

Warning – ComponentOne's PayPal component is VERY insecure!!

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2005-09/msg02175.html>

- *From:* Alan Silver <alan-silver@xxxxxxxxxxxxx>
 - *Date:* Sun, 11 Sep 2005 16:33:35 +0100
-

Hello,

I've just been looking at the free PayPal component from ComponentOne and am somewhat amazed how insecure it is. They include all the transaction details in plain text in the querystring, meaning that any rank novice can click the Buy button on your site, then when the PayPal page loads, change the amount for the transaction and press Enter. This reloads the page with the new amount. This is so obvious that anyone could do it.

The result is that someone can place an order on your site and change the amount to 0.01, with the order still being placed. You are powerless to stop this. What's even worse, is that it looks like they could enter a negative amount and get a refund!!

If anyone is using this component, I recommend you check this issue immediately as your site could be open to abuse.

I contacted C1's (lack of) technical support who were typically unhelpful. They avoided the issue and gave obscure answers to questions I hadn't asked. This is consistent with my previous experience of their technical support.

On a related issue, is anyone using PayPal's ASP.NET SDK? I just had a look at that too and wondered how easy it is to use.

--

Alan Silver

(anything added below this line is nothing to do with me)

.