在正常的xss中可能它不一定会生效，但是在DOM操作中去获取历史记录可能会有xss。 DOM操作去获取值修改输入框中的值，这种方式的修改可能会使一些信息直接渲染到页面上。（没有经过过滤）

文件上传xss

#SVG-XSS

SVG(Scalable Vector Graphics)是一种基于XML的二维矢量图格式，和我们平常用的jpg/png等图片格式所不同的是SVG图像在放大或改变尺寸的情况下其图形质量不会有所损失，并且我们可以使用任何的文本编辑器打开SVG图片并且编辑它，目前主流的浏览器都已经支持SVG图片的渲染。

```
<svg xmlns="http://www.w3.org/2000/svg" version="1.1">

<circle cx="100" cy="50" r="40" stroke="black" stroke-width="2" fill="red" />

<script>alert(1)</script>

</svg>
```

#PDF-XSS

1、创建PDF，加入动作JS ![[Pasted image 20250804130802.png]]

在页面选项中右键点击属性，添加动作选择执行一段js代码

2、通过文件上传获取直链

3、直链地址访问后被触发

#SWF-XSS

-制作swf-xss文件：

1、新建swf文件

2、F9进入代码区域

3、属性发布设置解析

//取m参数

var m=_root.m;

//调用html中Javascript中的m参数值

flash.external.ExternalInterface.call(m);

触发：?m=alert(/xss/)

项目：Adobe Flash Professional CS6

-测试swf文件xss安全性：

1、反编译swf文件

2、查找触发危险函数

3、找可控参数访问触发

xss一是指执行恶意js，那么为什么说flash xss呢？是因为flash有可以调用js的函数，也就是可以和js通信，因此这些函数如果使用不当就会造成xss。常见的可触发xss的危险函数有：getURL，navigateToURL，ExternalInterface.call，htmlText，loadMovie等等

项目：JPEXS Free Flash Decompiler

#html-xss 上传html格式的xss看能不能行

功能逻辑触发xss

#PostMessage XSS

一个用于在网页间安全地发送消息的浏览器API。它允许不同的窗口（例如，来自同一域名下的不同页面或者不同域名下的跨域页面）进行通信，而无需通过服务器。通常情况下，它用于实现跨文档消息传递（Cross-Document Messaging），这在一些复杂的网页应用和浏览器插件中非常有用。

安全原因：当发送参数可控且接收方处理不当时，将导致XSS

模拟漏洞挖掘场景：

打开http://192.168.1.4:82/60/xssreceive.html

分析源码：