Wt - Bug #9591

SAML Authentication Behind TLS Terminating Reverse Proxy

01/09/2022 12:55 AM - Aaron Wright

Status:	Closed	**Start date:**	01/09/2022
Priority:	Normal	**Due date:**	
Assignee:	Roel Standaert	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	4.7.0		

Description

I'm very excited about SAML support being added. Thank you so much!

I'm trying to get it to work with Microsoft Azure AD, and I'm running into an issue. I run my Wt application in Kubernetes. Our Kubernetes uses nginx to terminate TLS connections and then reverse proxy to my Wt application. This works in general, but in the case of SAML authentication, I get this error:

```
[error] "Auth.Saml.Service: OpenSAML.MessageDecoder.SAML2POST (thread: 140186616833792): POST targ
eted at (https://<host>/acs), but delivered to (http://<host>/acs)"
```

I did some investigation, and it appears that the appendOriginalUrl function in the Wt::Auth::Saml::Service class creates an "original URL" based on the request that was POST'ed to the "/acs" endpoint, but that the request returns "http" for the URL scheme, instead of "https". Technically the request is right, it is an "http" request, but in this situation, the "original URL" needs to be one that is on the other side of the reverse proxy. My reverse proxy is sending some helpful header to assist with this:

```
X-Forwarded-For: 127.0.0.1
X-Forwarded-Host: <host>
X-Forwarded-Port: 443
X-Forwarded-Proto: https
```

Would it be possible to get support for SAML from behind a reverse proxy?

History

#1 - 01/10/2022 09:35 AM - Roel Standaert

- Status changed from New to Confirmed

- Target version set to 4.6.2

At first, I was thinking you just didn't configure <trusted-proxy-config> (or the deprecated <behind-reverse-proxy>, but it seems we indeed do not look at that yet in Wt::Http::Request::urlScheme(), so that will have to be fixed.

#2 - 01/10/2022 09:36 AM - Roel Standaert

- Target version changed from 4.6.2 to 4.7.0

I guess I'll set this to 4.7.0, since it's still an observable change in default behavior.

#3 - 01/10/2022 05:13 PM - Aaron Wright

Roel Standaert wrote in #note-2:

> I guess I'll set this to 4.7.0, since it's still an observable change in default behavior.

In the mean time, I would appreciate a patch for 4.6.1. :)

I got everything to work this weekend by hardcoding "https" in the appendOriginalUrl, but I don't want to ship like that, obviously.

FYI, on a side topic, that <trusted-proxy-config> setting is hard for me to use in my Kubernetes environment. I don't know the IP addresses of the reverse proxy server. I get connections from several different IP addresses so there must be load balancing going on up front, and I have a feeling that the addresses can change when the department in charge of Kubernetes decides to redeploy something. I guess I could set the <trusted-proxy-config> to 0.0.0.0/0, and call that good.

#4 - 01/10/2022 06:07 PM - Roel Standaert

I think you may still be able to define a certain broader range that's not quite 0.0.0.0/0?

Of course, if you're sure that your application server is never directly accessed from the outside you can set it to 0.0.0.0/0.

#5 - 01/10/2022 06:48 PM - Roel Standaert

- Status changed from Confirmed to InProgress

#6 - 01/10/2022 06:48 PM - Roel Standaert

- Status changed from InProgress to Review

#7 - 01/10/2022 06:49 PM - Roel Standaert

- File 0001-WT-9591-make-Http-Request-urlScheme-look-at-X-Forwar.patch added

I attached the patch that is currently in review for inclusion in Wt 4.7.0.

#8 - 01/10/2022 11:47 PM - Aaron Wright

Roel Standaert wrote in #note-7:

> I attached the patch that is currently in review for inclusion in Wt 4.7.0.

Thanks so much! That's some good customer service.

I tested the patch and it does work for me.

#9 - 03/10/2022 10:59 AM - Roel Standaert

- Status changed from Review to Implemented @Emweb

- % Done changed from 0 to 100

#10 - 03/10/2022 03:26 PM - Roel Standaert

- Status changed from Implemented @Emweb to Resolved

#11 - 03/10/2022 04:23 PM - Roel Standaert

- Assignee set to Roel Standaert

#12 - 03/11/2022 02:27 PM - Roel Standaert

- Status changed from Resolved to Closed

Files

0001-WT-9591-make-Http-Request-urlScheme-look-at-X-Forwar.patch	4.39 KB	01/10/2022	Roel Standaert