

Re: Cookies question

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2005-03/0263.html>

From: Joe Kaplan \((MVP - ADSI)\) (joseph.e.kaplan_at_removethis.accenture.com)

Date: 03/24/05

Date: Thu, 24 Mar 2005 15:22:31 -0600

Speaking of tools for debugging HTTP, also check out IEHttpHeaders. It doesn't do as much as Fiddler, but it works over SSL (which Fiddler doesn't the last time I checked) and does show you cookies info (since they are headers). This is one of my favorite tools these days.

Joe K.

"Dominick Baier [DevelopMentor]" <dbaier@pleasepleasenosspamdevelop.com> wrote in message <news:174336632472641746102975@news.microsoft.com>...

> *Hello Joe,*

>

> *if you can close down all browser windows and with a new one bypass the login then you _have_ to have some persistence going on. this is the only explanation - maybe something with you session cookie??*

>

> *check your code and inspect the http communication by using a tool like fiddler (www.fiddlertool.com).*

>

> *HTH*

>

> -----

> *Dominick Baier - DevelopMentor*

> *<http://www.leastprivilege.com>*

>

>> *Dominick,*

>> *Thanks for the response.*

>> *I use temp cookies because I use code like this:*

>> *Web.Security.FormsAuthentication.RedirectFromLoginPage(UID, False)*

>> *I think it is related to spawning a 2nd browser session from the first*

>> *by*

>> *using Ctrl-N.*

>> *In this case the 2nd browser instance "inherits" the in memory cookies*

>> *from*

>> *the first.*

>> *The users were using a link to an Intranet site - maybe this link had*

>> *the same effect by spawning a 2nd instance from the first somehow.*

>>

>> I guess what I don't understand is how they can close all browser
>> instances
>> and then click this link and still bypass the log in page. If the
>> cookie is
>> temporary and in memory, isn't it destroyed when browser is closed?
>> Or is it really stored on disk somewhere until it expires? (I could
>> not find
>> it and a re-boot makes it disappear.)
>> Thanks for any more input.
>>
>> "Dominick Baier [DevelopMentor]"
>> <dbaier@pleasepleasenosspamdevelop.com> wrote in message
>> news:169758632471743413041942@news.microsoft.com...
>>
>>> Hello Joe,
>>>
>>> cookie storage depends – if it is a temporary cookie it is only store
>>> in browser memory and delete when you shut down the process –
>>> persistent
>>>
>>> cookies
>>>
>>> are stored in the user profile.
>>>
>>> So when do you deal with persistent and when with temporary...
>>>
>>> a cookie that has an expiration time in the future is persisten until
>>> that point of time.
>>>
>>> In FormsAuthentication – when you use RedirectFromLoginPage – the
>>> last
>>>
>>> parameter
>>>
>>> is a boolean – if true the cookie is persistent (some silly timespan
>>> like 50 years in the future), if false you will end up with a temp
>>> cookie.
>>>
>>> When you use persistent cookies, the behaviour with the 2nd browser
>>> window is like you described it
>>>
>>> Always use temp cookies – you don't want digital ids of your webapp
>>> stored on a clients machine, do you?
>>>
>>> -----
>>> Dominick Baier – DevelopMentor
>>> <http://www.leastprivilege.com>
>>>> I use forms authentication for my app.
>>>> After I log in successfully each request by the browser contains 2
>>>> cookies.
>>>> One for the SessionID and one for forms authentication which

>>>> *contains*
>>>> *my*
>>>> *ticket.*
>>>> *Can someone please explain where these cookies are stored? I think*
>>>> *it*
>>>> *is in memory in the browser but am not sure.*
>>>> *Also, some users have stated that they can do the following:*
>>>> *1. Start a browser, hit the site and log in.*
>>>> *2. Start a 2nd browser.*
>>>> *3. Hit the site.*
>>>> *4. BYPASS the log in page and go directly to the Home page.*
>>>> *They claim they can also close all browser sessions, start a new one*
>>>> *and still Bypass the log in page.*
>>>> *How is this possible?*
>>>> *Why would the 2nd browser session have the cookies noted above?*
>>>> *I assume once the authentication ticket expires in 30 minutes of*
>>>> *inactivity that neither scenario would be possible. They would have*
>>>> *to*
>>>> *re-log in first.*
>>>> *Thanks for any info on this.*
>>>>
>
>
>