Subject: Skylark session verification
Posted by Xemuth on Sun, 03 May 2020 00:28:55 GMT
View Forum Message <> Reply to Message

Hello,

I'm currently using Skylark to developpe my own website and I have a little doubt about skylark session.

On my website, I want user authenticate themself. so Actually I'm using a form with $post_identity() to start a session.
When user send is data to be logged on, I check if he is legitimate then, if he is, I do this :

```
if(Data sent by user is good){
   http.NewIdentity(); //Set new session identity
   http.SessionSet("RIGHT", AsString(us->GetRight())); //Set Right of user
   http.SessionSet("USERNAME", us->GetLogin()); //Set username of user
   http.Redirect(PrivateScreen); //Redirect to the privateScreen
  }else{
   http.Redirect(Auth); //Else redirect to authentification page
  }
```

On other page (like PrivateScreen) for example, I do this to ensure the user is connected :

```
 if( !http[".USERNAME"].ToString().IsEmpty()){
  ...Process everythings
 }else{
  http.Redirect(Auth); //Else redirect to authentification page
 }
```

Is this way of working is safe ? should I instead, generate a special ID related to sessionID of the user, send it to cookies and comparing it every time ?

Thanks in advance

Subject: Re: Skylark session verification
Posted by deep on Mon, 04 May 2020 16:44:52 GMT
View Forum Message <> Reply to Message

I think using USERNAME in the header is not not safe. Impersonation possible.

Some explanation available here.

https://security.stackexchange.com/questions/36318/store-use rname-in-cookie-for-a-web-site

Subject: Re: Skylark session verification
Posted by Xemuth on Mon, 04 May 2020 19:31:55 GMT
View Forum Message <> Reply to Message

Hello Deep,

I don't think session variable and header value are the same, from my point of view, session are only available at server. Maybe I'm wrong ?

Subject: Re: Skylark session verification
Posted by deep on Tue, 05 May 2020 16:27:15 GMT
View Forum Message <> Reply to Message

Hi Xemuth,

Xemuth wrote on Sun, 03 May 2020 05:58
http.SessionSet("RIGHT", AsString(us->GetRight())); //Set Right of user
http.SessionSet("USERNAME", us->GetLogin()); //Set username of user

I think you should use only sessionid. And should get username and user rights from server for every request based on sessionid.

Do not set it (username and rights) as a part of http session params. This is my suggestion.

Subject: Re: Skylark session verification
Posted by Xemuth on Tue, 05 May 2020 22:31:56 GMT
View Forum Message <> Reply to Message

Hello Deep,

I will follow it, thanks

Subject: Re: Skylark session verification
Posted by deep on Sun, 31 May 2020 08:30:40 GMT
View Forum Message <> Reply to Message

Xemuth

I think what you were doing was okay. What gets transmitted is only session id.
Every thing else is stored at server end.

You can use anything to store in session. Skylark will retrieve it from server side local storage.

I checked this with couple of examples.