CUNY Academic Commons - Bug #7235

Can't access sites

2016-12-24 08:48 PM - Raffi Khatchadourian

Status:	Resolved	**Start date:**	2016-12-24
Priority name:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category name:		**Estimated time:**	0.00 hour
Target version:	Not tracked		

Description

I am getting an SSL error when trying to access any site on the commons, e.g., http://dev.commons.gc.cuny.edu. My browser says that the certificate is invalid. If I add a security exception and proceed, no matter from which site I am trying to access, the contents of the page seems to be something to the extent of "The Barry S. Brook Center For Music Research And Documentation."

History

#1 - 2016-12-27 10:06 AM - Matt Gold

Hi Raffi,

Sorry for the late response. This issue (a server configuration error) should be fixed now; please let us know whether the issue is solved for you.

#2 - 2016-12-27 11:06 AM - Raffi Khatchadourian

Matt Gold wrote:

> Hi Raffi,
>
> Sorry for the late response. This issue (a server configuration error) should be fixed now; please let us know whether the issue is solved for you.

No problem, Matt. But, why are these sites being served over HTTPS? What is the sensitive information that is being transferred? Of course, I understand that forms asking for passwords need to be posted via HTTPS but why the entire site in general?

Using HTTPS unnecessarily not only wastes computational resources on the server but also negatively affects SEO.

#3 - 2016-12-27 11:18 AM - Matt Gold

- Status changed from New to Assigned

Hi Raffi. Central IT now requires that any CUNY website containing a login form be served over https. Since the sitewide header (the black band at the top of the CAC) includes a log-in mechanism, we are required to server over https.

#4 - 2016-12-27 11:27 AM - Raffi Khatchadourian

Matt Gold wrote:

> Hi Raffi. Central IT now requires that any CUNY website containing a login form be served over https. Since the sitewide header (the black band at the top of the CAC) includes a log-in mechanism, we are required to server over https.

Thanka, Matt. But, shouldn't only the POST sent when the login form is submitted be over HTTPS? Why would the form itself (i.e., the text boxes) need to be secured?

#5 - 2016-12-27 11:32 AM - Boone Gorges

> Using HTTPS unnecessarily not only wastes computational resources on the server but also negatively affects SEO.

Our eventual goal is to serve all content over SSL/TLS. Browsers will increasingly enforce this policy, by disabling various features and showing scary notices for non-secure pages. See https://https.cio.gov/everything/ for a helpful overview of why HTTPS everywhere is a good policy.

#6 - 2016-12-27 03:23 PM - Raffi Khatchadourian

Boone Gorges wrote:

> Using HTTPS unnecessarily not only wastes computational resources on the server but also negatively affects SEO.

> Our eventual goal is to serve all content over SSL/TLS. Browsers will increasingly enforce this policy, by disabling various features and showing scary notices for non-secure pages. See https://https.cio.gov/everything/ for a helpful overview of why HTTPS everywhere is a good policy.

Ah, okay. Thanks for the clarification, Boone.

#7 - 2017-01-01 09:45 PM - Boone Gorges

- Status changed from Assigned to Resolved

- Target version set to Not tracked