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)
- Visit website, browse public pages
- Login with username and password
- Consult private information

(b)
- Visit website, browse public pages
- Login with username and password
- Consult private information

(c)
- Visit website, browse public pages
- Login with username and password
- Consult private information
**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](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](http://SecAppDev.org)
  - Week-long course focused on practical security
The web used to be server-centric
Hackers actively exploit critical vulnerability in sites running Joomla

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."

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

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.”

The Web has become client-centric
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/
But we use HTTPS for sensitive data
  – Sufficient to counter passive eavesdropping attacks
  – But what about active network attacks?
3 VARYING LEVELS OF HTTPS

(a) Visit website, browse public pages
   Login with username and password
   Consult private information

(b) Visit website, browse public pages
   Login with username and password
   Consult private information

(c) Visit website, browse public pages
   Login with username and password
   Consult private information
PREVENTING THE TRANSITION FROM HTTP TO HTTPS
PREVENTING THE TRANSITION FROM HTTP TO HTTPS

Visit http://some-shop.com

Welcome, please log in

Login as Philippe

Welcome Philippe

Rewrite HTTPS to HTTP

Visit http://some-shop.com

Login as Philippe

Welcome Philippe

some-shop.com
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.

Sneaky SSL stripping attacks prevent the use of HTTPS
Sneaky SSL stripping attacks prevent the use of HTTPS

GET http://www.websec.be
200 OK
<html>...</html>

POST http://www.websec.be
200 OK
<html>...</html>

Rewrite HTTPS URLs to HTTP

GET http://www.websec.be
200 OK
<html>...</html>

Rewrite HTTPS URLs to HTTP

GET https://www.websec.be
301 Moved ...
GET https://...
200 OK

POST http://www.websec.be
200 OK
<html>...</html>

POST https://...
200 OK
**Strict Transport Security against SSL Stripping**

- **Strict Transport Security** converts all HTTP requests to HTTPS

  ![Diagram showing the process of converting HTTP to HTTPS](image)

  - **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

<table>
<thead>
<tr>
<th>From version ...</th>
<th>4</th>
<th>4</th>
<th>7</th>
<th>11</th>
<th>4.4.4</th>
<th>7.1</th>
</tr>
</thead>
</table>

@PhilippeDeRyck
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

GET https://websec.be

200 OK

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

GET https://websec.be

200 OK

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

GET https://websec.be

200 OK

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

GET https://www.websec.be

200 OK

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

GET https://www.websec.be

200 OK

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

GET https://www.websec.be

200 OK

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

GET https://www.websec.be

200 OK

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

GET https://www.websec.be

200 OK

Strict-Transport-Security: max-age=31536000; includeSubDomains
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 \texttt{Strict-Transport-Security} header with a short \texttt{max-age}
  - Test your configuration
  - Increase max-age after successful testing

- Chrome’s \texttt{net-internals} allow inspection
  - \texttt{dynamic_sts} is the HSTS mechanism
Fun Fact: Chrome handles HSTS as a redirect
TIME TO GET ON THE HSTS TRAIN

https://trends.builtwith.com/docinfo/HSTS
But how do you make the first connection over HTTPS?

GET https://www.websec.be

200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains

GET https://websec.be

200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains

GET https://www.websec.be

200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains

GET https://www.websec.be

200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains
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

Number of Chromium HSTS preload entries – Stable Releases
Lucas Garron – February 18, 2016
(Including projections for Chrome 49 and Chrome 50.)
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

@PhilippeDeRyck
https://www.websec.be
philippe.deryck@cs.kuleuven.be
/in/philippederyck