基本信息

漏洞类型：XSS跨站注入漏洞

漏洞等级：中危

厂商信息：此处需要手动搜索

漏洞简述

漏洞描述

跨站脚本攻击的英文全称是Cross Site Script，为了和样式表区分，缩写为XSS。发生的原因是网站将用户输入的内容输出到页面上，在这个过程中可能有恶意代码被浏览器执行。跨站脚本攻击,它指的是恶意攻击者往Web页面里插入恶意html代码，当用户浏览该页之时，嵌入其中Web里面的html代码会被执行，从而达到恶意用户的特殊目的。

漏洞危害

1.窃取cookies，读取目标网站的cookie发送到黑客的服务器上  
 2.读取用户未公开的资料，如果：邮件列表或者内容、系统的客户资料，联系人列表等等。

漏洞详情

网站漏洞报表

注入网址:http://tctkyb.cn/htm/lxwm.asp?biaoti=%3C%2Fscript%3E%22%3E%3Cscript%3Eprompt%281%29%3C%2Fscript%3E

漏洞参数:biaoti

请求方式:POST

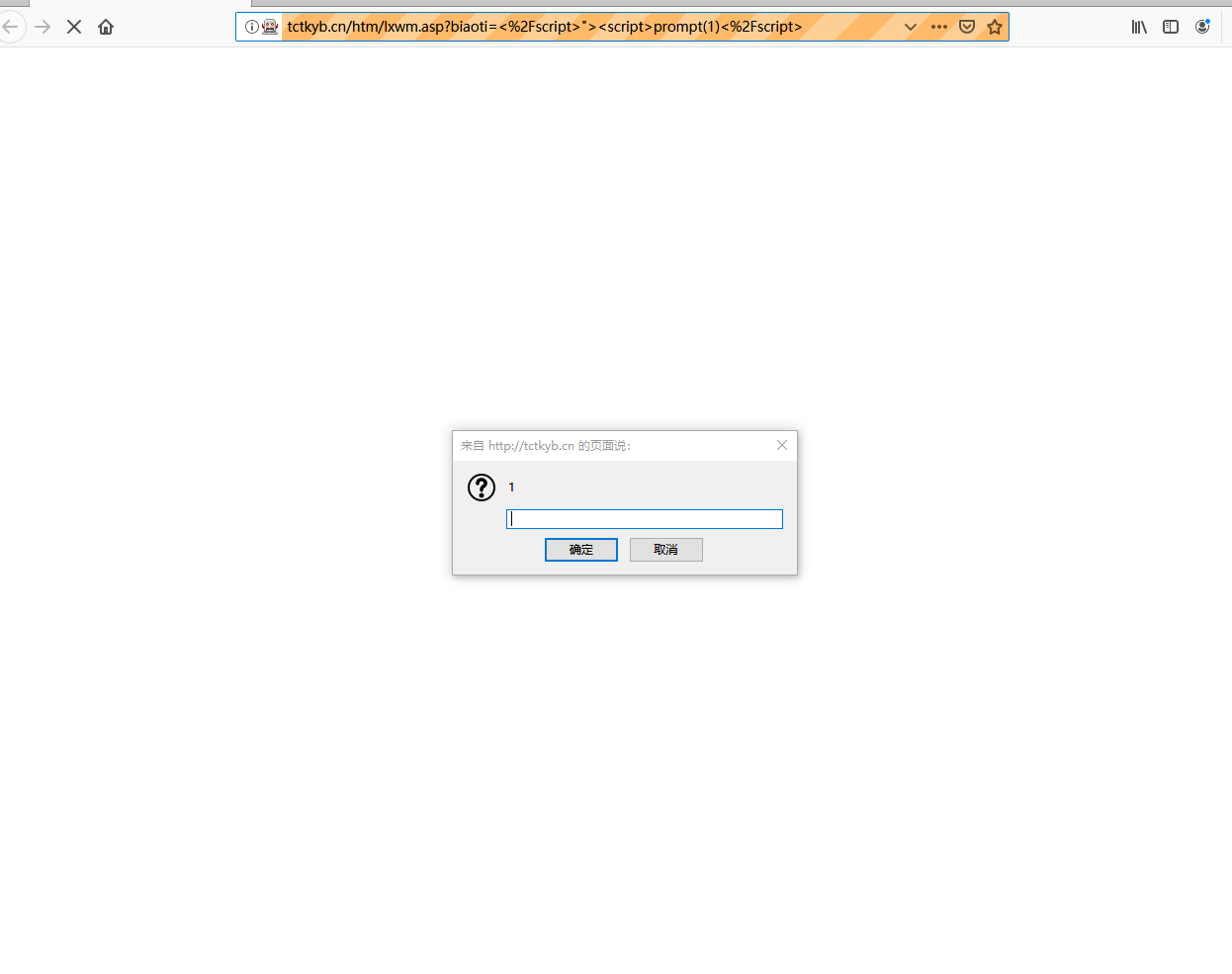
攻击载荷:</script>"><script>prompt(1)</script>

网站漏洞复现(使用Firefox浏览器)

访问链接

http://tctkyb.cn/htm/lxwm.asp?biaoti=%3C%2Fscript%3E%22%3E%3Cscript%3Eprompt%281%29%3C%2Fscript%3E

返回结果



复现完成，验证存在反射型XSS漏洞

修复建议

代码原理防护

1、 输入验证：某个数据被接受为可被显示或存储之前，使用标准输入验证机制，验证所有输入数据的长度、类型、语法以及业务规则。  
 2、 输出编码：数据输出前，确保用户提交的数据已被正确进行entity编码，建议对所有字符进行编码而不仅局限于某个子集。  
 3、 明确指定输出的编码方式：不要允许攻击者为你的用户选择编码方式(如ISO 8859-1或 UTF 8)。  
 4、 注意黑名单验证方式的局限性：仅仅查找或替换一些字符(如"<" ">"或类似"script"的关键字)，很容易被XSS变种攻击绕过验证机制。  
 5、 警惕规范化错误：验证输入之前，必须进行解码及规范化以符合应用程序当前的内部表示方法。请确定应用程序对同一输入不做两次解码。对客户端提交的数据进行过滤，一般建议过滤掉双引号（”）、尖括号（<、>）等特殊字符，或者对客户端提交的数据中包含的特殊字符进行实体转换，比如将双引号（”）转换成其实体形式&quot;，<对应的实体形式是&lt;，<对应的实体形式是&gt;