Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 37

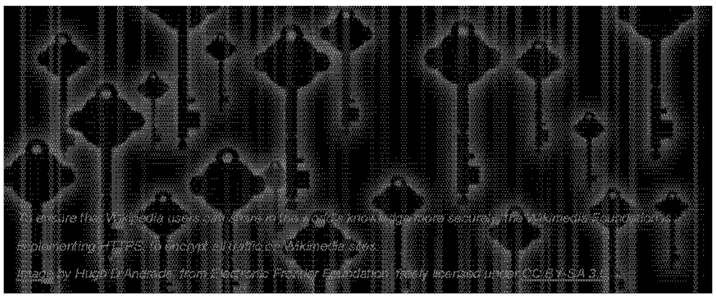
FOUNDATION, LEGAL, PLATFORM ENGINEERING, TECHNOLOGY, WIKIPEDIA

Securing access to Wikimedia sites with HTTPS

By Yana Welinder
Victoria Baranetsky, Wikimedia Foundation
Brandon Black, Wikimedia Foundation

June 12th, 2015

The Wikimedia Foundation is happy to announce that we are implementing HTTPS to encrypt all traffic on Wikimedia sites. With this change, nearly half a billion monthly visitors on Wikipedia and its sister projects will be able to share in the world's knowledge more securely.



To ensure that Wikipedia users can share in the world's knowledge more securely, the Wikimedia Foundation is implementing HTTPS to encrypt all traffic on Wikimedia sites.
Image by Hugo D'Andrade, from Electronic Frontier Foundation, freely licensed under CC BY-SA 3.0.

To be truly free, access to knowledge must be secure and uncensored. At the Wikimedia Foundation, we believe that you should be able to use Wikipedia and the Wikimedia sites without sacrificing privacy or safety.

Today, we're happy to announce that we are in the process of implementing HTTPS to encrypt all Wikimedia traffic. We will also use HTTP Strict Transport Security (HSTS) to protect against efforts to 'break' HTTPS and intercept traffic. With this change, the nearly half a billion people who rely on Wikipedia and its sister projects every month will be able to share in the world's knowledge more securely.

The HTTPS protocol creates an encrypted connection between your computer and Wikimedia sites to ensure the security and integrity of data you transmit. Encryption makes it more difficult for governments and other third parties to monitor your traffic. It also makes it harder for Internet Service Providers (ISPs) to censor access to specific Wikipedia articles and other information.

HTTPS is not new to Wikimedia sites. Since 2011, we have been working on establishing the infrastructure and technical requirements, and understanding the policy and community implications of HTTPS for all Wikimedia traffic, with the ultimate goal of making it available to all users. In fact, for the past four years, Wikimedia users could access our sites with HTTPS manually, through HTTPS Everywhere, and when directed to our sites from major search engines. Additionally, all logged in users have been accessing via HTTPS since 2013.

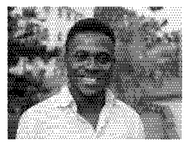
GET CONNECTED

GET OUR EMAIL UPDATES

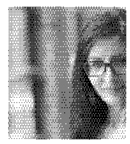
Your email address

Subscribe

MEET OUR COMMUNITY



The one-man band writing the history of Nigerian cinema into Wikipedia



Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics tea

ARCHIVES

FEBRUARY 2018

JANUARY 2018

Over the last few years, increasing concerns about government surveillance prompted members of the Wikimedia community to push for more broad protection through HTTPS. We agreed, and made this transition a priority for our policy and engineering teams.

We believe encryption makes the web stronger for everyone. In a world where mass surveillance has become a serious threat to intellectual freedom, secure connections are essential for protecting users around the world. Without encryption, governments can more easily surveil sensitive information, creating a chilling effect, and deterring participation, or in extreme cases they can isolate or discipline citizens. Accounts may also be hijacked, pages may be censored, other security flaws could expose sensitive user information and communications. Because of these circumstances, we believe that the time for HTTPS for all Wikimedia traffic is now. We encourage others to join us as we move forward with this commitment.

The technical challenges of migrating to HTTPS

HTTPS migration for one of the world's most popular websites can be complicated. For us, this process began years ago and involved teams from across the Wikimedia Foundation. Our engineering team has been driving this transition, working hard to improve our sites' HTTPS performance, prepare our infrastructure to handle the transition, and ultimately manage the implementation.

Our first steps involved improving our infrastructure and code base so we could support HTTPS. We also significantly expanded and updated our server hardware. Since we don't employ third party content delivery systems, we had to manage this process for our entire infrastructure stack in-house.

HTTPS may also have performance implications for users, particularly our many users accessing Wikimedia sites from countries or networks with poor technical infrastructure. We've been carefully calibrating our HTTPS configuration to minimize negative impacts related to latency, page load times, and user experience. This was an iterative process that relied on industry standards, a large amount of testing, and our own experience running the Wikimedia sites.

Throughout this process, we have carefully considered how HTTPS affects all of our users. People around the world access Wikimedia sites from a diversity of devices, with varying levels of connectivity and freedom of information. Although we have optimized the experience as much as possible with this challenge in mind, this change could affect access for some Wikimedia traffic in certain parts of the world.

In the last year leading up to this roll-out, we've ramped up our testing and optimization efforts to make sure our sites and infrastructure can support this migration. Our focus is now on completing the implementation of HTTPS and HSTS for all Wikimedia sites. We look forward to sharing a more detailed account of this unique engineering accomplishment once we're through the full transition.

Today, we are happy to start the final steps of this transition, and we expect completion within a couple of weeks.

Yana Welinder, Senior Legal Counsel, Wikimedia Foundation
Victoria Baranetsky, Legal Counsel, Wikimedia Foundation
Brandon Black, Operations Engineer, Wikimedia Foundation

40 Comments on Securing access to Wikimedia sites with HTTPS

Uityyy 7 months

How do I manually force unencrypted access on an old mobile browser that does not support HTTPS?
I have one that 's failing to access en.m.wikipedia.org, apparently because of this, and I see no solution here.
Any magic "en.insecure.wikipedia.org"?

Share

DECEMBER 2017

NOVEMBER 2017

OCTOBER 2017

OLDER POSTS 26

Frushi 8 months

HTTPS is a 'must have' in present internet. When Google said it's gonna take a closer look for a website that don't use SSL it become clear that even websites which don't need them (because they don't have any secure infomation) will have to go to HTTPS from old http.

Share

Tom 1 year

Following the huge fail of the french ISP Orange redirecting wikipedia.fr and others, why wikipedia.fr is not protect with https/HSTS ?
http://www.theregister.co.uk/2016/10/18/orange_blows_up_french_gov_website/

Share

bart 1 year

Google usually has an alternate (cache) for each wiki link.
I just use these cache pages.

Share

Rodion 2 years

I also want there is a way to use wikipedia with plain HTTP if necessary. Currently there is a stupid debate between our government and local wiki representatives (I could not decide which of them is more stupid, I'm sorry) about restricting access to certain pages (about drugs). Providers can do this for single page if it is accessed with HTTP, but they need to deny access to whole website if it is accessed via HTTPS.

So it would be good if we have some fallback, perhaps with banner explaining "all horrible consequences" of reading wiki in plain HTTP. In my personal opinion being super-obsessed with security measures may sometimes create unwanted problems to other people :(

Share

Creg 3 years

Flo said

"Concerning privacy: when you browse Wikipedia the URLs contain the topic you are reading thus any sniffer can track what you are currenly reading. Only the *contents* is encrypted, but the contents is visible by anybody anyway (in contrast to the content of my bank account)."

False. The root domain (wikipedia.org) can be inferred from the IP address of the server during the TCP/IP request but the complete URL and exact page you're reading cannot.

Read the article on https.

Share

Flo 3 years

Is there *any* way to use Wikipedia *without* https?
I have an old device which is not capable of using https. And please don't tell me to buy new hardware or software.
So please offer a possibility to read Wikipedia *without* forced https!!!!

BTW: I cannot follow the reasons to *enforce* https:
Concerning privacy: when you browse Wikipedia the URLs contain the topic you are reading (e.g.:

https://en.wikipedia.org/wiki/CMAC) thus any sniffer can track what you are currenly reading. Only the *contents* is encrypted, but the contents is visible by anybody anyway (in contrast to the content of my bank account).

Concerning "integrity of data": nobody will guarantee that the content of Wikipedia is accurate because everybody can contribute to it. Thus I do not *fully* rely to anything I read in Wikipedia.

Share

omtim 3 years

Great step for sure, actually, in digital world https is more imperative

Share

Gary Smith 3 years

All the points are explained very clearly, Great source of information. Thanks for en-lighting us with your knowledge, it is helpful for many of us.

Share

Sports Fan Stan 3 years

All well and good to force everyone to use https. Would it be too much to ask to employ a real SSL certificate that doesn't rely on a wildcard. At present, we can't even use Wikipedia anymore because we can't trust the website. Uggghhh…

Share

astrodevamm 3 years

Very good step indeed, in fact, in cyber world https is more important because of security issues. Know a days users check website also they check that website https not. If they found https is not they click on cut button and skip from website…

Share

Pushpendra Pal 3 years

Great move team. Web is becoming a tool for governments and enforcement agencies to surveillance on citizens. SSL helps website visitors to send and receive encrypted data.

I also want to move my website http://careervendor.com from HTTP to HTTPS. I am fearing about loosing traffic, backlink and ranking. Can anyone please suggest a way for proper migration.

Share

astrodevamm 3 years

Very good step indeed, in fact, in cyber world https is more important because of security issues. Know a days users check website also they check that website https not. If they found https is not they click on cut button and skip from website…

Share

Ron 3 years

> There are two reasons someone might ask for any form of downgrade or opt-out to be permitted:

Make that three reasons.
I run in DOS, and I like to keep the functionality of Arachne.

Yes, I also run Links, Elinks and Lynx in DOS, but Arachne is more versatile than all of them – except for a lack of SSL.

Share

zzo38 3 years

I *really* want the ability to connect without HTTPS. I want to avoid the overhead required by HTTPS please.

Share

Mat2 3 years

"Because then a man in the middle can replace anyone's user agent details with another user agent, and bingo, nobody any longer has any encryption at all. Invisibly and undetectably."
Such an attack is already possible with tools such as sslstrip. Therefore user-agent sniffing doesn't decrease security for other users out there: it will make life easier neither for criminals nor for companies that want to monitor traffic.
Wikipedia is going to use HSTS and add itself to HSTS preload lists in browsers: that will block downgrade to HTTP for new browsers.

"Upgrading from IE6 to a secure browser is entirely possible for every single user on the planet. There is no sane reason for anyone, anywhere, to use an insecure browser."
Not every computer user can do this, unfortunately.

Google makes sure that IE6 still works:
https://www.ssllabs.com/ssltest/analyze.html?d=google.com&s=74.125.239.96&hideResults=on
Wikipedia is such an important site on the internet.

Share

dewimorgan 3 years

"Wouldn't it be possible to add some user-agent sniffing" NO! No it would not. Because then a man in the middle can replace anyone's user agent details with another user agent, and bingo, nobody any longer has any encryption at all. Invisibly and undetectably. Why would wikimedia hand attackers such a gift on a plate?

Upgrading from IE6 to a secure browser is entirely possible for every single user on the planet. There is no sane reason for anyone, anywhere, to use an insecure browser. The very worst smartphone and smartwatch in the world can browse securely. Even Lynx can handle secure browsing, and that's been ported to just about everything.

There are two reasons someone might ask for any form of downgrade or opt-out to be permitted: 1) they are grievously uninformed; or 2) they are maliciously requesting the downgrade on behalf of some organization which wants a MitM attack to work.

One wonders how many of each group is commenting here.

Share

Mat2 3 years

Now all IE6 users will be cut off from using Wikipedia:
https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org

Wouldn't it be possible to add some user-agent sniffing so that these browsers could still access Wikipedia? They are usually used by poorer people.

Share

Ron Clarke 3 years

Steve,
> Why now adding a SSL/TLS support to that browser instead, is this really something very hard to do, or just not a priority?

Adding SSL to Arachne would be wonderful, and we wish we could. But.....we have a lack of suitably skilled coders with an interest in DOS browsers, and Arachne in particular.

Any volunteers ?

Share

dewimorgan 3 years

@Glenn McCorkle and Ron Clarke:

"Ron & I are active developers of DOS Arachne"

This ship has sailed.

Every single .gov domain will be HTTPS-only by next year. Many already are.

For active developers of web browsers which don't support HTTPS, implementing it should have been the number one priority for the last few years, because other browsers – even other command-line browsers that can run on legacy hardware – support it just fine. Like an FTP program without FTPS or SFTP, or an email program without STARTTLS, you'll lose market share and relevance.

Oh, and IPv6 URLs are a thing now, too.

Share

MORE COMMENTS

Comments are closed.