Cross site Script hacking using the GET method

Posted At : 30 July 2009 14:57 | Posted By : Shaun McCran
Related Categories: Security, Coldfusion, Best practices, Internet Explorer

I've dealt with Cross Site scripting (XSS) attacks before (http://www.mccran.co.uk/index.cfm/2009/4/6/Cross-Site-scripting-hack-test-form), so I'm familiar with the principles involved. In this example there is a subtle difference.

In the example above the vulnerability was created by POSTING a text string through the form action. In this example we will examine a similar vulnerability using GET. IE we will simply pass the attacking string through the url of the form, setting the form field value in the traditional 'url?variable=N' way.

To demonstrate this create a simple form:

```
<cfparam name="attributes.formValue" default="">

<form>

ype="text" name="formValue" size="20" value="<cfoutput>#attributes.formValue#</cfo
<input type="submit" name="Action" value="Send">

</form>
```

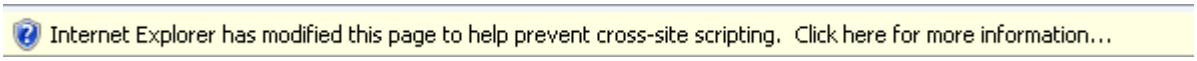
Call your form in a browser. Now append on the end of that url the text string below.

?attributes.formValue==>">

Reading through the string you'll notice that it is an Iframe constructor that is calling a url, in this case www.Google.com.

As the url is setting the value of 'attributes.formValue' this will be inserted into the form on the submit action. We are not posting it, so it will not be picked up by any custom POST action code.

One interesting point to mention here is that testing this in IE 8, it will actually be blocked by default, as it has detected that scripts are running over different domains.



So if you are in the habit of writing POST detection scripts, make sure you handle any other submissions as well!