Cross Site scripting hack test form

Posted At : 6 April 2009 16:32 | Posted By : Shaun McCran
Related Categories: Security, Best practices, HTML, Web technologies

One of the more basic cross site scripting hacks is where the user simply 'injects' other web templates into yours, using a form.

By submitting a string through a form and allowing it to return the value in an *unencoded* format a user can inject malicious code. In this example we will create a frameset, and set the source as a different domain than the originating site.

To test this yourself create a simply form, and set the value of the text field to the value that the user enters.

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

                                <form method="post">

t type="text" name="formValue" size="30" value="<cfoutput>#form.formValue#</cfoutp
                    <input type="submit" name="Action" value="Send">

                                        </form>
```

I'm using ColdFusion, but the language itself doesn't matter, the vulnerability is the same. Next submit the form using a string like the one below. This string is built up of the form field name, and a valid html frameset, surrounded by escape characters.

```
:/iframe></script></form></td></tr><br><iFraMe src=http://www.google.com width=900
```

Submit the form, and you will be returned to the same template, but it has translated the html string, and is now proudly displaying someone else's site on your domain.

This is only possible because the form is returning the form value in raw html. You can eliminate this issue by simply adding a html stripping routine to the form. Something like HTMLCodeFormat replaces special characters in a string with their HTML-escaped equivalents.

```
#HTMLCodeFormat(form.formValue)#
```