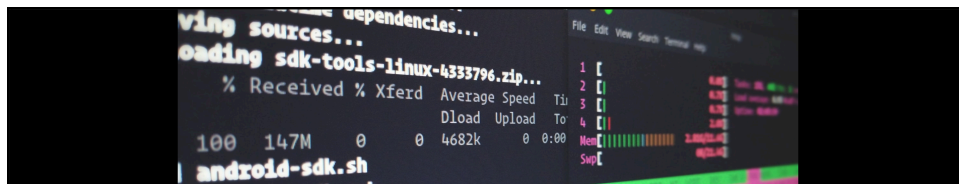


Firefox 3 disallows cross-site XBL

Martin Paul Eve

28 February 2008 (last updated 6 September 2026)



Cite as: Martin Paul Eve, "Firefox 3 disallows cross-site XBL", *eve.gd: Martin Paul Eve*, February 28, 2008,
<https://doi.org/10.59348/vz0z6-bn678>.

DOI: <https://doi.org/10.59348/vz0z6-bn678>

Available at: <https://eve.gd/2008/02/28/firefox-3-disallows-cross-site-xbl/>

Well, I decided to play around a little with Firefox 3 Beta 3 today and discovered that it looks like the ever popular `-moz-binding` css attribute is now rendered a little less useful. It is now impossible to load off-site XBL via this method.

However, all is not lost. For in patching one of the biggest holes in Firefox's security model, the infinite wisdom of the FF devs is that it is now possible to embed a `-moz-binding` URL tag inline, like this:

```

```

Using this method provides for no use of a fragment identifier, indeed it is only possible to use the first element. The above XBL decodes to:

```
<?xml version="1.0"?>
<bindings xmlns="http://www.mozilla.org/xbl">
  <binding id="loader">
    <implementation>
      <constructor>

        var url = "alert.js";
        var scr = document.createElement("script");
        scr.setAttribute("src",url);
        var bodyElement = document.getElementsByTagName("html").item(0);
        bodyElement.appendChild(scr);CLOSE CDATA>
      </constructor>
    </implementation>
  </binding>
</bindings>
```

which essentially creates a nice new DOM script element that loads alert.js.

References

This reference list has been generated, in many cases, through an automated process and may therefore contain errors or incomplete metadata. It is provided purely as assistance for finding the items mentioned within this post.

‘Mozilla XML Namespace’, *Mozilla* <<http://www.mozilla.org/xbl>>