20171116 HTTPS Webmasters Presentation

Meeting Details

Date: 11/16/2017

Time: 2:00 PM

Location: Graduate Student Center

Presenters: Rachell Underhill, William Earnhardt

Meeting Notes

Rachell's Presentation

- Push to move everything to HTTPS over the last 10 years
    - Cannot be ignored now with the changes
- What is HTTPS
    - Secure
    - Way of confirming sites
    - Encryption of information passed to/from site
    - This is the standard being pushed by big institutions.
    - In past, only used for financial transactions or password related items.
        - Also, there were performance issues
- HTTPS is the future
    - HTTP2 will be required for new calls here soon.
    - There are features that will only be available using HTTP2
- Benefits
    - Google is prioritizing websites that use HTTPS higher than basic HTTP sites
    - Browsers are providing content warning messages to sites that do not use HTTPs
- Browser User Notifications
    - New warning
        - Mixed content
        - Bad certificates
        - Form sent over HTTP
        - Etc.
    - Not secure Notification
        - Chrome is displaying a "not secure" message in the browser bar window for any site not using HTTPS
        - Firefox
            - Provides an icon to denote if a site is serving content properly and providing secure information
    - Bad certificate
        - Provides a browser warning to user and does not display site by default
        - A user must perform extra actions to access the site.

    - Chrome form warning
        - When you start typing on field, if the page is not secure, the browser bar will notify you
    - Chrome in the Near Future
        - If the site is not HTTPS, a red warning will display to the users at all times
- Common pitfalls when switching to HTTPS
    - Invalid or missing SSL certs
    - Mixed content
    - SEO Problems
    - JavaScript errors, API errors or broken websites
- Mixed Content
    - Occurs when an HTTPS website pulls in not secure content
    - Protocol relative links no longer recommended
        - Now a security issue.
    - Find and fix mixed content on your source code or by using the browser error messages.
    - Chrome console will notify you of any warnings related to security
- Redirects and SEO
    - Use a proper 301 redirect to push users form http:// https://.
    - Do not use 302 as it will affect search rankings
- JavaScript or API errors
    - 3rs party content
    - Forms
    - iframes
    - Analytics tools
- Resources
    - Qualys SSL labs
        - Can test the SSL validity of a site with details about what is working and what is not.
        - Will provide you with a letter grade for the SSL rating for your URL
    - Badssl.com
        - Series of test pages so you will know how a browser will notify a user for various issues.
    - Why No Padlock
        - Basic analysis site
    - HTTPS checker desktop app and Mixed Content Scan
        - 2 sites for checking mixed content

William's Presentation

- Overview
    - General process for switching site over
    - Helpful tips for making change
    - What is being done on campus sites
    - A couple of tools
- HTTP Strict Transport Security (HSTS)
    - Mostly removes the need for redirecting users from http:// to https://

    - Makes browser always use an https:// connection
        - Even when clicking http:// link
        - Even when typing in the browser bar
    - Removes the ability for users to click through the warning about invalid certificates
    - Basic Implementation
        - Set a header with a max age
        - Policy is refreshed each time the page is refreshed
    - Strongest Implementation
        - Provides additional values
            - IncludeSubDomains
                - This forces all subdomains to conform to this rule
            - Preload
                - Will enable this inclusion to be in the browser preload list.
    - HSTS Preloading
        - Created/managed by Chrome security team
        - List of domains where this value is set by default
            - This is shipped with the browser and cannot be changed by the user
        - Chrome security team started and run it, but it is honored by multiple browsers
- Migration Process
    - Install certificate(s)
    - Enable https:// but do not force redirectWeb.
        - Allow issue best connections
    - Live browser testing
    - Scan code using grep (or similar tools) for hardcoded http:// value
    - Possibly run a search/replace in the database for http://
    - Force redirect to https://
    - Turn on HSTS header
- Sites.unc.edu migration strategy
    - Stop redirecting to http://
        - Can access sites from either one
    - Force all new sites to be created as HTTPS from the beginning
    - 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
    - One by one switch sites to HTTPS
        - Confirm certificate
        - Search-replace sites tables to fix images, links, etc. in the database
        - Crawl the site using Mixed Content scan tool
    - Increase the HSTS max-age value returned for migrated sites
- Sites.unc.edu process
    - Roughly 45-50% complete with the migration
- Web.unc.edu migration plan
    - Overview
        - Will not start until sites.unc.edu is complete
        - Has to be automated with over 15K sites

        - HSTS on primary web.unc.edu site will have includeSubdomains
        - Some custom domains will not be migrated over
        - Changes to domain mapping process for the custom ones
- 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 missed content report for download
- How to get a certificate
    - UNC InCommon License
        - Go to the software acquisition office
    - Lets Encrypt
        - Feed, depending on host
- HTTPS resources
    - The HTTPs-Only standard
        - https://https.cio.gov
    - Mozilla Developer Network HSTS Documentation
        - Link in PowerPoint
- WordPress Tools
    - WP-CLI
        - Command line tool for search replace
        - Will address serialized data in the database
    - Search-Replace DB
    - Better Search Replace Plugin
        - Powerful WP Plugin

Questions

- How does the browser store the HSTS?
    - In the browser structure
    - Per browser implementation
-