

Re: BASIC authentication Issues with IE – Part II – Solved but WHY?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-03/0707.html>

From: Wade A. Hilmo [MS] (wadeh_at_microsoft.com)

Date: 03/27/04

Date: Sat, 27 Mar 2004 08:40:35 -0800

Hi Hector,

I've been following this thread for some time. From what I've seen, you have been given good information and advice so far. I would like to clarify a few points to try and help you narrow this down.

First and foremost, inetinfo.exe is not integrated with IE in any way. It is the host process for the IIS web server core. It runs on the server side and services requests from all HTTP clients without distinction. In other words, it does not know the difference between a request from IE or from some other HTTP client. In fact, we have many users of IIS that have written their own custom HTTP clients that are not browsers in the traditional sense at all.

Second, the way that IIS handles Basic authentication is, well, basic. Per the HTTP spec, a client authenticates by sending an "Authorization" header in the request. If no authorization header is present, IIS authenticates the request as anonymous. If an authorization header is present and it specified Basic Authentication, and IIS is configured to accept Basic, then IIS authenticates the request as the user in the base64 encoded part of the authorization header. Some other authentication schemes are more complicated, but Basic is just this simple.

Third, the credential cache that you keep mentioning has nothing to do with this issue. The credential cache is a performance optimization. It turns out that it can be very expensive (in terms of performance) to ask the operating system to produce a token from user credentials. For this reason, IIS can sometimes remember the token for a particular set of credentials so that, if those same credentials come in on another request, we can reuse the token instead of asking the operating system for a new one. This only affects where we get the token from, and has no affect whatsoever on whether we authenticate or not.

Given these three things, I can say with very high confidence that you are looking at an issue with the client, and it has nothing to do with IIS. As such, this post is off topic on this newsgroup. I just look a look at the

Microsoft newsgroups in hopes of pointing you to a better place, and unfortunately, it doesn't look like there is one central IE newsgroup. It looks like they are pretty well broken up by version. Lots of folks that read this newsgroup probably have an interest in the client as well, so hopefully somebody reading this can suggest an active newsgroup with a focus on IE. In any case, you are not guaranteed a response by Microsoft on a newsgroup anyway, so your best bet if you want this is to open a case with product support.

That said, I can think of several scenarios where any client might not persist – or appear to not persist – credentials between basic authenticated requests. Note that I know nothing about the internals of IE. My only experience with IE is as a user, and seeing the HTTP that it puts on the wire. What follows is just my own personal speculation on this topic. For definitive answers, you should be talk to someone who specializes on IE.

First off, it's very important that the client not forward basic authenticate credentials indiscriminately. The reason for this is that basic authentication does not protect the password in any way. If you give me your basic authorization header, I can base64 decode it in no time and then I can become you. Because of this, I would expect that no client would preauthenticate ("preauthenticate" is the term used to say that the client forwards the credentials without first seeing a 401 from the server) without having very good reason to believe that the request is going to the same place as some previous request which successfully authenticated. I would speculate that the client would consider the target server, and possibly some part of the URL namespace to make this determination.

Also, the client could, if it chooses, implement some logic to authenticate without prompting, based on the realm returned in the basic challenge from the server. In other words, if the server response with a 401 and www-authenticate header for basic, it will include a realm. The client could then search its own credential cache and see if it has credentials for that realm without asking the user. I have no idea if IE does this or not.

Finally, I can see some timing scenarios where you might get unexpected authentication popups on the client. Specifically, if you make a request that results in a bunch of other requests (ie. if there are frames involved, if there are frames on the page, if there are 301 or 302 redirections, etc.) it's possible that the client makes some number of those requests before it gets back a 401 from any of them. In that case, there is no way that the client could preauthenticate all of the requests. And even if the following 401 responses all contain the same realm (and the client uses this information), it's possible that timing issues in a local credential cache on the client could cause it to prompt for credentials more times than you think it should.

I would guess that someone very familiar with HTTP could probably explain the behavior that you are seeing by studying a sniffer trace of the traffic between the client and server. Note that log files may not be sufficient. A sniffer trace is going to show you the actual packets that are hitting the

wire, complete with timing information, how the packets are broken up, and sequence numbers.

Thank you,
–Wade A. Hilmo,
–Microsoft

"hector" <nospam@nospam.com> wrote in message
news:ebwazA8EEHA.1228@TK2MSFTNGP11.phx.gbl...
>
> "Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message
> news:eW33\$%235EEHA.3064@tk2msftngp13.phx.gbl...
> > Hi,
>
>
> > OK, now's where things get a bit interesting. I tried doing what I think
> > you're doing:
> > a) create a page on myserver.com (page1.asp) which requires Basic
> > authentication.
> > b) create some links on the page – one link points to page2.asp on the
> > same
> > server. Page2.asp also requires Basic Authentication
> > c) Goto page1.asp, enter username/password, get access to page1.asp
> > d) Click on the link to page2.asp, but choose "Open in New Window". IE
> > automatically sends credentials, and I'm giving access.
> > e) Now, I close the second window, and return to my first window. I
click
> > the link to page2.asp again (but without choosing "open in new window").
> IE
> > sends by credentials, and I'm logged in fine.
>
> In step c, how do you "Goto Page1.asp"?
>
> Do this by creating a simple Default Home Page with a link to this
page1.asp
>
> If you type the url on the IE address bar, you will not see the problem.
>
> > Now, you seem certain that this is a bug. I would call Microsoft PSS
> > (Product Support Services), and open a call to debug the issue.
Certainly
> > it's a not common problem (otherwise lots of people be having problems
> > with
> > Basic Authentication), and it doesn't manifest itself on my copy of IE,
> > nor
> > any other copy of IE that I've had before. If there is a bug in IE that
> > you
> > are using, then you will not have to pay – it'll be fixed for free by
> > Microsoft.
>
> Ken, this is has been a long time issue. I've been down this route before,

- > including calling them on the matter and/or related issue where you are not
- > losing credentials but it was cached and used again automatically in the
- > Explorer "Previewing" logic. Like I said, this has been an issue for a long
- > time and I am not the only one. And you know perfectly well, Microsoft is
- > will be mum on the subject closed related with security. I am just trying
- > to figure it out once and for all. I'm not a USER, well yeah of course I
- > am, I am a user of my own creation as well as hundreds of thousands of
- > user/customers. So we have to satisfy their reports too. But like I
- > said, for this particular "lost of authentication", I was one of the few
- > within our own product reporting it and know I find out "how" it happens.
- >
- > I am going to try one more thing and that is put the URL in the Favorites
- > likes instead. I can't do it know until I close Outlook and all Microsoft
- > software that has the IE logic integrated with the INETINFO.EXE credential
- > caching. PS: Do a search for this and you will see it how its all related,
- > and how there is difference with XP vs. others, how Microsoft solved the URL
- > shortcut automatic authentication security hole in XP but not others for
- > some "legacy reason." Yes, incoherent and all very inconsistent which is
- > what I am trying to get all straight once and for all.
- >
- > --
- > Hector Santos, Santronics Software, Inc.
- > <http://www.santronics.com>
- >
- >
- >
- >