一个IE浏览器漏洞的安全测试及分析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E4_B8_80_E4_B8_AAIE_E6_B5_c100_460847.htm 今天在网上看到一个IE的小小漏洞，做了下简单的分析，利用方法如下： 程序代码： onLoad="document.write（‘ Cannot Find File！ ’）；" onError="document.write（‘ File Exists！ ’）；"> 刚开始很奇怪这个sysimage://是个什么协议，于是在IE中打入： sysimage://C：\WINNT\Explorer.exe 结果返回是个Explorer的图标。而利用程序后面的777又表示了什么呢？ 于是很习惯的又写上sysimage://C：\WINNT\Explorer.exe，777，显示IE返回该页无法显示 看来问题是出在这个777上了。既然是IE的本地文件存在探测漏洞，那么就是说这个777是一个构造的东西，那么我把777改成了2.结果返回了另外一个图标。很显然…… 这个777类似的数字是调用文件内部图标号的东西，类似我们平时常见的desktop.ini中icon=somefile.exe，7这样的东西，那么这段代码就是说，如果一个文件中有定义了图标存在，而且这个文件是的确存在的，那么IE就返回这个文件的第N个图标（N是自己定义的，如果不定义，默认是第一个图标），如果文件不存在，那么系统将会返回一个文件夹的图标，所以这样IE就出现了问题。 首先。我们可以让IE返回一个图标，如果正确，那么将返回这个程序的第N个图标，如果不存在这个图标，那么IE会有个ERROR，那么用ONERROR就能给出一个答案，而如果文件不存在的话，IE会返回一个文件夹的图标，也就是说ONERROR不成立，那么就执行ONLOAD的事件。这样就清楚了。呵呵。 至于如何利用，

个人感觉利用价值不大。也许有的时候我们可以利用他结合其他的一些漏洞有目的性的返回一些东西…… 比如：sysimage://C：\Documents and Settings\Administrator\Cookies\administrator@icehack.com[1].txt 这样的，也许再加点什么可做到COOKIE的跨站点获取什么的。我也没有继续想下去了。 程序代码：onLoad="document.write（‘ Cannot Find File！ ’）；" onError="document.write（‘ 这里写上转向到XXX跨站COOKIE截取程序b> ’）；"> 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com