Why Traditional Web Security Technologies no Longer Suffice to Keep You Safe

Philippe De Ryck

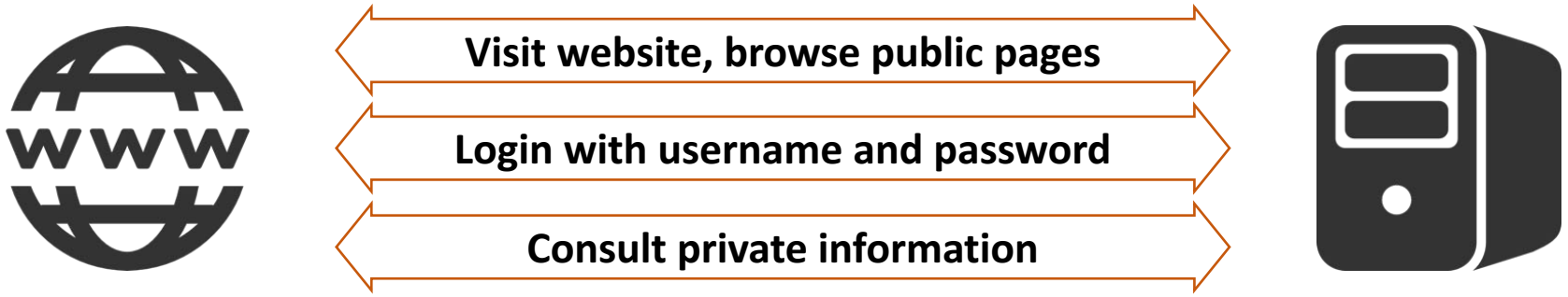
OWASP Belgium, February 2017

https://www.websec.be

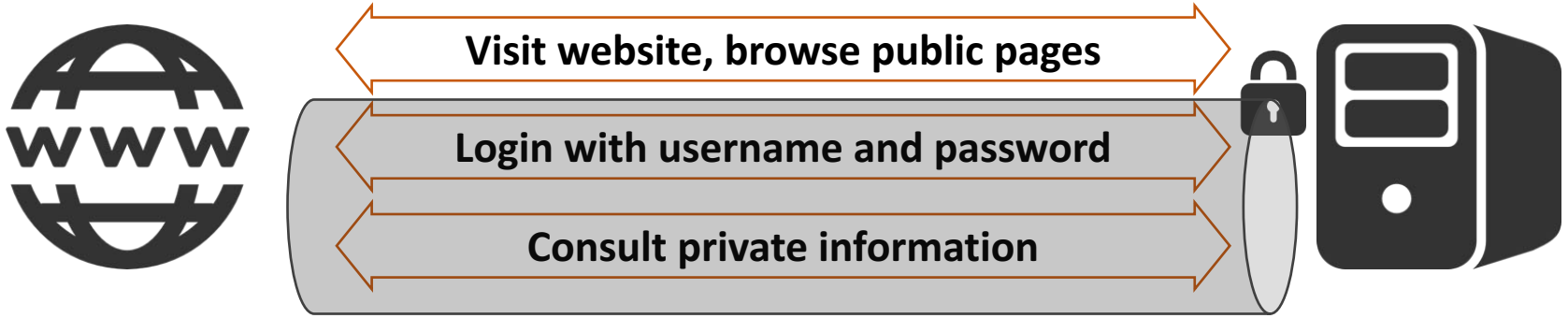
@PhilippeDeRyck

Which scenario would you consider to be secure?

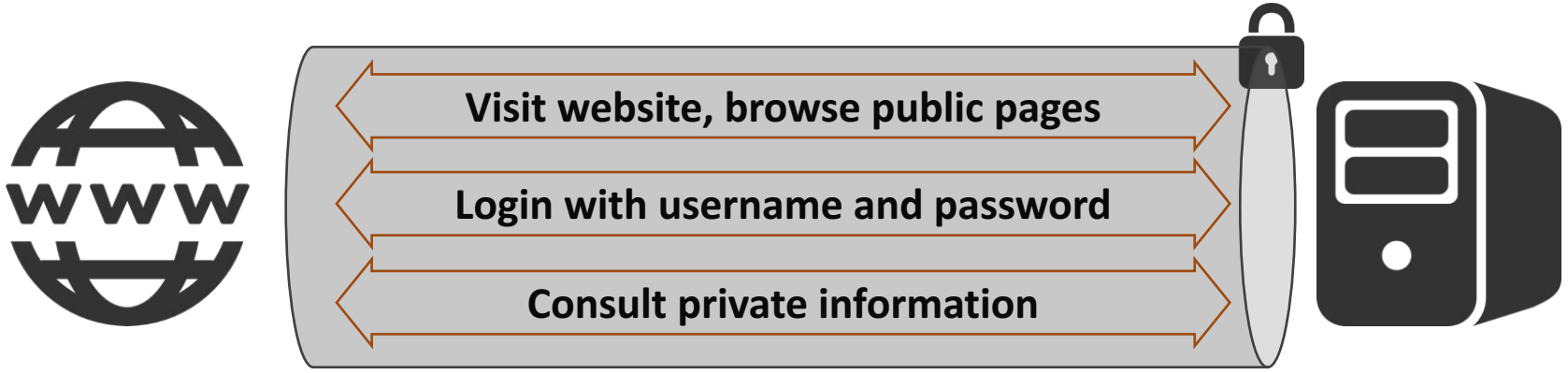
(a)



(b)

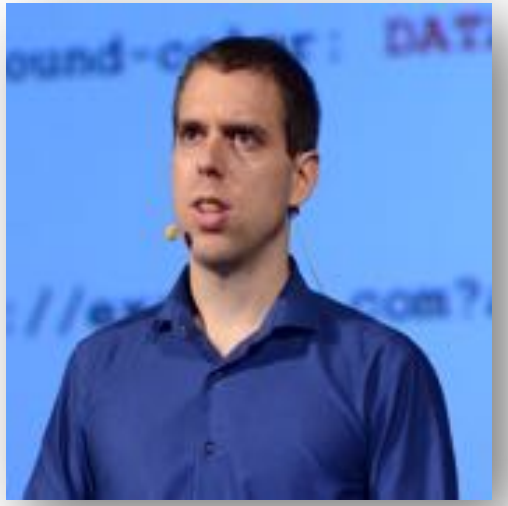


(c)

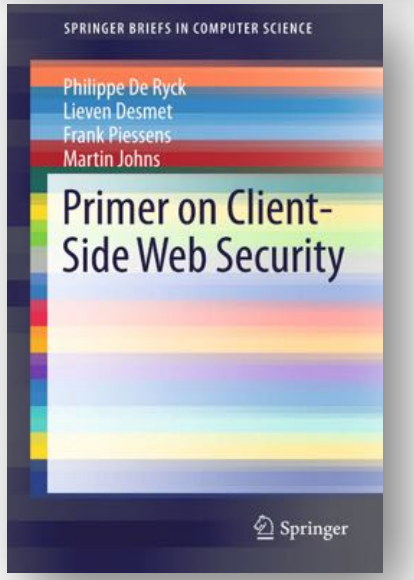


About me – Philippe De Ryck

- My goal is to help you build secure web applications
  - In-house training programs at various companies
  - Hosted web security training courses at DistriNet (KU Leuven)
  - Talks at various developer conferences
  - Slides, videos and blog posts on **https://www.websec.be**

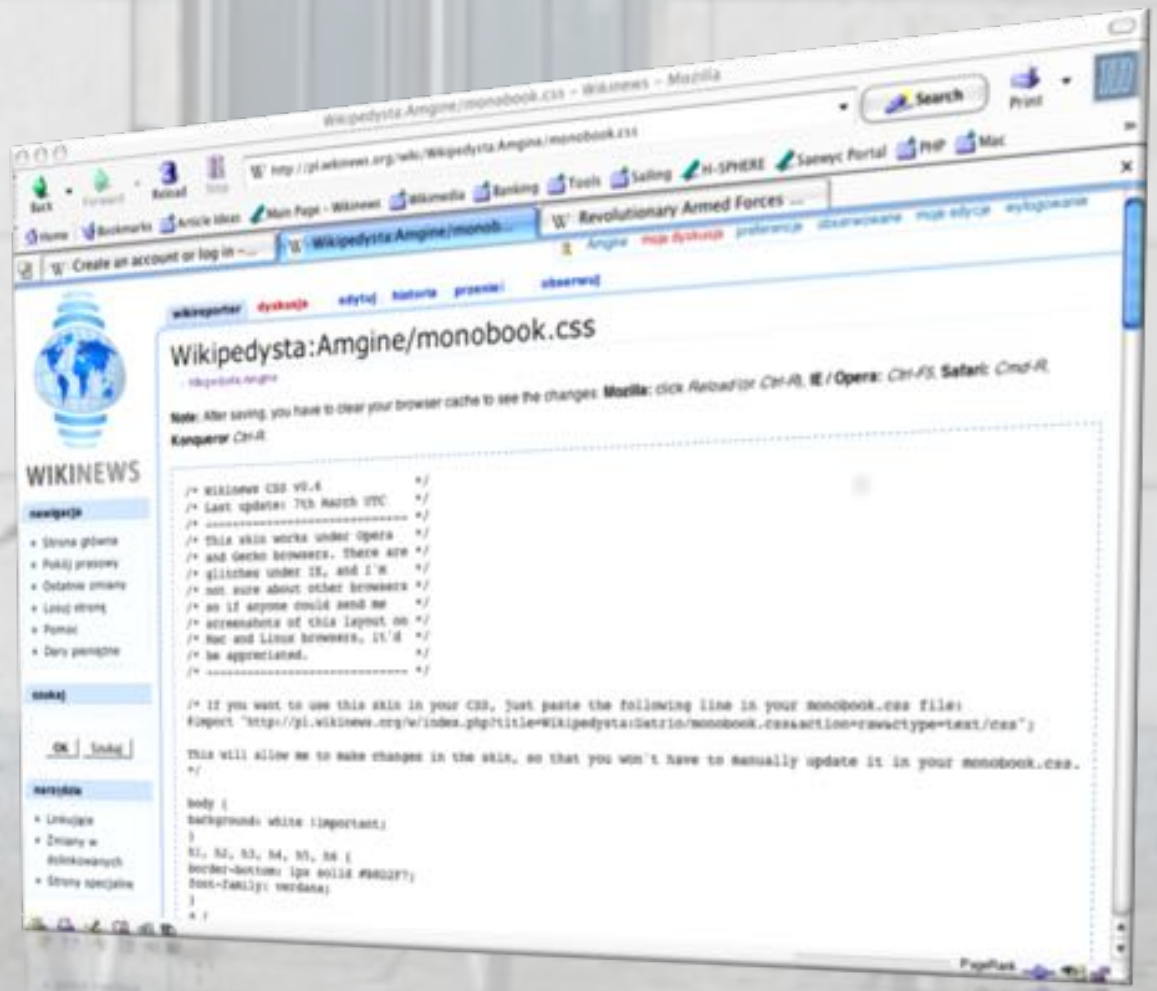


- I have a broad security expertise, with a focus on Web Security
  - PhD in client-side web security
  - Main author of the *Primer on client-side web security*

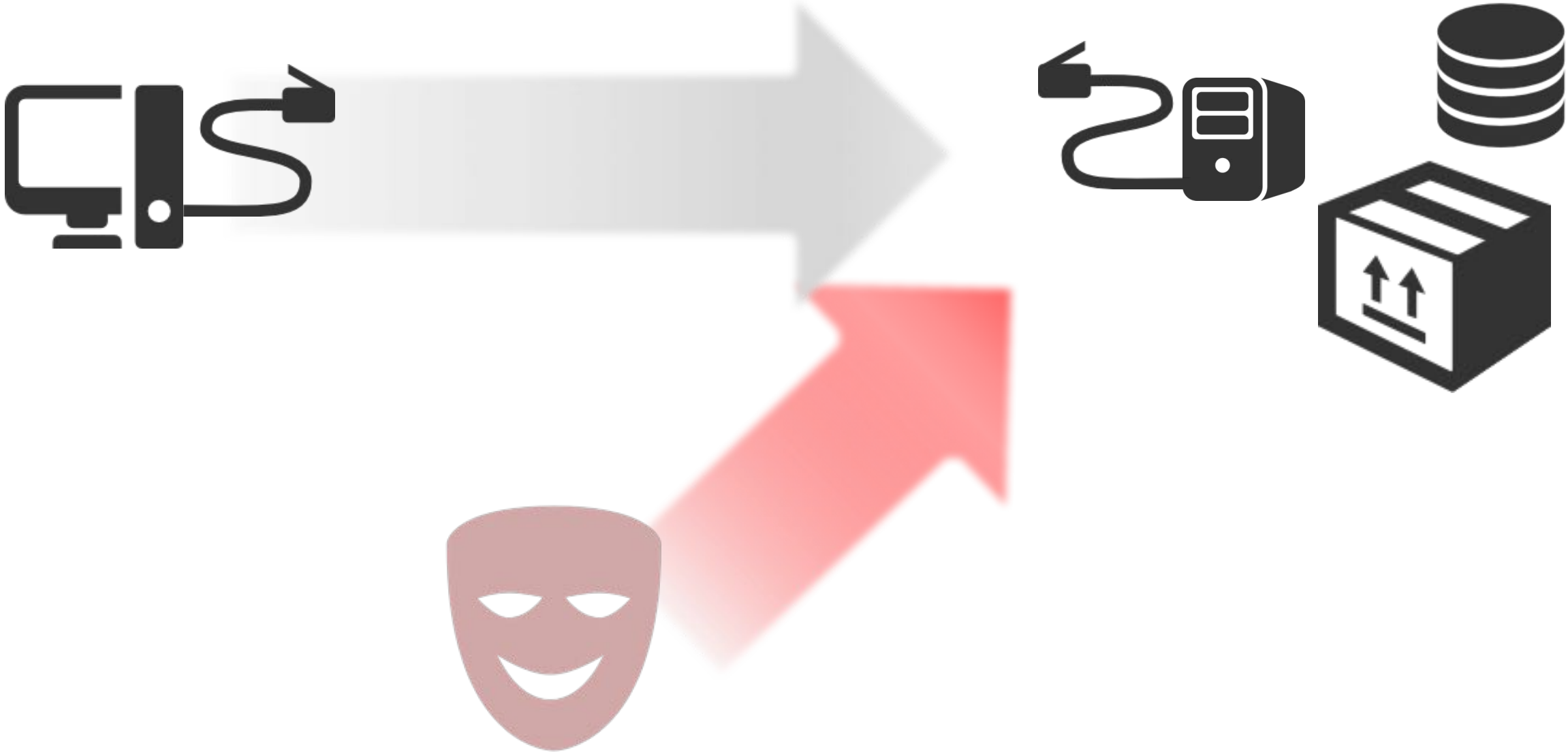


- Part of the organizing committee of ***SecAppDev.org***
  - Week-long course focused on practical security


YAHOO!
Yahoo! Auctions
coins, cards, stamps
Toshiba Laptop Giveaway!
ON SALE at COST
Find a loan
Win $10,000
Search
advanced search
Yahoo! Games - Play online chess, bridge, spades, hearts and more
Arts & Humanities
Literature, Photography
Business & Economy
Companies, Finance, Jobs
Computers & Internet
Internet, WWW, Software, Games
Education
College and University, K-12
Entertainment
Cool Links, Movies, Humor, Music
Government
Military, Politics, Law, Taxes
Health
Medicine, Diseases, Drugs, Fitness
News & Media
Full Coverage, Newspapers, TV
Recreation & Sports
Sports, Travel, Autos, Outdoors
Reference
Libraries, Dictionaries, Quotations
Regional
Countries, Regions, US States
Science
Biology, Astronomy, Engineering
Social Science
Archaeology, Economics, Languages
Society & Culture
People, Environment, Religion
In the News
Marketplace
Inside Yahoo!
World Yahoo!s
Enter Zip Code


Wikipedysta:Amgine/monobook.css
WIKINEWS
Search
Print
Revolutionary Armed Forces
Create an account or log in
Note: After saving, you have to clear your browser cache to see the changes. Mozilla: click Reload or Ctrl-R, IE / Opera: Ctrl-F5, Safari: Cmd-R, Konqueror Ctrl-R
/* Wikinews CSS v0.4 */
/* Last update: 7th March UTC */
/* This skin works under Opera */
/* and Gecko browsers. There are */
/* glitches under IE, and I'm */
/* not sure about other browsers */
/* so if anyone could send me */
/* screenshots of this layout on */
/* Mac and Linux browsers, it'd */
/* be appreciated. */
/* If you want to use this skin in your CSS, just paste the following line in your monobook.css file:
@import "http://pl.wikinews.org/w/index.php?title=Wikipedysta:Gatrin/monobook.css&action=raw&ctype=text/css";
This will allow me to make changes in the skin, so that you won't have to manually update it in your monobook.css.
*/
body {
background: white !important;
}
h1, h2, h3, h4, h5, h6 {
font-family: verdana;
}

The web used to be Server-Centric



With a lot of server-side problems

Hackers actively exploit critical vulnerability in sites running Joomla

Wave of attacks grows. Researchers advise sites to install just-released patch.

by **Dan Goodin** - Dec 14, 2015 6:39pm CET

Share Tweet Email 24

A patch for the vulnerability, which affects versions 1.5 through 3.4.5, was released Monday morning. It was too late: the bug was already being exploited in the wild, researchers from security firm Sucuri warned in a blog post. The attacks started on Saturday from a handful of IP addresses and by Sunday included hundreds of exploit attempts to sites monitored by Sucuri.

"Today (Dec 14th), the wave of attacks is even bigger, with basically every site and honeypot we have being attacked," the blog post reported. "That means that probably every other Joomla site out there is being targeted as well."

http://arstechnica.com/security/2015/12/hackers-actively-exploit-critical-vulnerability-in-sites-running-joomla/

With a lot of server-side problems

One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids

WRITTEN BY LORENZO FRANCESCHI-BICCHIERAI

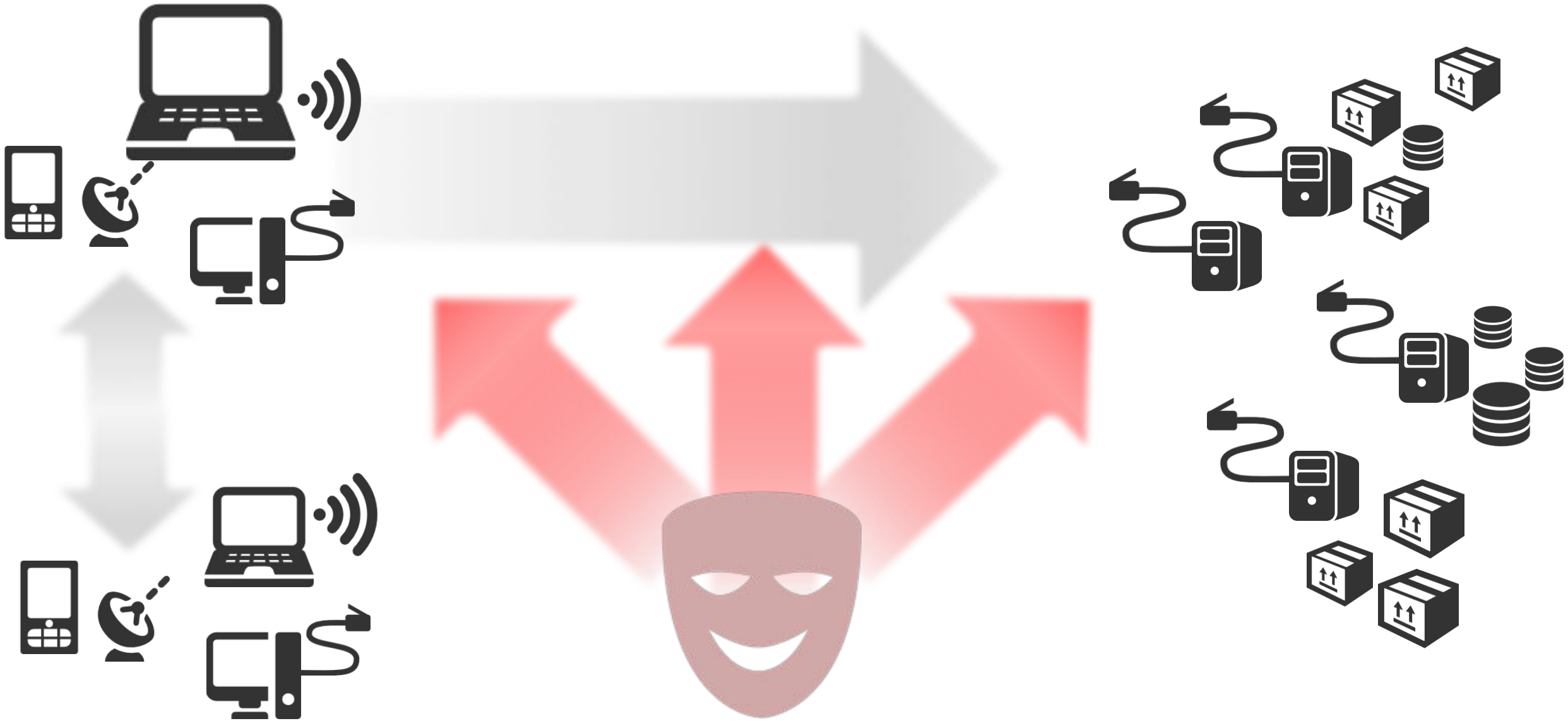
November 27, 2015 // 11:08 AM EST

When pressed, VTech did not provide any details on the attack. But the hacker, who requested anonymity, told Motherboard that they gained access to the company's database using a technique known as SQL injection. Also known as SQLi, this is an ancient, yet extremely effective, method of attack where hackers insert malicious commands into a website's forms, tricking it into returning other data.

"We were not aware of this unauthorized access until you alerted us."

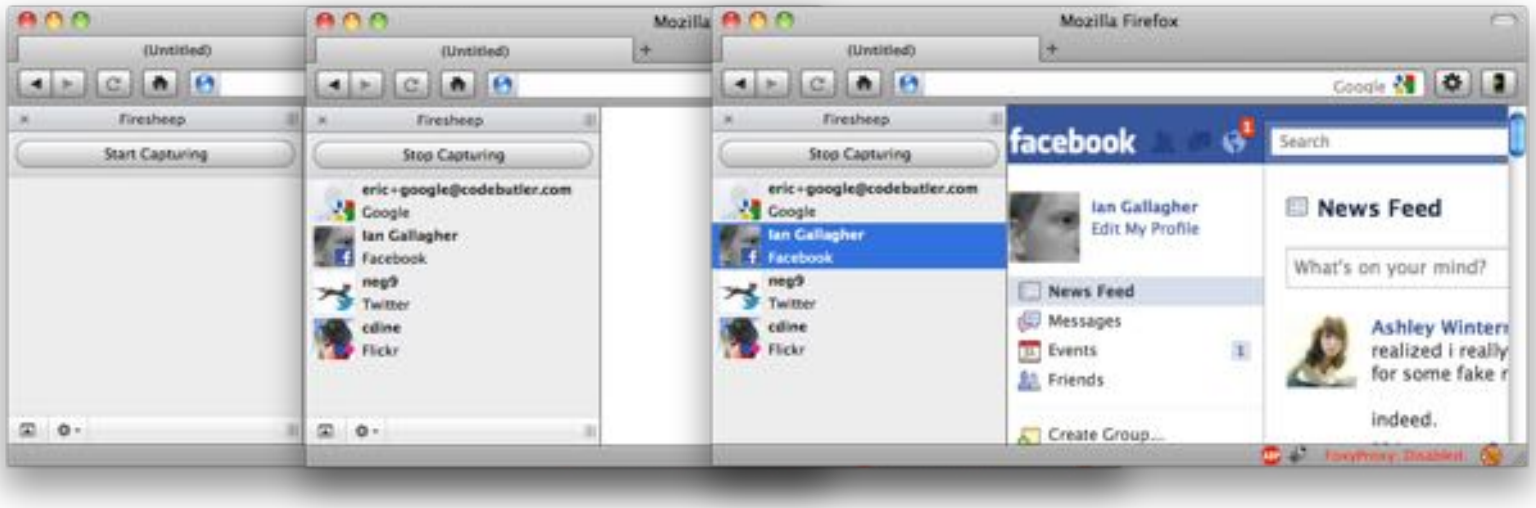
http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids

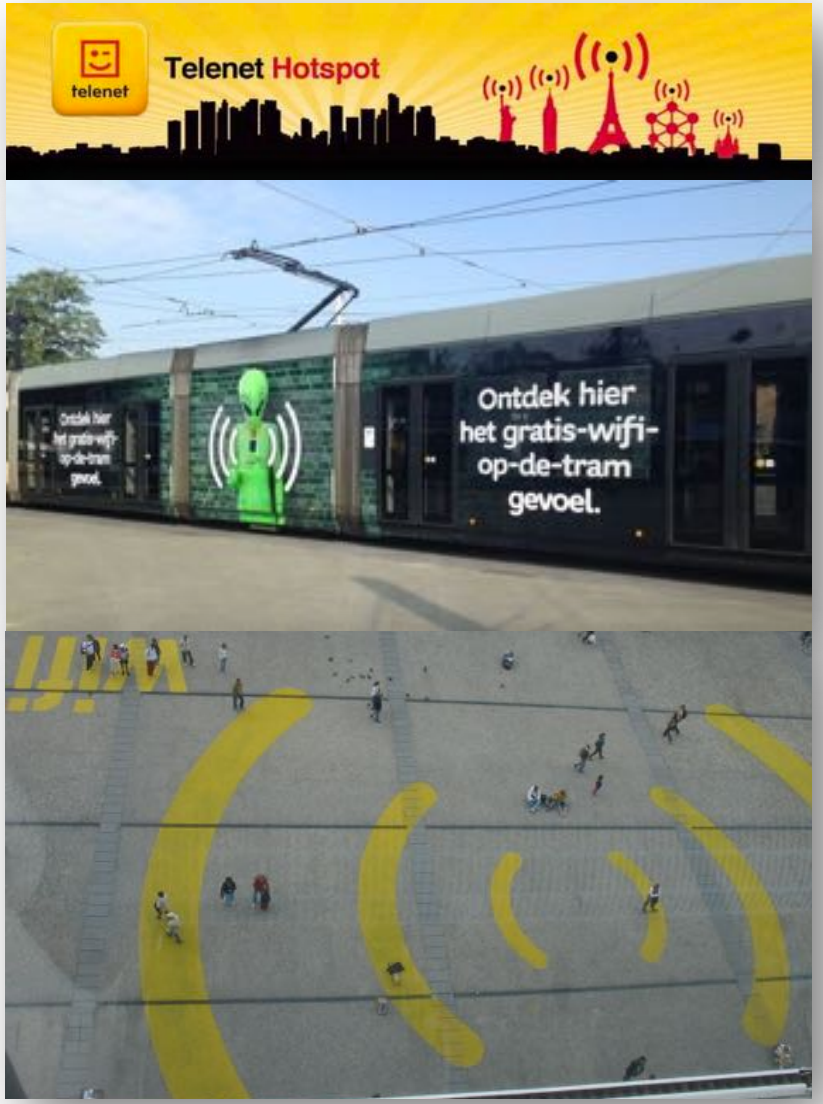
The Web has become client-centric



Networks Are Everywhere

- We happily connect to any network we can find
  - Without knowing who has control over the network
- People know about eavesdropping attacks
  - Sniffing usernames, passwords, session identifiers, …





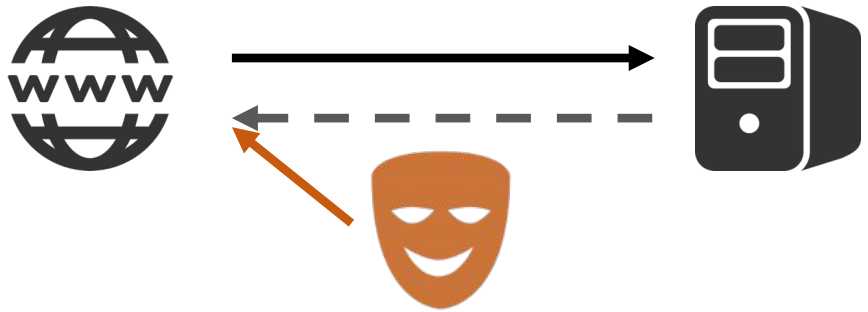
https://www.flickr.com/photos/djimison/222214205/
http://codebutler.com/firesheep/

The Communication Channel Is Insecure

- But we use HTTPS for sensitive data
  - Sufficient to counter passive eavesdropping attacks
  - But what about active network attacks?

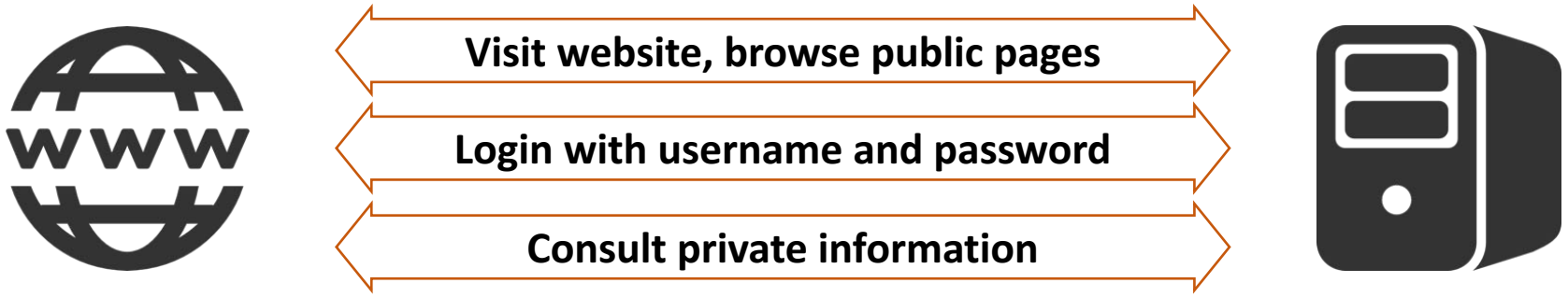
Man in the Middle

Man on the Side

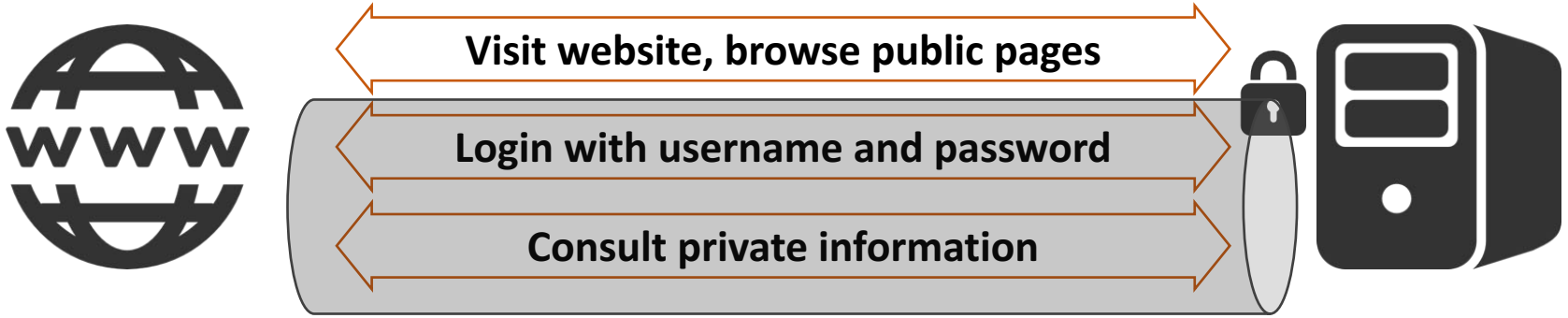


3 VARYING LEVELS OF HTTPS

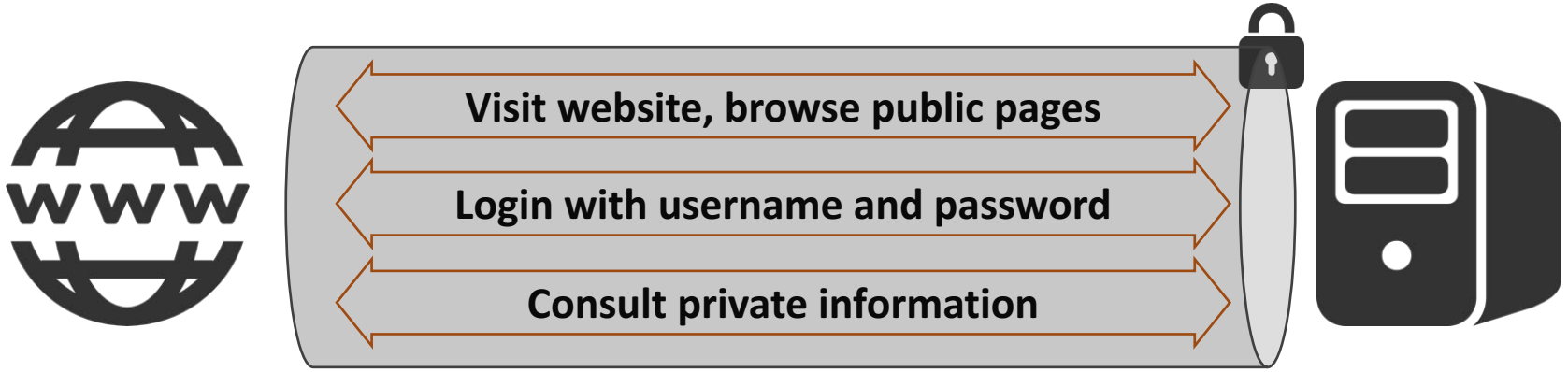
(a)



(b)

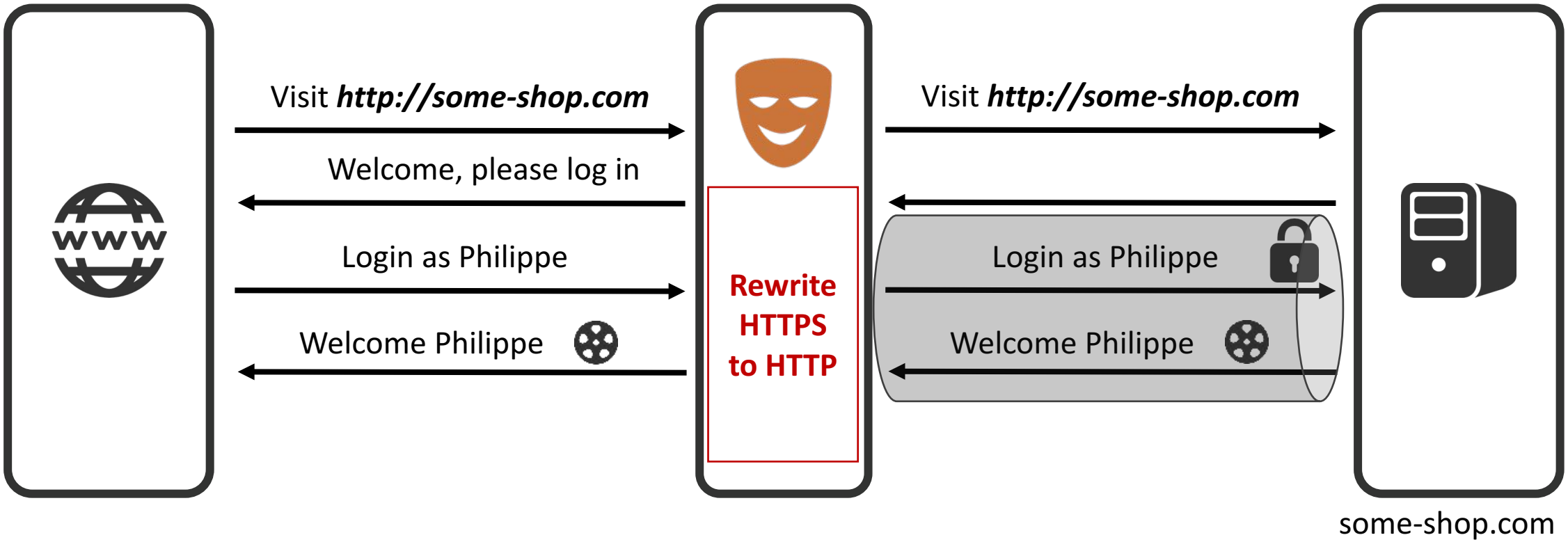


(c)

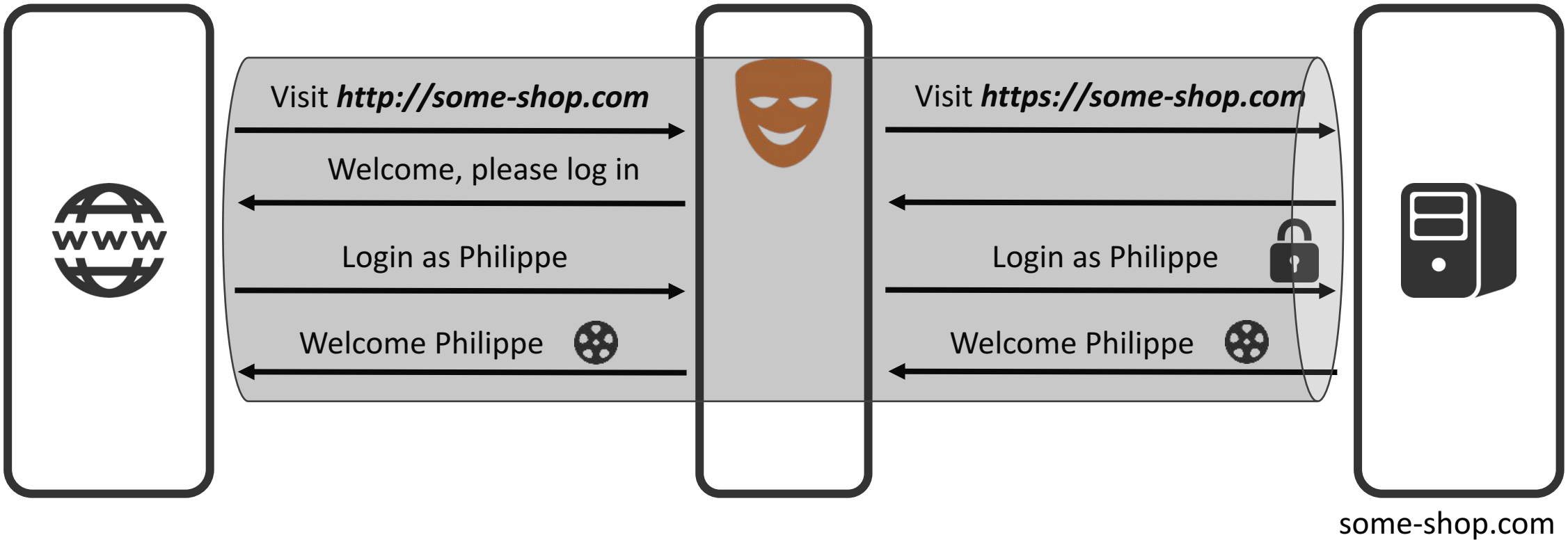


PREVENTING THE TRANSITION FROM HTTP TO HTTPS

Preventing the transition from HTTP to HTTPS



TIME TO MOVE TOWARDS HTTPS



HTTP WEAKENS HTTPS SITES

95% of HTTPS servers vulnerable to trivial MITM attacks

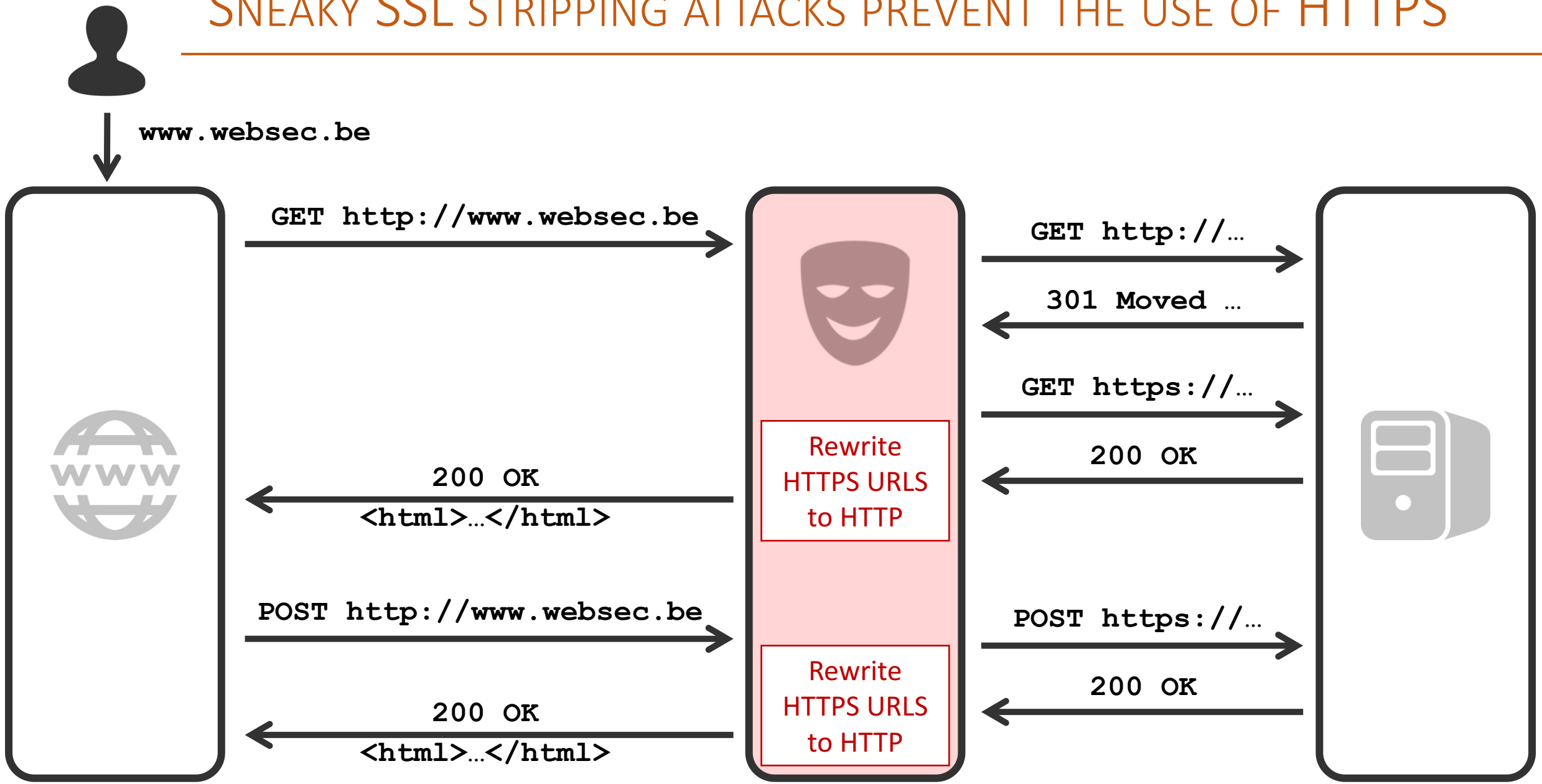
It would be extremely difficult for the attacker to obtain a valid certificate for a domain he does not control, and using an invalid certificate would cause the victim's browser to display an appropriate warning message. Consequently, man-in-the-middle attacks against HTTPS services are hard to pull off, and often not very successful. However, there are plenty of realistic opportunities to use the unencrypted HTTP protocol to attack most HTTPS websites.

Encrypted communications are an essential requirement for banks and other financial websites, but HTTPS alone is not sufficient to defend these sites against man-in-the-middle attacks. Astonishingly, many banking websites lurk amongst the 95% of HTTPS servers that lack a simple feature that renders them still vulnerable to pharming and man-in-the-middle attacks. This missing feature is HTTP Strict Transport Security (HSTS), and only 1 in 20 secure servers currently make use of it, even though it is supported by practically all modern browsers.

https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html

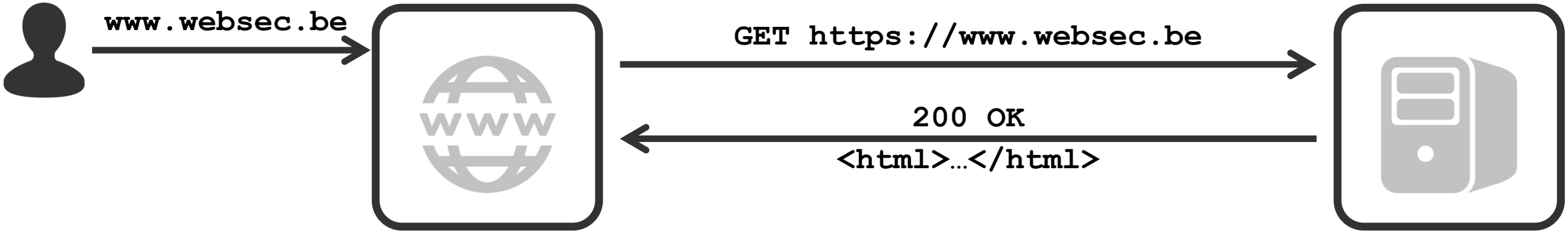
Sneaky SSL stripping attacks prevent the use of HTTPS

SNEAKY SSL STRIPPING ATTACKS PREVENT THE USE OF HTTPS



Strict Transport Security against SSL Stripping

- Strict Transport Security converts all HTTP requests to HTTPS



- Modern browsers support HTTP Strict Transport Security (HSTS)
  - HTTP response header to enable Strict Transport Security
  - When enabled, the browser will not send an HTTP request anymore

From version …	4	4	7	11	4.4.4	7.1

HSTS CAN BE ENABLED WITH A SIMPLE ONE-LINER

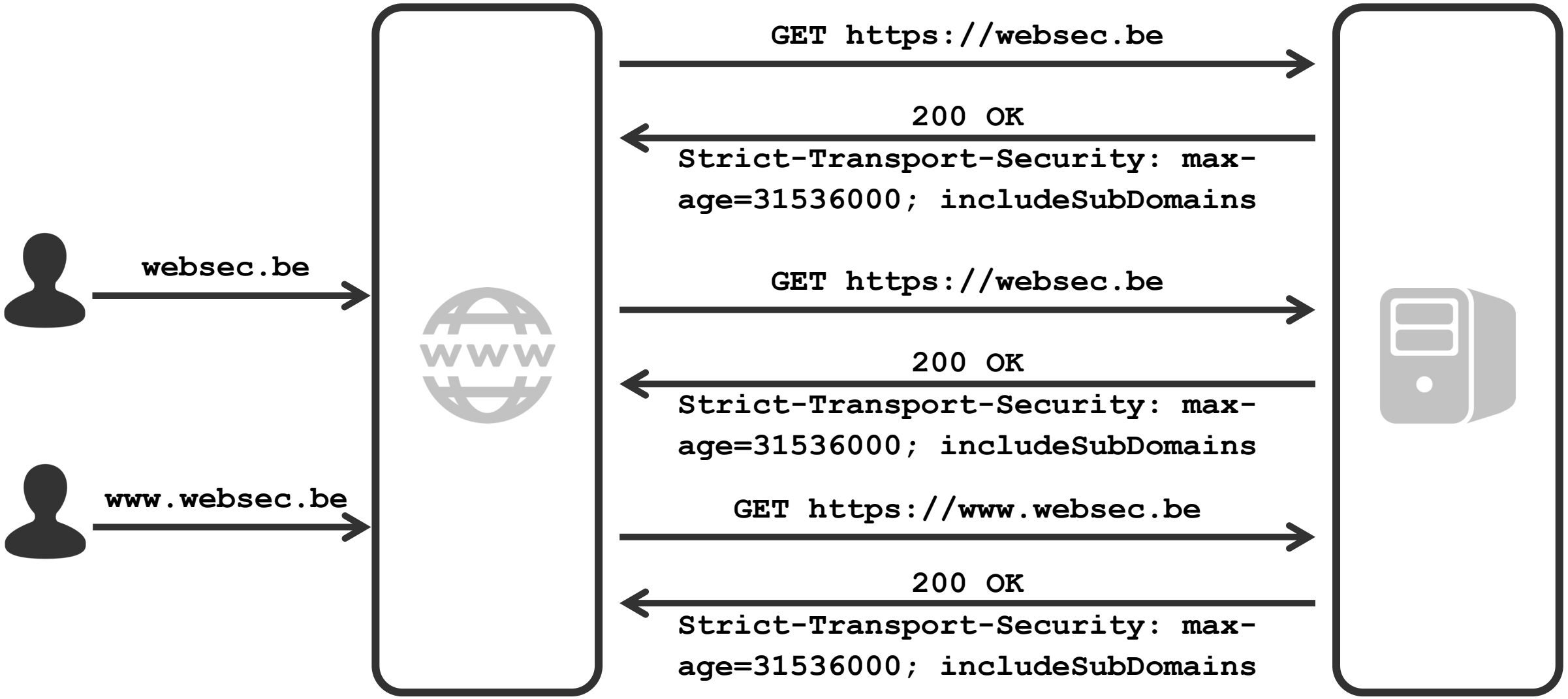
- The policy is controlled by the **`Strict-Transport-Security`** header
  - **`max-age`** specifies how long the policy should be enforced in seconds
  - Make sure this is long enough to cover two subsequent visits
  - If necessary, the policy can be disabled by setting **`max-age`** to 0

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

- The policy can be extended to automatically include subdomains
  - This behavior is controlled by the **`includeSubDomains`** flag
  - Before enabling this, carefully analyze the services you are running on your domain

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

HSTS IN ACTION

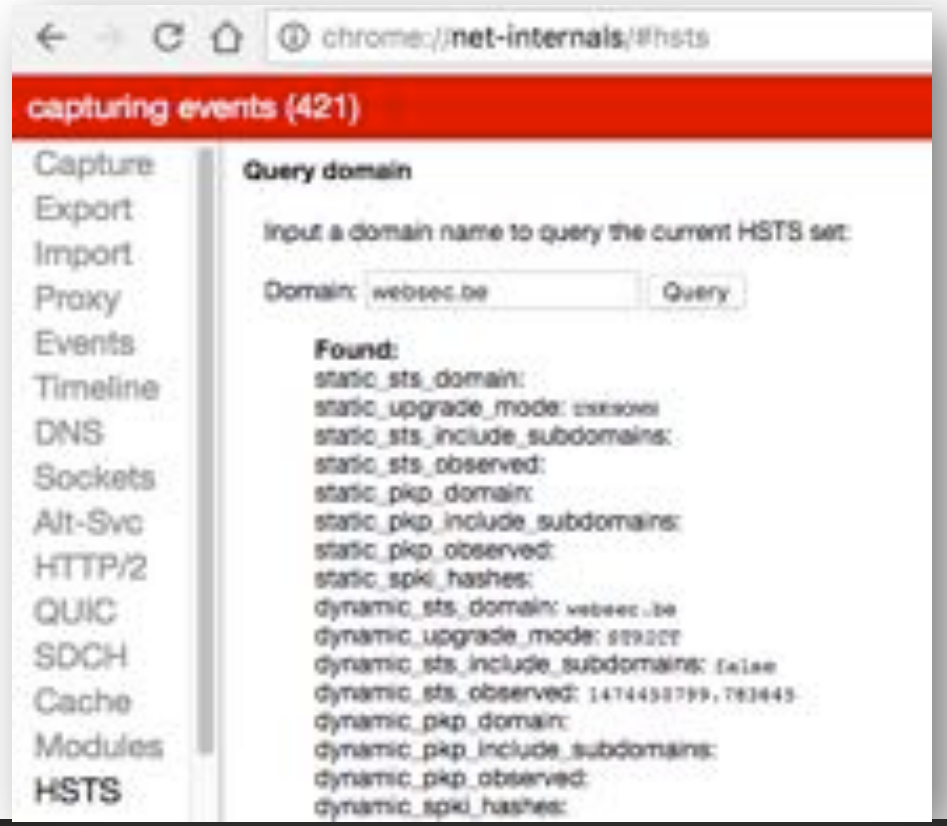


Policy details of HSTS

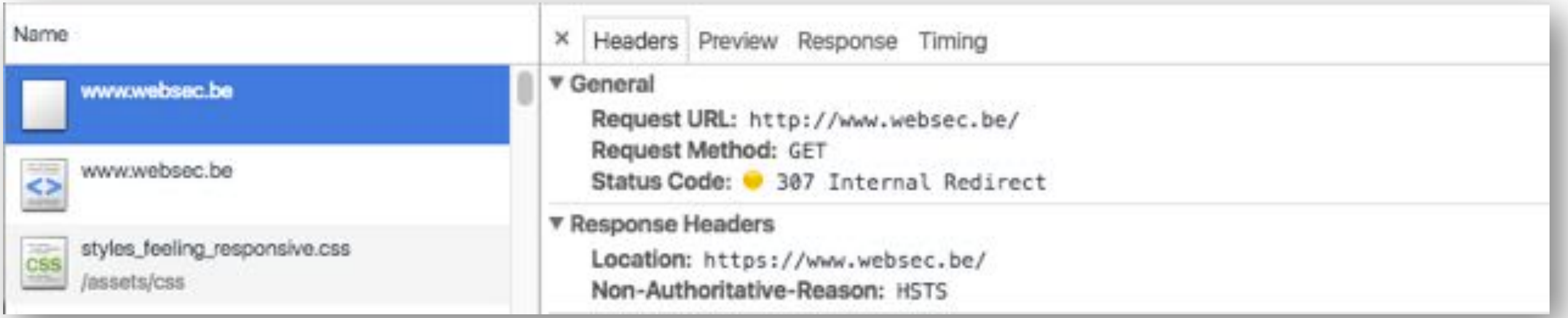
- HSTS does not care about TCP ports
  - Policy matches are determined based on the hostname only
  - Port 80 is translated to port 443, but other ports are preserved
- HSTS policies can only be set over a secure connection
  - The certificate used must be valid
  - HSTS policies set on insecure connections are ignored
- Disabling HSTS must be done by explicitly setting `max-age` to 0
  - Omitting a HSTS header from a HSTS-enabled host does nothing

Enabling HSTS in practice

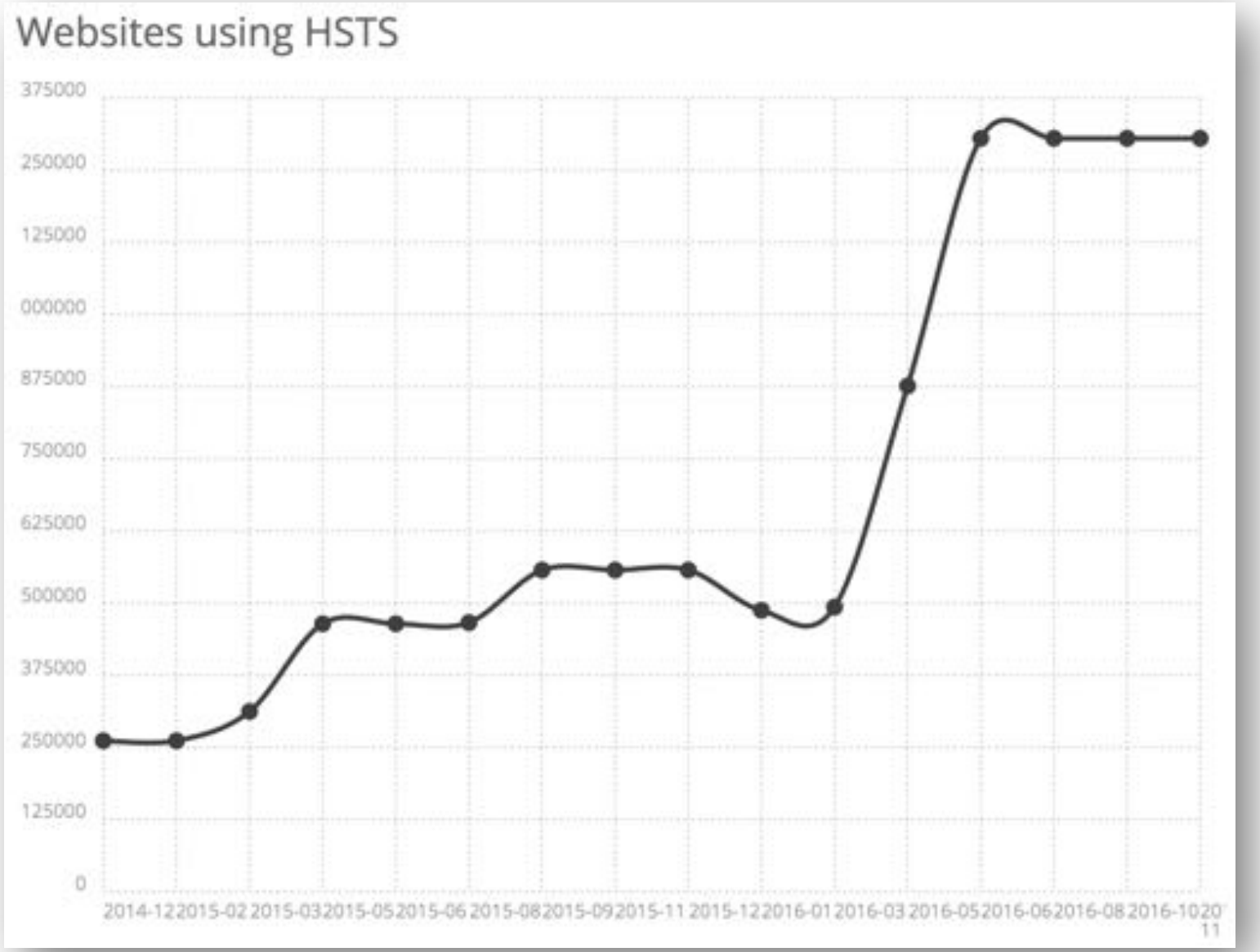
- The step-by-step guide towards enabling HSTS
  - Setup HTTPS correctly
  - Send the `Strict-Transport-Security` header with a short `max-age`
  - Test your configuration
  - Increase max-age after successful testing
- Chrome's `net-internals` allow inspection
  - `dynamic_sts` is the HSTS mechanism



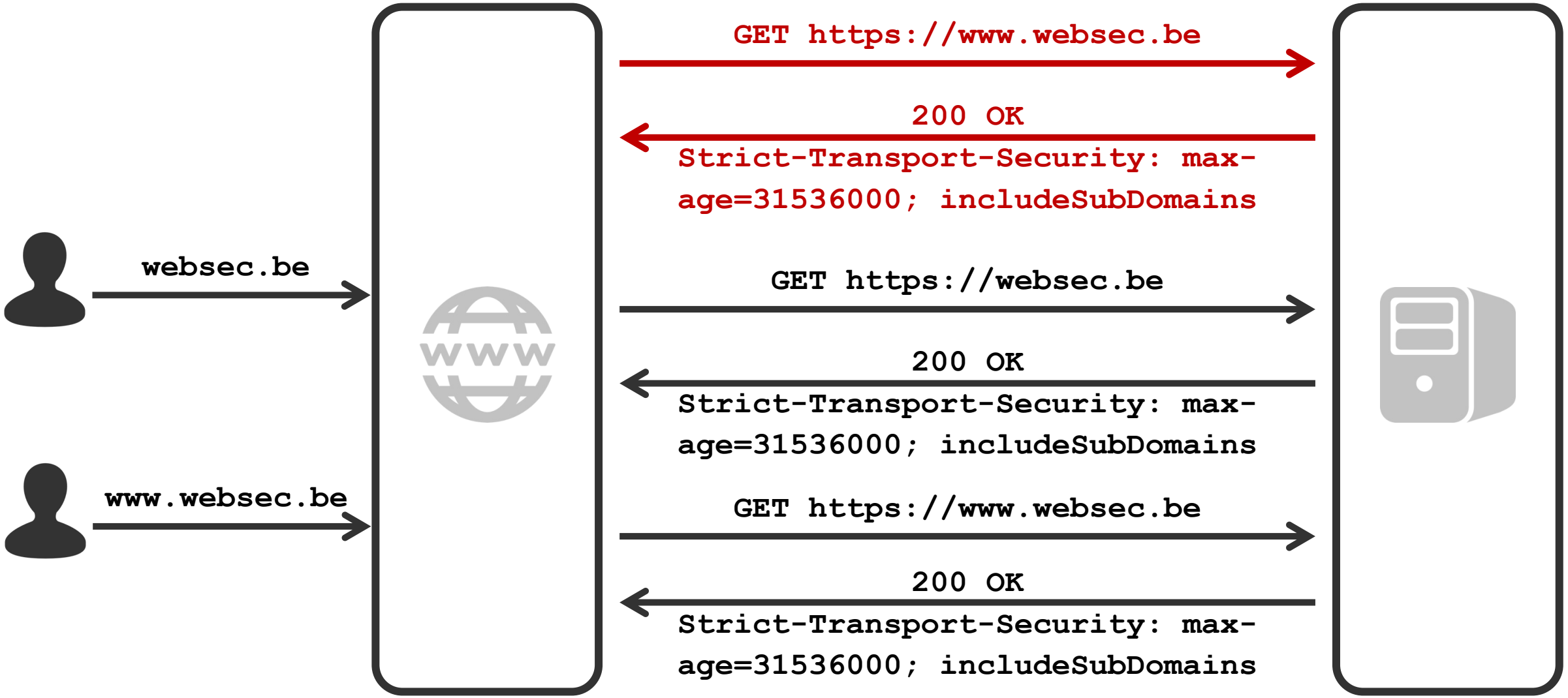
Fun Fact: Chrome handles HSTS as a redirect



TIME TO GET ON THE HSTS TRAIN

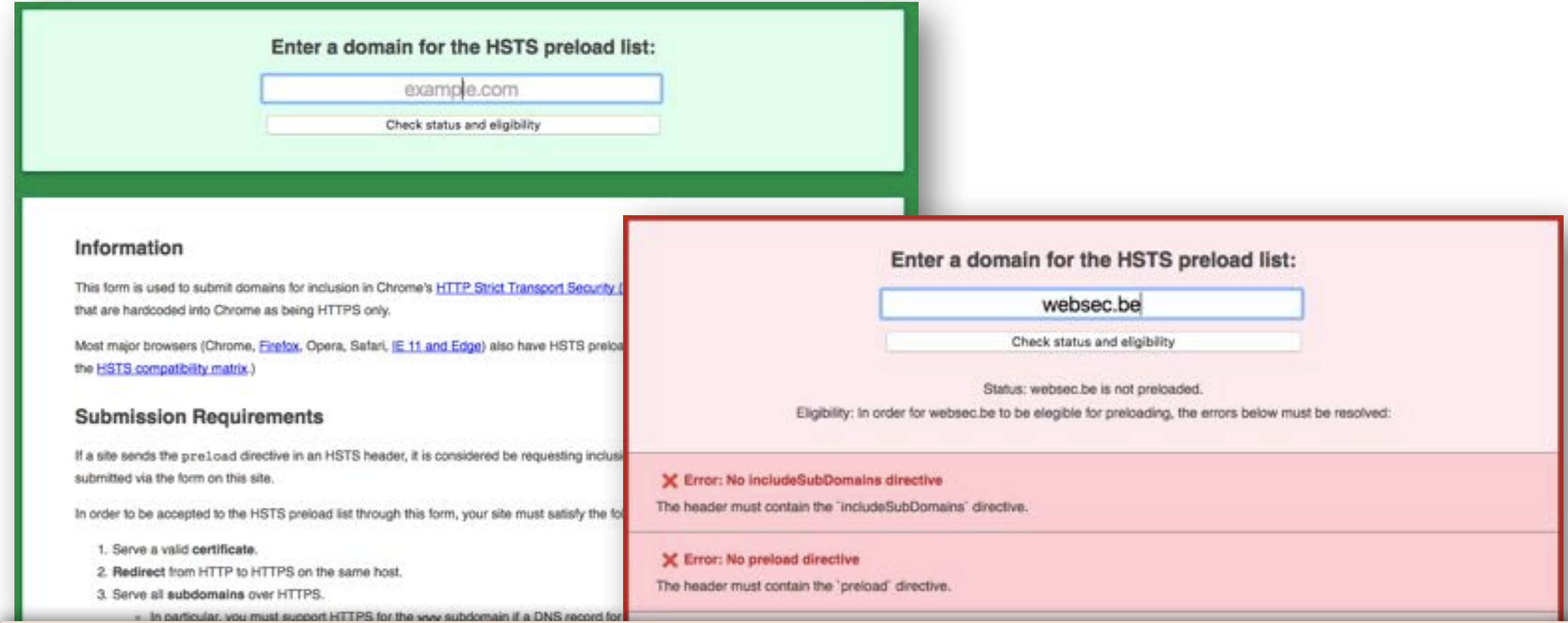


But how do you make the first connection over HTTPS?



http://www.bbcgoodfood.com/howto/guide/ingredient-focus-tofu

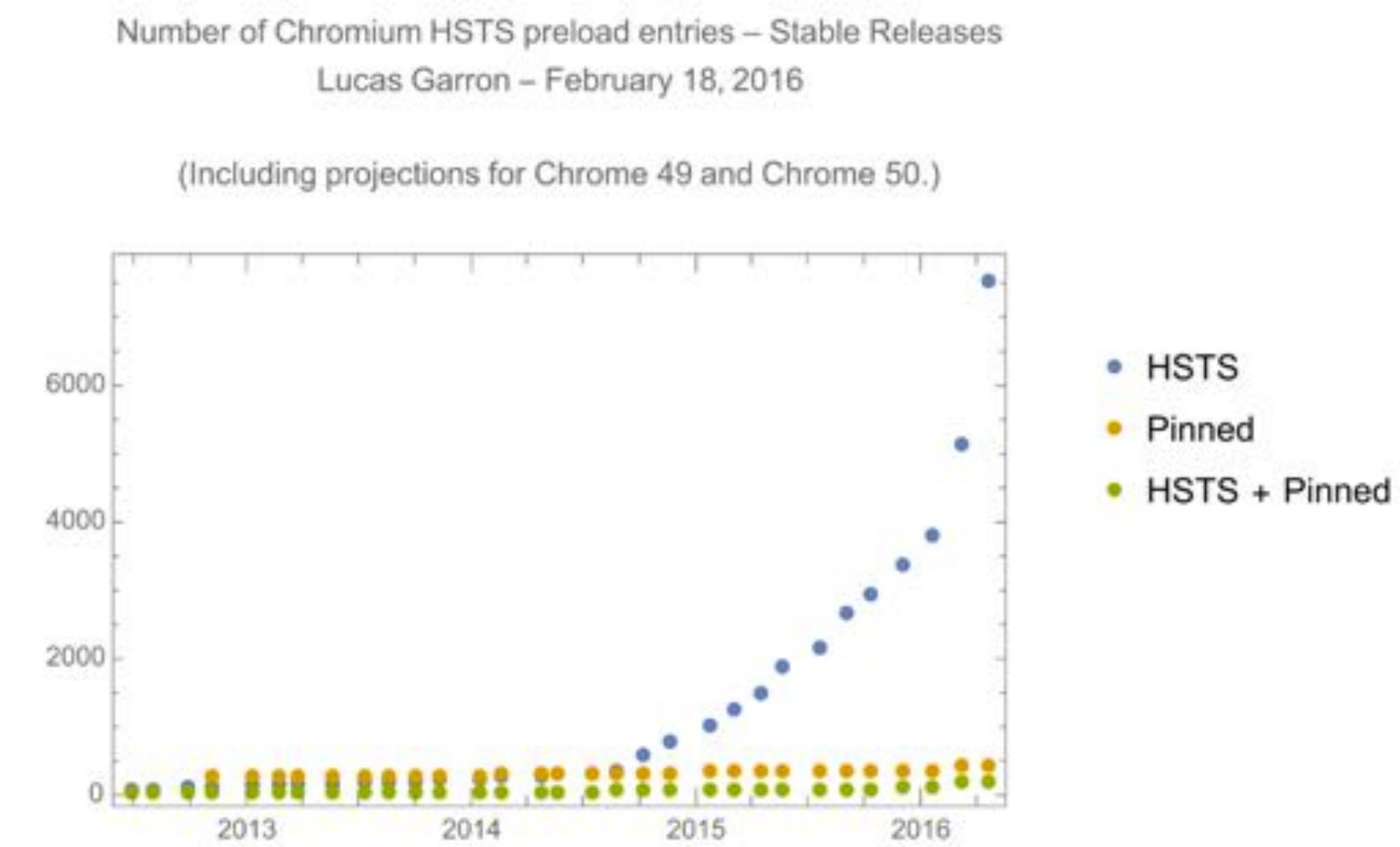
PRELOADING HSTS INTO THE BROWSER




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

https://hstspreload.appspot.com/?

PRELOADING IS ON THE RISE



All Interactions Should Happen over HTTPS

- There is a big push for HTTPS on the Web
  - Google uses HTTPS as a ranking signal
  - Active mixed content is blocked in modern desktop browsers
  - The Secure Contexts specification limits use of sensitive features
- There is plenty of support for easily enabling HTTPS
  - Rate your deployment with the SSL Server Test
  - Get free, automated certificates from Let's Encrypt
- HSTS is essential for a modern HTTPS deployment
  - For complex environments, start with subdomains

https://www.ssllabs.com/ssltest/
https://letsencrypt.org/

Knowledge is the key to building secure applications

- The use of HTTPS and HSTS is only the tip of the iceberg
  - Numerous new security policy have been added in the last 5 years
- These new technologies require explicit knowledge and action
  - Developers need to why and how to use them
- We offer specialized training covering the Web security landscape
  - Hosted training courses and customizable in-house trainings
  - Broad spectrum of topics, such as HTTPS, authentication, authorization, XSS
  - Various Web technologies, including modern MVC frameworks (AngularJS, …)
  - Effective combination of lectures and hands-on sessions

Web Security Essentials

April 24 – 25, Leuven, Belgium

Security in 4 key areas

Secure communication

Strong authentication

Avoiding authorization bypasses

Neutralizing code injection attacks

Up-to-date & actionable advice

Directly applicable security advice

Overview of essential best practices

Strong theoretical foundation

Practical hands-on experience

https://essentials.websec.be

Thanks for providing this course packed with very up-to-date information.

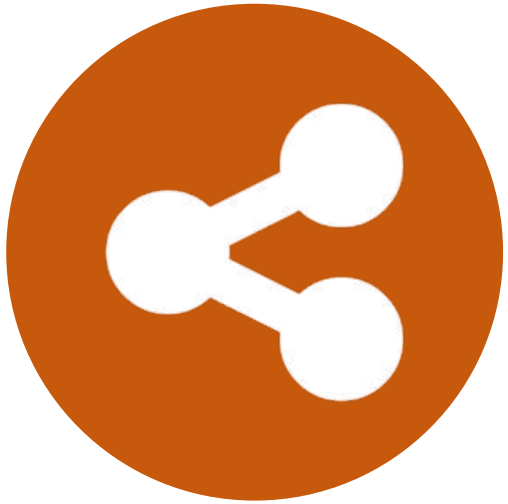
Excellent hand-outs, providing concise but complete information

I would recommend this training to all web developers and architects

Now it's up to you ...

Secure

Follow



Share