

Secure website (cookie/session)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2005-06/0038.html>

From: IkBenHet (ikbenhet79_at_hotmail.com)

Date: 06/03/05

Date: 3 Jun 2005 02:17:45 -0700

Hello,

First of all, I am aware that there is already a lot of information about this subject on this and other resources. Probably the question I am going to ask is already asked. But in the information I can find, I am losing track of what is useful for me. So, Sorry for maybe asking a question that is already been posted.

I want to do something very simple. Secure a part of my website. The site is mainly ASP based. The webserver is an IIS6 and I do NOT have access to server settings (session timeout, security,...).

I use sessions to secure it.

Basically you are redirected to a form where you can give a username and password, this is validated with the values in a database. If the password and username are ok a session value is set
<%=Session("Validated")=True%>.

At the beginning of each secure page I start with:

```
<%If Session("Validated") = False Then Response.Redirect("Login.asp")
End If%>
```

So if the session value 'validated' is true you can see the secured pages else you are redirected to the logon page.

The default timeout value for session is 20 minutes. Because the session should stay alive during the complete time of the visit I was thinking of putting the session.timeout to 60 minutes. I set this at the beginning of every secure page: <%=Session.timeout=60%>

Users keep on contacting me saying that they have to RE-logon quite often. This also seems to happen when a user is not on the website for 20 minutes already. I tested it myself and have the feeling that I am indeed regularly redirected. Sometimes after 10 minutes, other times 30 minutes, ... There seems not to be any logic in the time that users are redirected to the logon page.

microsoft.public.inetserver.iis.security: Secure website (cookie/session)

Because the website is used to fill in a lot of HTML forms, it is very frustrating for the users when they are completing a form and then pressing "Submit" being redirected to the logon page and lose all entered data.

I was thinking of changing from a session based to a cookie based system. So i.o. setting the session variable 'validated' to true, writing a cookie. (Maybe with the valuez Response.Cookie("Validated").Domain and .Path to more secure it)

Now I face the problem that I only can set the expiration time for the cookie to Date+1. This actually means that if a user other then the validated user is browsing the same website. He/She is able to access the secured website. And this for the rest of that day. A possible solution could be setting no expiration date, but than you are again using sessions (or am I wrong in this?), which was the main reason to use cookie i.o. sessions.

Basically I want to secure a website using ASP (because I am not able to change security settings on the webserver of my ISP). The user must logon EVERYTIME he STARTS using the secure website and this process should end when he is closing his browser (so no user other then the validated one can abuse it credentials). I already buildin a "Logoff" that removes the cookie, but nobody seems to be using it. The users may NEVER be redirected when submitting data so we do not lose time re-submitting it because the use was redirect to the logon screen.

I am open for all suggestions, please help! In the future there are also money transactions going over this website, so it has to be secure! I will use HTTPS.

Thanks for you help!