HTTPS, Mixed Content

& Why It Matters

httpschecker.net

About Us

The httpschecker.net service offers our HTTPS Checker scanning app and HTTPS Reporter real-time issue reporting tool to identify mixed content issues. We typically follow a “freemium” model so as many businesses as possible can benefit from our apps for free, with advanced features or scaled up versions available to purchase.

To get HTTPS Checker & HTTPS Reporter visit https://httpschecker.net/

What Is HTTPS?

HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol that protects the integrity and confidentiality of your users' data as it is sent from their computer to your website, including public networks such as WiFi hot spots. This is visible to users when browsing websites because it displays a green padlock in their browser.

Why Is HTTPS So Important?

Privacy is a very serious concern and users want to be reassured that their data is secured, especially when they enter valuable data via forms, for example logging in to a site, making a purchase or subscribing to newsletters. This information can be exploited by criminals if they are able to view the data or interfere with it as it flows between the user and the site, something called “man-in-the-middle” attacks. Keeping data encrypted stops others being able to view and exploit it for criminal purposes. Login data is valuable because it can be used to steal identities or access sensitive data on any other sites you access using the same login details.

64% Of Internet Users Use The Same Passwords On All Or Most Websites!

According to Ofcom’s 2015 Adults’ Media Use & Attitudes report, nearly two thirds of internet users have a single password that they use to login to all or most of the websites they visit. This is up from 57% in 2013.

Users Want Better Security!

Users increasingly expect better security and the use of ‘formal judgements’ (e.g. padlocks or system messages) has increased, from 43% to 55% according to the same 2015 Ofcom report. It is therefore in the best interests of website operators to provide secure transmission of data via HTTPS.

How Do You Move To HTTPS?

Implementing "HTTPS" protocol starts by installing an SSL certificate ideally on an entire site, or at least on those parts which capture sensitive data, and the browser will then display the familiar green padlock to users *unless there is "mixed content"*.

Google's Guide To Securing Your Site With HTTPS

For more information on moving to HTTPS, use Google's guide to securing your site with HTTPS

What Is "Mixed Content" & Why Does It Break HTTPS?

Mixed content issues occur whenever a secure HTTPS page contains a reference to a non-https resource, for example a link to a Javascript file or an image that starts with "http://" rather than "https://".

Some types of resources have more serious implications than others because they affect how a page works or looks and this is called "**active mixed content**". Resources include Javascript, CSS and fonts; modern browsers will not load these resources meaning the page may not work as required or display properly to visitors. This could lose revenues or lead generating opportunities as well as undermining confidence in your site.

"**Passive mixed content**" includes resources which have a lot less impact on page behaviour, such as links to "http" versions of images, audio and videos; browsers will load these pages but without https meaning you lose the green padlock which users are looking for.

WARNING: Active Or Passive Content Can Both Be Exploited!

Whilst active and passive content may be different in how they affect a page load, **both types of mixed content can still be exploited by hackers**.

Example Exploit: **Daniel Goes To Lunch**

Daniel pops out for a coffee at lunchtime and decides to use the free WiFi available at his coffee shop. Being a customer, the waiter helpfully gives over today's WiFi password and Daniel connects and starts browsing for some shoes on his favourite menswear site. He finds just the right pair and places his order. Daniel then goes onto some of his favourite sites for 10 minutes, checks some account balances, responds to an urgent email and then goes back to work.

The Exploit

A hacker sits at a table near to the coffee shop and gets their WiFi code without asking because it was posted onto an app like WiFiMap (which anyone can browse to get passwords for public WiFi hot spots). The hacker sniffs the network using a freely available tool and sees Daniel browsing for shoes. The hacker starts to watch for insecure resources and, finding a page which has mixed content, uses a simple method to capture his login details. Daniel didn't spot that the green padlock was missing because it was ok on previous visits. The hacker continues to see all of the other sites Daniel visits and decides to log into each of them to see if he uses the same login details. Bingo, it works on 2 out of 3 of them.

Daniel's accounts have now been compromised, the level of impact will now depend on the type of sites he was on and the value these can deliver to criminals.

Read more detail about mixed content attacks on White Hat Security's blog.

Worried You've Been A Victim Of Cybercrime?

Find out how to report online scams in the UK at Action Fraud or the FBI in the US.

Let's Remember, It's Not Just About Exploits…

Whilst exploits represent the scarier end of HTTPS issues, it is still important to remember that increasingly users are looking out for green padlocks or warning messages and may abandon their purchase or enquiry if an issue is apparent.

How Does HTTPSchecker.net Help?

We provide 2 tools to proactively scan sites initially and then capture and report ad hoc issues in real-time. They can be used independently of one another.

Our HTTPS Checker app proactively crawls your site to detect pages with mixed content which you can then update to use secure resources. This is much easier than trying to perform manual checks across all pages, especially on larger sites.

It provides an overview of issues by severity plus a PDF report and downloadable data in CSV format which administrators can work from to fix issues.

HTTPS Checker also includes warnings about other common issues and offers advanced settings, for example crawling with different user agents such as mobile browsers, and robots.txt style pattern-matching to split down crawls on large sites.

Our HTTPS Reporter tool captures mixed content issues from across your entire site *as and when they are visited by users*. Our HTTPS Reporter tool can collate these reports as they come in so you have an easy fix list to work from. This works in conjunction with you setting up a Content Security Policy on your site.

Do All Businesses Need To Do This?

The short answer is yes, especially if you collect any type of data on your site. There is a big push for businesses to move to “SSL everywhere”, with a reputable new organisation called Let’s Encrypt offering free SSL certificates, and governments amongst others advocating adoption of HTTPS. Google confirmed on 6th August 2014 that HTTPS had become a lightweight ranking signal so there is even a small SEO benefit to be gained too.

Where Can I Find Out More About HTTPS?

Read more about https from Google’s support forum, the US government, the Chrome Browser team, Mozilla Developer Network, Infosec Institute.

References

Man In The Middle Attacks: https://en.wikipedia.org/wiki/Man-in-the-middle_attack
Ofcom’s 2015 Adults’ Media Use & Attitudes:
http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit-10years/2015_Adults_media_use_and_attitudes_report.pdf
Google’s Guide To Securing Your Site With HTTPS:
https://support.google.com/webmasters/answer/6073543?hl=en
White Hat Security’s blog:
https://www.whitehatsec.com/blog/why-is-passive-mixed-content-so-serious/
Action Fraud: http://www.actionfraud.police.uk/
FBI: https://www.fbi.gov/scams-safety/fraud/internet_fraud
Let’s Encrypt: https://letsencrypt.org/
Google Ranking Announcement 6th August 2014:
https://googlewebmastercentral.blogspot.co.uk/2014/08/https-as-ranking-signal.html
US Government: https://https.cio.gov/

Chrome Browser Team:
https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure
Mozilla Developer Network:
https://developer.mozilla.org/en-US/docs/Security/Mixed_content
Infosec Institute:
http://resources.infosecinstitute.com/https-mixed-content-vulnerability/