参考：
http://www.youknowi.xin/2018/10/%e5%89%8d%e7%ab%af%e9%bb%91%e5%ae%a2%e8%af%bb%e5%90%8e%e6%84%9f%e5%86%8d%e6%8e%a2%e7%a9%b6%ef%bc%88xss%e5%a7%bf%e5%8a%bf%ef%bc%89/

个人觉得当<>’” onclick 特殊事件 特殊关键字 都被过滤或者转义就没有说的情况了

值得注意的是任何 htnl 中的输出都有可能成为 xss，这个情况才是最有意思的，看平时的积累