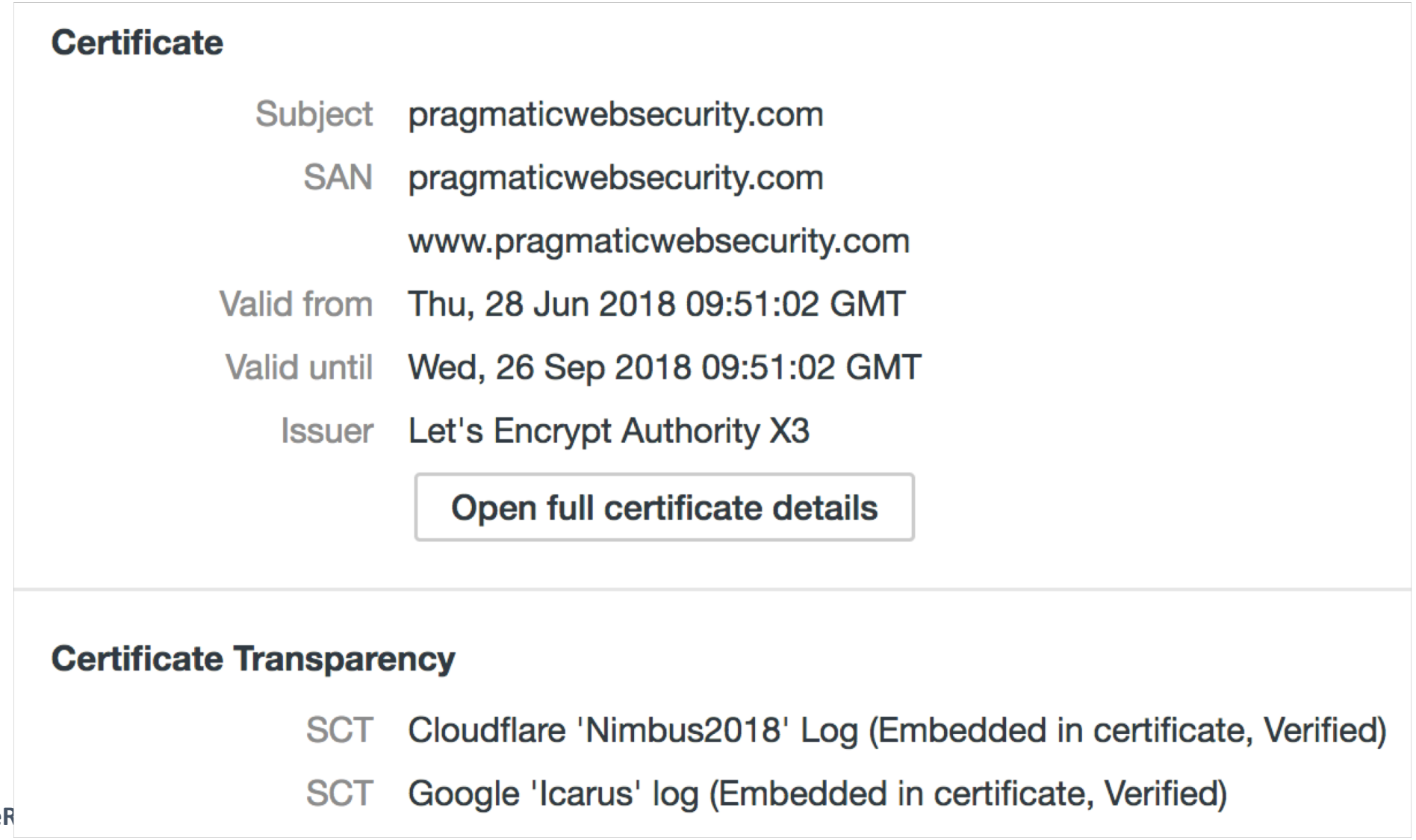
Always designate a backup CA as a fallback

Certificate Transparency



Let's Encrypt embeds SCT information in the certificate

Easy to inspect in Chrome's Security tools



How CT improves the current situation

- CT is a detective measure, not a preventive one
  - An attacker can still attempt to get a fraudulent certificate for any domain
  - But because of Certificate Transparency, that certificate will be in a public log
  - That is why Chrome started requiring the presence of SCT information in 04/2018
    - Apple requires CT to be present for certificates issued after October 2018
- Requiring certificates to be published is only the first step
  - If nobody monitors the logs, then nothing will change
  - You should setup log monitoring for your domains
  - If an attacker tricks a CA into creating a fraudulent certificate, you will get an alert
- Widespread adoption of CT enables quick revocation of fraudulent certs

Introducing our Certificate Transparency Monitoring tool

PROTECT THE GRAPH · TUESDAY, DECEMBER 13, 2016

> **Facebook's Product Security team developed and runs a system that continuously checks major public CT logs for new certificates issued on behalf of domains that we own.**

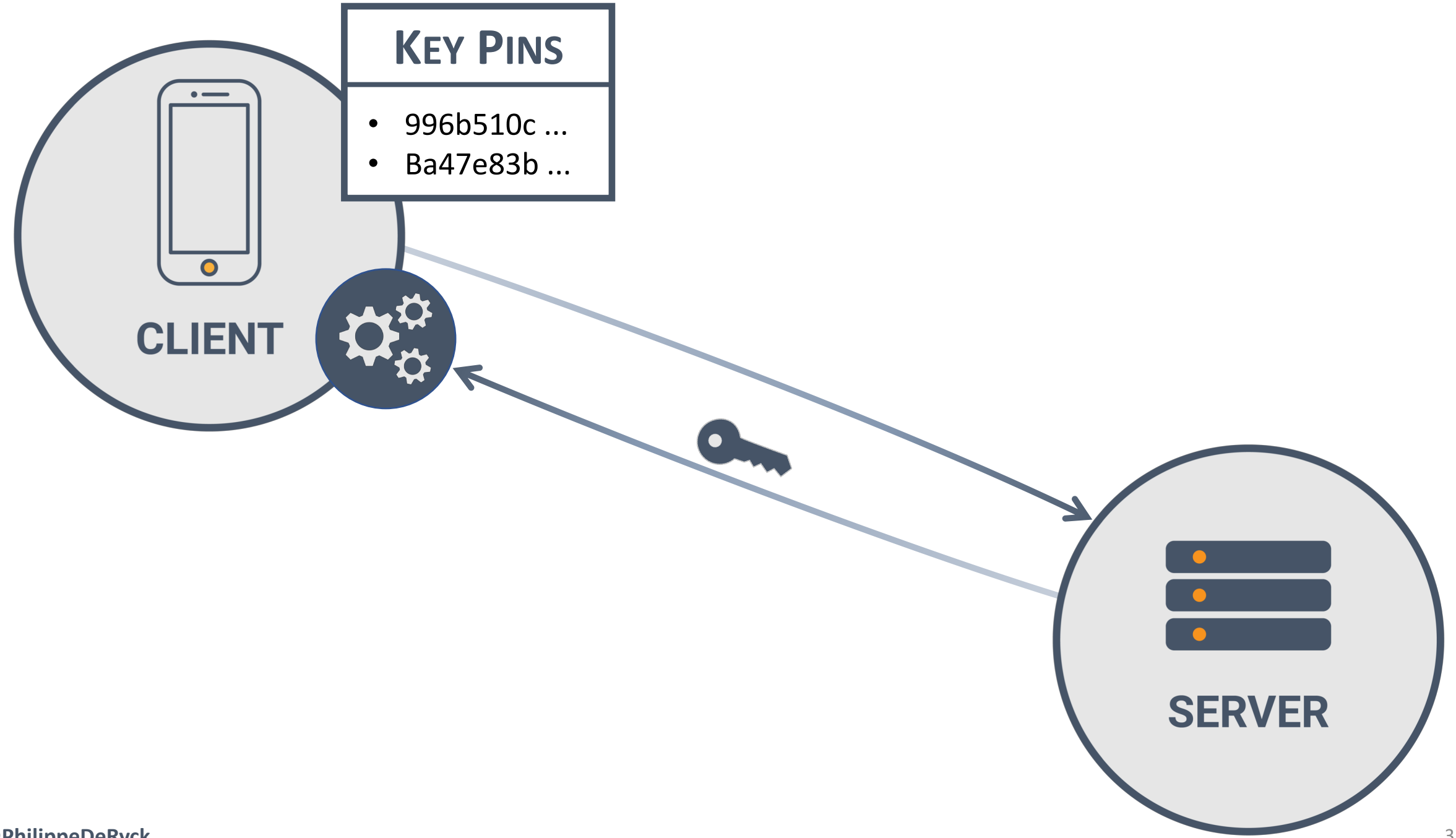
Domains	Subject	Issuer	Validity	Certificate
angularmasterclass.pragmaticwebsecurity.com	CN=angularmasterclass.pragmaticwebsecurity.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Jun 28, 2018 - Sep 26, 2018	Show Details
angularmasterclass.pragmaticwebsecurity.com	CN=angularmasterclass.pragmaticwebsecurity.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Jun 28, 2018 - Sep 26, 2018	Show Details (CT Precertificate)
www.pragmaticwebsecurity.com pragmaticwebsecurity.com	CN=pragmaticwebsecurity.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Jun 28, 2018 - Sep 26, 2018	Show Details (CT Precertificate)
www.pragmaticwebsecurity.com pragmaticwebsecurity.com	CN=pragmaticwebsecurity.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Jun 28, 2018 - Sep 26, 2018	Show Details
essentials.pragmaticwebsecurity.com	CN=essentials.pragmaticwebsecurity.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Jun 28, 2018 - Sep 26, 2018	Show Details
essentials.pragmaticwebsecurity.com	CN=essentials.pragmaticwebsecurity.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Jun 28, 2018 - Sep 26, 2018	Show Details (CT Precertificate)

Subject	Issuer	# DNS names	Valid from	Valid to	# CT logs	
14021.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	1	18 Jul 2017	23 Sep 2018	3	See details
T90PANL.1J01.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	2	3 May 2017	13 Jul 2018	3	See details
54082-ssoservices.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	1	6 Sep 2017	8 Sep 2019	3	See details
54082-ssoservices-dev.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	1	1 Jun 2017	2 Jun 2019	3	See details
T90PANL.1G01.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	2	17 Jul 2017	7 Aug 2018	2	See details
14021-nonprod.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	1	23 Oct 2017	4 Nov 2018	1	See details
51034-nonprod-bp.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	1	16 May 2017	17 Jul 2018	2	See details
14021.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	1	18 Jul 2017	23 Sep 2018	1	See details
48472-NonProd-crmtool.bankofamerica.com	Symantec Class 3 Secure Server CA - G4	1	17 May 2017	29 Jul 2018	3	See details
53561.bankofamerica.com	Symantec Class 3 EV SSL CA - G3	1	15 Aug 2017	17 Aug 2018	2	See details

Certificate Transparency

Ensure that all certificates have CT information

Setup a rigorous CT monitoring process


KEY PINS
• 996b510c ...
• Ba47e83b ...
CLIENT
SERVER

Google: Chrome is backing away from public key pinning, and here's why

Google wrote the HTTP public key pinning standard but now considers the web security measure harmful.

By Liam Tung | October 30, 2017 -- 12:44 GMT (12:44 GMT) | Topic: Security

“Security researchers have highlighted a number of problems with HPKP, including the possibility for an attacker to install malicious pins or for a site operator to accidentally block visitors.”

KEY PINNING EXAMPLES ON ANDROID

```
URL targetURL = new URL(dest);
HttpsURLConnection targetConnection = (HttpsURLConnection) targetURL.
targetConnection.connect();
if (validatePinning(targetConnection, PINS)) {
    final String updateText = "Key pinning succeded for: " + dest;
    runOnUiThread(new Runnable() {
        @Override
        public void run() {
            textView.setText(updateText);
        }
    });
} else {
    final String updateText = "Key pinning failed for: " + dest;
    runOnUiThread(new Runnable() {
        @Override
        public void run() {
            textView.setText(updateText);
        }
    });
}
```

Pinning on Android N

If your minimum SDK is Android N (API 24) then the implementation couldn't be simpler as Android has a new API in town the Network Security Configuration. Even better this configuration even works for WebViews with no additional effort on your part.

Through a simple entry in your AndroidManifest.xml file you specify an XML configuration file that defines the pins you require. Of course being XML based this isn't useful if you want to dynamically specify your pins.

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config>
        <domain includeSubdomains="true">appmattus.com</domain>
        <pin-set>
            <pin digest="SHA-
256">4hw5tz+scE+TW+mlai5YipDfFWn1dqvfLG+nU7tq1V8=</pin>
            <pin digest="SHA-
256">YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=</pin>
        </pin-set>
    </domain-config>
</network-security-config>
```

Recommendations for public key pinning

- Key pinning is an extremely powerful security measure
  - It gives you full control over which keys and certificates are considered legitimate
  - It prevents the use of illegitimate keys and certificates, even when issued by a CA
- The problem with public key pinning is updating the pins over time
  - If the pins go out of sync with the server's keys, the connection breaks
  - For web applications, this also breaks the update channel for fixing the pins
  - Mobile/native applications have an out-of-band update channel
    - Pins can be fixed by pushing an update through the app store
- Pinning is deprecated for web applications, but recommended for others
  - Pinning can be done on different levels (server, intermediate CA, root CA)
  - It's safer to pin a key than to pin a certificate
  - If possible, also pin a backup key in case of emergency

Public Key Pinning

Stay away from key pinning in web applications

Use it for sensitive applications with an out-of-band update channel

Modern HTTPS deployments

Serve everything over HTTPS

Deploy HSTS, preferably on the top-level domain

Configure CAA to restrict valid CAs

Monitor CT logs for your domains

Use public-key pinning for applications with an out-of-band update channel

Oct. 15th – 16th 2018

Leuven, Belgium

Oct. 18th – 19th 2018

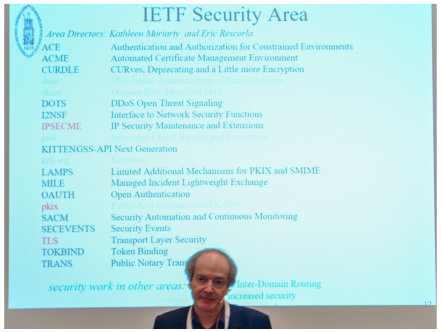
Web Security Essentials

Angular Security Masterclass

https://pragmaticwebsecurity.com/#courses

SecAppDev 2019

February 18 - 22, Leuven, Belgium



1-day workshops

Building secure web & web service applications
Jim Manico

Whiteboard hacking (aka hands-on Threat Modeling)
Sebastien Deleersnyder

Securing Kubernetes the hard way
Jimmy Mesta

5-day dual-track program

Crypto, AppSec Processes, web security, access control, mobile security, ...

Pragmatic Web Security

Security training for developers

/in/PhilippeDeRyck

@PhilippeDeRyck

philippe@pragmaticwebsecurity.com