
Subject: Re: RSINC web mini-bug ??

Posted by [Antonio Santiago](#) on Tue, 21 Mar 2006 17:03:50 GMT

[View Forum Message](#) <> [Reply to Message](#)

Jean H. wrote:

> It is called a session.
>

I think the ugly thing isn't the session but the GET method instead the POST one.

See ID's and that kind of information in the URL is a bad idea, although they aren't too many dangerous, because can give some bad ideas to the bad boys.

> change the value after wid= and the name will disappear... if you have
> time to loose, you might even find somebody else name!
>
> webserver delete the sessions, on the server side, every now and then..
> when people don't put the session ID in a link, it is not a problem as
> each new user (visitor) will receive a new session ID.
>
> Your online bank account works the same.... fear it! :)

>
> Jean H.
>

> Antonio Santiago wrote:

>
>> Hi group,
>>
>> trying to find some information on the net about iTools I found this
>> beautifull link:
>>
>> http://www.google.com/url?sa=t&ct=res&cd=3&url=http%3A//www.rsinc.com/services/techtip.asp%3Fttid%3D3528%26wid%3D2861072%26s%3D1497&ei=BHoarI7ZPI7iiALs5fnXAw&sig2=ofQoPF4gqPb9_SDkFVINYA
>>
>>

>> Why is it interesting??
>> I suppose because you are semi-login as:

>>
>>>> Hello Andrzej Pindor

>>
>> My name is not Andrzej Pindor, but can be logged as him for a moments.
>> I suppose it is not a serious bug, because a bad boy needs to be the
>> cookies of Andrzej with some kind of information to login as him 100%.
>>
>> Bye.

>>

--

Antonio Santiago Piñerez
(email: santiago@grahi.upc.edu)
(www: <http://www.grahi.upc.edu/santiago>)
(www: <http://asantiago.blogspot.org>)

GRAHI - Grup de Recerca Aplicada en Hidrometeorologia
Universitat Politècnica de Catalunya
