THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

HTTPS

Webmasters - November 16, 2017

William Earnhardt
ITS Digital Services

HTTP Strict Transport Security (HSTS)

- (Mostly) removes the need for redirecting users from `http://` to `https://`
- Makes the browser always use an `https://` connection
  - Even when clicking on an `http://` link
  - Even after typing a domain into the location bar without specifying a protocol
- Removes the ability for users to click through warnings about invalid certificates.

HTTP Strict Transport Security (HSTS)

Basic Implementation:

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

Strongest Implementation:

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

HTTP Strict Transport Security (HSTS)

HSTS Preloading

- Created/managed by Chrome security team
- List of domains that get Strict Transport Security enabled automatically by the browser
- Follow instructions and submit domain at https://hstspreload.org/

General HTTP > HTTPS Migration Strategy

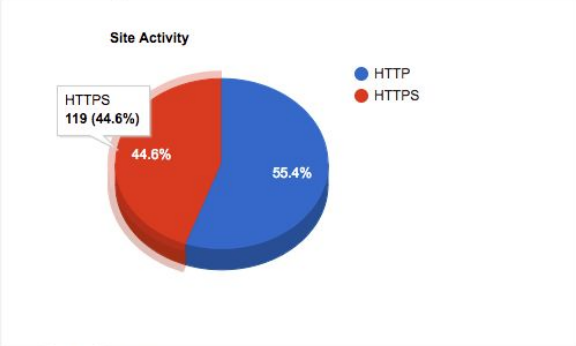
1. Install certificate(s)
2. Enable `https://` but don't force a redirect
3. Live browser testing of the site to check for breakages
4. Scan code using `grep` (or similar tools) for hardcoded `http://` urls for images, scripts, stylesheets, fonts, etc.
5. Maybe run a search/replace on database for:

   http://yoursite.unc.edu > https://yoursite.unc.edu
6. Force redirect to `https://`
7. Turn on HSTS

Sites.unc.edu HTTP > HTTPS Migration Strategy

1. ☑ Stop redirecting to `http://`
2. ☑ Force all new sites to be created as HTTPS from the beginning
3. ☑ Write code to force sites that have been converted to HTTPS:
    - Always redirect `http://` to `https://`
    - Return an HSTS header with a short `max-age` value
4. ➡ One by one switch sites to HTTPS:
    - Confirm Certificate
    - Search-Replace site's tables to fix images, links, etc in the database
    - Crawl the site using Mixed Content Scan tool
5. Increase the HSTS `max-age` value returned for migrated sites

HTTPS Migration Dashboard



Show 10 entries Search:

ID	Site	Last Updated
2	studentaid.sites.unc.edu/	2017-11-16 15:53:31
7	cci.sites.unc.edu/	2017-10-16 13:05:06
8	software.sites.unc.edu/	2017-11-16 16:07:32
9	registrar.sites.unc.edu/	2017-11-16 03:50:35
10	help.sites.unc.edu/	2017-11-16 15:01:17
11	uncmain.sites.unc.edu/	2017-11-16 11:55:16
15	devnet.sites.unc.edu/	2017-11-15 22:26:29
20	academicpersonnel.sites.unc.edu/	2017-10-11 19:55:39
21	art.sites.unc.edu/	2017-10-26 12:56:51
22	ackland.sites.unc.edu/	2017-11-13 19:26:59

Showing 1 to 10 of 148 entries Previous Next

Rudimentary HTTPS Migration Dashboard

Web.unc.edu Migration Plan

- Won’t begin until after sites.unc.edu is complete
- Has to be automated
- HSTS on primary web.unc.edu site will have `includeSubdomains`
- Some custom domains will not get converted
- Changes to Domain Mapping process

Planned Project Tools

- Content Security Policy reporting of mixed-content
  - Write mixed-content error data into application logs
  - Use Splunk to aggregate and generate mixed-content error reports
- Web-based site scanning tool for campus websites
  - Enter a domain and generate a mixed content report for download

How to get a certificate

UNC InCommon License

https://software.sites.unc.edu/certificates

LetsEncrypt

https://letsencrypt.org/

HTTPS Resources

- The HTTPS-Only Standard

  https://https.cio.gov/

- Mozilla Developer Network HSTS Documentation

  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

HTTPS Migration Tools

- Mixed Content Scan
  https://github.com/bramus/mixed-content-scan/

WordPress Search-Replace

- WP-CLI
  https://developer.wordpress.org/cli/commands/search-replace/
- Search-Replace DB
  https://interconnectit.com/products/search-and-replace-for-wordpress-databases/
- Better Search Replace Plugin
  https://wordpress.org/plugins/better-search-replace/