Attacking Users - Using Frameset

I recently did something on how attackers could use *iframes* to hide links on a webpage to trigger unintended traffic from a client. Well, I have been carrying on looking as to other ways this could be done and there is another way. It is not as easy or simple but it does accomplish the same thing. It uses a much hated web design trick using frames. Lets look a simple example..

```
<html>
<head>
  <title>main</title>
</head>
<frameset cols="100,*" framespacing="0" frameborder="0" border="0">

<frame src="one.html" name="one" marginheight="0" frameborder="0" border="0"
 noresize="noresize" scrolling="no">

<frame src="two.html" name="two"
 marginheight="0" frameborder="0" border="0" noresize="noresize"
 scrolling="no">

</frameset>
</html>
```

That is the code for a very simple webpage. Lets start with the *frameset* tag..

```
<frameset cols="100,*" framespacing="0" frameborder="0" border="0">
```

What this is basically saying is that you want your page to be seperated into two columns, the first is a 100 pixels wide and the second takes up the rest of the space. You can have mutiple columns, you could have rows instead as well. The other settings speak about whether borders should be visible, etc. We are going to concentrate on the column setting. Viewing this page shows the first page *"one.html"* in a narrow column on the left and the second page *"two.html"* is shown in the rest of the window. I am sure you can see where this is going..

Now back to initiating unintended but hidden traffic. If you change the *frameset* code to..

```
<frameset cols="0,*" framespacing="0" frameborder="0" border="0">
```

Now what happens when you browse the page, you see the second page referenced *"two.html"*, but you cannot see the first page *"one.html"*. But even though you cannot see it, your browser still "*browses*" to the page. According to your traffic you are browsing both pages, even though you are actually only seeing one . Now we can go ahead and change the source for the first column to display or access any web resource we want, or accomplish any of the other nasty tricks we looked at by using iframes.

Final Words
Using the *frameset* code is not as '*elegant*' as using iframes but it does the same thing, and it does the same thing in normal accepted html code. I raise the use of frameset simply because it does work, and it a proven fact that the bad guys like to have more then one way to do things. Well actually that is true of the good guys as well, but regardless, if attackers cannot get iframes to work on you, they could easily try framesets. You could even script a page that tries one and if it does not work, then try the next one. Lastly, much like with the iframes, bear in mind that traffic shown as belonging to a browser, does not mean it is traffic belonging to the user.