反射型：

1 <img src=”null” onerror=”alert(1)”/>

2、<p onclick=”alert(“点我”)”>点我</p>

2、http://localhost:3000/?xss=<iframe src=”http://www.baidu.com”></iframe>

过滤

移除用户上传的DOM属性，如onerror等

移除用户上传的Style节点，SCript节点，iframe节点等

校正

避免直接对html Entity解码

使用DOM Parse转换，校正不配对的DOM标签