MADISON PHP

WORDPRESS AND HTTPS

@andreaincode | https://joind.in/talk/01bbf

HI, I'M ANDREA

- Senior Web Developer at Forte in Madison
  - Work on Marketing Team where I build & manage five custom WordPress sites including forteresearch.com
- I volunteer with Codecinella and MadNorSki which have WordPress sites
- Plus some personal sites: wisconsinverbs.com & andrearoenning.com

FEEDBACK

- Please leave feedback on Joind.In https://joind.in/talk/01bbf
- Or reach me on Twitter @andreaincode

LESSONS LEARNED FROM DECEMBER 2016

A mission to change all of Forte’s customer-facing web properties from **HTTP** to **HTTPS**

- Large amounts of existing content on several sites
- Intra-site links and cross-site links
- Links to external resources: fonts, scripts, HubSpot marketing automation
- SEO - Don’t want to loose good search placement

DISCLAIMERS

- Mostly focused on LAMP Stack, I don’t know much about Windows server
- Google Search Console was formerly known as Google Webmaster Tools

WHAT IS HTTPS?

- HTTP served over TLS or SSL for encryption

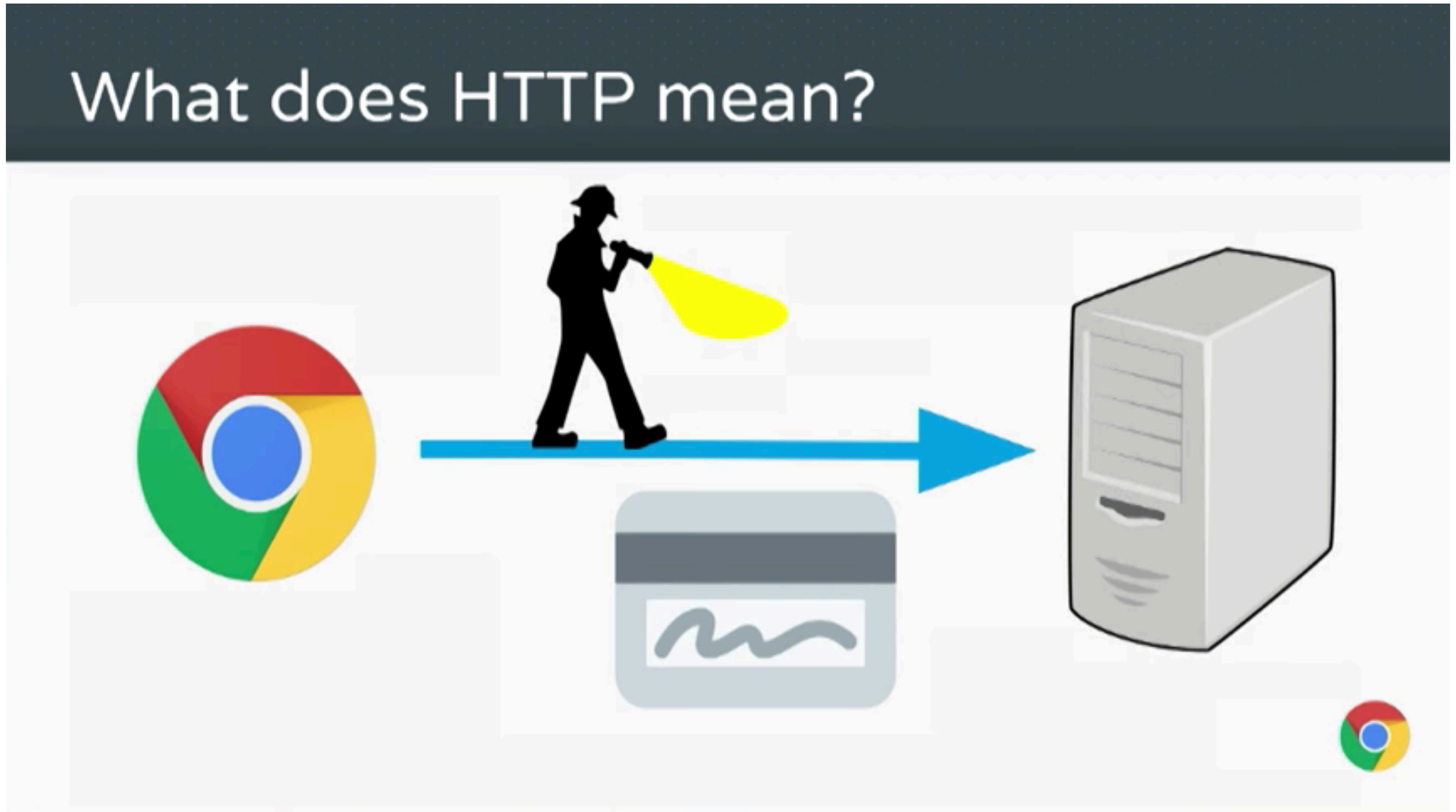
“When you visit a regular HTTP website, the web server responds to requests from your browser and simply hands over the website's unencrypted data. When you visit an HTTPS site, however, your browser and the server first perform an exchange of cryptographic keys. Those keys allow the server and browser to send messages only the other one can decrypt, locking out all eavesdroppers.”

- Wired - Hacker Lexicon: What Is HTTPS?

WHY SWITCH TO HTTPS?

1. SOMEONE IS LISTENING TO YOUR USERS' WEB TRAFFIC.

- A better name for HTTP is "Insecure HTTP"



What does HTTP mean?

Emily Stark at Dev Summit 2016: Real Talk About HTTPS
https://www.youtube.com/watch?time_continue=2&v=iP75a1Y9saY

1. SOMEONE IS LISTENING TO YOUR USERS' WEB TRAFFIC.

- If you're using insecure coffee shop wi-fi all of your packets are available to be read.
- Your ISP could be tracking all of your data

"It's pretty safe to assume that at least somebody is listening to your traffic … if you use HTTPS, I don't think you should be worried that your traffic is able to be decrypted. The actual cryptography is very sound."

- April King, Security Engineer at Mozilla
  ShopTalk Show #250 Web Security

2. MAN-IN-THE-MIDDLE ATTACKS ARE QUITE COMMON.

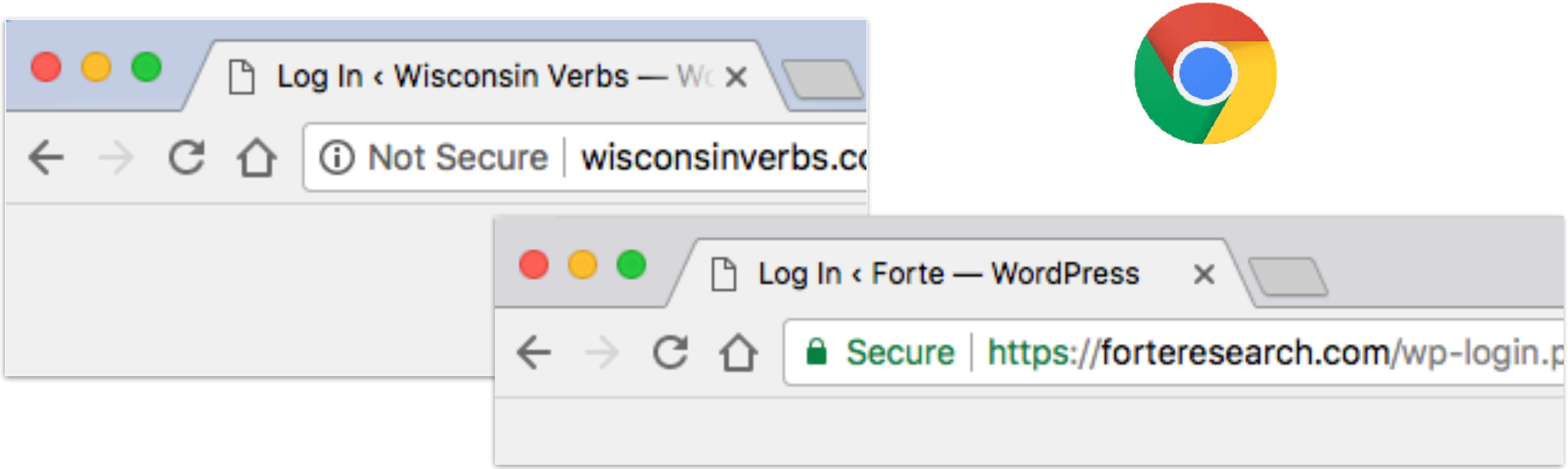
- An attacker can intercept data between the server and the user and inject:
    - Advertisements
    - JavaScript keystroke logging
    - All sorts of bad stuff

3. HTTPS CONFIRMS THAT YOUR SITE IS WHO YOU SAY YOU ARE.

- In addition to encryption, your certificate verifies that the server delivering the HTTPS website is authorized to do so.
- Prevents phishing attacks with a site that may look like yours, but is really an attacker who has intercepted the traffic.

4. HTTPS ESTABLISHES USER TRUST.

- Browsers have added UI elements to call out insecure HTTP so users can be educated about the risks.
- In July 2018, Chrome will mark all HTTP sites as “not secure”



Log In ‹ Wisconsin Verbs — W

ⓘ Not Secure | wisconsinverbs.c

Log In ‹ Forte — WordPress

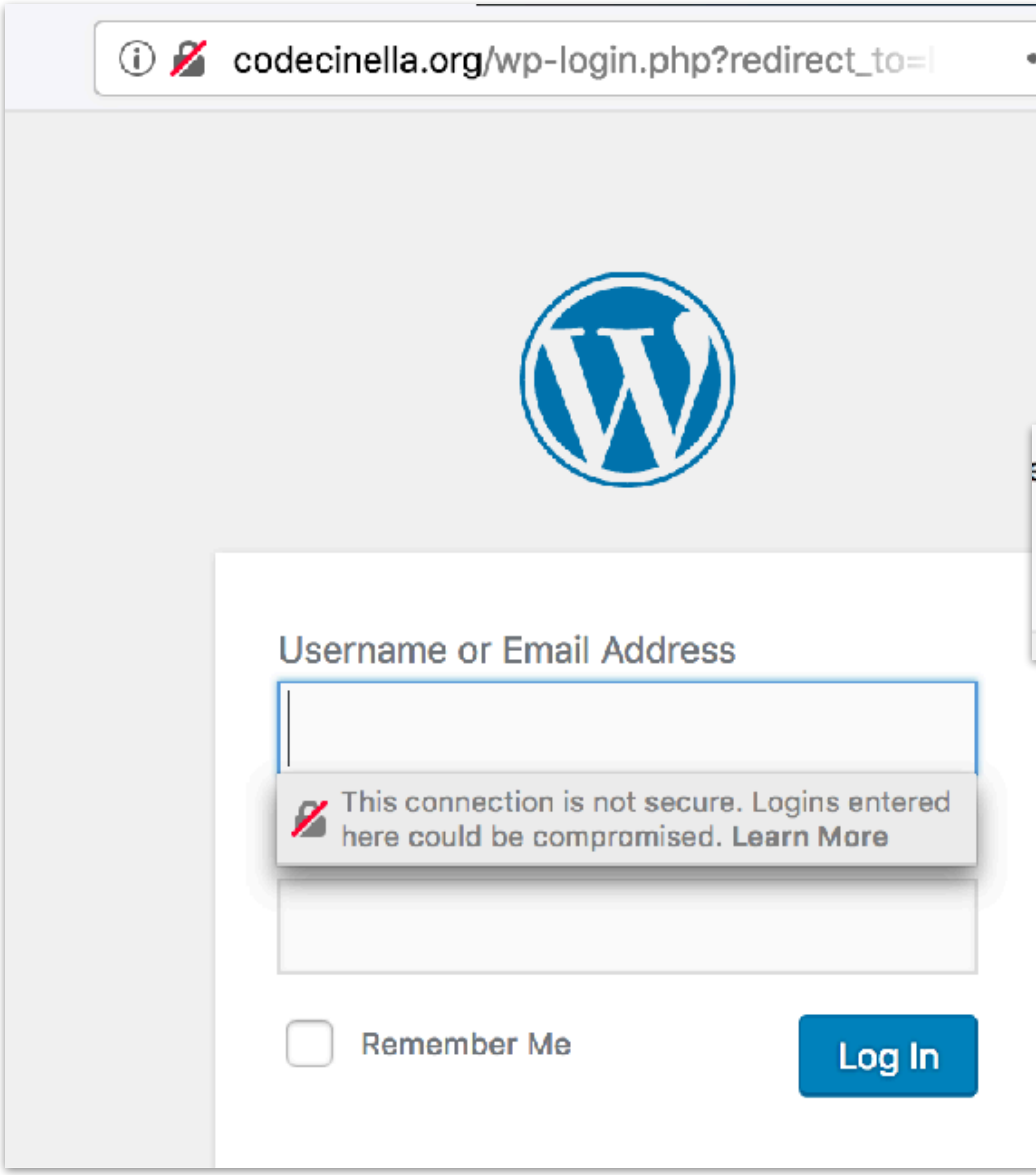
Secure | https://forteresearch.com/wp-login.p

4. HTTPS ESTABLISHES USER TRUST.

Google Developer Videos on HTTPS

- Emily Stark at Dev Summit 2016: Real Talk About HTTPS https://www.youtube.com/watch?v=iP75a1Y9saY
- Pierre Far and Ilya Grigorik at Google I/O 2014: HTTPS everywhere https://www.youtube.com/watch?v=cBhZ6S0PFCY

4. HTTPS ESTABLISHES USER TRUST.

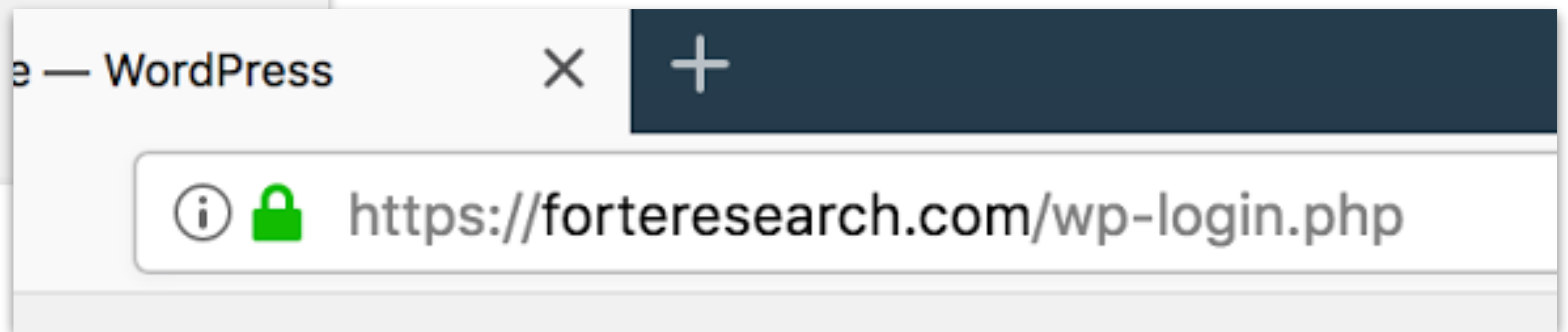


codecinella.org/wp-login.php?redirect_to=

Username or Email Address

This connection is not secure. Logins entered here could be compromised. **Learn More**

Firefox 58



https://forteresearch.com/wp-login.php

5. HTTPS BOOSTS YOUR SEO.

- There may be an initial hit in search results, but Google indexes HTTPS sites higher than HTTP

6. HTTPS IS REQUIRED FOR SOME EXCITING NEW WEB TECHNOLOGIES.

- Geolocation
- Service Workers
- Payments API
- Credentials API
- HTTP/2

6. COMPLIANCE WITH SECURITY STANDARDS.

- PCI Compliance for credit card information
- HIPAA Compliance for health care information

BUT I JUST HAVE A SIMPLE WORDPRESS BLOG,

DO I REALLY NEED HTTPS?

YEA, PROBABLY.

WORDPRESS REQUIREMENTS:

https://wordpress.org/about/requirements/

- PHP 7.2 or greater
- MySQL 5.6 or greater OR MariaDB 10.0 or greater
- The mod_rewrite Apache module
- **HTTPS support**

WORDPRESS SITES ARE HACKABLE

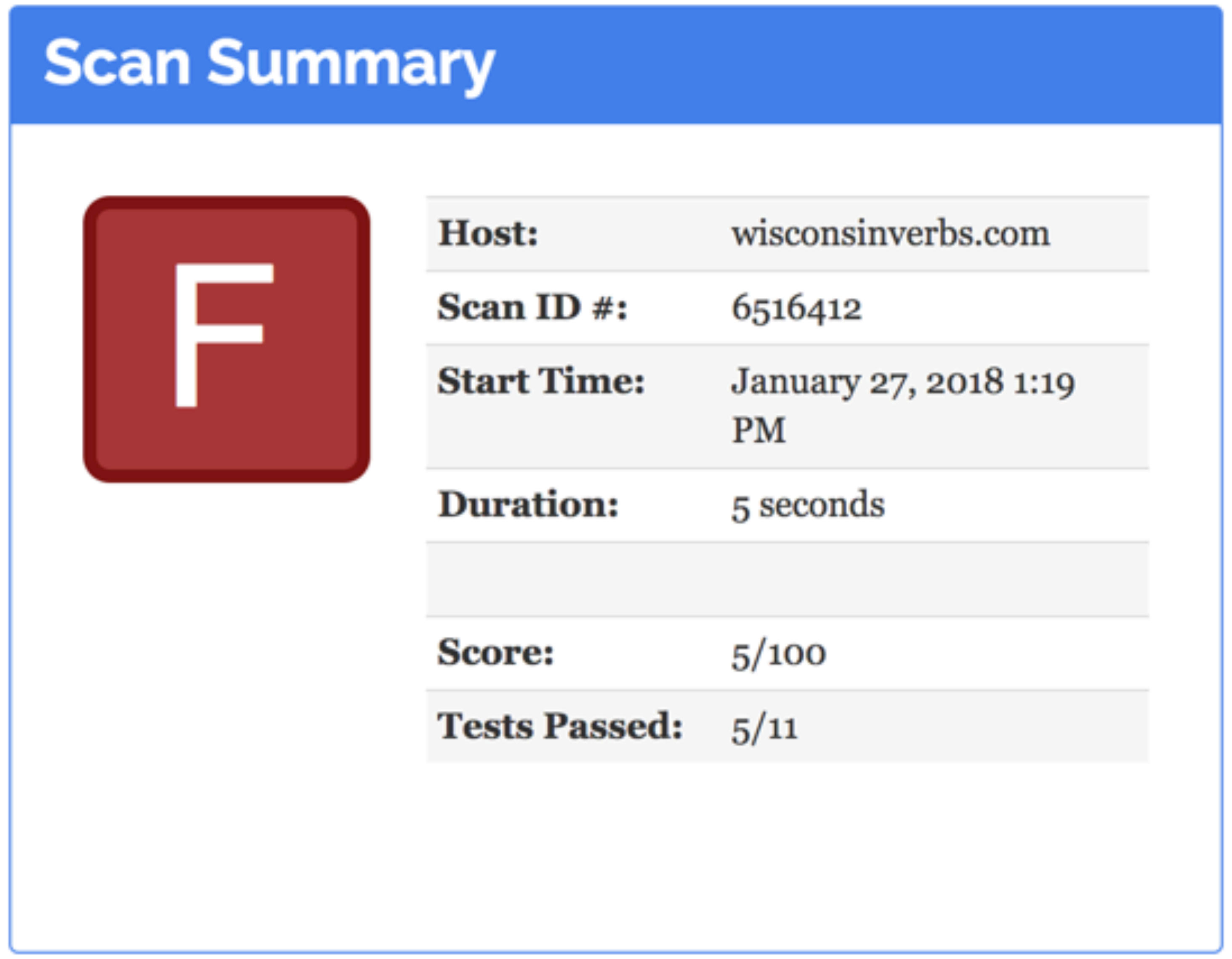
- All WordPress websites utilize a username and password to get to the admin panel
- For examples of what can happen when someone has access to your WordPress admin, refer to Beth Tucker Long's Madison PHP Meetup talk about WordPress Hacks from November 2017
- WordPress websites account for 30% of the web, so they are a hacker favorite

TESTING YOUR SITE SECURITY

MOZILLA OBSERVATORY

https://observatory.mozilla.org/

- Test your site URL
- Don’t be shocked if you get an “F” if you’re not forcing HTTPS yet



Scan Summary

F

Host:	wisconsinverbs.com
Scan ID #:	6516412
Start Time:	January 27, 2018 1:19 PM
Duration:	5 seconds
Score:	5/100
Tests Passed:	5/11

HOW TO ADD HTTPS TO AN EXISTING SITE

CONSIDERATIONS

- Updating Site URLs
- Absolute links in your WordPress code & database
- Making sure that users see the HTTPS version and not the Insecure HTTP version
- Keeping your SEO rankings up

STEP 1. SET UP AN SSL CERTIFICATE ON YOUR WEB SERVER

Some options:

- Check with your host to see if there is an easy SSL Certificate option.
- Get a free certificate from Let’s Encrypt or purchase one from a trusted certificate authority.
- Use CloudFlare’s SSL service which acts as an intermediary to secure content between your site and the user.

STEP 2. TEST THE HTTPS VERSION OF YOUR WEBSITE.

- You may have access to an HTTP and HTTPS version of your site at the same time at this point.

STEP 3. UPDATE YOUR WORDPRESS URLS.

- Update the URL from the WP Admin or wp-config.php file
    - WP Admin under Settings > General
- Or update your variables in wp-config.php

```
define('WP_HOME','https://yoursite.com');
define('WP_SITEURL','https://yoursite.com');
```

STEP 4. UPDATE YOUR CUSTOM PHP CODE THAT HAS HARD CODED URLS

- If you created a custom theme, do a search / replace for
  - Your own site URL
  - Outside resource links
- Either replace urls from **http://**yoursite.com to **https://**yoursite.com

STEP 5. UPDATE ABSOLUTE SITE URLS IN THE WP DATABASE

WordPress saves links to assets as absolute URLs in your database. (Remember to do a backup first)

A few ways to do a find/replace:

- Better Search Replace Plugin
- WP-CLI search replace function
- Or run a batch of SQL Queries if you are cool with touching the database

STEP 5. UPDATE ABSOLUTE SITE URLS IN THE WP DATABASE

WP Database SQL Queries for a new site*

```
UPDATE wp_options SET option_value = replace(option_value, 'http://mysite.com',
'https://mysite.com') WHERE option_name = 'home' OR option_name = 'siteurl';

UPDATE wp_posts SET guid = replace(guid, 'http://mysite.com','https://mysite.com');

UPDATE wp_posts SET post_content = replace(post_content, 'http://mysite.com',
'https://mysite.com');

UPDATE wp_postmeta SET meta_value = replace(meta_value,'http://mysite.com',
'https://mysite.com');
```

*remember to update your URLs and database prefix. May be missing some custom tables.

STEP 6. UPDATE CANONICAL LINKS ON PAGES TO HTTPS://

```
<link rel="canonical" href="https://yoursite.com/" />
```

- Yoast SEO plugin updates this automatically
- Or you could code this into your theme's header file

STEP 7. FORCE YOUR SITE TO LOAD THE HTTPS VERSION

- Add to your .htaccess file

```
RewriteEngine On
RewriteCond %{HTTPS} !on
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

- Or update your server config virtual host file
- *Your website host may have already taken care of this step for you when you set up your certificate

STEP 8. SET A HSTS HEADER TO GUARANTEE HTTPS ACCESS

- Add to .htaccess or to your server config virtual host file

```
Header always set Strict-Transport-Security "max-age=63072000"
```

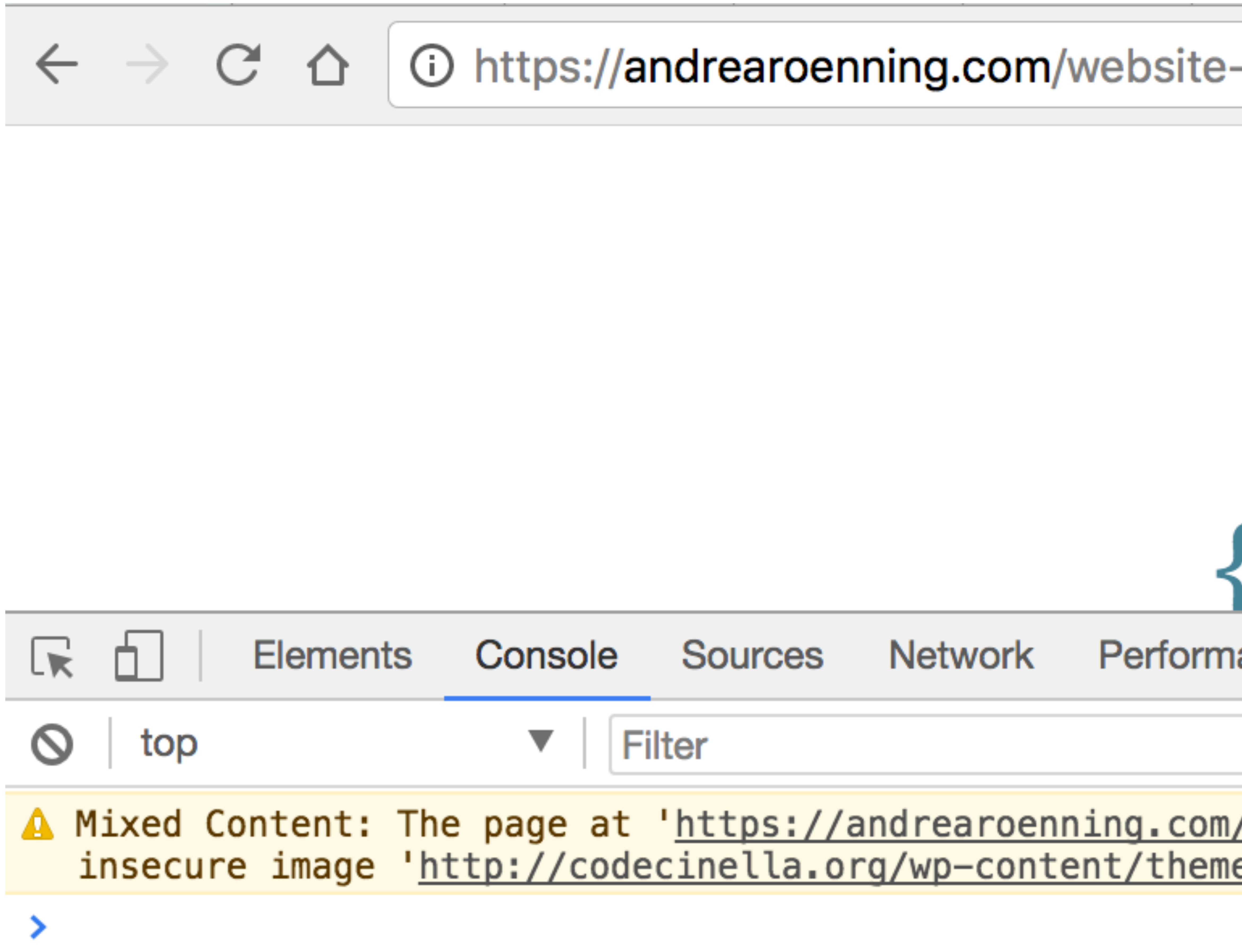
This is going to help with that Mozilla Observatory score

Learn more about HSTS

STEP 9: TEST YOUR SITE

Look for mixed content warnings in your browser's inspector

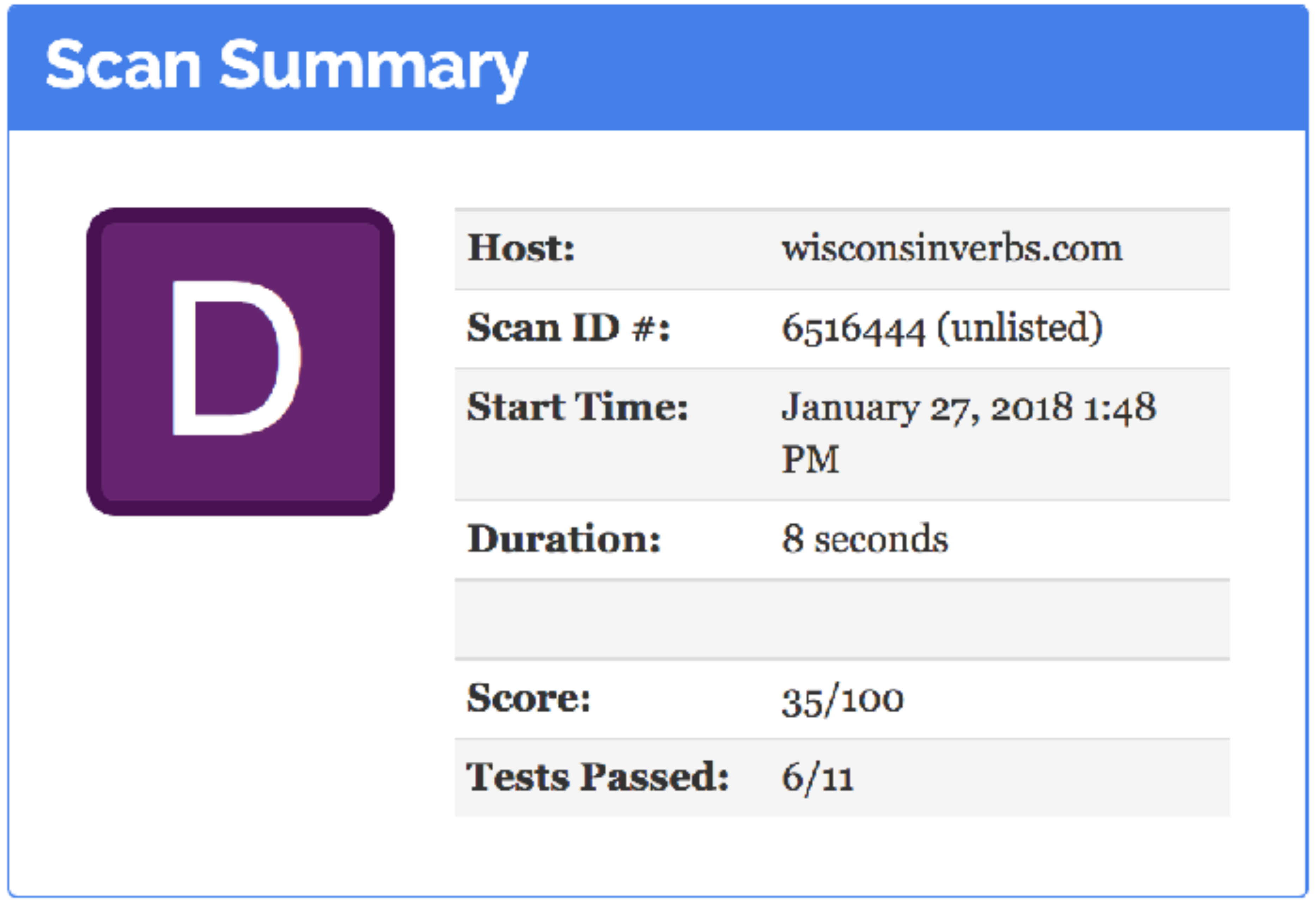
- CDN Links
- Plugin CSS or JS resources
- Fonts



```
Mixed Content: The page at 'https://andrearoenning.com/
insecure image 'http://codecinella.org/wp-content/theme
```

STEP 9: TEST YOUR SITE

Check your Mozilla Observatory score



Scan Summary

D

Host:	wisconsinverbs.com
Scan ID #:	6516444 (unlisted)
Start Time:	January 27, 2018 1:48 PM
Duration:	8 seconds
Score:	35/100
Tests Passed:	6/11

STEP 9: TEST YOUR SITE

Still see issues with your SSL Certificate?

- Check SSL Labs Directly for more detail
  https://www.ssllabs.com/ssltest/
- Why No Padlock also has some good information
  https://www.whynopadlock.com/

SEO / KEEPING GOOGLE HAPPY

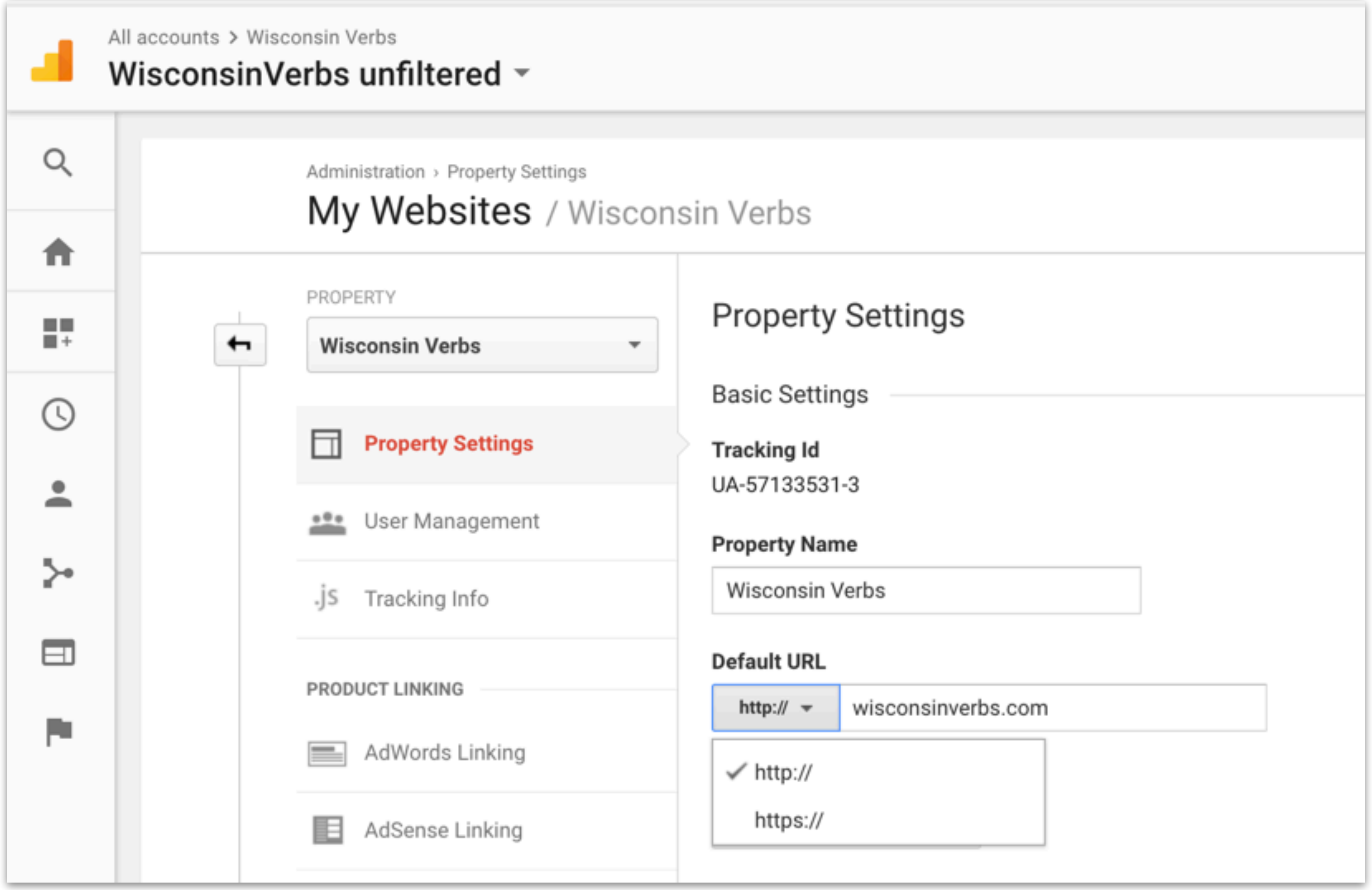
DIFFERENT URLS IN THE EYES OF GOOGLE

- https://www.yoursite.com
- http://www.yoursite.com
- https://yoursite.com
- http://yoursite.com

Setting your Canonical URL helps but make sure that your site redirects all of these URLs to your preferred URL

UPDATE GOOGLE ANALYTICS DEFAULT URL TO HTTPS

- Admin > Property > Property Settings > Default URL



All accounts > Wisconsin Verbs

WisconsinVerbs unfiltered

Administration › Property Settings

My Websites / Wisconsin Verbs

PROPERTY

Wisconsin Verbs

Property Settings

Basic Settings

Tracking Id
UA-57133531-3

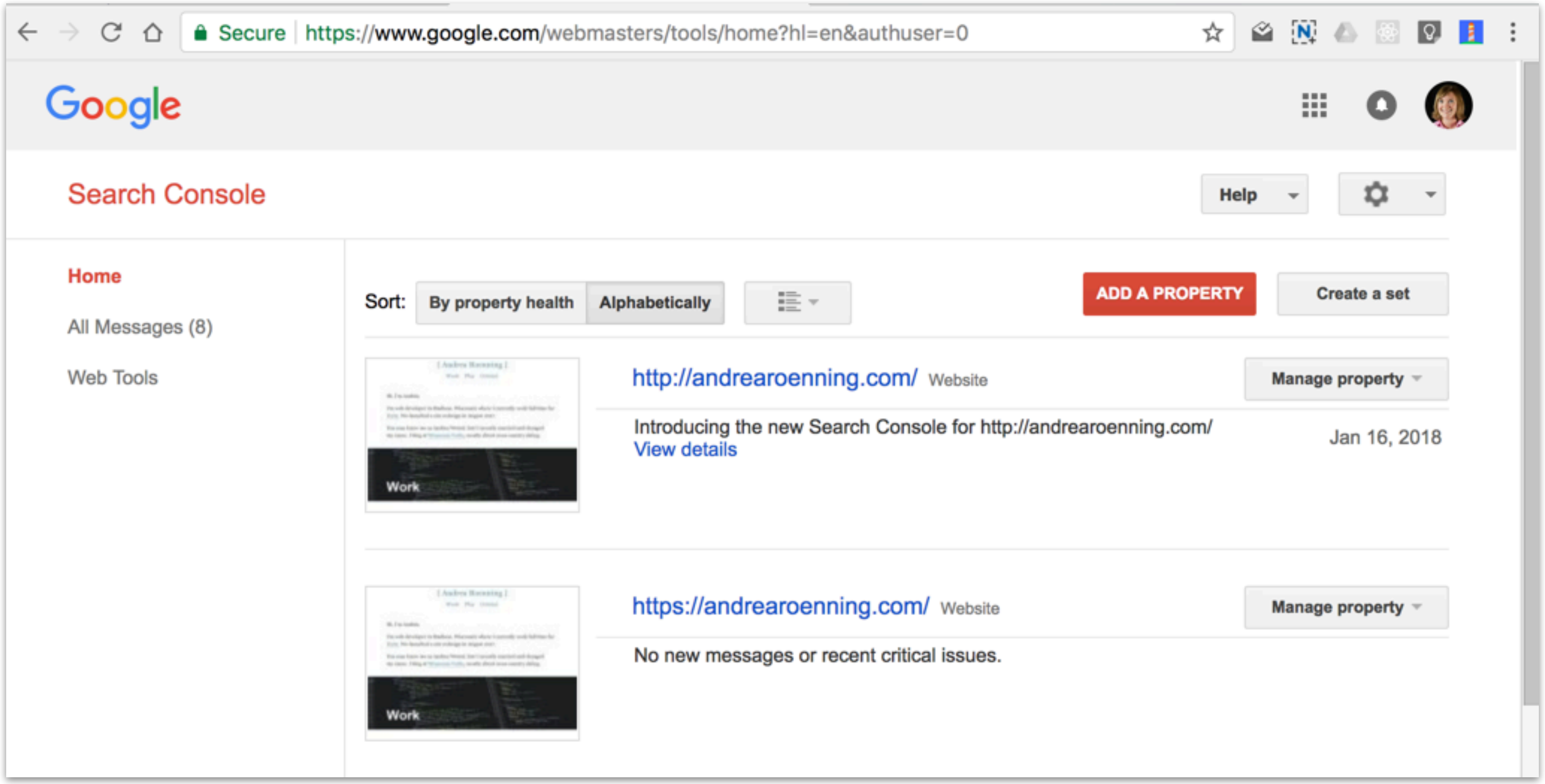
Property Name
Wisconsin Verbs

Default URL
http:// wisconsinverbs.com

✓ http://
https://

ADD HTTPS URL TO GOOGLE SEARCH CONSOLE

- Add your web properties and verify them.
  Track, HTTP, HTTPS, www and non-www versions



https://www.google.com/webmasters/tools/home?hl=en&authuser=0

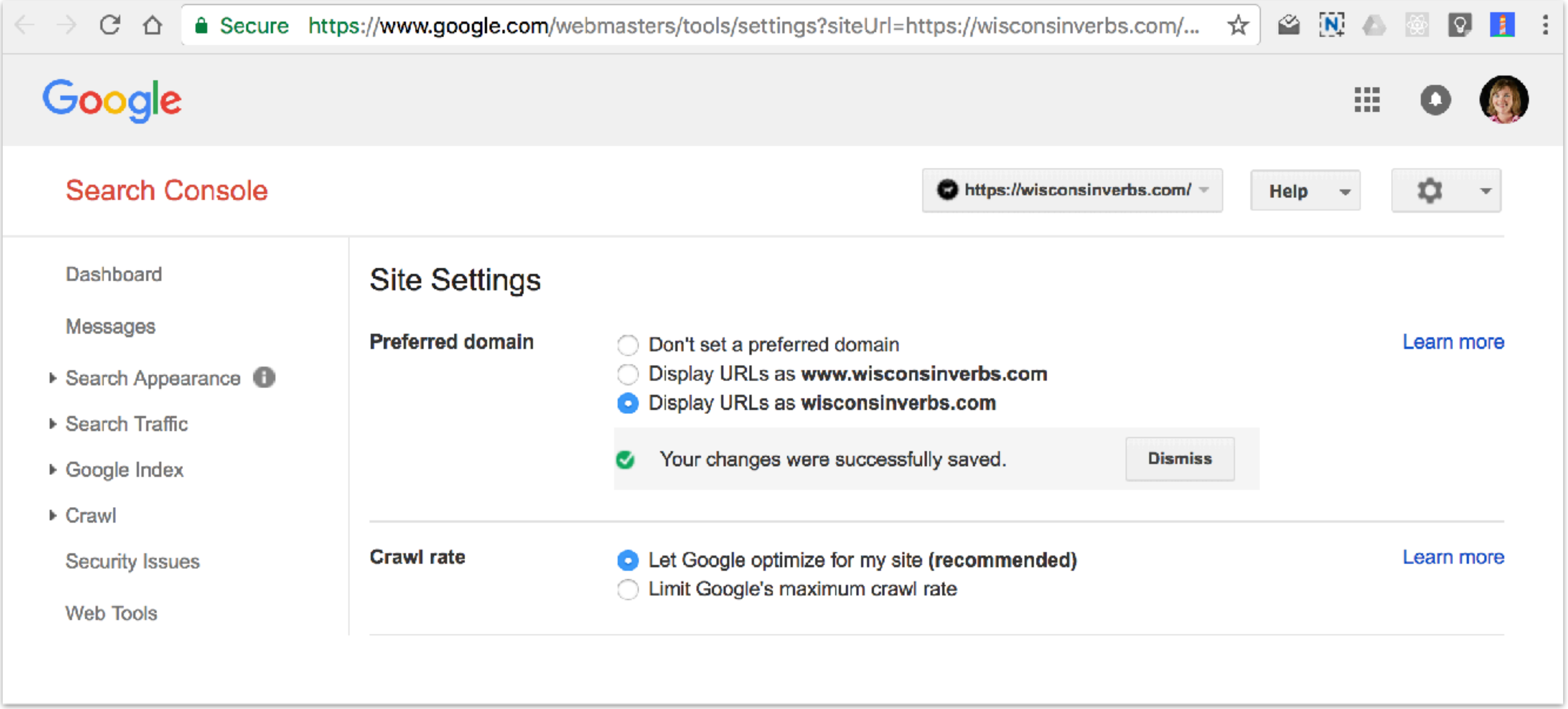
http://andrearoenning.com/ Website

Introducing the new Search Console for http://andrearoenning.com/
View details
Jan 16, 2018

https://andrearoenning.com/ Website

No new messages or recent critical issues.

SET PREFERRED DOMAIN



Site Settings

Preferred domain

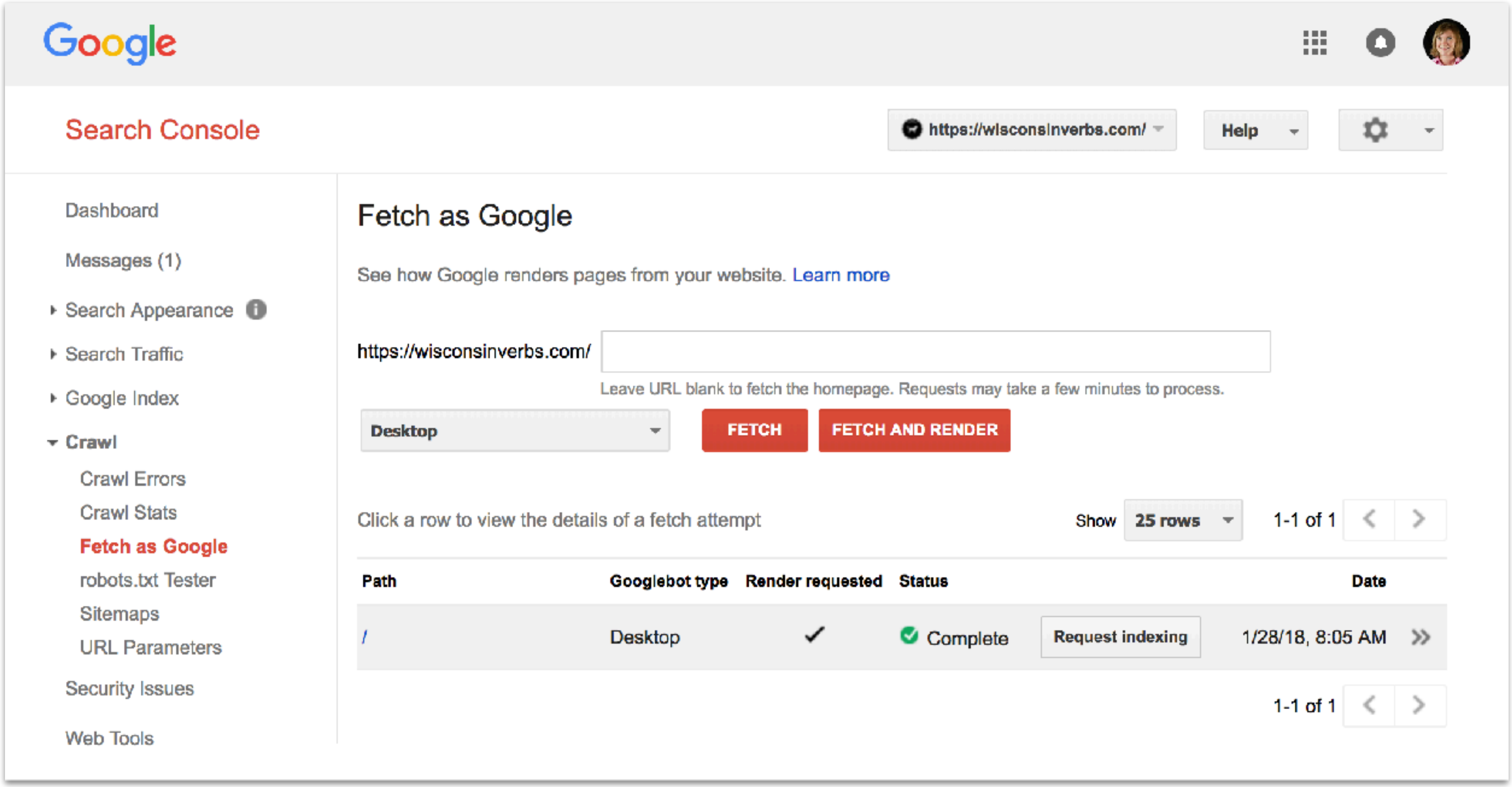
○ Don't set a preferred domain
○ Display URLs as **www.wisconsinverbs.com**
● Display URLs as **wisconsinverbs.com**

✓ Your changes were successfully saved.

Crawl rate

● Let Google optimize for my site **(recommended)**
○ Limit Google's maximum crawl rate

FETCH AS GOOGLE AND SUBMIT TO INDEX



Fetch as Google

See how Google renders pages from your website. Learn more

https://wisconsinverbs.com/

Leave URL blank to fetch the homepage. Requests may take a few minutes to process.

Click a row to view the details of a fetch attempt

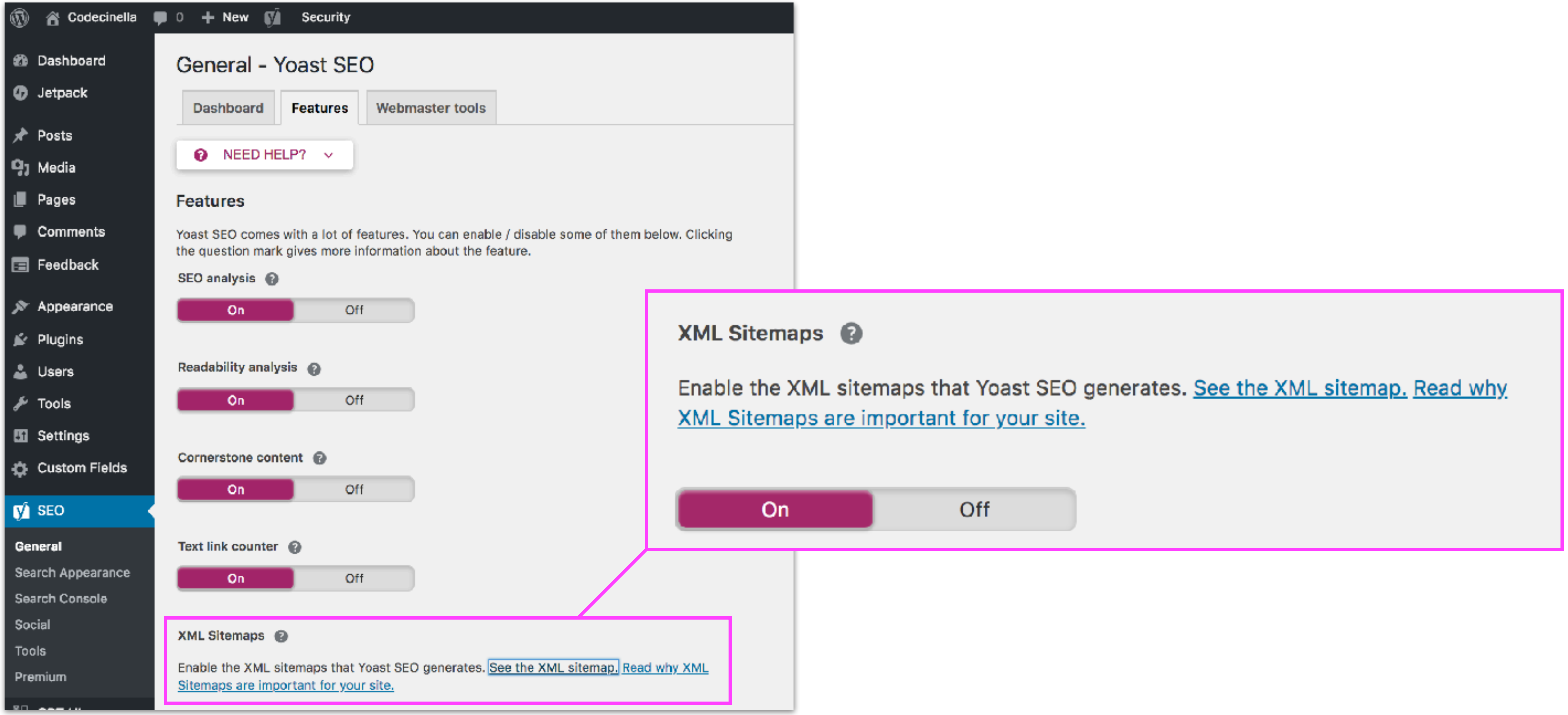
Path	Googlebot type	Render requested	Status		Date
/	Desktop	✓	✓ Complete	Request indexing	1/28/18, 8:05 AM

SUBMIT YOUR SITEMAP TO GOOGLE

- Visit your WP Admin Panel / Yoast SEO / Features Tab > Click on the question mark next to XML Sitemaps*
- Copy the “See the XML Sitemap” link (it looks like https://yoursite.com/sitemap_index.xml)
- In Google Search Console visit Crawl / Sitemaps and add your sitemap

*New location of Sitemap link since Yoast SEO 7.0

SUBMIT YOUR SITEMAP TO GOOGLE: YOAST



General - Yoast SEO

Features

Yoast SEO comes with a lot of features. You can enable / disable some of them below. Clicking the question mark gives more information about the feature.

SEO analysis: On | Off

Readability analysis: On | Off

Cornerstone content: On | Off

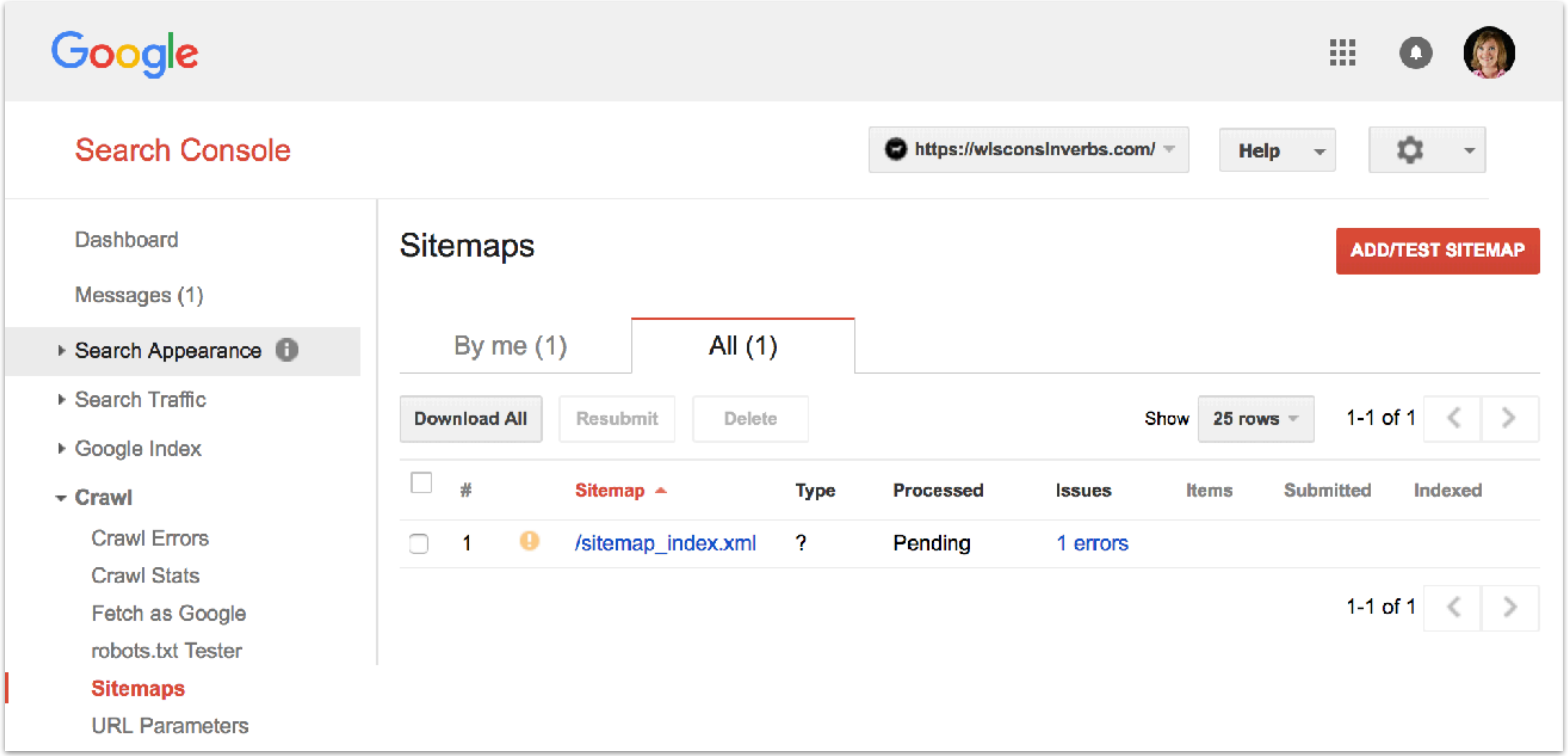
Text link counter: On | Off

XML Sitemaps

Enable the XML sitemaps that Yoast SEO generates. See the XML sitemap. Read why XML Sitemaps are important for your site.

On | Off

SUBMIT YOUR SITEMAP TO GOOGLE: ADD TO SEARCH CONSOLE



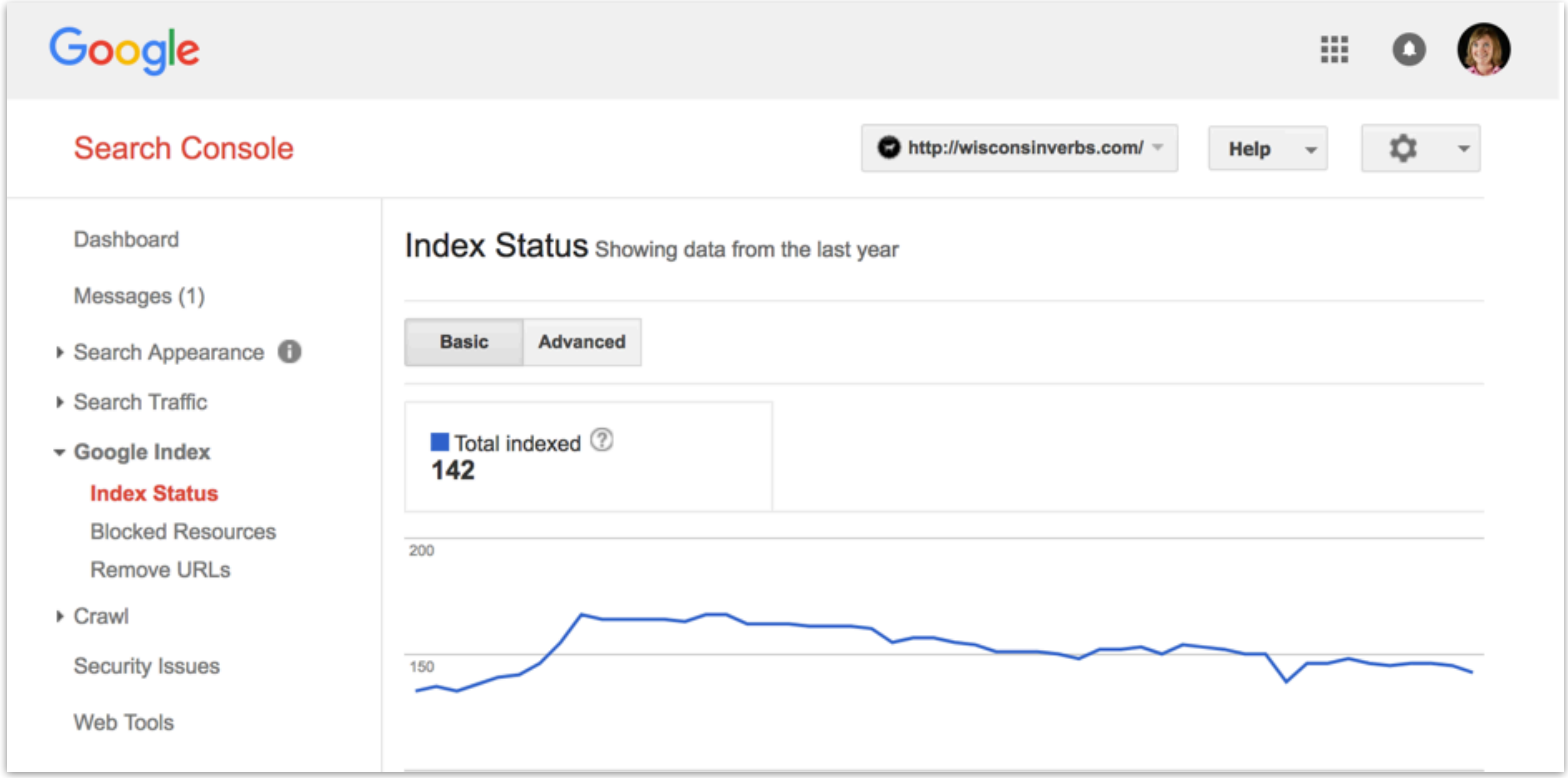
Sitemaps

☐	#		Sitemap ▲	Type	Processed	Issues	Items	Submitted	Indexed
☐	1	!	/sitemap_index.xml	?	Pending	1 errors			

1-1 of 1

AFTER SOME TIME, CHECK INDEX STATUS FOR BOTH URLS

You should see the index drop for your HTTP version and rise for the HTTPS version.



Index Status Showing data from the last year

🟦 Total indexed
142

WHY WOULDN'T YOU SWITCH TO HTTPS?

SPEED?

- Nope, it’s fast now. Add HTTP/2 and it’s really fast. https://istlsfastyet.com

COST?

- Nope, Let’s Encrypt is free and pretty great.

AD DELIVERY?

- Maybe
- There may still be ad networks serving over HTTP which would cause mixed content warnings. Presumably that's why sites like madison.com are still using insecure HTTP
- But, there has been an increase in secure news sites in recent years including jsonline.com & nytimes.com

TRENDS IN HTTPS

DEFAULT PROTOCOL HTTPS

https://w3techs.com/technologies/details/ce-httpsdefault/all/all

“27.1% of all websites and 68.4% of the top 1000 sites redirect to https.”

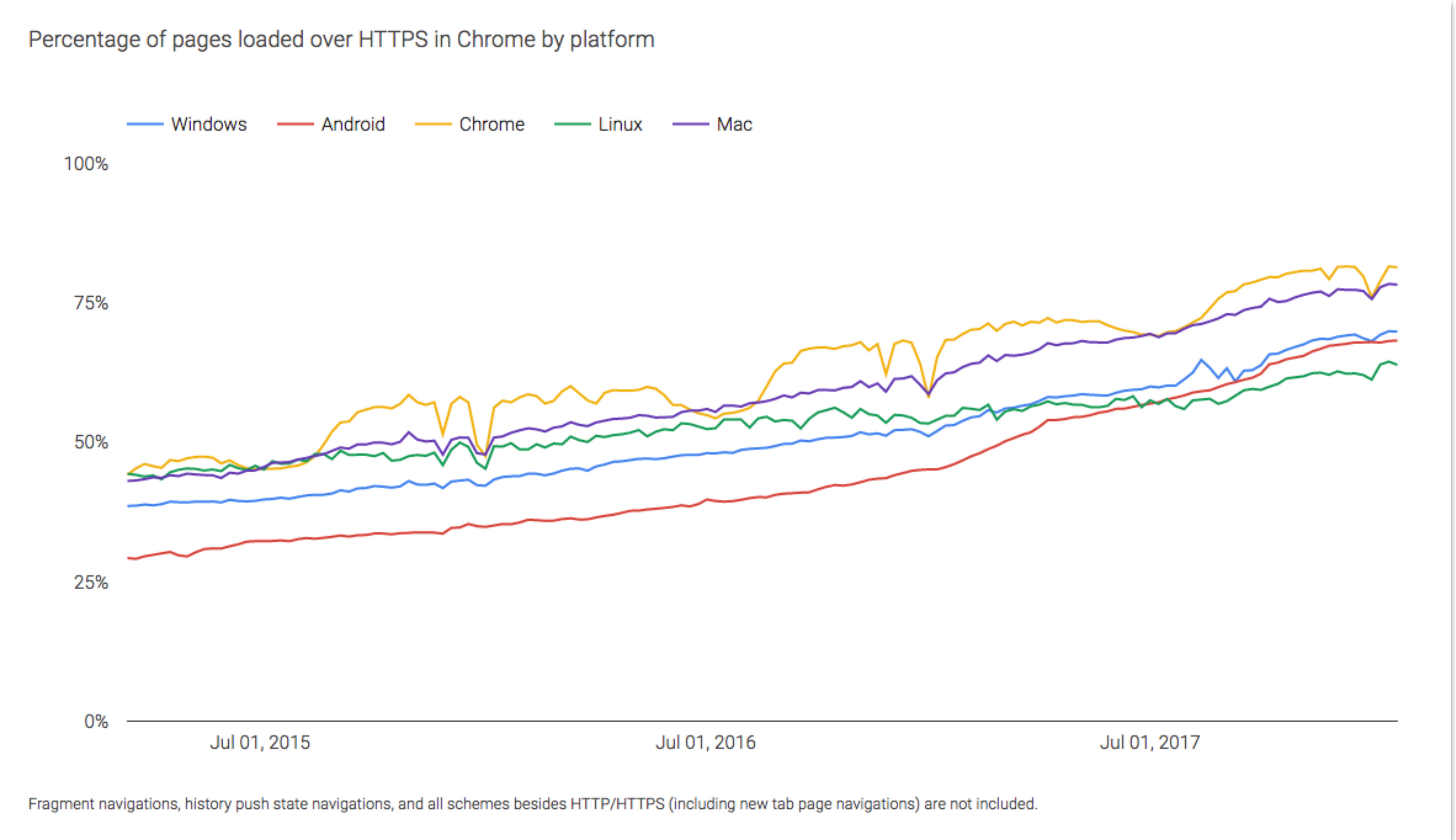
- w3tech.com

GOOGLE TRANSPARENCY REPORT

https://transparencyreport.google.com/https/overview

- Google has launched a transparency on their own sites' traffic over HTTPS. They're at 92% today.
- They also track all Chrome traffic to HTTPS sites by percentage of pages and percentage of browsing time, both of which has increased steadily.

GOOGLE TRANSPARENCY REPORT

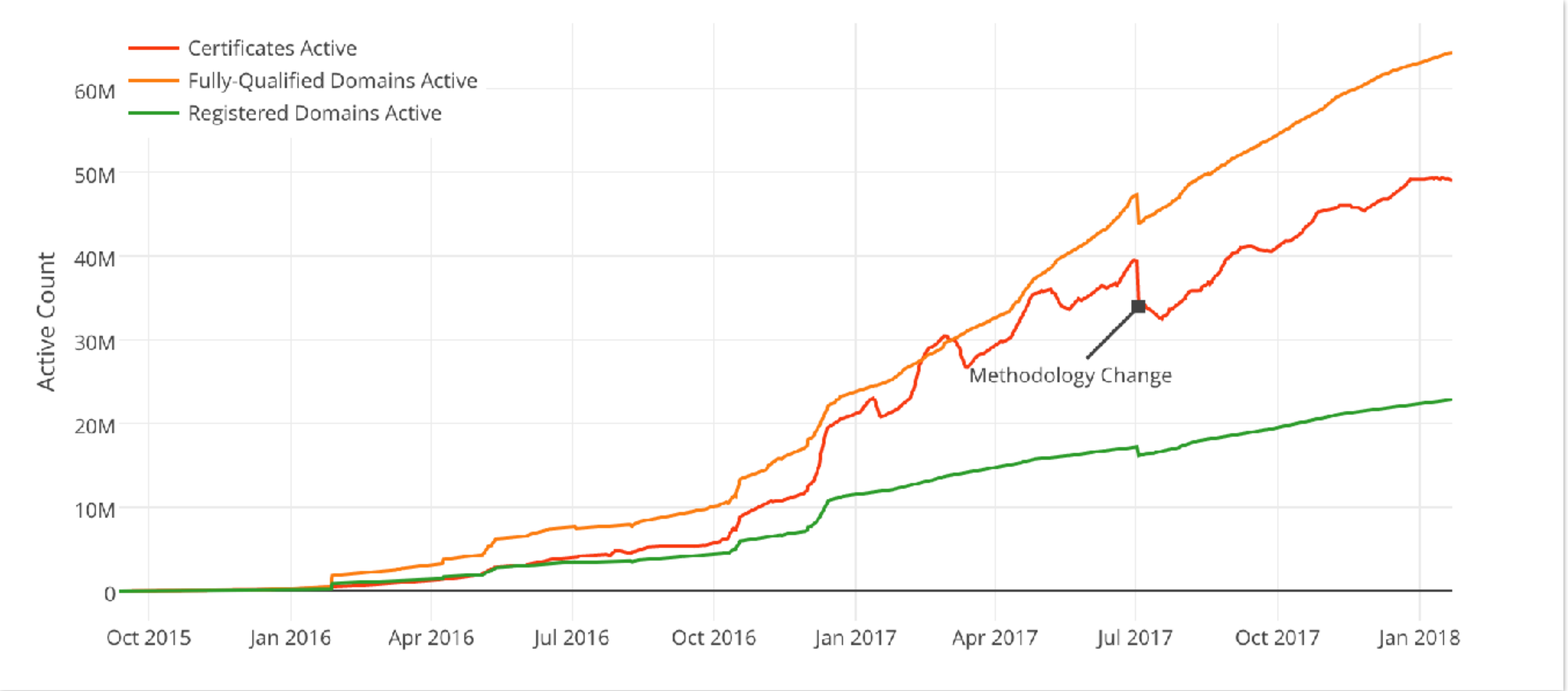


Percentage of pages loaded over HTTPS in Chrome by platform

Fragment navigations, history push state navigations, and all schemes besides HTTP/HTTPS (including new tab page navigations) are not included.

LET'S ENCRYPT USAGE IS ON THE RISE

https://letsencrypt.org/stats/



IN CONCLUSION

HTTPS IS A GOOD IDEA EVEN FOR PERSONAL SITES

While working on this talk, I was painfully aware that I hadn't yet secured my personal websites or the non profit sites that I work on. This gave me the motivation I needed.

The sites I have on NearlyFreeSpeech.net were crazy easy to secure because there is integrated Let's Encrypt which even handled the canonical URLs.

All I had to do was run: `tls-setup.sh` in the command line.

Shoptalk Show Podcast Security Episode
https://shoptalkshow.com/episodes/250-web-security-april-king-alex-sexton/

HTTPS Videos
https://www.youtube.com/watch?v=cBhZ6S0PFCY
https://www.youtube.com/watch?v=iP75a1Y9saY

WordPress HTTPS Posts
https://make.wordpress.org/support/user-manual/web-publishing/https-for-wordpress/
https://css-tricks.com/moving-to-https-on-wordpress/
https://premium.wpmudev.org/blog/ssl-https-wordpress/
https://wordpress.org/about/requirements/
https://yoast.com/rel-canonical/

SEO
https://support.google.com/webmasters/answer/6073543?hl=en
https://support.google.com/webmasters/answer/139066?hl=en

Verification Tools
https://observatory.mozilla.org/
https://www.ssllabs.com/ssltest/
https://www.whynopadlock.com/

Trends

https://transparencyreport.google.com/https/overview
https://letsencrypt.org/stats/
https://w3techs.com/technologies/details/ce-httpsdefault

General Security Posts

https://blog.chromium.org/2018/02/a-secure-web-is-here-to-stay.html
https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html
https://support.google.com/webmasters/answer/6073543
https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https
https://blog.mozilla.org/security/
https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/
https://istlsfastyet.com/
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
https://www.paulirish.com/2010/the-protocol-relative-url/

THANK YOU

- Please leave feedback at https://joind.in/talk/01bbf
- Slides are available on Twitter @andreaincode