Site fixes - Support #120

How to deal with HttpOnly cookies?

06/13/2022 09:26 PM - jacobk

Status:	Closed	**Start date:**	06/13/2022
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

I wrote a fix for https://startlivehealthonline.com/loginConsumer.htm to allow logging in, but because I couldn't figure out how to get the CSRF token from an "HttpOnly" cookie, I added an additional input box where the user can paste the CSRF token (from the "Storage" tab in the dev toolbar). Obviously, this is not very convenient, and since the official scripts submit the token automatically, it should be possible for a script in Haketilo to do the same. I do not know how the site's official scripts are adding the token to the request though (I generally don't look at the site's own scripts (with an exception noted in this fix that I saw the beginning of a script that sets the visibility of the page, and the method seemed like the obvious method, so I thought it better to explicitly copy that then to try to come up with something dissimilar after seeing the official method).).

The fix I wrote is attached, and it does allow logging in if you paste the CSRF token in the proper spot. Even if you don't have an account, you should be able to just click on the login button and a request without any login info will be sent, but the token will still be sent. Do you know how the official scripts might be accessing HttpOnly cookies, or how the scripts might affect the page so the CSRF token is part of the form?

History

#1 - 06/14/2022 11:52 PM - koszko

I don't know how the site does it. I am going to look at it tomorrow, after I release the new Hydrilla version with Python 3.7 support fixed

#2 - 06/15/2022 06:03 PM - koszko

I think I found it ^^

When on the login page, try executing this:

```
fetch('https://startlivehealthonline.com/touchSession.htm')
    .then(resp => console.log(resp.headers.get('csrf-token')))
```

#3 - 06/23/2022 04:21 AM - jacobk

Thanks! I uploaded a better version of the script here: https://codeberg.org/JacobK/unfinished-site-fixes/src/branch/main/LiveHealth/livehealth-login.js (I decided to upload my "unfinished" scripts to that repository, though there's some I didn't upload, mostly due to hardcoded authentication keys and stuff. Anyway, they're not meant to be included in any repository yet, but I figured it would be good to publish them in case others happen to be working on a site that I'm not working on anymore.)

#4 - 06/23/2022 08:36 AM - koszko

jacobk wrote:

> Thanks!

YW :)

I decided to upload my "unfinished" scripts to that repository [...]

Good idea

#5 - 08/17/2022 01:10 PM - koszko

- Status changed from New to Closed

- % Done changed from 0 to 100

Files

livehealth-login.js	1.38 KB	06/13/2022	jacobk